



FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

BITU3923 - WORKSHOP II

FINAL REPORT

PREPARED BY:

NAME	MATRIC NUMBER
MUHAMMAD FIRDAUS BIN JANALUDIN	B031610457
NUR KHAIRUNNISA BINTI MOHD AZMI	B031610351
SYAHIDAH BINTI MOHD SUHAINI	B031610245
ABDUL JABBAR BIN KAMAROZAMAN	B031610409
ABDULRAHMAN AKRAM ABDULRAHMAN AL-EMAD	B031610395
YUGENDRAH A/L SUBRAMANIAM	B031610443
MOHAMMAD FAHMY IZUDDIN BIN AZHAR	B031610270
SYAZWANI BINTI SHAMSUDDIN	B031610228
NUR RAIHAN BINTI MUHAMAD ROSDI	B031610224

SUPERVISOR: DR. WAHIDAH BINTI MD SHAH (M)
PM DR. FAIZAL BIN ABDULLAH (S)

EVALUATOR: MR. SUHAIMI BIN BASRAH

ACKNOWLEDGEMENT

First and foremost, we would like to thank our project supervisor, Dr. Wahidah binti Md. Shah and our co-supervisor PM Dr.Mohd Faizal bin Abdullah 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 team for this project. Their willingness to motivate us contributed tremendously to our project. We also would like to thank them for showing us some examples that are related to the services in our project which helped us to understand our project better. 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 better and great. All of this guidance helped us to complete our project on time. We would also like to thank our evaluator for this workshop, Mr.Suhaimi bin Basrah and Mr.Ariff Bin Idris 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 have.

We also would like to thank the authority of Universiti Teknikal Malaysia Melaka (UTeM) for providing us with a good environment and facilities to complete this project. Finally, an honourable mention goes to our families and friends for their understandings and supports for us in completing this project. With the help of everyone that was mentioned above, we were able to overcome many problems that occurred during the workshop 2 and we were able to 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 on time and who will do what service. It is very important to manage and organizes every task given in order to avoid any problems and error later on. Our main objective in this Workshop II is for this project to be successful and able to go through the obstacles and challenges faced while completing the task given. Next our objective also is to have deeper understanding about the service on how it works and we are grateful to experience this as it helped us to be more prepared in our industrial training. Our group had decided to use Windows 2012 in server 1 (Window), Fedora 28 in server 2 (Fed) and Ubuntu 16.04 in server 3 (Linux). We chose this server operating system because it the latest version and has many benefits. Our group also was assigned to set up 31 services listed. The 30 services listed are DNS (IPv4 & IPv6), DHCP (IPv4), DHCP (IPv6), Server Virtualization, Linux Email Server, Secured FTP, Routing & NAT, Access Control List (ACL), Samba, Inter VLAN, IPv6 web tunneling (IPv6 Web test run from neighbouring group), Proxy Server, Web, SSL & Virtual Hosting, Authentication, Authorization & Accounting (AAA), Active Directory with GPO, Cloud Server, Media Streaming Server, Network Management System (NMS), Security Policy, Remote login using SSH, Harden Linux server, Harden Windows server, Router hardening, Authentication user by integrating AD with Linux, Installation IDS (port mirror), IPSec VPN, Samba Security, Port Security, VLAN Security and Wireless authentication user. During the Workshop II, we faced several problems but still managed to overcome it and finish this project on time and successfully completed the services.

ABSTRAK

Dalam Projek Bengkel 2 ini, kami harus menentukan, melaksanakan dan menguruskan tugas-tugas yang telah diberikan. Tugasan kami bermula dengan memilih seorang ketua untuk mengetuai projek ini dari awal hingga ke akhir projek bengkel 2 ini. Setiap ahli kumpulan telah dibahagikan dengan tugas secara sama rata dan sebuah jadual telah dihasilkan di mana jadual itu digunakan untuk memastikan bahawa tugas itu disiapkan dalam masa yang ditetapkan. Setiap tugas harus diuruskan dengan sebaik mungkin untuk mengelakkan daripada menimbulkan sebarang masalah dan kesilapan. Objektif utama Bengkel 2 ini adalah untuk melaksanakan projek ini dengan jayanya dan untuk mengatasi sebarang halangan dan cabaran yang dihadapi semasa menyelesaikan tugas yang diberikan sepanjang semester ini. Selain itu, mendapatkan pemahaman mengenai servis-servis yang perlu ada di setiap rangkaian komputer juga merupakan salah satu objektif bengkel ini. Kami sangat berterima kasih kepada pengalaman yang bernilai ini kerana projek ini banyak membantu kami supaya bersedia untuk latihan industri akan datang. Kumpulan kami telah membuat keputusan untuk menggunakan Windows 2012 server (Window), Fedora 28 server (Fed) and Ubuntu 16.04 server (Linux). Kami memilih sistem operasi pelayan ini kerana ianya versi terbaru dan banyak manfaatnya. Kumpulan kami juga telah ditugaskan untuk membekalkan 30 servis kepada rangkain kami. Antara 30 servis yang disenaraikan adalah DNS (IPv4 & IPv6), DHCP (IPv4), DHCP (IPv6), Server Virtualization, Linux Email Server, Secured FTP, Routing & NAT, Access Control List (ACL), Samba, Inter VLAN, IPv6 web tunneling (IPv6 Web test run from neighbouring group), Proxy Server, Web, SSL & Virtual Hosting, Authentication, Authorization & Accounting (AAA), Active Directory with GPO, Cloud Server, Media Streaming Server, Network Management System (NMS), Security Policy, Remote login using SSH, Harden Linux server, Harden Windows server, Router hardening, Authentication user by integrating AD with Linux, Installation IDS (port mirror), IPsec VPN, Samba Security, Port Security, VLAN Security and Wireless authentication user. Sepanjang Projek Bengkel 2 dijalankan, kami menghadapi banyak masalah tetapi masih dapat diatasi dengan baik, projek disiapkan tepat pada masa dan berjaya menyempurnakan kesemua servis.

TABLE OF CONTENTS

ACKNOWLEDGEMENT	i
ABSTRACT	ii
ABSTRAK	iii
TABLE OF CONTENTS	iv
LIST OF TABLES	ix
LIST OF FIGURES	x
Figure Chapter 3	x
Figure Chapter 5	x
Figure Chapter 6	xx
CHAPTER 1 – INTRODUCTION	1
1.1 INTRODUCTION	1
1.2 OBJECTIVE	2
1.3 PROJECT PLAN	2
1.4 CONCLUSION.....	4
CHAPTER 2 - PROJECT REQUIREMENT	5
2.1 INTRODUCTION	5
2.2 TYPES OF OPERATING SYSTEM.....	5
2.3 OPERATING SYSTEM BACKGROUND	5
2.3.1 Windows Server 2012 R2	5
2.3.2 Linux Ubuntu 16.04	6
2.3.3 Linux Fedora 28	6
2.4 OPERATING SYSTEM JUSTIFICATION	7
2.4.1 Window Server 2012 R2.....	7
2.4.2 Linux Ubuntu 16.04	7
2.4.3 Linux Fedora 28	7
2.5 HARDWARE REQUIREMENT	8
2.6 HARDWARE JUSTIFICATION	10
2.7 CONCLUSION.....	11
CHAPTER 3 – DESIGN	12
3.1 INTRODUCTION	12
3.2 SECURITY POLICY	12
3.2.1 Router and Switch Policy.....	12
3.2.2 Wireless Communication Policy.....	15

3.2.3	Password Protection Policy.....	15
3.2.4	Ipv6 web policy.....	18
3.2.5	Remote Access Policy.....	18
3.2.6	Remote Access Tools Policy.....	20
3.2.7	Samba Policy	21
3.2.8	Email Server Policy	21
3.2.9	Acceptable Use Policy	23
3.2.10	Clean Desk	29
3.7	PHYSICAL DESIGN	31
3.8	LOGICAL DESIGN	32
3.9	CONCLUSION.....	33
CHAPTER 4 – SERVICES	34
4.1	INTRODUCTION	34
4.2	LIST OF SERVICES	34
4.2.1	Services for BITC Students.....	34
4.2.2	Services for BITZ Students.....	35
4.3	BRIEF OVERVIEW FOR SERVICES	35
4.3.1	Domain Name System (DNS).....	35
4.3.2	Dynamic Host Configuration Protocol (DHCP)	36
4.3.3	Dynamic Host Configuration Protocol version 6 (DHCPv6).....	36
4.3.4	Virtual LAN (VLAN)	37
4.3.5	Routing and Network Address Translation (NAT)	37
4.3.6	Active Directory.....	38
4.3.7	Proxy Server.....	38
4.3.8	Samba.....	39
4.3.9	Network Management System (NMS).....	39
4.3.10	Server Virtualisation	39
4.3.11	AAA (Authentication, Authorization, and Accounting) using Radius	40
4.3.12	Access Control List (ACL)	41
4.3.13	Secure FTP.....	41
4.3.14	Web, SSL and Virtual Hosting	41
4.3.15	Linux Email Server	42
4.3.17	Media Streaming Server.....	43
4.3.18	Cloud Server	43
4.3.19	Security Policy	43
4.3.20	Router Hardening.....	44

4.3.21	Remote login using SSH	45
4.3.22	Linux server hardening and Windows server hardening.....	45
4.3.23	Authentication user by integrating AD with Linux.....	46
4.3.25	IDS with port mirror	47
4.3.26	IPsec VPN for remote employees	47
4.3.27	Samba security services	47
4.3.28	Port Security.....	48
4.3.29	VLAN security	48
4.4	CONCLUSION	48
CHAPTER 5 - INSTALLATION AND CONFIGURATION	49
5.1	INTRODUCTION	49
5.2	SERVICES INSTALLATION AND INDIVIDUAL WHO RESPONSIBLE FOR THE TESTING	49
5.2.1	DNS (Domain Name Server (IPv4 & IPv6))	51
5.2.2	DHCP (IPv4).....	86
5.2.3	DHCP (IPv6).....	92
5.2.4	Inter VLAN and VLSM addressing	96
5.2.5	Routing & NAT	101
5.2.6	Active Directory.....	103
5.2.7	Proxy Server.....	122
5.2.8	Samba.....	127
5.2.9	Network Management System	131
5.2.10	Server Virtualization.....	135
5.2.11	AAA (Authentication, Authorization, and Accounting) using Radius	154
5.2.12	Access Control List (ACL)	171
5.2.13	Secured FTP	172
5.2.14	Web, SSL & Virtual Hosting Linux Email Server.....	174
5.2.15	Linux Email Server	189
5.2.16	IPv6 Web with IPv6 Tunneling	194
5.2.17	Media streaming server	199
5.2.18	Cloud server	202
5.2.19	VLAN Security	206
5.2.20	Router hardening.....	208
5.2.21	Remote login using SSH.....	214
5.2.22	Linux server hardening	218
5.2.23	Windows server hardening.....	222

5.2.24	Authentication user by integrating AD with Linux.....	242
5.2.25	Wireless user authentication using Radius server	247
5.2.26	IDS with port mirror	264
5.2.27	IPsec VPN for remote employees	272
5.2.28	Samba security services	290
5.2.29	Port Security.....	292
CHAPTER 6 - TESTING	294
6.1	INTRODUCTION	294
6.2	SERVICES TESTING	294
6.2.1	DNS (IPv4 & IPv6).....	295
6.2.2	DHCP (IPv4).....	296
6.2.3	DHCP (IPv6).....	297
6.2.4	Inter VLAN and VLSM addressing	298
6.2.5	Routing & NAT	299
6.2.6	Active Directory.....	300
6.2.7	Proxy Server.....	303
6.2.8	Samba.....	305
6.2.9	Network Management System	307
6.2.10	Server Virtualization	310
6.2.11	AAA (Authentication, Authorization, and Accounting) using Radius	313
6.2.12	Access Control List (ACL)	315
6.2.13	Secured FTP	317
6.2.14	Web, SSL & Virtual Hosting Linux Email Server.....	320
6.2.15	Linux Email Server	322
6.2.16	IPv6 Web with IPv6 Tunneling	324
6.2.17	Media streaming server.....	326
6.2.18	Cloud server	328
6.2.19	VLAN Security	330
6.2.20	Router hardening.....	331
6.2.21	Remote login using SSH.....	335
6.2.22	Linux server hardening	340
6.2.23	Windows server hardening.....	341
6.2.24	Authentication user by integrating AD with Linux.....	344
6.2.25	Wireless user authentication using Radius server	345
6.2.26	IDS with port mirror	347
6.2.27	IPsec VPN for remote employees	348

6.2.28	Samba security services	354
6.2.29	Port Security.....	358
6.3	CONCLUSION.....	360
CHAPTER 7 – CONCLUSION.....		361
7.1	INTRODUCTION	361
7.2	PROJECT ADVANTAGES	362
7.3	PROJECT DISADVANTAGES	363
7.4	PROJECT LIMITATION	363
7.5	CONCLUSION.....	364
BIBLIOGRAPHY		365
APPENDIX.....		366

LIST OF TABLES

Table 1 : Hardware requirement windows 2012	8
Table 2 : Hardware requirement Ubuntu 16.04	9
Table 3 : Hardware requirement Fedora	9
Table 4 : IP Addressing.....	100
Table 5 : Port Range	100

LIST OF FIGURES

Figure Chapter 3	
Figure 3. 1 : Physical design	31
Figure 3. 2 : Logical design	32
Figure Chapter 5	
Figure 5. 1: Put correct IP address	51
Figure 5. 2: DNS Server Wizard.....	51
Figure 5. 3: Select Zone Type	52
Figure 5. 4: Select Active Directory Zone Replication Scope	53
Figure 5. 5: Zone Name	54
Figure 5. 6: Dynamic Update.....	54
Figure 5. 7: DNS Server Wizard.....	56
Figure 5. 8: New Zone (Reverse Lookup Zone)	57
Figure 5. 9: DNS Server Wizard.....	57
Figure 5. 10: Zone type	58
Figure 5. 11: Zone replication.....	58
Figure 5. 12 : Select IPv4 Reverse Lookup Zone Name (IPv4)	59
Figure 5. 13: Reverse Lookup Zone Name	60
Figure 5. 14: Dynamic Update.....	60
Figure 5. 15: Completing the New Zone Wizard.....	61
Figure 5. 16: Pointer (PTR)	61
Figure 5. 17: Enter the Host IP Address	62
Figure 5. 18: New Host (A or AAAA).....	62
Figure 5. 19: New Host IPv4	63
Figure 5. 20: Put correct IP address, Subnet Mask,	64
Figure 5. 21: New Zone	64
Figure 5. 22: Welcome the New Zone Wizard	65
Figure 5. 23: Zone Type.....	65
Figure 5. 24: Zone Type.....	66
Figure 5. 25: IPv6 Reverse Lookup Zone	66
Figure 5. 26: IPv6 Address Prefix	67
Figure 5. 27: Dynamic Update.....	67
Figure 5. 28 : Completing the New Zone.....	68
Figure 5. 29 New Pointer (PTR)	68
Figure 5. 30 Enter the Host IP Address and Host name.....	69
Figure 5. 31: New Host (A or AAAA).....	69
Figure 5. 32: New Host.....	70
Figure 5. 33: Put correct IP address,	71
Figure 5. 34: Install bind9	71
Figure 5. 35 : Bind9 configuration file path.....	72
Figure 5. 36 : Bind9 configuration file	72
Figure 5. 37 : Bind9 status	73
Figure 5. 38: New Zone (Reverse Lookup Zone)	73
Figure 5. 39: DNS Server Wizard.....	74
Figure 5. 40: Zone type	74
Figure 5. 41: Zone replication.....	75
Figure 5. 42: Select IPv4 Reverse Lookup Zone Name (IPv4).....	75
Figure 5. 43: Reverse Lookup Zone Name	76
Figure 5. 44: Dynamic Update.....	77
Figure 5. 45: Completing the New Zone Wizard of.....	77
Figure 5. 46: Pointer (PTR)	78

Figure 5. 47: New Resource Record	78
Figure 5. 48: New Host (A or AAAA).....	79
Figure 5. 49: New Host IPv4	79
Figure 5. 50: Put correct IP address, Subnet Mask,	80
Figure 5. 51: New Zone	80
Figure 5. 52: Welcome the New Zone Wizard	81
Figure 5. 53: Zone Type.....	81
Figure 5. 54: Zone Replication scope	82
Figure 5. 55: IPv6 Reverse Lookup Zone	82
Figure 5. 56: IPv6 Address Prefix.....	83
Figure 5. 57: Dynamic Update.....	83
Figure 5. 58 : Completing the New Zone Wizard of IPv6.....	84
Figure 5. 59: New Pointer (PTR)	84
Figure 5. 60: Enter the Host IP Address and Host name	85
Figure 5. 61 : Server Manager	86
Figure 5. 62 : Server Roles	86
Figure 5. 63: DHCP Summary	87
Figure 5. 64: DHCP Manager	87
Figure 5. 65: New Scope.....	88
Figure 5. 66: Rename the new scope as clientIPv4.....	88
Figure 5. 67: IP Address Range	89
Figure 5. 68: Add Exclusion and Delay.....	89
Figure 5. 69: Lease Duration	90
Figure 5. 70: WINS Servers.....	90
Figure 5. 71: DHCP Options.....	91
Figure 5. 72: Complete New Scope	91
Figure 5. 73: Click tools then click dhcp	92
Figure 5. 74: Right click on IPv6 and click scope	92
Figure 5. 75: Click next	93
Figure 5. 76: New name for IPv6 scope.....	93
Figure 5. 77: Set IPv6 address	94
Figure 5. 78: Set scope lease time	94
Figure 5. 79: Click finish once done the configuration.....	95
Figure 5. 80: Labelling switch name.....	96
Figure 5. 81: Assign name for ‘vlan 5’	96
Figure 5. 82: Assign name for ‘vlan 10’	96
Figure 5. 83: Assign name for ‘vlan 20’	96
Figure 5. 84: Assign name for ‘vlan 30’	96
Figure 5. 85: Assign name for ‘vlan 101’	96
Figure 5. 86: Assign name for ‘vlan 102’	96
Figure 5. 87: Execution of copy run start.....	97
Figure 5. 88: Assign port 19 to 21 for vlan Client	97
Figure 5. 89: Assign port 16 to 18 for vlan AP.....	97
Figure 5. 90: Assign port 4 to 6 for vlan WinServer.	97
Figure 5. 91: Assign port 7 to 9 for vlan UbuServer.....	97
Figure 5. 92: Assign port 10 to 12 for vlan FedoServer.....	97
Figure 5. 93: Assign port 23 and 24 for vlan Trunk.....	98
Figure 5. 94: Interface G0/0.101 (Client).	98
Figure 5. 95: Interface G0/0.102 (AP).	98
Figure 5. 96: Interface G0/0.10 (WinServer).....	98
Figure 5. 97: Interface G0/0.20 (UbuServer).....	98

Figure 5. 98: Interface G0/0.30 (FedoServer).....	98
Figure 5. 99: Interface G0/0.5 (Trunk).	98
Figure 5. 100: IP-Helper on G0/0.101 (Client).....	99
Figure 5. 101: IP-Helper on G0/0.102 (AP).....	99
Figure 5. 102: Configuration of NAT.	101
Figure 5. 103: List of configuration.	101
Figure 5. 104: List of configuration.	102
Figure 5. 105: Click Add roles and feature form server manager.....	103
Figure 5. 106: Check on Active Directory Domain Services.....	103
Figure 5. 107: Click on Install on the confirmation window.....	104
Figure 5. 108: Click on Post-deployment Configuration.....	104
Figure 5. 109: Specify the foot domain name as group7.com	105
Figure 5. 110: Assign Password for the Directory.....	105
Figure 5. 111 : DNS Options	106
Figure 5. 112 : Active Directory (Additional Options).....	106
Figure 5. 113 : All Prerequisites Check	107
Figure 5. 114: Open Active Directory Users and Computers	108
Figure 5. 115: Adding a computer to our domain controller	108
Figure 5. 116 : Creating Group7 organizational Unit.	109
Figure 5. 117 : Adding User to our domain controller.....	109
Figure 5. 118 : Setup the information	110
Figure 5. 119 : Setup password of the New User.....	110
Figure 5. 120 : Show all created users.	111
Figure 5. 121 : Create other Group	111
Figure 5. 122 : Navigate to Group and then New.	112
Figure 5. 123 : Select then click OK to continue.	112
Figure 5. 124 : Add another user to Group.	113
Figure 5. 125 : Select then click OK to continue.	113
Figure 5. 126 : Show a new folder that can store SharedFolderHome.....	114
Figure 5. 127 : Navigate to Properties.	114
Figure 5. 128 : Navigate to Sharing tab	115
Figure 5. 129 : Click on the arrow and choose Everyone	115
Figure 5. 130 : Go to the Profile tab and tick at.....	116
Figure 5. 131 : Check the result after specifying the	116
Figure 5. 132 : Create a new group policy	117
Figure 5. 133 : Create group policy for BITC.....	117
Figure 5. 134 : Show that BITC_GPO is linked	118
Figure 5. 135 : Show that BITZ_GPO is linked	118
Figure 5. 136 : Editing BITC_GPO file.	119
Figure 5. 137 : Click on All Removable Storage classes Deny all access.	119
Figure 5. 138 : Enabled denying all removable devices.	120
Figure 5. 139 : Enabling the policy to not allow password to be saved.....	120
Figure 5. 140 : Maximum the password age for BITZ users.	121
Figure 5. 141 : Install Squid.....	122
Figure 5. 142 : Downloading package	122
Figure 5. 143 : Edit squid configuration	123
Figure 5. 144 : File of squid configuration	123
Figure 5. 145 : Http port	124
Figure 5. 146 : Edit block domain.....	124
Figure 5. 147 : Websites	125
Figure 5. 148 : Keywords.....	125

Figure 5. 149 : Restart service	125
Figure 5. 150 : File of squid configuration	126
Figure 5. 151 : Install samba.....	127
Figure 5. 152 : Enable smb	127
Figure 5. 153 : Allow samba to work.....	127
Figure 5. 154 : Open port.....	128
Figure 5. 155 : Home directory.....	128
Figure 5. 156 : Add user	128
Figure 5. 157 : Restart samba	129
Figure 5. 158 : Add new directory	129
Figure 5. 159 : Samba configuration.....	129
Figure 5. 160 : File located	130
Figure 5. 161 : File permission	130
Figure 5. 162 : Label file.....	130
Figure 5. 163 : Update Ubuntu.....	131
Figure 5. 164 : Installing package.....	131
Figure 5. 165 : Extract Apache to server.....	131
Figure 5. 166 : User ‘newnagios’ been added.....	131
Figure 5. 167 : Group ‘newnagioss’ added.....	131
Figure 5. 168 : Permission and grouping.....	131
Figure 5. 169 : Group the new user to a group.	131
Figure 5. 170 : Installing Nagios.....	131
Figure 5. 171 : Installer setup.	132
Figure 5. 172 : Installing boot configuration.	132
Figure 5. 173 : Command mode installation.....	132
Figure 5. 174 : Install other configuration files for Nagios.....	132
Figure 5. 175 : Web configure installation.	132
Figure 5. 176 : Copy the eventhandler.....	132
Figure 5. 177 : Give permission to read in nagios directory.....	132
Figure 5. 178: ‘Nagios.cfg’ file setting.	132
Figure 5. 179 : Set nagios tu running state.....	132
Figure 5. 180 : Set the password.....	133
Figure 5. 181 : Nagios configuration checking.....	133
Figure 5. 182 : Nagios configuration enabling.....	133
Figure 5. 183 : Allowing selected port.....	133
Figure 5. 184 : Installation of ip table persistent.....	133
Figure 5. 185 : Execute nagios application.	133
Figure 5. 186 : Nagios module enabling.....	133
Figure 5. 187 : CGI module enabled.....	133
Figure 5. 188 : Windows configuration for services and host.	134
Figure 5. 189 : Install hyperv	135
Figure 5. 190 : Installation type	135
Figure 5. 191 : Server selection	136
Figure 5. 192 : Add features	136
Figure 5. 193 : Server roles	137
Figure 5. 194 : Features	137
Figure 5. 195 : hyperv installation	138
Figure 5. 196 : Virtual switch manager.....	138
Figure 5. 197 : Authentication protocol	139
Figure 5. 198 : Default location for hard disk files	139
Figure 5. 199 : Confirm installation hyperv.....	140

Figure 5. 200 : hyperv installed	140
Figure 5. 201 : Install virtual machine	141
Figure 5. 202 : Name and location virtual machine.....	141
Figure 5. 203 : Specify generation.....	142
Figure 5. 204 : Assign memory.....	142
Figure 5. 205 : Assign connection	143
Figure 5. 206 : Create virtual hard disk	143
Figure 5. 207 : Installation operating system	144
Figure 5. 208 : Ubuntu installed.....	144
Figure 5. 209 : Create a ftp file and text file	145
Figure 5. 210 : Create a folder in ftp file and text fie.....	145
Figure 5. 211 : install vsftpd	146
Figure 5. 212 : vsftpd installed.....	146
Figure 5. 213 : Open config file	146
Figure 5. 214 : config file	147
Figure 5. 215 : Add group ftp user.....	147
Figure 5. 216 : Add user into group ftp user	147
Figure 5. 217 : Change mode permission and change owner directory	148
Figure 5. 218 : Restart vsftpd and access ftp localhost	148
Figure 5. 219 : Send document text file	148
Figure 5. 220 : Get document text file	149
Figure 5. 221 : Files in home directory	149
Figure 5. 222 : File text in folder in ftp file	150
Figure 5. 223 : Restart vsftpd.....	150
Figure 5. 224 : Testing ftp.....	151
Figure 5. 225 : Create ssl certificates vsftpd	151
Figure 5. 226 : open vsftpd configuration file	152
Figure 5. 227 : comment command	152
Figure 5. 228 : Add command point to certificate	152
Figure 5. 229 : Command force use of SSL.....	152
Figure 5. 230 : Add command to deny annoynymous over SSL	153
Figure 5. 231 : Add command ssl_tlsv1 only	153
Figure 5. 232 : Command allow ftp client without SSL	153
Figure 5. 233 : Command restart vsftpd	153
Figure 5. 234 : Server Manager	154
Figure 5. 235 : Add Roles and Features.....	154
Figure 5. 236 : Select server roles.....	155
Figure 5. 237 : Installation progress.....	155
Figure 5. 238 : Network Policy Server	156
Figure 5. 239 : Enable NPS.....	156
Figure 5. 240 : New radius client.....	157
Figure 5. 241 : Verify Address.....	157
Figure 5. 242 : New network policies	158
Figure 5. 243 : Policy Name	159
Figure 5. 244 : Specify Condition.....	159
Figure 5. 245 : Select group	160
Figure 5. 246 : Check names.....	160
Figure 5. 247 : User groups.....	161
Figure 5. 248 : Access permission	161
Figure 5. 249 : Authentication method	162
Figure 5. 250 : Configure constraint	162

Figure 5. 251 : Configure settings.....	163
Figure 5. 252 : Attribute information.....	163
Figure 5. 253 : Vendor specific.....	164
Figure 5. 254: Attribute value	165
Figure 5. 255 Successful created network policy	165
Figure 5. 256 : Accounting in Network Policy Server.....	166
Figure 5. 257: Introduction in accounting configuration	166
Figure 5. 258 : Select accounting option.....	167
Figure 5. 259: Configure file logging	167
Figure 5. 260 : Conclusion.....	168
Figure 5. 261 : Configuration in putty for aaa new model.....	169
Figure 5. 262: Configuration in putty for authentication	169
Figure 5. 263 : Configuration in putty for server name	170
Figure 5. 264 : Show run in putty	170
Figure 5. 265: ACL Configuration.....	171
Figure 5. 266: Save ACL Configuration.....	171
Figure 5. 267: Show ACL configuration	171
Figure 5. 268: Create group by the name “G7sftp”	172
Figure 5. 269: Create and add new user to G7sftp with permission.	172
Figure 5. 270: Set password for user “sftp7”	172
Figure 5. 271: Directory named “shareSFTP” has been created.....	172
Figure 5. 272: Read and execute has been allowed	172
Figure 5. 273: Create ‘file’ folder and give permission read,	172
Figure 5. 274: Assign ‘G7sftp’ which is group, to share directory.....	172
Figure 5. 275 : Access the configuration file	173
Figure 5. 276 : Changing the subsystem SFTP to internal only.....	173
Figure 5. 277: Declare the variable	173
Figure 5. 278: Add role in server	174
Figure 5. 279: Select Role-based or Feature-based Installation.....	174
Figure 5. 280: Select Role-based or Feature-based Installation.....	175
Figure 5. 281: Select Web Server (IIS).....	175
Figure 5. 282: Add Roles and Features wizard	176
Figure 5. 283: Keep clicking next until reaching to confirmation page.....	176
Figure 5. 284: Installing conformation	177
Figure 5. 285: Installing progress	177
Figure 5. 286: IIS manager to adding new web	178
Figure 5. 287: IIS manager to adding new web	178
Figure 5. 288: Installing progress	179
Figure 5. 289 : Server Certificates	180
Figure 5. 290: Server Certificates	180
Figure 5. 291: Specify name for certificate.....	181
Figure 5. 292 : List of Certificate.....	181
Figure 5. 293: Add site binding for SSL.....	182
Figure 5. 294: SSL setting	182
Figure 5. 295: Change SSL setting	183
Figure 5. 296 : Add new website	184
Figure 5. 297 : Add new Default Document	184
Figure 5. 298 : New html File	185
Figure 5. 299: Create a new zone.....	185
Figure 5. 300: Choose a zone type	186
Figure 5. 301: Zone Replication Scope.....	186

Figure 5. 302: Dynamic update DNS	187
Figure 5. 303: The New Zone wizard complete.....	187
Figure 5. 304: Create a new host.....	188
Figure 5. 305: Setting up postfix.....	189
Figure 5. 306: Type in domain name for system mail name.....	189
Figure 5. 307: Editing configuration of postfix	190
Figure 5. 308: Configuring the dovecot.conf file.....	190
Figure 5. 309 : Installing Rainloop	191
Figure 5. 310 : Set web server user	191
Figure 5. 311 : Editing virtual hosting file.....	192
Figure 5. 312 : Save and reload Apache2	192
Figure 5. 313 : Editing domain setting.....	193
Figure 5. 314: Set up email account.....	193
Figure 5. 315: New zone in forward lookup zones	194
Figure 5. 316: Add new host in.....	194
Figure 5. 317 : New host added	195
Figure 5. 318: Create personal certificate for ssl	195
Figure 5. 319: Add site binding for web	196
Figure 5. 320 : Add site binding using ssl certificate.....	196
Figure 5. 321: Interface tunnel0	197
Figure 5. 322: IPv6 address of the tunnel interface	197
Figure 5. 323: Tunnel interface.....	197
Figure 5. 324 Neighbour Ipv6 address.....	198
Figure 5. 325: Choose Platform “Linux” and distribution “Ubuntu”	199
Figure 5. 326 : Show Plex web interface “Login Page”	200
Figure 5. 327 : Set Plex Server name	200
Figure 5. 328 : Click add library button to add media files	201
Figure 5. 329 : Add media files to library	201
Figure 5. 330 : Root environment	202
Figure 5. 331 : Install LAMP Server.....	202
Figure 5. 332 : Download Nextcoud.....	202
Figure 5. 333 : Move the file	202
Figure 5. 334 : Change the permission	202
Figure 5. 335 : Mysql.....	202
Figure 5. 336 : Configure MariaDB	203
Figure 5. 337 : Create Nextcoud Database	203
Figure 5. 338 : Disable the MariaDB	204
Figure 5. 339 : Configure apache server	204
Figure 5. 340 : Create the nextcloud.conf file.....	204
Figure 5. 341: Create the nextcloud.conf file.....	205
Figure 5. 342 : Restart apache server	205
Figure 5. 343 : Nextcloud User Interface	205
Figure 5. 344 : Switchport nonegotiate.....	206
Figure 5. 345 : Show vlan	206
Figure 5. 346 : Create VLAN 60 named unusedPorts	206
Figure 5. 347 : Suspend VLAN 60	206
Figure 5. 348 : Assign all unused port into VLAN 60	206
Figure 5. 349 : Assign all usable VLANs into trunk ports.....	207
Figure 5. 350 : Putty.....	208
Figure 5. 351 : Putty.....	208
Figure 5. 352 : Putty.....	209

Figure 5. 353 : Putty.....	209
Figure 5. 354 : Putty.....	210
Figure 5. 355 : Putty Configuration	211
Figure 5. 356 : Select session log file name.....	211
Figure 5. 357 : Putty Configuration	212
Figure 5. 358 : Putty.....	213
Figure 5. 359 : Putty.....	213
Figure 5. 360 : Configuration for router	214
Figure 5. 361 : Login local.....	214
Figure 5. 362 : IP SSH v2	215
Figure 5. 363 : Configuration on Ubuntu.....	215
Figure 5. 364 : Configuration file of sshd.....	216
Figure 5. 365 : Configuration file of sshd.....	216
Figure 5. 366 : Install openssh-server	217
Figure 5. 367: g7@fedora-group7-com:/home/g7	218
Figure 5. 368 : g7@fedora-group7-com:/home/g7	218
Figure 5. 369 : g7@fedora-group7-com:/home/g7	219
Figure 5. 370 : g7@fedora-group7-com:/home/g7	219
Figure 5. 371 : g7@fedora-group7-com:/home/g7	219
Figure 5. 372 : g7@fedora-group7-com:/home/g7	220
Figure 5. 373: g7@fedora-group7-com:/home/g7	220
Figure 5. 374 : g7@fedora-group7-com:/home/g7	220
Figure 5. 375 : g7@fedora-group7-com:/home/g7	221
Figure 5. 376 : g7@fedora-group7-com:/home/g7	221
Figure 5. 377 : Administrative Tools	222
Figure 5. 378 : First Page of the Security Configuration Wizard	222
Figure 5. 379 : Configuration Action	223
Figure 5. 380 : Select Server.....	223
Figure 5. 381: Processing Security Configuration Database	224
Figure 5. 382: Role-Based Service Configuration Page	224
Figure 5. 383 : Select Server Roles.....	225
Figure 5. 384 : Client Features.....	225
Figure 5. 385 : List of Administration and Other Options	226
Figure 5. 386 : List Administration and Other Options (cont).....	226
Figure 5. 387 : Additional Services	227
Figure 5. 388 : Handling Unspecified Services	227
Figure 5. 389 : Confirm service changes	228
Figure 5. 390 : Network Security	228
Figure 5. 391 : Network Security Rules.....	229
Figure 5. 392 : Registry Setting	229
Figure 5. 393 : Require SMB Security Signatures.....	230
Figure 5. 394 : LDAP Signing	230
Figure 5. 395 : Outbound Authentication Methods	231
Figure 5. 396 : Outbound Authentication using.....	231
Figure 5. 397: Registry Setting Summary.....	232
Figure 5. 398 : Audit Policy.....	232
Figure 5. 399 : System Audit Policy	233
Figure 5. 400 : Audit Policy Summary	233
Figure 5. 401 : Save Security Policy.....	234
Figure 5. 402 : Security Policy File Name.....	234
Figure 5. 403 : Apply Security Policy.....	235

Figure 5. 404 : Security Configuration Wizard Complete	235
Figure 5. 405 : Server Manager	236
Figure 5. 406 : Active Directory Users and Computers.....	236
Figure 5. 407 : Disable Guest Account.....	237
Figure 5. 408 : Server Manager	237
Figure 5. 409 : Local Security Policy	238
Figure 5. 410 : Audit Privilege use Properties	238
Figure 5. 411 : Search Windows Update	239
Figure 5. 412 : Windows Update Settings	239
Figure 5. 413 : Server Manager	240
Figure 5. 414 : Windows Firewall with Advanced Security.....	240
Figure 5. 415 : Run dialog Box.....	241
Figure 5. 416 : Disable Distributed Transaction Coordinator Properties.....	241
Figure 5. 417 : Check computer's hostname.....	242
Figure 5. 418 : Install required libraries and packages	242
Figure 5. 419: kinit and klist command	243
Figure 5. 420 : Samba Configuration.....	243
Figure 5. 421 : Restart SMBD, NMBD and WinBind Service	244
Figure 5. 422 : Join Group7 Domain	244
Figure 5. 423 : NSSwitch Configuration	245
Figure 5. 424 : AD Users	245
Figure 5. 425 : PAM Configuration	246
Figure 5. 426 : Get AD User's Password	246
Figure 5. 427 : Create group7 in group7.com	247
Figure 5. 428: Create user fahmy in group7.com.....	247
Figure 5. 429 : Assign password for the user.....	248
Figure 5. 430 : List of users that has been created.....	248
Figure 5. 431 : The confirmation before installation	248
Figure 5. 432 : Select installation type.....	249
Figure 5. 433 : Server selection	249
Figure 5. 434 : Selecting Server Roles for installing AD CS.....	250
Figure 5. 435 : Select feature for installation	250
Figure 5. 436 : Selecting Role Services for Certification Authority	251
Figure 5. 437 : Confirmation for installation selection	251
Figure 5. 438 : Specify credentials to configure role services	252
Figure 5. 439 : Selecting Role Services for Certification Authority	252
Figure 5. 440 : Selecting Specify Setup Type.....	253
Figure 5. 441 : Selecting Specify CA Type	253
Figure 5. 442 : Setting up the Private Key	254
Figure 5. 443 : Configuring Cryptography for CA	254
Figure 5. 444 : Configuring CA Naming	255
Figure 5. 445 : Setting the validity Period	255
Figure 5. 446 : Configuring Certificate Database	256
Figure 5. 447 : Confirmation the Installation Selections	256
Figure 5. 448 : Showing Certificate Installation Results	257
Figure 5. 449 : Showing Microsoft Management Console to add Certificate.....	257
Figure 5. 450 : Starting Certificate Enrolment.....	258
Figure 5. 451 : Selecting Certificate Enrolment Policy	258
Figure 5. 452 : Showing Certificate Enrolment	259
Figure 5. 453 : Command run for NPS	259
Figure 5. 454 Selecting 802.1X Connections Type	259

Figure 5. 455 : Selecting specify a RADIUS client	260
Figure 5. 456 : Adding new RADIUS Client for wireless	260
Figure 5. 457 : Configuring an Authentication Method.....	260
Figure 5. 458 : Specifying User Group	261
Figure 5. 459 : Showing Configure Traffic Controls.....	261
Figure 5. 460 : Successfully Completing Wireless Connections	262
Figure 5. 461 : Showing Microsoft Management Console	262
Figure 5. 462 : Showing Certificate Export Wizard	263
Figure 5. 463 : Specifying the name of the file.....	263
Figure 5. 464 : Showing successfully	263
Figure 5. 465 : Required Libraries	264
Figure 5. 466 : Required Packages.....	264
Figure 5. 467 : DAQ	264
Figure 5. 468 : Decompress DAQ.....	264
Figure 5. 469 : Change Directory to DAQ.....	265
Figure 5. 470 : Install DAQ	265
Figure 5. 471 : Install Snort with Source Fire enable	265
Figure 5. 472 : Create a systemd link.....	265
Figure 5. 473 : Create a link to sbin folder	265
Figure 5. 474 : Snort Version.....	265
Figure 5. 475 : Add Snort Group and User	265
Figure 5. 476 : Create Snort's folder in etc	266
Figure 5. 477 : Create black list, white list and local rules	266
Figure 5. 478 : Copy configuration and map to /etc/snort	266
Figure 5. 479 : Copy community rules to rules directory	266
Figure 5. 480 : Protected IP	267
Figure 5. 481 : Path to rules	267
Figure 5. 482 : Path to black list and white list IPs.....	268
Figure 5. 483 : Output Snort to log file.....	268
Figure 5. 484 : Uncomment any rules available	268
Figure 5. 485 : Verify Snort's Configuration	269
Figure 5. 486 : Snort Successfully Verify Configuration	269
Figure 5. 487 : Create a startup script	269
Figure 5. 488 : Snort.Service	269
Figure 5. 489 : Reload Daemon	269
Figure 5. 490 : Snort Status.....	270
Figure 5. 491 : Create monitor session	271
Figure 5. 492 : Monitor Session 1.....	271
Figure 5. 493 : SoftEther VPN Setup Wizard	272
Figure 5. 494 : Software Components to Install	272
Figure 5. 495 : End User License Agreement	273
Figure 5. 496 : Important Notices	273
Figure 5. 497 : Directory to Install.....	274
Figure 5. 498 : Ready to Install.....	274
Figure 5. 499 : Setup is in Progress	275
Figure 5. 500 : Setup Finished	275
Figure 5. 501 : SoftEther VPN Server Manager	276
Figure 5. 502 : Edit localhost (This server)	276
Figure 5. 503 : Change Administrator Password	277
Figure 5. 504 : SoftEther VPN Server Manager	277
Figure 5. 505 : SoftEther VPN Server / Bridge Easy Setup.....	278

Figure 5. 506 : Easy Setup – Decide the Virtual Hub Name	278
Figure 5. 507 : Dynamic DNS Function	279
Figure 5. 508 : IPsec / L2TP / EtherIP / L2TPv3.....	279
Figure 5. 509 : VPN Azure Service Settings	280
Figure 5. 510 : VPN Easy setup Tasks.....	280
Figure 5. 511 : Create User	281
Figure 5. 512 : Manage Users	281
Figure 5. 513 : Create New Certificate	282
Figure 5. 514 : Save Certificate and Private Key.....	282
Figure 5. 515 : Specify a file name where you want to save the certificate.....	283
Figure 5. 516 : IPSec VPN folder	283
Figure 5. 517 : SoftEther VPN Setup Wizard.....	284
Figure 5. 518 : Software Components to Install	284
Figure 5. 519 : End User License Agreement	285
Figure 5. 520 : Important Notices	285
Figure 5. 521 : Directory to Install.....	286
Figure 5. 522 : Ready to Install.....	286
Figure 5. 523 : Setup is in Progress	287
Figure 5. 524 : Setup Finished	287
Figure 5. 525 Add VPN Connection.....	288
Figure 5. 526 VPN Connection Setting Properties	288
Figure 5. 527 : SoftEther VPN Client Manager.....	289
Figure 5. 528 : Samba Group Configuration.....	290
Figure 5. 529 : Samba User's Directory	291
Figure 5. 530 : Command on Ubuntu	292
Figure 5. 531 : Command on Fedora	292
Figure 5. 532 : Command on Windows	292
Figure 5. 533 : Command for Ubuntu.....	293
Figure 5. 534 : Command for Fedora.....	293
Figure 5. 535 : Command for Windows	293
Figure Chapter 6	
Figure 6. 1 : nslookup IPv4 and IPv6.....	295
Figure 6. 2 : Ipconfig	296
Figure 6. 3 : Show ipconfig.....	297
Figure 6. 4 : Command prompt fedora.....	298
Figure 6. 5 : Command prompt fedora.....	298
Figure 6. 6 : Command prompt fedora.....	298
Figure 6. 7 : NAT mapping.....	299
Figure 6. 8 : Ping public ip address neighbour from Router.....	299
Figure 6. 9 : Show that our group policy is applied on Saleh user.....	301
Figure 6. 10 : Run Snipping Tool	301
Figure 6. 11 : Error window for disable sniping tool to the user.	302
Figure 6. 12 : Browser's setting	303
Figure 6. 13 : LAN settings.....	303
Figure 6. 14 : Insert IP Address	304
Figure 6. 15 : Connection refuse	304
Figure 6. 16 : Check status smb nmb	305
Figure 6. 17 : Testing samba by sharing file.....	305
Figure 6. 18 : Shared file in client pc.....	306
Figure 6. 19 : Nagios core homepage.	307
Figure 6. 20 : Nagios host page.....	307

Figure 6. 21 : Services on Nagios has been installed to monitor.....	308
Figure 6. 22 : Extend for nagios service page.....	308
Figure 6. 23 : Router histogram	309
Figure 6. 24 : Nagios map.....	309
Figure 6. 25 : Send document text file	310
Figure 6. 26 : Get document text file	310
Figure 6. 27 : Files in home directory	311
Figure 6. 28 : File text in folder in ftp file	311
Figure 6. 29 : Restart vsftpd.....	312
Figure 6. 30 : Testing ftp.....	312
Figure 6. 31 : Test sftp in FileZilla	312
Figure 6. 32 : Putty configuration	313
Figure 6. 33 : G7daus in groupadmin for AAA	313
Figure 6. 34 : G7nisa in groupuser for AAA	313
Figure 6. 35 : In the system32.....	314
Figure 6. 36 : ACL Configuration.....	315
Figure 6. 37 : Before ACL Configuration.....	315
Figure 6. 38 After ACL Configuration	315
Figure 6. 39 : Before ACL Configuration.....	316
Figure 6. 40 : After ACL Configuration	316
Figure 6. 41 : Establishing SFTP connection.....	317
Figure 6. 42 : Checking local directory and inside the directory.....	317
Figure 6. 43 : Downloading ‘jabba.txt’ file from SFTP server.....	317
Figure 6. 44 : Uploading ‘Sftp7Cuba.txt’ to SFTP server	317
Figure 6. 45 : End the SFTP connection.....	318
Figure 6. 46 : Estabilsh connection using Filezilla.....	318
Figure 6. 47 : Local directory selected.....	318
Figure 6. 48 : Upload and download operation using Filezilla.....	319
Figure 6. 49 : Web testing using domain name.....	320
Figure 6. 50 : Web testing using IP Address.....	320
Figure 6. 51 : Testing Secure browser.	321
Figure 6. 52 : Testing virtual hosting web.	321
Figure 6. 53 : Login to RainLoop Email server	322
Figure 6. 54 : Compose email from RainLoop Email server	322
Figure 6. 55 : Receive email	323
Figure 6. 56 : Testing website using hostname	324
Figure 6. 57 : Testing website using Ipv6 address	324
Figure 6. 58 : Website group7 in neighbour’s group	325
Figure 6. 59 : Login using the username.....	326
Figure 6. 60 : Plex dashboard.....	326
Figure 6. 61 : Media file is playing from client site.....	327
Figure 6. 62 : Nextcloud login page.....	328
Figure 6. 63 : Nextcloud admin page	328
Figure 6. 64 : Nextcloud login page.....	329
Figure 6. 65 : Upload and Download the file.....	329
Figure 6. 66 : Play the video	329
Figure 6. 67 : VLAN brief	330
Figure 6. 68 : Putty.....	331
Figure 6. 69 : Putty.....	331
Figure 6. 70 : Putty.....	332
Figure 6. 71 : Putty.....	332

Figure 6. 72 : Desktop.....	333
Figure 6. 73 : Log - Notepad.....	333
Figure 6. 74 : Putty.....	334
Figure 6. 75 : Putty.....	334
Figure 6. 76 : Putty configuration	335
Figure 6. 77 : Login Ubuntu	335
Figure 6. 78 : Putty configuration	336
Figure 6. 79 : Login Fedora	336
Figure 6. 80 : Router	337
Figure 6. 81 : Fedora.....	337
Figure 6. 82 : Putty Configuration	338
Figure 6. 83 : Router	338
Figure 6. 84 : Putty Configuration	339
Figure 6. 85 : Ubuntu	339
Figure 6. 86 : g7@fedora-group7-com:/home/g7	340
Figure 6. 87 : g7@fedora-group7-com:/home/g7	340
Figure 6. 88 : Local Security Policy	341
Figure 6. 89 : Windows Firewall with Advanced Security.....	341
Figure 6. 90 : Password Policy	342
Figure 6. 91 : Account Lockout Policy	342
Figure 6. 92 : Kerberos Policy	343
Figure 6. 93 : Login GUI	344
Figure 6. 94 : Change User	344
Figure 6. 95: Connect to group6 network	345
Figure 6. 96 : Enter the username and password	345
Figure 6. 97 Confirmation to connect	346
Figure 6. 98 : Connected to group7 network	346
Figure 6. 99 : Snort Running.....	347
Figure 6. 100 : Snort's Log file	347
Figure 6. 101 : Internet Connection	348
Figure 6. 102 : Control Panel.....	348
Figure 6. 103 : Network and Internet.....	349
Figure 6. 104 : Network and Sharing Centre	349
Figure 6. 105 : Set Up a Connection or Network.....	350
Figure 6. 106 : Connect to a Workplace	350
Figure 6. 107 : Connect to a Workplace	351
Figure 6. 108 : Connect to a Workplace	351
Figure 6. 109 : Pop-up window of WiFi.....	352
Figure 6. 110 : Windows Security	352
Figure 6. 111 : VPN Connection.....	353
Figure 6. 112 : Command Prompt.....	353
Figure 6. 113 : Run dialog box	354
Figure 6. 114 : Samba's files	354
Figure 6. 115 : Login box	355
Figure 6. 116 : New folder shown.....	355
Figure 6. 117 : Yap's file	356
Figure 6. 118 : SSH to fedora	356
Figure 6. 119 : Login box	357
Figure 6. 120 : Samba's file directory	357
Figure 6. 121: yap.txt.....	357
Figure 6. 122 : Testing the ports that have been configured.....	358

Figure 6. 123 : Summary of shutdown ports.....	358
Figure 6. 124 : Status of all port interface.....	359

CHAPTER 1 – INTRODUCTION

1.1 INTRODUCTION

The subject BITU 3923, Workshop II, is taken by BITC and BITZ students before graduation. This subject is the platform for students to train and prepare for their Industrial Training. The students are divided into group with 9 students, 6 students from BITC and 3 students from BITZ. This project requires the students to analyse, design, built, manage, maintain and test the network. It will also train students to work in group and solve the problems that arise together like the actual environment in industry which emphasize on being a good team player and critical thinker. We also provided with three servers, one network interface card, one router, one manageable switch, 15 meters long UTP cable, 12 RJ-45 connectors and one crimping tool set.

The students will use all the skills and knowledge that had learnt before in this subject. Besides, the students can learn and use new technologies and services that are required to build the network. Student need to setup the infrastructure for company XYZ that covers all networking functions for internal and external IT communications (router, DNS servers, file servers etc.), user management, port management, security, remote access to the network for telecommuters, and network monitoring.

We are required to design, set up, maintain and monitor a network environment for company XYZ with basic server applications and fundamental services. 15 network services and 12 security services are required to implement in the network infrastructure. Different Operating Systems are required to install in each servers such as Window server, Ubuntu server and also Fedora server.

1.2 OBJECTIVE

The following are the main objectives:

- i. To be able to maintain the network services which ensure all able to communicate each other all the time efficiently.
- ii. To ensure the security services is invulnerable to protect all the data on network-connected host.
- iii. To implement the security policies that cover four key elements, which are physical security, general security, network security and application security.

1.3 PROJECT PLAN

In week 1 all, the members- had attended workshop 2 speech to have a clear idea in what are we going to do for this project. Within week 1, all group members would have the first group meeting to discuss and prepare the final project proposal that includes the details of the project such as the executive summary, logical and physical network design. The design is to show the network topology, Gantt chart to show the timeline of the project and project distribution where the project manager will distribute the tasks to all the members. Last thing that we would do in the first week is meeting our supervisor so she can identify all group members and check our first draft proposal so we can modify it depending on her notes.

In week 2 we will submit the finalized proposal and we will take the needed equipment such as router, switch, UTP cable, networking interface card, etc. from the faculty to start implemented our project by crimping network cable, and connect it to the devices and install the needed operating system such as Ubuntu and Windows Server. From week 3 to week 5, we will set up the first 5 needed services for this project and preparing (progress report 1) that will consists of the details of the setup and installation of the services. Starting form Week 3 we prepare the report of setting up and installing DNS and DHCP. Within week 4 we aim to finish two more services which are (VLAN and VLSM

addressing) and active directory services. Within week 5, the last week to finish report progress one, we intend to done it with the last two services required on report 1, which are Server Virtualization and Samba. We will submit the finalized Progress Report I that has been approve by the end of week 5.

From week 6 to week 10, we plan to proceed to set up the 25 other services for achieve progress Report 2 requirements as follow. For week 6, will start doing the setting up for Routing & NAT, Web, SSL & Virtual Hosting, ACL, Samba, Linux Email Server, Secured FTP, and Radius Server for Network Accounting. For week 7, we intend to do Network Management System, Proxy Server, Security Hardening, Security Policy, Authentication using radius server (AAA), User authentication and authorization - different user. Server For week 8, we aim to set up Remote login using SSH, Harden Ubuntu Server, Harden Fedora Server, Harden Windows Server, Harden Web Server, Print Server, Authentication user by integrating AD with Linux.

For week 9, we aim to finish Installation IDS (port mirror), IPsec between server and user, Samba Security Services, Port Security and VLAN Security. In week 10, we aim to finish all 25 services (progress report 2) and submit it to our supervisor.

During week 11 to week 12, we will proceed towards completing the setup of the whole network and setup of all services required. At the same time, we will prepare a video and a poster that shows one of the services that has been set up. After the completion of the network, we will demonstrate our respective task individually to the supervisor and evaluator while the video and poster prepared will be present during the project demonstration for the purpose of updates for the final exhibition at week 14.

At week 13, the final report and individual logbook will be revised if there is any error and improve. At week 14, the video and poster

produced during week 11 to week 12 will be used in the video and poster exhibition. The completed video and poster will be evaluated by the supervisors and evaluator. The finalized final report and individual logbook will be submitted during study week, which is equivalent to week 15.

1.4 CONCLUSION

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

CHAPTER 2 - PROJECT REQUIREMENT

2.1 INTRODUCTION

For the workshop II, we have to define, implement and manage network services starts from selecting project manager to lead the project from beginning until the ends of task. Task has been given to implement network with 31 services. We have 14 services for network and 17 services for security. Each member will be implementing their services following the schedule to get the task done. We are being grateful to this task and make us prepared for industrial training and work. In this workshop II, we are using 3 different operating systems which are Windows Server 2012 R2, Linux (Ubuntu 16.04) and Linux (Fedora 28) for setup on the servers and virtual machines that provided by UTeM and personal laptop. All Linux operating system doesn't require any license as it provided as open source and able download through online.

2.2 TYPES OF OPERATING SYSTEM

In order to ensure the server are setup with proper operating system, we chosen the most recommended version of operating system which are Linux (Ubuntu 16.04 and Fedora) which is the most stable for server usage. All the recommendation and review each respective operating system are able to search through internet. In this workshop II, we used both Linux based operating system and Microsoft Windows based operating system. Each of operating system has their unique characteristics and configuration method.

2.3 OPERATING SYSTEM BACKGROUND

2.3.1 Windows Server 2012 R2

Windows server 2012 R2 is one of Microsoft server line of operating system. This software is intended for evaluation and deployment planning purposes only. It was released to manufacturing on August 1, 2012 and launched on September 4, 2012.

2.3.2 Linux Ubuntu 16.04

Although Ubuntu itself is primarily a desktop Linux distribution, the brand also includes one of the most powerful free server distributions around. Ubuntu Server boasts a fast and frequent update cycle and comes bundled with a useful and diverse set of package groups. The best feature in Ubuntu is that it features a unified package repository for all its different versions, which makes it such a formidable choice. We decided to use Ubuntu 14.04 LTS which is older version but it able to support 32-bit and greater stability instead of Ubuntu Server 16.04.1 LTS which is latest version and support guaranteed until April 2021 but only can support on 64-bit.

2.3.3 Linux Fedora 28

Fedora is a Linux distribution developed by the community-supported Fedora Project and sponsored by Red Hat. Fedora contains software distributed under various free and open-source licenses and aims to be on the leading edge of such technologies. Fedora is the upstream source of the commercial Red Hat Enterprise Linux distribution. Fedora has a reputation for focusing on innovation, integrating new technologies early on and working closely with upstream Linux communities. Making changes upstream instead of specifically for Fedora ensures the changes are available to all Linux distributions. We decide to use Fedora 28 which is the most stable and latest version of Fedora with less bugs. Fedora 28 was released on 1 May 2018.

2.4 OPERATING SYSTEM JUSTIFICATION

2.4.1 Window Server 2012 R2

We decided to use Windows Server 2012 R2 because it provides organizations with the ability to deliver rich Web-based experiences efficiently and effectively. It also provides valuable new functionality and powerful improvements to the operating system. Moreover, Windows Server 2012 supplies all the features and tools provided by the standard edition that contains full-function server operating system. It automatically comes with most of the technical, security, management and administrative features such as the rewritten networking stack (native IPv6, native wireless, and speed and security improvements).

2.4.2 Linux Ubuntu 16.04

We have chosen Ubuntu 16.04, because it is the latest Ubuntu 16.04 version which is stable and minimize risk compared to Ubuntu 14.04 which has many bugs until now. Ubuntu 16.04 comes with new requirement which is hardware recognition and it can automatically detect our pc screen resolution, soundcard and others devices. Ubuntu is always free for anyone to use, modify, and distribute. It is built by people across the globe who works together as a community for the Ubuntu Project.

2.4.3 Linux Fedora 28

We will be using Ubuntu 28 for this project. Fedora is an operating system based on the Linux kernel, developed by the community-supported Fedora Project and sponsored by Red Hat. Fedora contains software distributed under a free and open-source license and aims to be on the leading edge of such technologies. This server is reliable and powerful OS for the computer network.

2.5 HARDWARE REQUIREMENT

Component	Requirement
Processor	Intel® Xeon® CPU E5-2650 v3@2.30 GHz
Memory	<ul style="list-style-type: none"> • 12 GB • Recommended: 6 GB (for Windows Server 2012) and 12 GB (for Windows Server 2012 R2 standard)
Available Disk Space	<ul style="list-style-type: none"> • Minimum: 12 GB • Recommended: 32 GB or greater
Drive	DVD-ROM drive
Display and Peripherals	<ul style="list-style-type: none"> • Higher-resolution monitor • Keyboard • Microsoft Mouse or compatible pointing device • No pen or Touch input is available

Table 1 : Hardware requirement windows 2012

Components	Requirement
Processor	Intel® Celeron® CPUB815@ 1.60 GHz
Memory	2 GB
Operating System	Ubuntu 16.04 LTS 64-bit (Linux)
Hard Drive	25GB
Graphic	Intel® Haswell Desktop
Drive	Light Scribe DVD RW

Table 2 : Hardware requirement Ubuntu 16.04

Components	Requirement
Processor	Minimum: 1GHz <u>Recommended:</u> faster
Memory	1.5 GB
Disk Space	Minimum: 20GB Recommended: 20GB or greater
Drive	CD and DVD drive

Table 3 : Hardware requirement Fedora

2.6 HARDWARE JUSTIFICATION

1. Servers

- ✓ Three servers will be installing with Windows Server 2008 Standard Edition, Linux Ubuntu 14.04 and Linux Fedora 24.
- ✓ In Window Server we have installed DNS, DHCP, IPv6 Web, Web, SSL & Virtual Hosting, Radius Server, Active Directory, Hardening, IPsec, network accounting, SSH, ACL..
- ✓ For Linux Ubuntu we have installed Linux Email Server, Network Management System (NMS), Proxy server, AD with Linux, hardening, IDS and port mirror.
- ✓ For Linux Fedora, we have installed Samba, Samba Security, hardening, Network Management System, Secure FTP.

2. NIC - NICs provide computers with a connection to the network, but they also handle an important data-conversion function.

- ✓ Network interface cards also have the ability of supplying a basic addressing system that can be used to get data from one computer to another on the network.
- ✓ Each NIC will be used for each server and will be able to provide network communication capabilities to and from a computer.

3. UTP Cable

- ✓ We are given about 15 meters long UTP cable for the entire project. □ Unshielded Twisted Pair (UTP) is a type of cable that can transmit voice or data signals that's way we choose to use this cable in our project. RJ-45 Connector
- ✓ The standard connector used for the UTP cable - RJ45 is the connection for the cable, we use from switch to other client computer to make connection over internet once cable are plugged in switch.

4. Switch

- ✓ The switch is used to connect all the three servers and the client.
- ✓ Also use to connect Computer to Internet.

5. Router

- ✓ To set IP address and to make connection between servers and client.
- ✓ To route your information to server. Other configuration routing we set at each server in router to make connection that we need.

2.7 CONCLUSION

As the conclusion, before installing Operating System, one should ensure that the computer meet the requirements. It is complicated for us to integrate three different types of Operating System with at least 20 different in a network infrastructure. We have to consider the demand of the operating system and decide which the best to implement is that we set to each server. Besides, we also have to state and research about the hardware requirements to make sure coincidentally of network. We have to make sure those requirements are suitable and afford to support our services for each server before we installed it. Perfect setting can make strength connection over internet.

CHAPTER 3 – DESIGN

3.1 INTRODUCTION

In this workshop II, we have to design, define, implement and manage network services. Every group need to implement own network design, in which needed to be applied in real device. Stated in the requirements, we need to design the network that include three different servers, one CISCO router, one CISCO switch and a client host for the design. We have supplied with RJ-45, UTP cable, console cable and a set of crimping tools. Furthermore, we were required to use different operating system to set the network environment. The operating system we chose was Windows Server 2012, Fedora 28 and Ubuntu 16.04.

3.2 SECURITY POLICY

3.2.1 Router and Switch Policy

Router and switch must be configured according following standards:

1. No local user accounts are configured on the router. Routers and switches must use TACACS+ for all user authentication.
2. The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device's support organization.
3. The following services or features must be disabled for security purposes by our technician:
 - a. IP directed broadcasts.
 - b. Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses.

- c. TCP small services.
 - d. UDP small services.
 - e. All source routing and switching.
 - f. All web services running on router
 - g. Cisco discovery protocol on Internet connected interfaces.
 - h. Telnet, FTP, and HTTP services.
 - i. Auto-configuration
4. The following services should be disabled by technician unless justification is provided by any employee:
- a. Cisco discovery protocol and other discovery protocols
 - b. Dynamic trunking
 - c. Scripting environments, such as the TCL shell
5. The following services must be configured:
- a. Password-encryption
 - b. NTP configured to a corporate standard source
6. All routing updates shall be done using secure routing updates.
7. Use corporate standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.
8. Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.
9. Access control lists for transiting the device are to be added as business needs arise.
10. The router must be included in the corporate enterprise management system with a designated point of contact.

11. Each router must have the following statement presented for all forms of login whether remote or local:

"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.

You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."

12. 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.
13. Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.
14. 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:
 - a. IP access list accounting
 - b. Device logging
 - c. Incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped
 - d. Router console and modem access must be restricted by additional security controls

3.2.2 Wireless Communication Policy

1. General Requirements

All wireless infrastructure devices that reside at a Group 7 site and connect to a Group 7 network, or provide access to information classified as Group 7 Confidential, or above must:

- Abide by the standards specified in the Wireless Communication Standard.
- Be installed, supported, and maintained by an approved support team.
- Use Group 7 approved authentication protocols and infrastructure.
- Use Group 7 approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Not interfere with wireless access deployments maintained by other support organizations.

3.2.3 Password Protection Policy

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

1. Password Creation

1.1 All user-level and system-level passwords must conform to the Password Construction Guidelines.

1.2 Users must not use the same password for Group 7 accounts as for other non-Group 7 access (for example, personal ISP account, option trading, benefits, and so on).

1.3 Where possible, users must not use the same password for various Group 7 access needs.

1.4 User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges.

1.5 Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to log in interactively. SNMP community strings must meet password construction guidelines.

2. Password change

2.1 All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis.

2.2 All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every four months.

2.3 Password cracking or guessing may be performed on a periodic or random basis by the Infosec Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to follow the Password Construction Guidelines.

3. Password protection

- 3.1. Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential Group 7 information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.
- 3.2. Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication.
- 3.3. Passwords must not be revealed over the phone to anyone.
- 3.4. Do not reveal a password on questionnaires or security forms.
- 3.5. Do not hint at the format of a password (for example, “my family name”).
- 3.6. Do not share Group 7 passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
- 3.7. Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- 3.8. Do not use the “Remember Password” feature of applications (for example, web browsers).
- 3.9. Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

3.2.4 Ipv6 web policy

Ipv6 is configured by our technician for various purposes and implemented in our company, such as:

1. SEND (Secure Neighborhood Discovery) must be configured because it can enable cryptographic confirmation that a host is who it claims to be at connection time.
2. End-to-end encryption.
3. Supported by all compatible device and system.

3.2.5 Remote Access Policy

It is the responsibility of Group 7 employees, contractors, vendors and agents with remote access privileges to Group 7's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Group 7.

General access to the Internet for recreational use through the Group 7 network is strictly limited to Group 7 employees, contractors, vendors and agents (hereafter referred to as "Authorized Users"). When accessing the Group 7 network from a personal computer, Authorized Users are responsible for preventing access to any Group 7 computer resources or data by non-Authorized Users. Performance of illegal activities through the Group 7 network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access. For further information and definitions, see the Acceptable Use Policy.

Authorized Users will not use Group 7 networks to access the Internet for outside business interests.

For additional information regarding Group 7's remote access connection options, including how to obtain a remote access login, free anti-virus software, troubleshooting, etc., go to the Remote Access Services website (company URL).

- Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases. For further information see the Acceptable Encryption Policy and the Password Policy.
- Authorized Users shall protect their login and password, even from family members.
- While using a Group 7-owned computer to remotely connect to Group 7's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, except for personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.
- Use of external resources to conduct Group 7 business must be approved in advance by InfoSec and the appropriate business unit manager.
- All hosts that are connected to Group 7 internal networks via remote access technologies must use the most up-to-date anti-virus software (place URL to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the Third-Party Agreement.
- Personal equipment used to connect to Group 7's networks must meet the requirements of Group 7-owned equipment for remote access as stated in the Hardware and Software Configuration Standards for Remote Access to Group 7 Networks.

3.2.6 Remote Access Tools Policy

All remote access tools used to communicate between Group 7 assets and other systems must comply with the following policy requirements.

Remote Access Tools Group 7 provides mechanisms to collaborate between internal users, with external partners, and from non-Group 7 systems. Because proper configuration is important for secure use of these tools, mandatory configuration procedures are provided for each of the approved tools. The approved software list may change at any time, but the following requirements will be used for selecting approved products.

- All remote access tools or systems that allow communication to Group 7 resources from the Internet or external partner systems must require multi-factor authentication. Examples include authentication tokens and smart cards that require an additional PIN or password.
- The authentication database source must be Active Directory or LDAP, and the authentication protocol must involve a challenge-response protocol that is not susceptible to replay attacks. The remote access tool must mutually authenticate both ends of the session.
- Remote access tools must support the Group 7 application layer proxy rather than direct connections through the perimeter firewall(s).
- Remote access tools must support strong, end-to-end encryption of the remote access communication channels as specified in the Group 7 network encryption protocols policy.
- All Group 7 antivirus, data loss prevention, and other security systems must not be disabled, interfered with, or circumvented in any way.

3.2.7 Samba Policy

Samba as a medium for different operating system to communicate with each other. Samba connections need to be configured by technician as below to follow security measures:

1. Perimeter firewall, configuration of the host server that is running Samba, and Samba itself.
2. Implements the latest protocol to permit more MS Window file and print operations.
3. Setting Access Control Entries (ACEs) in an Access Control List on the share themselves.
4. Configure host-based protection.

3.2.8 Email Server Policy

- All use of email must be consistent with Group 7 policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
- Group 7 email account should be used primarily for Group 7 business related purposes; personal communication is permitted on a limited basis, but non-company related commercial uses are prohibited.
- All Group 7 data contained within an email message or an attachment must be secured according to the Data Protection Standard.
- Email should be retained only if it qualifies as a Group 7 business record. Email is a Group 7 business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.

- Email that is identified as a Group 7 business record shall be retained according to Group 7 Record Retention Schedule.
- The Group 7 email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any Group 7 employee should report the matter to their supervisor immediately.
- Users are prohibited from automatically forwarding Group 7 email to a third-party email system (noted in 4.8 below). Individual messages which are forwarded by the user must not contain Group 7 confidential or above information.
- Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct Group 7 business, to create or memorialize any binding transactions, or to store or retain email on behalf of Group 7. Such communications and transactions should be conducted through proper channels using Group 7-approved documentation.
- Using a reasonable amount of Group 7 resources for personal emails is acceptable, but non-work-related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a Group 7 email account is prohibited.
- Group 7 employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.
- Group 7 may monitor messages without prior notice. Group 7 is not obliged to monitor email messages.

3.2.9 Acceptable Use Policy

1. General Use and Ownership

- Group 7 proprietary information stored on electronic and computing devices whether owned or leased by Group 7, the employee or a third party, remains the sole property of Group 7. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard.
- You have a responsibility to promptly report the theft, loss or unauthorized disclosure of Group 7 proprietary information.
- You may access, use or share Group 7 proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
- For security and network maintenance purposes, authorized individuals within Group 7 may monitor equipment, systems and network traffic at any time, per Infosec's Audit Policy.

- Group 7 reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

2. Security and Proprietary Information

- All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy.
- System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
- All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.
- Postings by employees from a Group 7 email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Group 7, unless posting is in the course of business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware

3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions while their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Group 7 authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Group 7-owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

1. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Group 7.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Group 7 or the end user does not have an active license is strictly prohibited.
3. Accessing data, a server or an account for any purpose other than conducting Group 7 business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate

management should be consulted prior to export of any material that is in question.

5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using a Group 7 computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any Group 7 account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior notification to Infosec is made.
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

13. Circumventing user authentication or security of any host, network or account.
14. Introducing honeypots, honeynets, or similar technology on the company's network.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
17. Providing information about, or lists of, Group 7 employees to parties outside Group 7.

2. Email and Communications Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Group 7's networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Group 7 or connected via Group 7's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

3. Blogging and Social Media

1. Blogging by employees, whether using Group 7's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Group 7's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Group 7's policy, is not detrimental to Group 7's best interests, and does not interfere with an employee's regular work duties. Blogging from Group 7's systems are also subject to monitoring.
2. Group 7's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any company confidential or proprietary information, trade secrets or any other material covered by Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of <Company Name> and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing

comments when blogging or otherwise engaging in any conduct prohibited by <Company Name>'s Non-Discrimination and Anti-Harassment policy.

3. Employees may also not attribute personal statements, opinions or beliefs to Group 7 when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Group 7. Employees assume any and all risk associated with blogging.
4. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Group 7's trademarks, logos and any other Group 7 intellectual property may also not be used in connection with any blogging activity Group 7's Confidential Information policy when engaged in blogging.

3.2.10 Clean Desk

1. Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
2. Computer workstations must be locked when workspace is unoccupied.
3. Computer workstations must be shut completely down at the end of the work day.
4. Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
5. File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.

6. Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
7. Laptops must be either locked with a locking cable or locked away in a drawer.
8. Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
9. Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
10. Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
11. Whiteboards containing Restricted and/or Sensitive information should be erased.
12. Lock away portable computing devices such as laptops and tablets.
13. Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer.
14. All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

3.7 PHYSICAL DESIGN

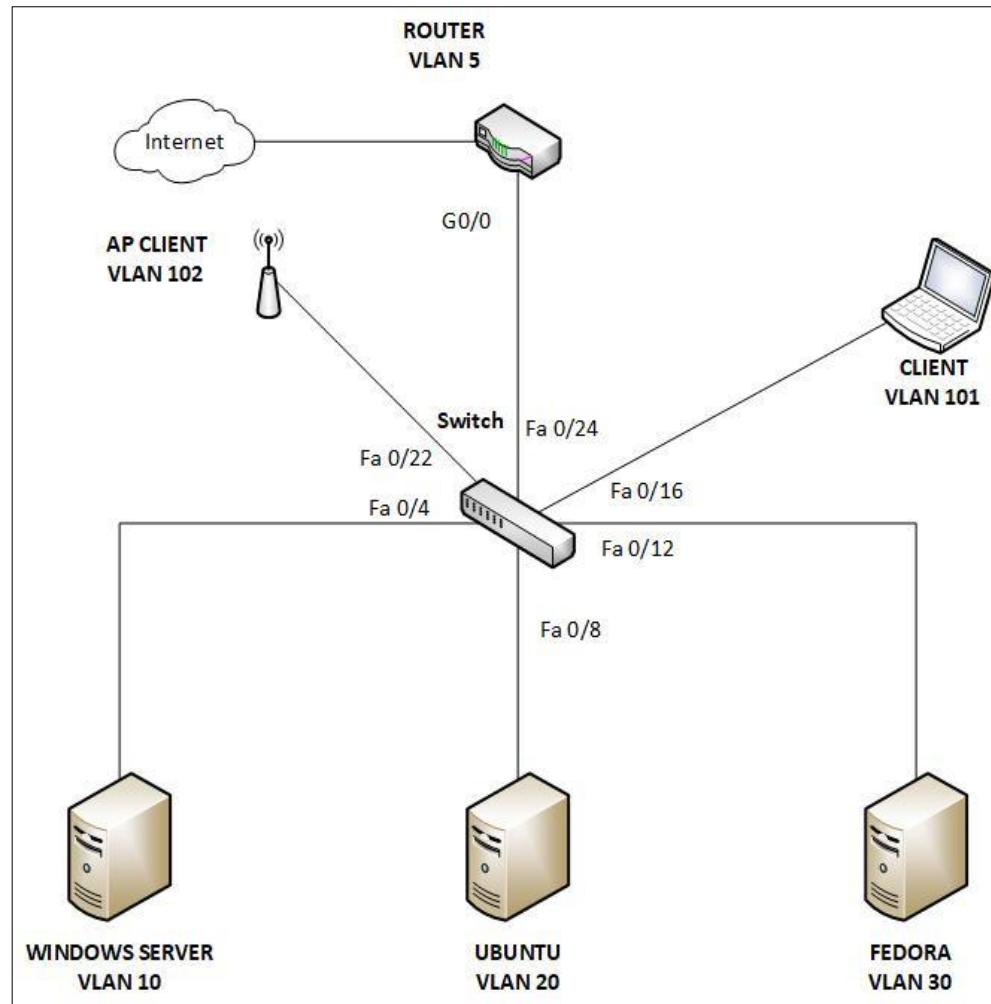


Figure 3. 1 : Physical design

3.8 LOGICAL DESIGN

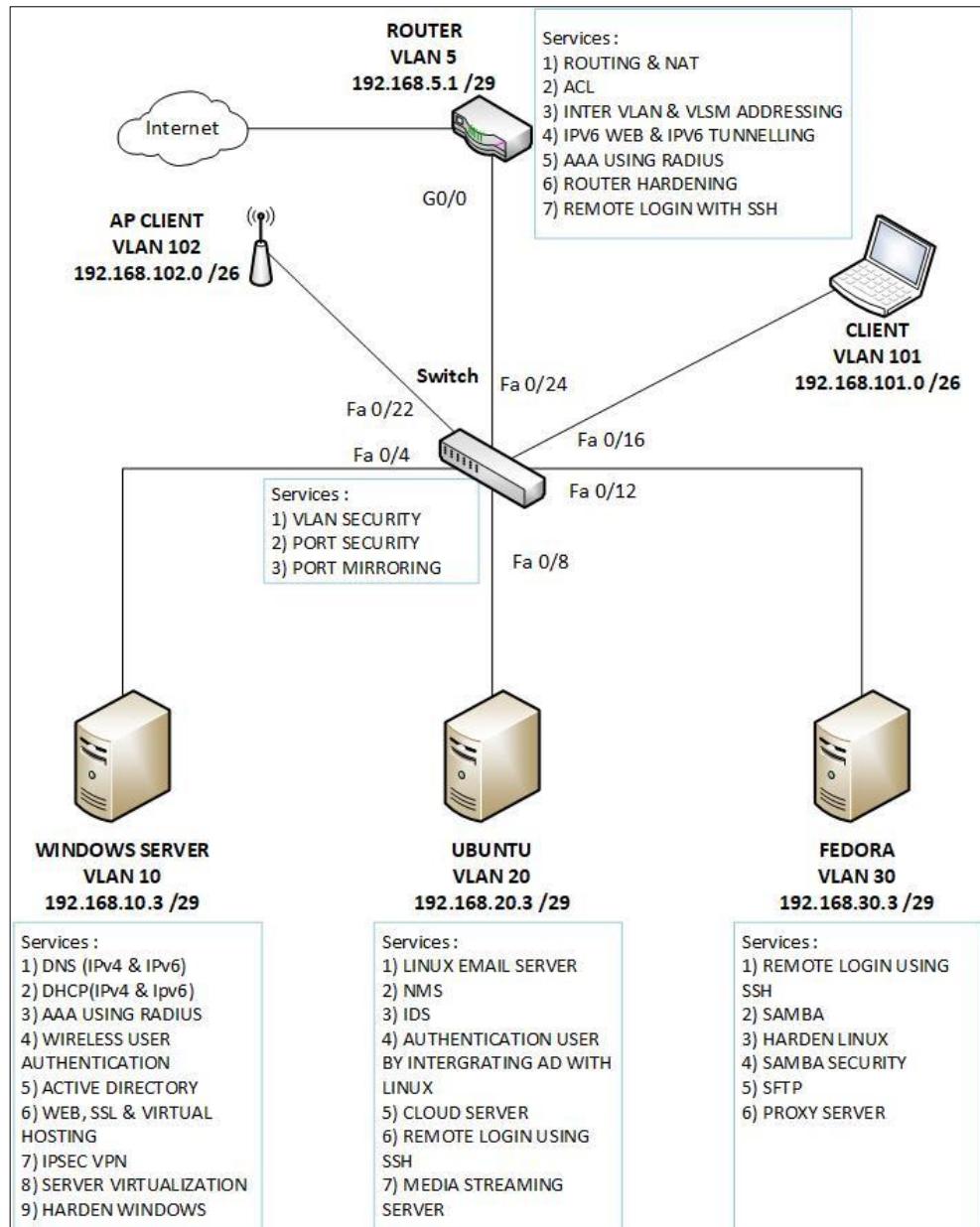


Figure 3. 2 : Logical design

3.9 CONCLUSION

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

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

CHAPTER 4 – SERVICES

4.1 INTRODUCTION

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

4.2 LIST OF SERVICES

4.2.1 Services for BITC Students

1. DNS (IPv4 & IPv6)
2. DHCP (IPv4)
3. DHCP (IPv6)
4. Inter VLAN and VLSM addressing
5. Routing & NAT
6. Active Directory
7. Proxy Server
8. Samba
9. Network Management System
10. Server Virtualization
11. AAA (Authentication, Authorization, and Accounting) using Radius
12. Access Control List (ACL)
13. Secured FTP; with authentication and encryption
14. Web, SSL & Virtual Hosting
15. Linux Email Server
16. IPv6 Web with IPv6 Tunneling
17. Media streaming server
18. Cloud server

4.2.2 Services for BITZ Students

1. Security Policy
2. Router hardening
3. Remote login using SSH
4. Linux server1 hardening
5. Windows server hardening
6. Authentication user by integrating AD with Linux
7. Wireless user authentication using Radius server (AD user account/Mac Address)
8. IDS with port mirror
9. IPsec VPN for remote employees
10. Samba security services; with minimum of 3 security features
11. Port Security
12. VLAN security

4.3 BRIEF OVERVIEW FOR SERVICES

4.3.1 Domain Name System (DNS)

DNS is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember “handle” for an Internet address. DNS are the Internet’s equivalent of a phone book. . We use the DNS to maintain a directory names and translate into our IP address. This is necessary because, although domain names are easy for people to remember, computers or machines, access websites based on IP addresses. The secondary DNS server was created at a second DNS provider to provide redundancy in the DNS network.

The secondary (slave) DNS server is an authoritative server that obtains information about a zone from the primary server via zone transfer. (RFC 2182) The secondary DNS server is slave to the primary server. By adding a second DNS provider, we have two separate DNS networks running

simultaneously. These two networks provide backup for each other and for users in the event one network is offline or has degraded performance.

4.3.2 Dynamic Host Configuration Protocol (DHCP)

DHCP (Dynamic Host Configuration Protocol) was the solution for IT department to set each desktop computer IP address, subnet mask, default gateway, DNS servers, and other network settings manually. If you'll try to perform this task manually you're probably going to waste a lot of time on sitting on each computer 5-10 minutes, beside time, you can for example accidentally enter wrong IP address to few clients, or to type the same IP address to few clients too. DHCP allows you to manage the networks IP addresses scopes and other TCP/IP settings like DNS, Default Gateway, etc. from central place, this central place called DHCP server. It provides reliable IP address configuration and reduced network administration for clients to access the network. DHCP assigns a local IP address to device connected to the local network from DHCP address pool. Network clients will be configured automatically by the DHCP service. Besides, any modification to the IP address of the router and DNS servers can be implemented easily.

4.3.3 Dynamic Host Configuration Protocol version 6 (DHCPv6)

The Dynamic Host Configuration Protocol version 6 (DHCPv6) is a network protocol for configuring Internet Protocol version 6(IPv6) hosts with IP addresses, IP prefixes and other configuration data required to operate in an IPv6 network. It is the IPv6 equivalent of the Dynamic Host Configuration Protocol for IPv4. IPv6 hosts may automatically generate IP addresses internally using stateless address auto configuration (SLAAC), or they may be assigned configuration data with DHCPv6. IPv6 hosts that use stateless auto configuration may require information other than an IP address or route. DHCPv6 can be used to acquire this information, even though it is not being used to configure IP addresses. DHCPv6 is not necessary for configuring hosts with the addresses of Domain Name System (DNS) servers, because

they can be configured using Neighbor Discovery Protocol, which is also the mechanism for stateless auto configuration

4.3.4 Virtual LAN (VLAN)

VLAN is used as segmentation of the network, segmentation also have an advantages that we implement to the network such as security. VLAN make the network more secure and more confidentiality. Besides that, VLAN also make the management of network more easy because of the segmentation. Others than that, we also implement VLAN because of adaptability in change of network requirements and relocate our workstation and server nodes in the network

4.3.5 Routing and Network Address Translation (NAT)

Routing is the process of selecting paths in a network along which to send network traffic. Routing directs packet forwarding, the transit of logically addressed packets from their source toward their ultimate destination through intermediate nodes. Therefore, we use Open Shortest Path First (OSPF) as our routing protocol. OSPF calculate the shortest route to a destination through the network based on an algorithm. Furthermore, it also supports the logical grouping of network segments into areas. So, it will suitable to use for our network topology. Besides that, it uses less bandwidth since transmission take place only when routing changes occur. Other than that, we use Network Address Translation (NAT) protocol to improve security by reusing IP addresses. The NAT router translates traffic coming into and leaving the private network. The main use of NAT in our network is to limit the number of public IP addresses and for the security purpose is the act of translating our address from one to another within the packet. The local inside network addresses maps to one or more global outside IP addresses and un-maps the global IP addresses on incoming packets back into local IP addresses. This helps ensure security since each outgoing or incoming request must go through a translation process that also offers the

opportunity to qualify or authenticate the request or match it to a previous request. Moreover, NAT allows network clients with private IP to communicate with public network such as the internet.

4.3.6 Active Directory

Active Directory (AD) is a Windows OS directory service that facilitates working with interconnected, complex and different network resources in a unified manner. Active Directory was initially released with Windows 2012 Server and revised with additional features in Windows Server 2012. Active Directory provides a common interface for organizing and maintaining information related to resources connected to a variety of network directories. The directories may be systems-based (like Windows OS), application-specific or network resources, like printers. Active Directory 38 serves as a single data store for quick data access to all users and controls access for users based on the directory's security policy.

4.3.7 Proxy Server

A proxy server is computer that functions as an intermediary between a web browser and the Internet. Proxy servers help improve web performance by storing a copy of frequently used webpages. Whenever the client connects to a web proxy server and makes a request for the resources that reside on a remote server, the proxy server forwards this requests to the target server on behalf of the client, to fetch the requested resource and deliver it back to the client. An example of client can be a user operated computer that is connected to the Internet. Proxy server can control employee internet usage because when network is accessed through a proxy, network administrator control which devices have access to the network and which site those device can visit.

4.3.8 Samba

Samba is a free software re-implementation that support Server Message Block (SMB) and Common Internet File System (CIFS) protocols used by Microsoft Operating System. Samba used to access shared files, printers, and serial ports between Microsoft Operating System with Linux Operating System. Samba provides file transfer services for Microsoft Windows clients and can integrate with a Microsoft Windows Server domain either as a Domain Controller (DC) or as a domain member. Samba act similar as File Transfer Protocol (FTP) but the amaze of Samba is Client and Server can simply communicate between them without need any authorization. This is because why Samba need to be more secured in terms of inter Networking.

4.3.9 Network Management System (NMS)

Network management system that we implement because of Network Management System is software that allow us to monitoring the network on performance, functional and troubleshoot. After that, Network Management System also allow us to check the integrity of the network in real-time monitoring. This help us to keep update about the network status and services that has been installed.

4.3.10 Server Virtualisation

Server Virtualization is the masking of server resources. From one physical server, we can create many virtual server inside it. The physical server act as server administrator uses a virtual server to divide one physical server into multiple virtual environments. In server virtualization, each virtual server runs multiple operating system instances at the same time. If one of the physical server in disaster immediately, server virtualization act as recovery. Server virtualization used to make more efficient use of server resource and to centralize server administration.

4.3.11 AAA (Authentication, Authorization, and Accounting) using Radius

The AAA server typically interacts with network access and gateway servers and with databases and directories containing user information. We need to use AAA using radius server because it is controlling who has access to a device, controlling what people can do when they've been granted access, and tracking their behaviour throughout the session. Since most devices are still managed via the CLI or a GUI, AAA remains an important tool to control device access. RADIUS is the abbreviation for Remote Authentication Dial-In Service. Initially, RADIUS was used to authenticate dial-in access to remote users. It is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use network service. It is a client/server protocol that runs in the application layer, using UDP as a transport medium. The RADIUS server can support a variety of methods to authenticate a user. When it is provided with the username and original password given by the user, it can support PPP, PAP or CHAP, UNIX login, and other authentication mechanisms. The RADIUS server works in a way that when a user tries to authenticate, the device sends a message to the RADIUS server. If the RADIUS server is configured to have the device as a client, RADIUS sends an “accept” or “reject” message back to the device.

The accounting function in RADIUS allows data to be sent at start and end of the sessions, showing the amount of resources (such as time, packets, bytes) used during the session. An Internet Service Provider may use RADIUS access control and accounting software to meet special security, billing needs, statistical purposes and general network monitoring. Transactions between the client and RADIUS server are authenticated using a shared secret, which is never sent over the network. In addition, user passwords are sent encrypted between the client and RADIUS server to eliminate the possibility that someone snooping on an insecure network could determine a user's password. The user environment on virtual and physical

level is kept in the working condition and out of use from unwanted people and threats.

4.3.12 Access Control List (ACL)

An access control list (ACL) is a table that tells a computer operating system which access rights each user has a system object, such as a file directory or individual file. Each object has a security attribute that identifies its access control list. The list has an entry for each system user with access privileges. The most common privileges include the ability to read a file (or all the files in a directory), to write to the file or files, and to execute the file (if it is an executable file, or program).

4.3.13 Secure FTP

Secured File Transfer Protocol (SFTP) is a secured version of File Transfer Protocol (FTP), we implement SFTP on our network because between the network can share or transfer any file to other workstation. Other than that, it also secure because of the encryption of the files contain and the confidentiality

4.3.14 Web, SSL and Virtual Hosting

SSL stands for Secure Sockets Layer. It is a standard security technology for forming an encrypted connection between a server and a client. It is commonly used in a web server and browser. SSL is security protocol that allows confidential information (credit card numbers, login credentials) to be transmitted securely. All browsers can interact with secured browsers using SSL protocol; however, the browser and server need a SSL Certificate to establish a secure connection. SSL Certificate has a pair of public and private key that work together to establish an encrypted connection. Virtual hosting is when a single server or a pool of server hosts multiple domain names. Virtual hosting allows one server to share its

resources without requiring all services provided to use the same host name. These types of virtual hosting are; name based, IP based and port based. Name- based virtual hosting uses the host name presented by the client. This saves IP addresses and the associated administrative overhead but the protocol being served must

4.3.15 Linux Email Server

We use email server to send and receive email. The mail service on any mail server has three components which is Mail user agent (MUA) is a component that the user sees and interacts with like Thunderbird and Microsoft Outlook, these user agents are responsible for reading mail and allowing you to compose mail. Mail transport agent (MTA) is a component is responsible for getting the mail from one site to another like Sendmail and Postfix. Mail delivery agent (MDA) is a component is responsible for distributing received messages on the local machine to the appropriate user mailbox like postfix-maildrop and Procmail. To setup Linux email server we need to install dovecot, postfix, apache2 and RainLoop. We use RainLoop as our email server in Linux. RainLoop is an open source, simple modern and fast web based email client.

4.3.16 IPv6 Web with IPv6 Tunneling

IPv6 tunneling is IP tunnels for sending IP packets over IP packets. We use to tunnel IPv6 web with others organization to allow them access our IPv6 web. We need determine our IPv6 address by convert the IPv4 address to hexadecimal in IPv6 form. Then, the most important things in do IPv6 tunneling are to change the tunnel mood to ipv6ip, the tunnel source which is our organization and tunnel destination is others organization. We create our tunnel interface in router and set public ip address for our organization.

4.3.17 Media Streaming Server

We use media streaming server to stream media file in local and also remote network. We use Plex as our media streaming server in Linux server. Plex is an open source. Plex is a client-server media player system and software suite comprising two main components. The Plex Media Server desktop application runs on Windows, macOS and Linux-compatibles including some types of NAS devices. The server desktop application organizes video, audio and photos from a user's collections and from online services, enabling the players to access and stream the media files from server.

4.3.18 Cloud Server

We use cloud server to create virtual server (rather than a physical server) running in a cloud computing environment. It is built, hosted and delivered via a cloud computing platform via the internet, and can be accessed remotely. We use Nextcloud as our cloud server. Nextcloud is an open source, self-hosted file share and communication platform. Access and synchronize your files, contacts, calendars & communicate and collaborate across your devices. Nextcloud also can use in smartphone. There have application for mobile phone to synchronize the file with other device that we have such as laptop and computer. Therefore, our group can access our cloud server account anywhere and anytime.

4.3.19 Security Policy

Security policy is a definition of what it means to be secure for a system, organization or other entity. For an organization, it addresses the constraints on behaviour of its members as well as constraints imposed on adversaries by mechanisms such as doors, locks, keys and walls. For systems, the security policy addresses constraints on functions and flow among them,

constraints on access by external systems and adversaries including programs and access to data by people.

If it is important to be secure, then it is important to be sure all the security policy is enforced by mechanisms that are strong enough. There are many organized methodologies and risk assessment strategies to assure completeness of security policies and assure that they are completely enforced. In complex systems, such as information systems, policies can be decomposed into sub-policies to facilitate the allocation of security mechanisms to enforce sub-policies. However, this practice has pitfalls. It is too easy to simply go directly to the sub-policies, which are essentially the rules of operation and dispense with the top-level policy. That gives the false sense that the rules of operation address some overall definition of security when they do not. Because it is so difficult to think clearly with completeness about security, rules of operation stated as "sub-policies" with no "super-policy" usually turn out to be rambling rules that fail to enforce anything with completeness. Consequently, a top-level security policy is essential to any serious security scheme and sub-policies and rules of operation are meaningless without it.

4.3.20 Router Hardening

Hardening a router means that the router is secured against attacks as best as possible. There are five types of hardening that being used in this project. First, enable the login banner. By enabling the login banner, it will inform unauthorized user that an offence of unauthorized access can only be committed if the offender knew at the access he/she intended to obtain was unauthorized. Secondly, disable log to console or monitor sessions. It is always advised to send logging information to the local log buffer, which can be view with the show logging command rather than to send log messages to monitor and console session. Next, enable configuration change notification and logging. Enabling configuration is to send notification of configuration changes to the software system logging (syslog) process. It allow the tracking of configuration changes enters by users on a per-session and per-user basis.

This tool allows administrator to track any configuration change made to the software running configuration and identify the user that made that change. Other than that, I had set at putty configuration panel to allow to save log files of putty sessions for debugging, analysis or future reference. Lastly, disable DNS lookup. This function only useful if the router utilizes a DNS server on the network. When an erroneous URL is typed, the DNS lookup will attempt to find the URL on the DNS server, if no DNS available, the user's computer will hang while the lookup is performed. To decrease user delays if no DNS server is configured, disable the DNS lookup function on the Cisco router.

4.3.21 Remote login using SSH

SSH, short Secure Shell is a UNIX-based command interface and protocol for getting secured access to a remote computer. Used to remotely control Web and other types of servers. SSH commands are encrypted and secure. The connection between the client and server is authenticated by using a digital certificate. The passwords are encrypted.

4.3.22 Linux server hardening and Windows server hardening

Server hardening is the process of improving of the server security through various means that comes up with a more secure server as a result. Hardened servers are more resistant to security issues and threats. Server hardening is very important to protect the server from security attacks. There are several common servers hardening tips:

- Using Data Encryption for communication.
- Avoid from using unsecure protocols that send information or password in plain text.
- Make sure that the operating system is kept up-to-date especially security patches.
- Use strong passwords for user accounts.
- Change passwords regularly and avoid reusing passwords.

- Lock accounts after too many login failures.
- Disable unnecessary services.
- Configure a proper firewall.
- Install Log watch to review emails daily for any suspicious activity on server.
- Maintain appropriate backups.
- Physical security of the server must be taken into consideration.

Windows Hardening is a configuration where all changes made into Windows Server R2 2012 will be logged and accounted for. Hardening process also will identify any unused port and services using NMAP and close it for security purposes.

4.3.23 Authentication user by integrating AD with Linux

Active Directory 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 computers. Any user from any department can login into company's network even though from Linux's based OS rather Windows OS only.

4.3.24 Wireless user authentication using Radius server

A user using wireless connection with authentication method: 802.1X with radius server. When connecting to network, it will ask the username and password which created by admin. Admin will assign whether a login according the Active Directory. The RADIUS server can support a variety of methods to authenticate a user. When it is provided with the username and original password given by the user, it can support PPP, PAP or CHAP, UNIX login, and other authentication mechanisms. Typically, a user login consists of a query (Access-Request) from the NAS to the RADIUS server and a corresponding response (Access-Accept or Access-Reject) from the

server. The Access-Request packet contains the username, encrypted password, NAS IP address, and port. In RADIUS, authentication and authorization are coupled together. If the username is found and the password is correct, the RADIUS server returns an Access-Accept response, including a list of attribute-value pairs that describe the parameters to be used for this session.

4.3.25 IDS with port mirror

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. Intrusion detection is a service that monitors all the packet flow from and to the server by help of port mirroring. IDS will log any packet flow whether suspicious websites, blacklisted IP, backdoor planted in client's PC and any attempt on password cracking techniques such as brute force. If any breach detected, IDS's logs will be reviewed first.

4.3.26 IPsec VPN for remote employees

Internet Protocol Security (IPsec) is a protocol suite for secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec can be used in protecting data flows between a pair of security gateways (network-to-network). IPsec includes a server and clients to communicate securely by using key phrase that only server and client know the key. Client will use the public IP to connect to other network without involving Internet. Username and password will be used to log into the network that has been set at Server. When client gets access to network, they can control the other network from their network.

4.3.27 Samba security services

Microsoft Windows networking uses a protocol that was originally called the Server Message Block (SMB) protocol. Each department will be

given a group in Linux server so that each user in the department has their own file sharing and group only sharing folder. Only assigned group can access to the specified folder and department's printer.

4.3.28 Port Security

Port security is a layer two traffic control feature on Cisco Catalyst switches. It enables an administrator configure individual switch ports to allow only a specified number of source MAC addresses increasing the port. We use port security with dynamically learned and static MAC addresses to restrict a port's ingress traffic by limiting the MAC addresses that can send traffic into the port. When you assign secure MAC addresses to a secure port, the port does not forward ingress traffic that has source addresses outside the group of defined addresses. If you limit the number of secure MAC addresses to one and assign a single secure MAC address, the device attached to that port has the full bandwidth of the port.

4.3.29 VLAN security

VLAN security is a configuration made for unused port that is not being assigned. These port are being group under Vlan 60 and be named as unused port. The used of these security is so that others network could not connect with these port and cause traffic network towards the network that had been made. Its secure the port for future.

4.4 CONCLUSION

Each services have their own function, service also have different types of software or packages to be installed on the server. Service can be simple but it can be very important such as NTP that only set the time and it have helped many network administrators to the exact time a server is down or have an error. Some service can integrate to work with other service making the servers work efficiently.

CHAPTER 5 - INSTALLATION AND CONFIGURATION

5.1 INTRODUCTION

All of 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. The configuration is to ensure the functioning of the service are successfully installed and configure.

5.2 SERVICES INSTALLATION AND INDIVIDUAL WHO RESPONSIBLE FOR THE TESTING

Task	Week	Date	Person in charge
Proposal	1,2	14/9/2018	All members
Install Operating System	3	17/9/2018	All members
Active Directory		24/9/2018	Abdulrahman
DNS	4	25/9/2018	Firdaus
DHCP IPv4		26/9/2018	Khairunnisa
INTER VLAN		27/9/2018	Jabbar
DHCP IPv6		28/9/2018	Yugendrah
Server Virtualization		1/10/2018	Syahidah
Service for Video		2/10/2018	All members
Integrate User With Linux	5	3/10/2018	Fahmy
Samba		4/10/2018	Syahidah
Samba Security		5/10/2018	Fahmy
Secured FTP		8/10/2018	Jabbar
Cloud Server		9/10/2018	Firdaus
Linux Email Server	6	10/10/2018	Yugendrah
Proxy Server		11/10/2018	Khairunnisa
Port security		12/10/2018	Syazwani
Vlan Security		15/10/2018	Syazwani

Remote login using SSH	7	16/10/2018	Raihan
Web, SSL & Virtual Hosting		17/10/2018	Abdulrahman
IDS (port mirror)		18/10/2018	Fahmy
Media streaming server		19/10/2018	Yugendrah

5.2.1 DNS (Domain Name Server (IPv4 & IPv6))

Primary DNS - Forward Lookup Zones (IPv4)

Step 1: Double click at Internet Protocol Version 2 (TCP/IPv4) to setup the IP address.

- IP address: 192.168.10.3
- Subnet mask: 255.255.255.248
- Default gateway: 192.168.10.1
- Preferred DNS server: 192.168.10.3

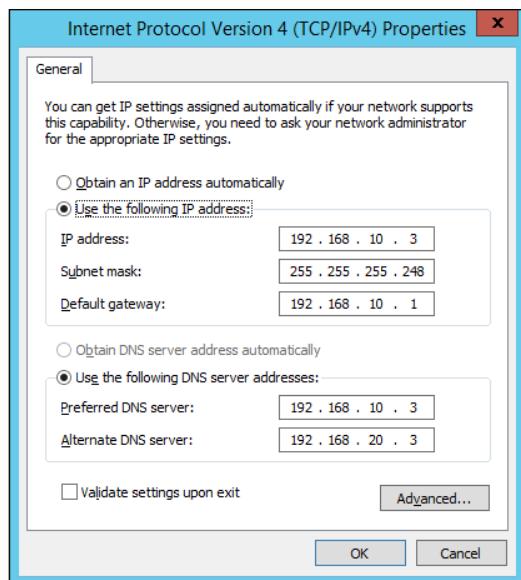


Figure 5. 1: Put correct IP address

Step 2: To create the forward lookup zone and click next to proceed.



Figure 5. 2: DNS Server Wizard

Step 3: Select the primary zone.

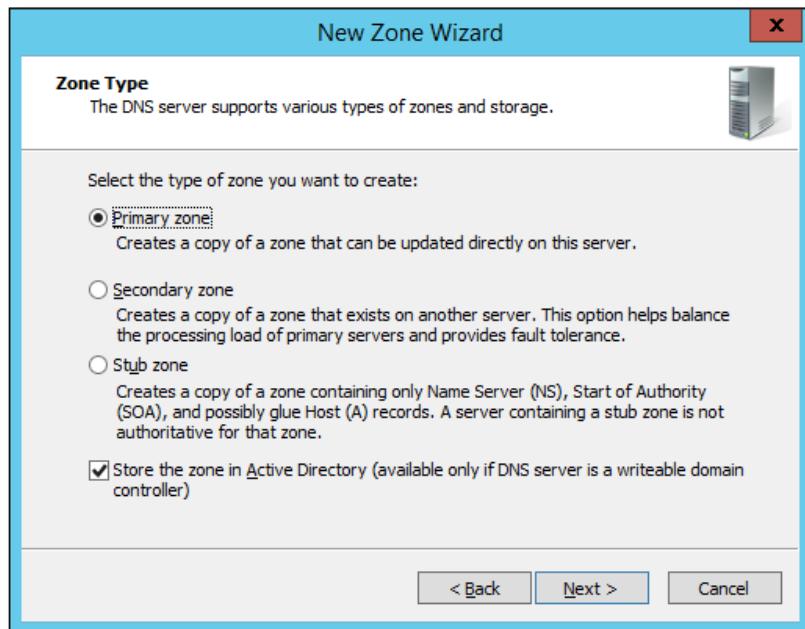


Figure 5. 3: Select Zone Type

Directory. Then click button Next>

The DNS Server service provides for three types of zones:

- Primary zone
- Secondary zone
- Stub zone

We choose primary zone because a primary zone is the only zone type that can be edited or updated because the data in the zone is the original source of the data for all domains in the zone. Updates made to the primary zone are made by the DNS server that is authoritative for the specific primary zone. Users can also back up data from a primary zone to a secondary zone.

A zone contains the resource records for all the names within the particular zone. Zone files are used if DNS data is not integrated with Active Directory. The zone files contain the DNS database resource records that define the zone. If DNS and Active Directory are integrated, then DNS data is stored in Active Directory.

When a zone that this DNS server hosts is a primary zone, the DNS server is the primary source for information about this zone, and it stores the master

copy of zone data in a local file or in ADDS. When the zone is stored in a file, by default the primary zone file is named group7.dns and it is in the %windir%\System32\DNS folder on the server.

We tick store the zone in Active Directory because DNS server running on domain controllers can store their zones in Active Directory Domain Services.

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

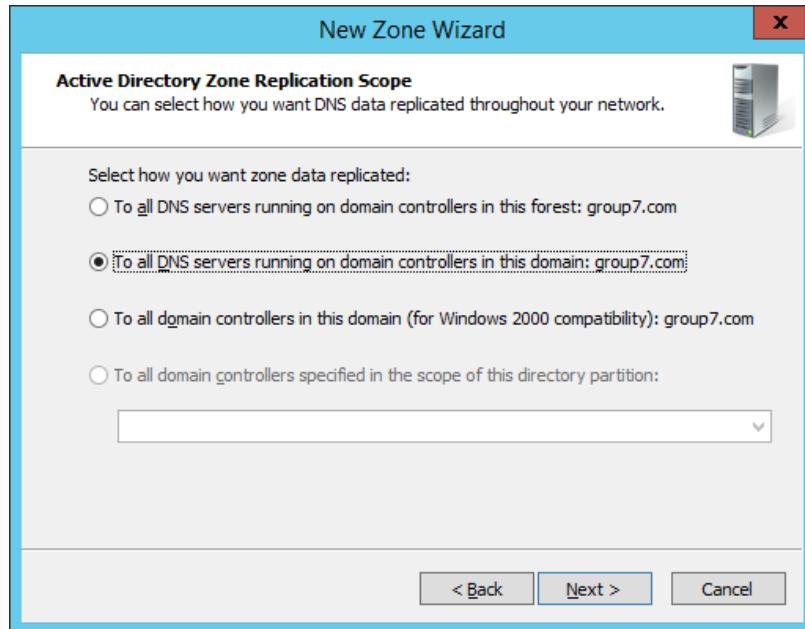


Figure 5. 4: Select Active Directory Zone Replication Scope

Step 5: In Zone Name window enter the Group 7's Zone name: group7.com

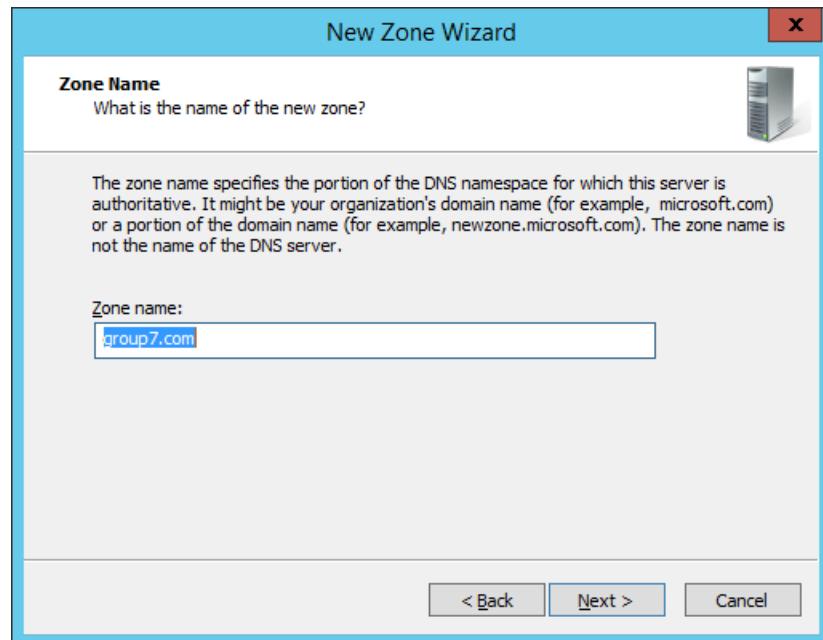


Figure 5. 5: Zone Name

Step 6: Select the type of dynamic updates you want to allow and click next.

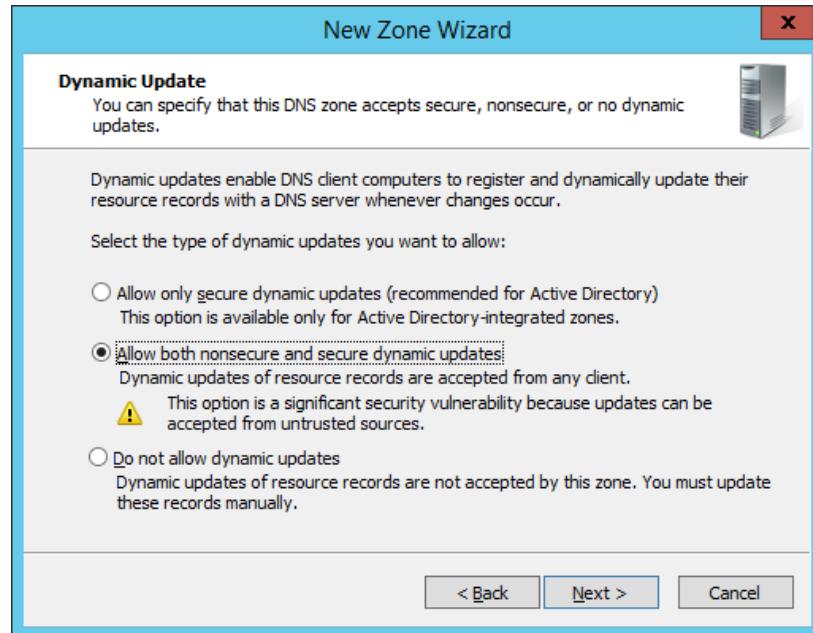


Figure 5. 6: Dynamic Update

The next screen (as shown below) will ask if dynamic updates should be allowed. For a non-Active Directory integrated zone the only two options are insecure/secure updates or none. From a security perspective it makes sense

to disable this functionality without AD. Choose an option and select Next. We choose this to on automatically the updates.

- **Secure only** – When this type of dynamic update is selected, only the computers that are members of the DNS domain can register themselves with the DNS server. The DNS server automatically rejects the requests from the computers that do not belong to the domain. This protects the DNS server from getting automatically populated with records of unwanted, suspicious and/or fake computers.
- **Nonsecure and Secure** – When this type of dynamic update is selected, any computer can send registration request to the DNS server. The DNS server in return automatically adds the record of the requesting computer in the DNS database, even if the computer does not belong to the same DNS domain. Although this configuration remarkably reduces administrative overhead, this 58 setting is not recommended for the organizations that have highly sensitive information available in the computers.
- **None** – When this option is selected, the DNS server does not accept any registration request from any computers whatsoever. In such cases, DNS administrators must manually add the IP addresses and the Fully Qualified Domain Names (FQDNs) of the client computers to the DNS database.

Step 7: In Configure a DNS Server Wizard click Next > to proceed

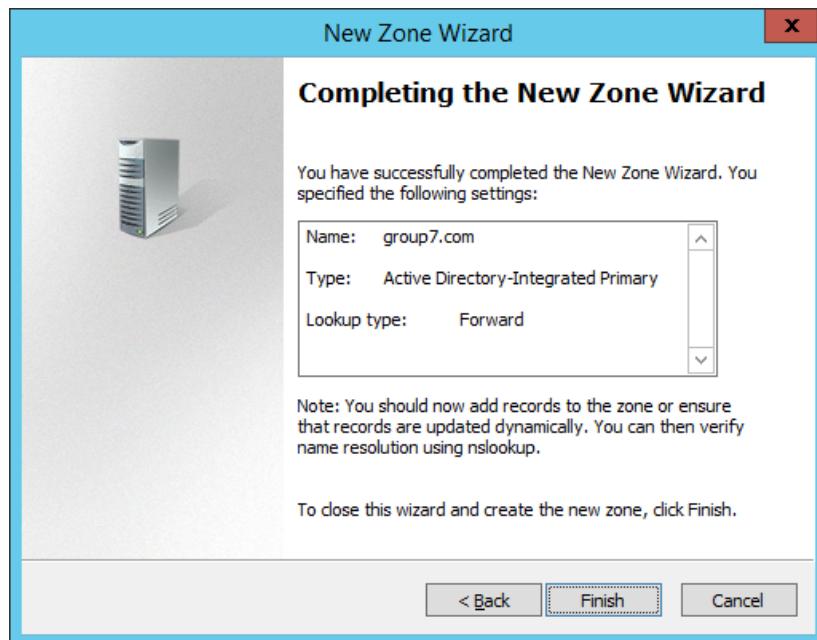


Figure 5. 7: DNS Server Wizard

Reverse Lookup Zones (IPv4)

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

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

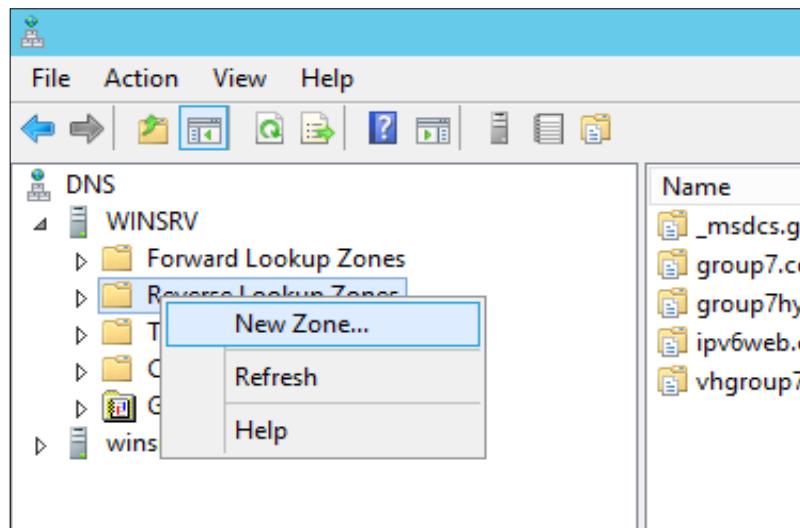


Figure 5. 8: New Zone (Reverse Lookup Zone)

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



Figure 5. 9: DNS Server Wizard

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

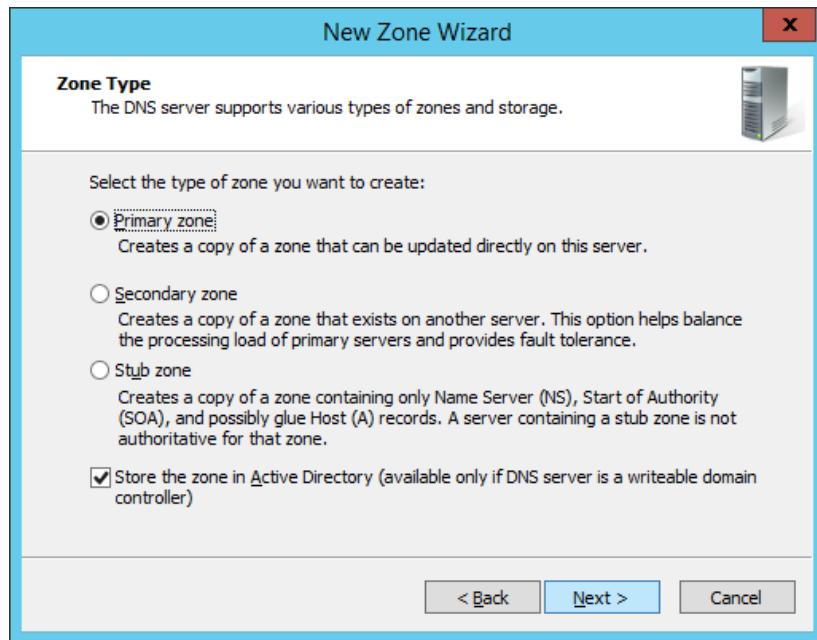


Figure 5. 10: Zone type

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

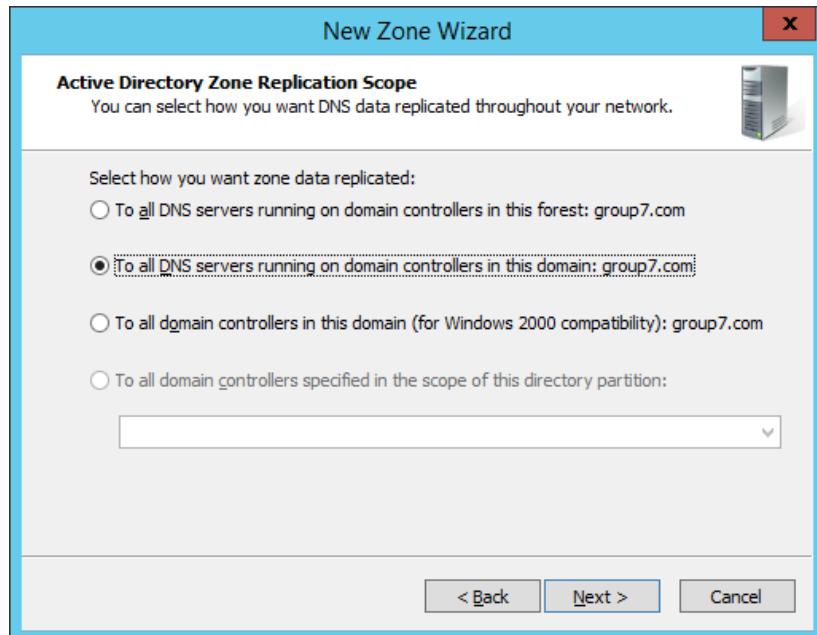


Figure 5. 11: Zone replication

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

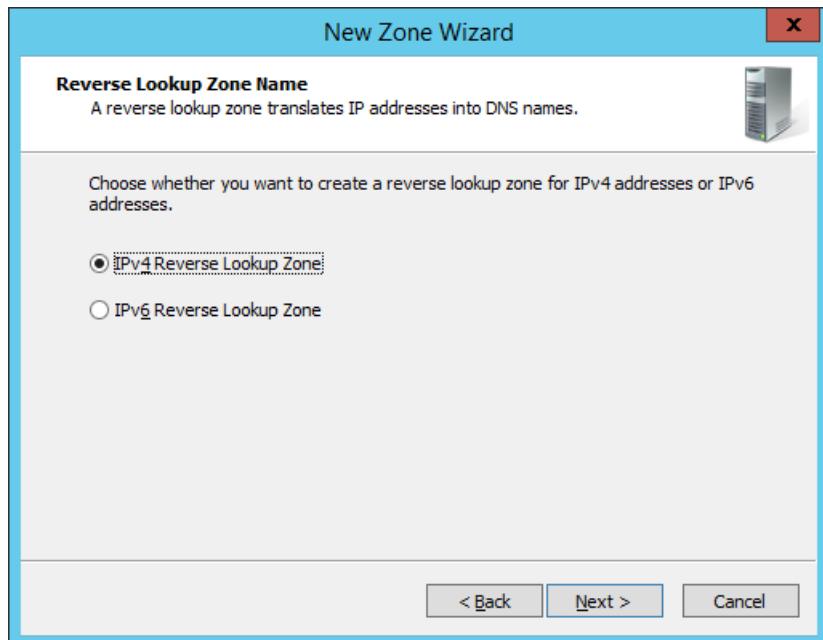


Figure 5. 12 : Select IPv4 Reverse Lookup Zone Name (IPv4)

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

When you create an IPv4 reverse lookup zone using the DNS Manager, the New Zone Wizard prompts you for a network ID, it is the portion of the IP address range for which the reverse lookup zone is responsible. For example, if the reverse lookup zone covers all addresses that begin with 192 (that is, 192.0.0.0 to 192.255.255.255), you enter 192.

To cover only those addresses in the subnet with an address in the range of 192.168.10.0 to 192.168.10.255, we enter 192.168.10. The wizard then constructs the reverse lookup zone name by reversing the order of the digit blocks and appending the result to the “root” domain name. For example, if we enter 192.168.10 in the wizard, the resulting name of the reverse lookup zone is 10.168.192.in-addr.arpa.

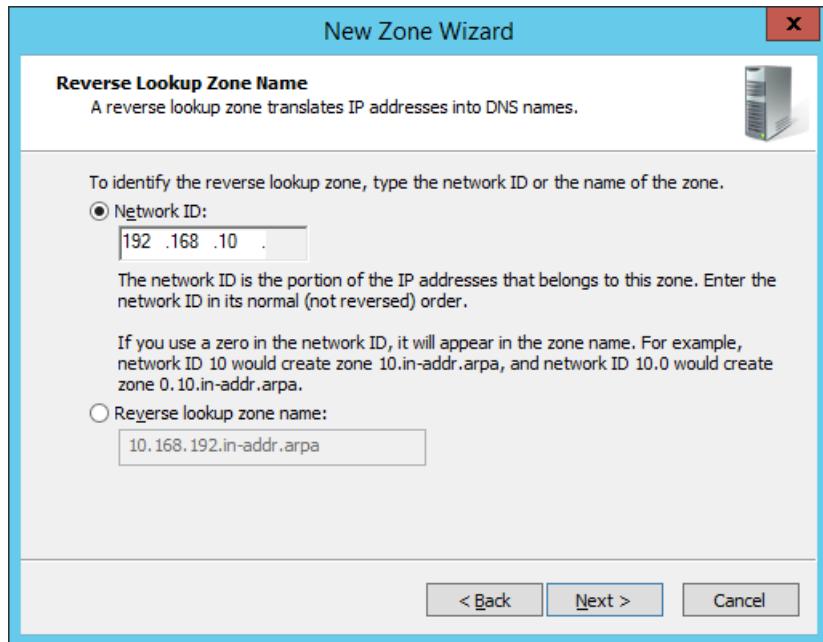


Figure 5. 13: Reverse Lookup Zone Name

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

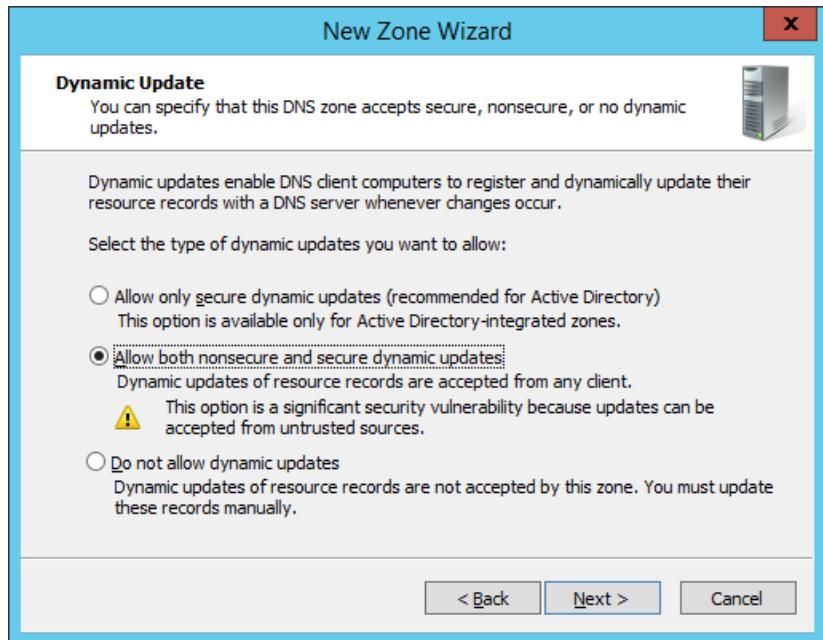


Figure 5. 14: Dynamic Update

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

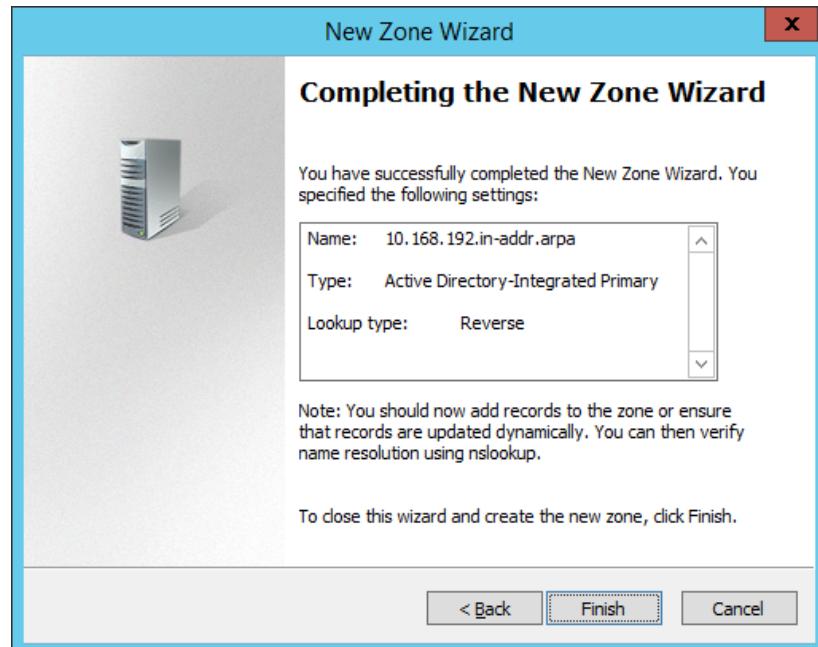


Figure 5. 15: Completing the New Zone Wizard

Step 9: Next, right click on IPv6 in Reverse Lookup Zones and click New Pointer (PTR).

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

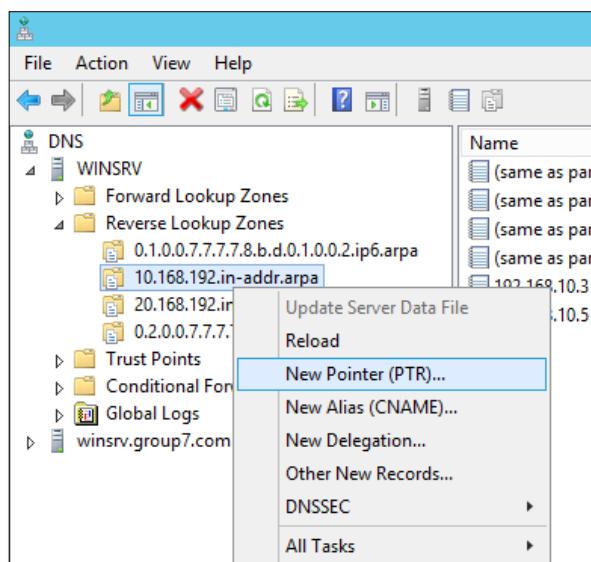


Figure 5. 16: Pointer (PTR)

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

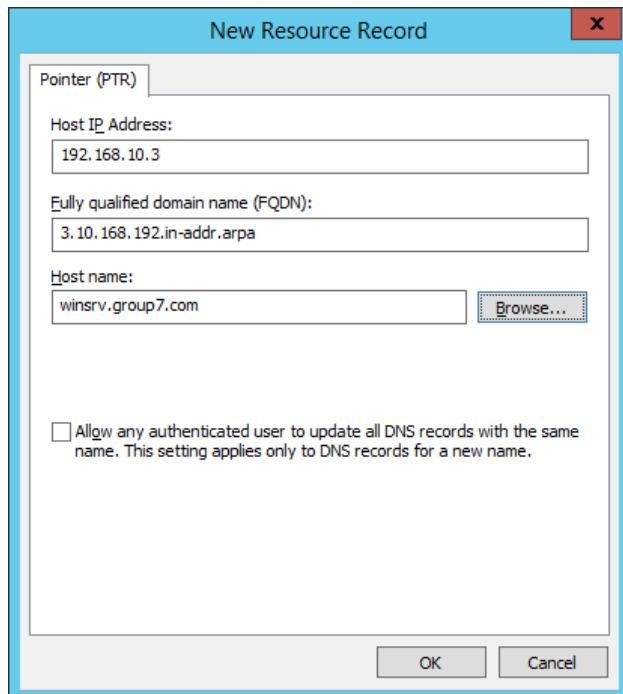


Figure 5. 17: Enter the Host IP Address

Step 11: Click on winsrv.group7.com and right click then click on New Host (A or AAAA). An A and AAAA record are primary DNS records. They associate a domain name with a specific IP address, so that when a user types in a web address, such as "winsrv.group7.com" their browser knows where to go for the actual website. The difference between A and AAAA is this: A is IPv4 and AAAA is the current IPv6 record.

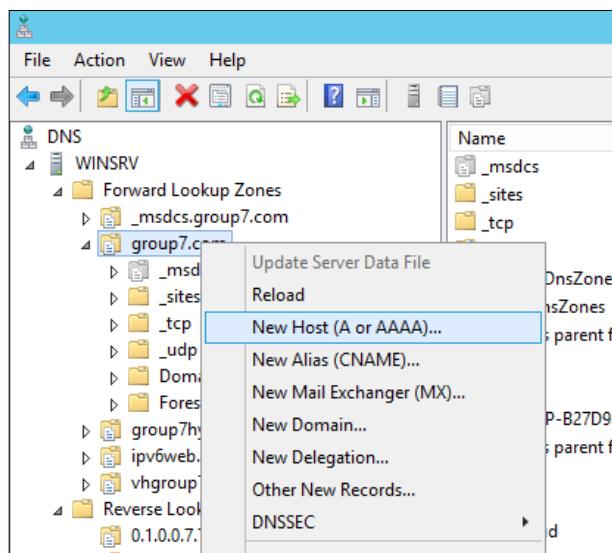


Figure 5. 18: New Host (A or AAAA)

Step 12: Enter the Name winsrv and IP address 192.168.10.3. Then click Add Host.

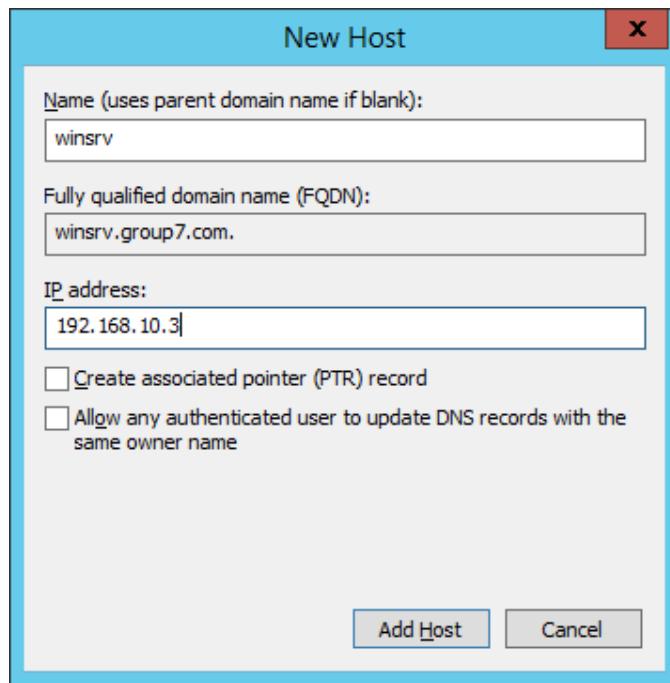


Figure 5. 19: New Host IPv4

Primary DNS - Forward Lookup Zones (IPv6)

Step 1: Double click at Internet Protocol Version 6 (TCP/IPv6) to setup the IP address.

- IP address : 2001:db8:7777:10::3
- Subnet prefix length: 64
- Default gateway : 2001:db8:7777:10::1
- Preferred DNS server : 2001:db8:7777:10::3, 2001:db8:7777:20::3

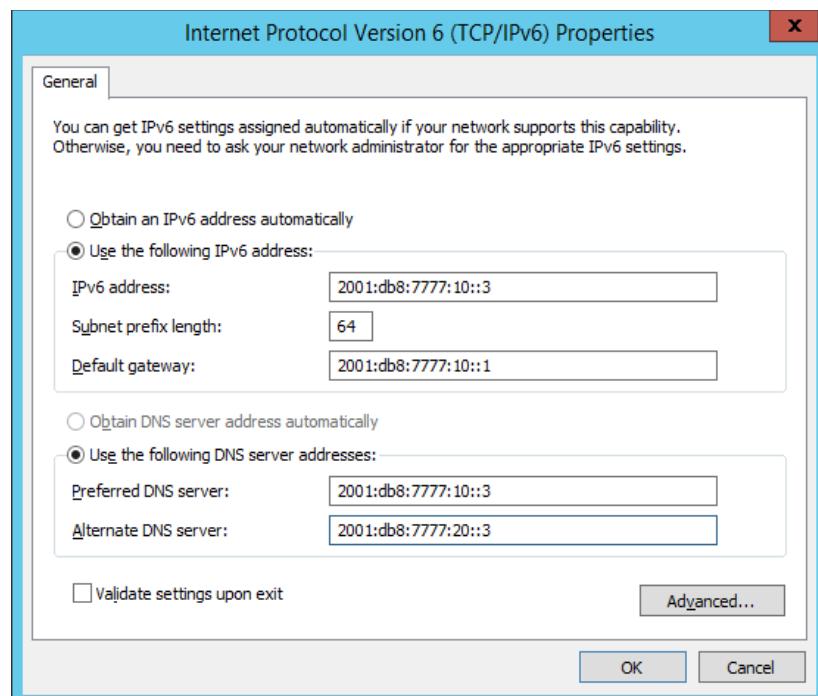


Figure 5. 20: Put correct IP address, Subnet Mask, Default Gateway and Preferred DNS Server

Step 2: Right click on Reverse Lookup Zones and click New Zone.

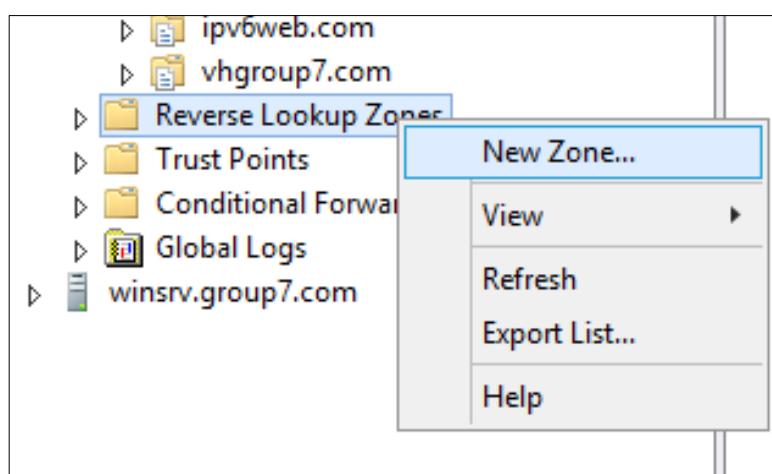


Figure 5. 21: New Zone

Step 3: In Welcome to New Wizard click Next>

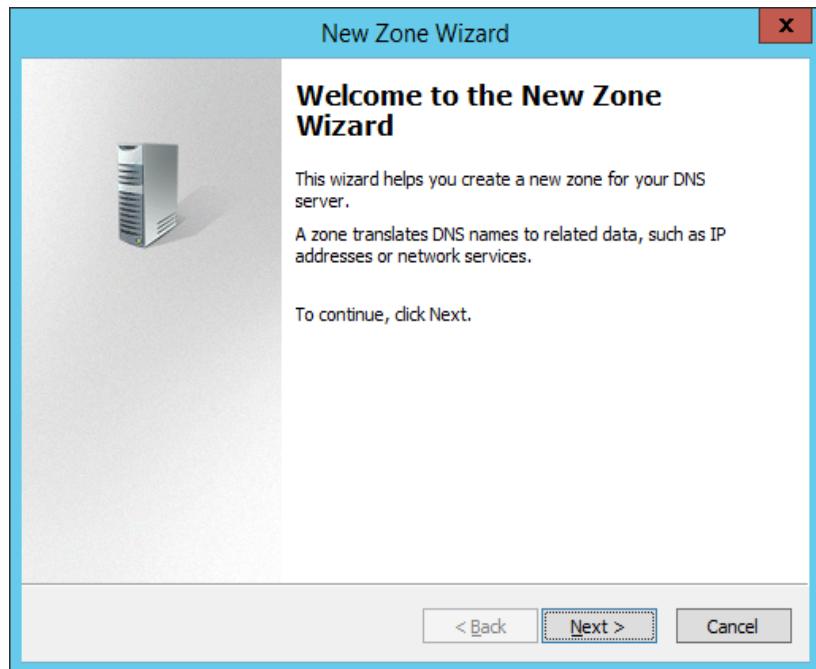


Figure 5. 22: Welcome the New Zone Wizard

Step 4: Then choose Primary zone. Tick on Store the zone in active AD. Then click next.

We tick store the zone in Active Directory because DNS server running on domain controllers can store their zones in Active Directory Domain Services.

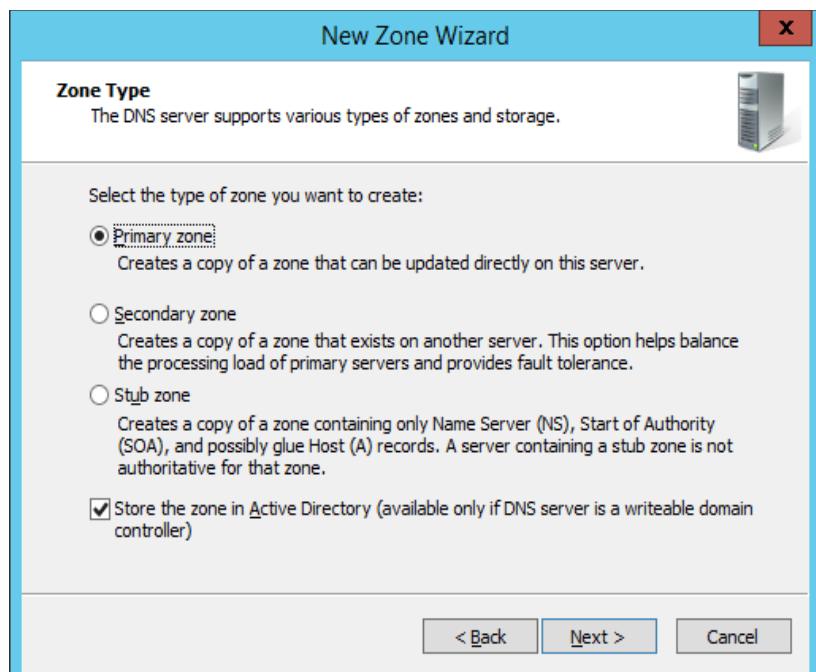


Figure 5. 23: Zone Type

Step 5: Select how we want the zone to replicate and click Next.

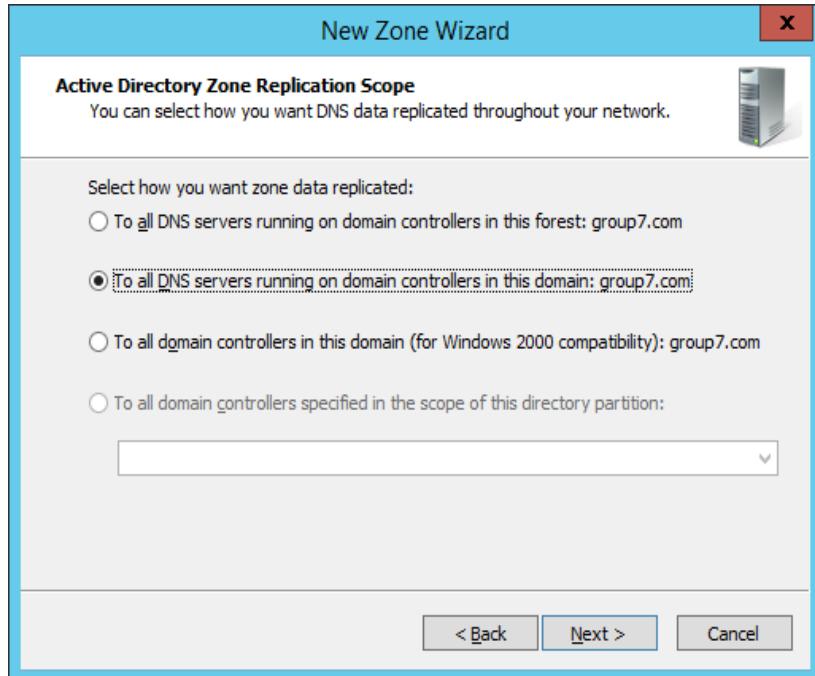


Figure 5. 24: Zone Type

Step 6: Next, choose IPv6 Reverse Lookup Zone.

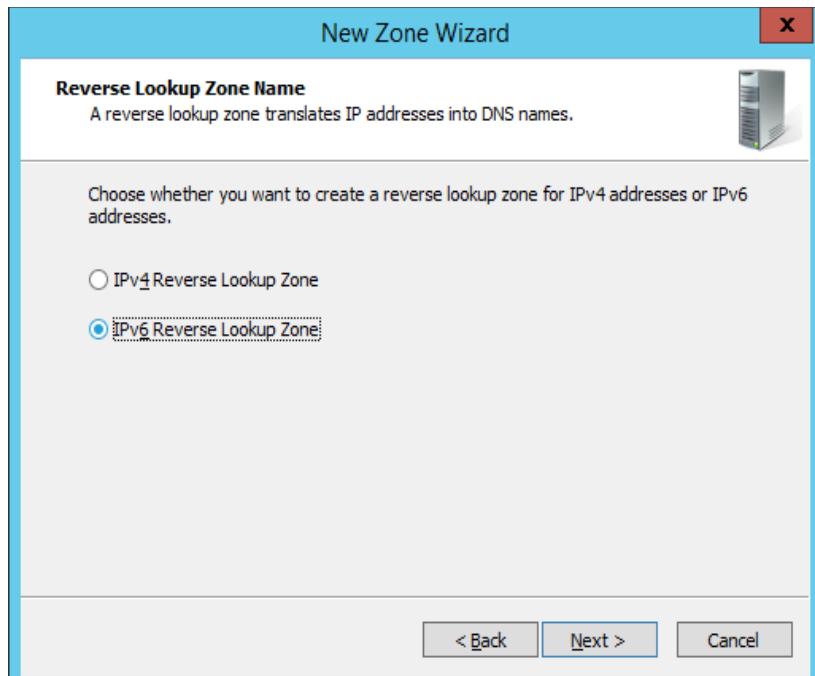


Figure 5. 25: IPv6 Reverse Lookup Zone

Step 7: In IPv6 Address Prefix, we enter 2001:db8:7777:10::/64 and Reverse Lookup Zones will automatically create.

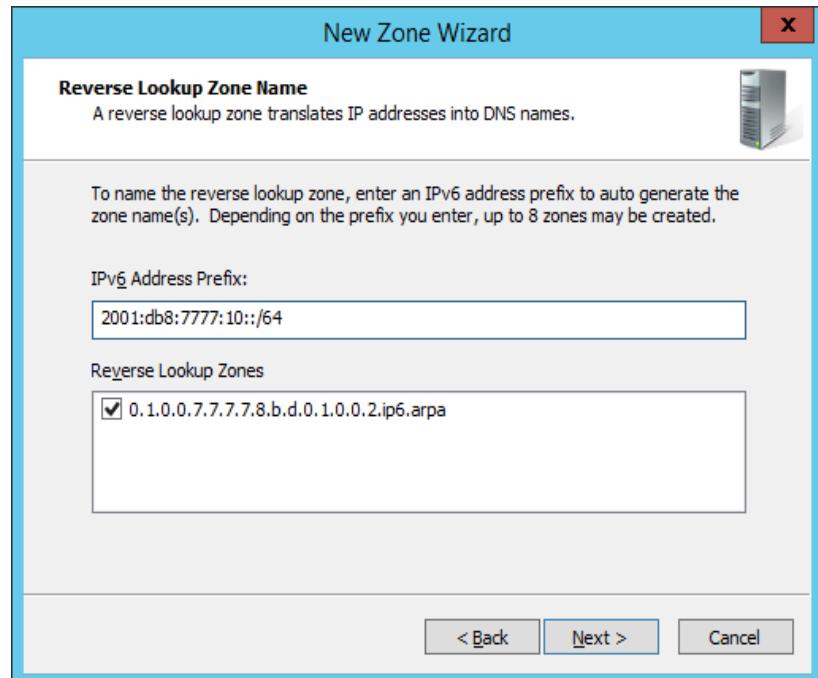


Figure 5. 26: IPv6 Address Prefix

Step 8: Select Allow both nonsecure and secure dynamic updates and click Next.

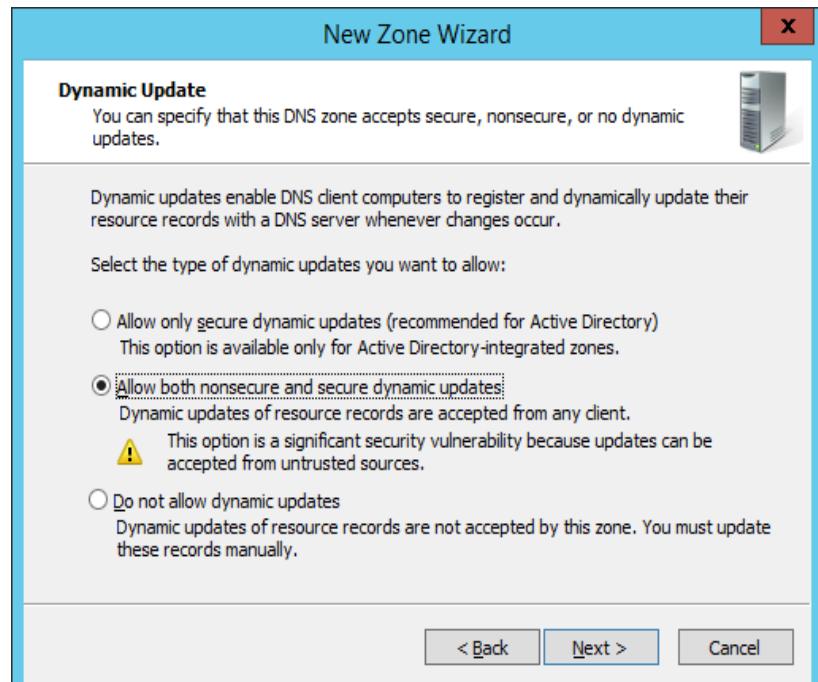


Figure 5. 27: Dynamic Update

Step 9: In Completing the New Zone Wizard click Finish to end it.

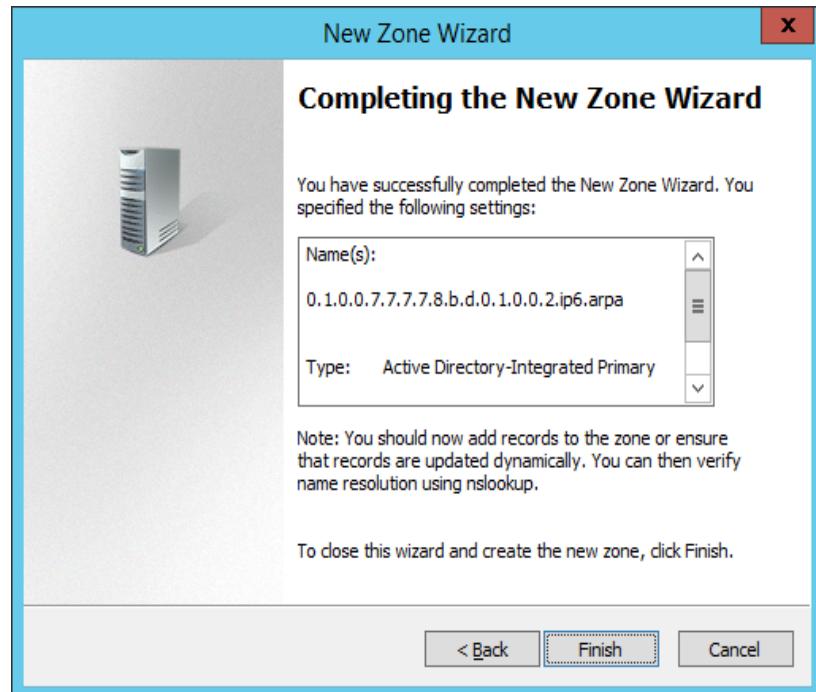


Figure 5. 28 : Completing the New Zone Wizard of IPv6 Reverse Lookup Zone

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

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

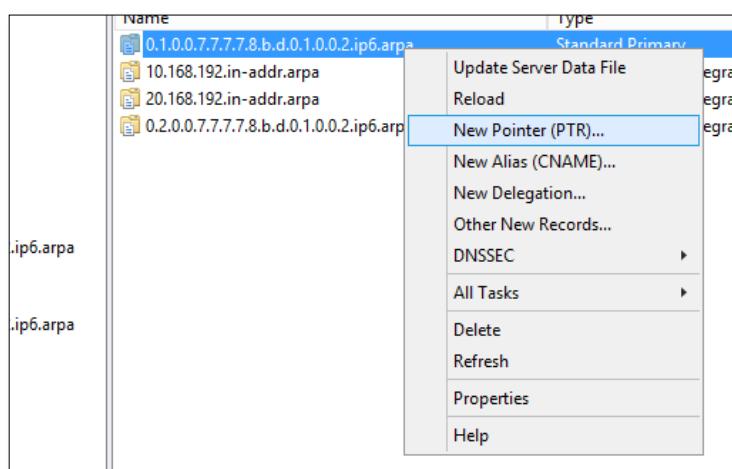


Figure 5. 29 New Pointer (PTR)

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

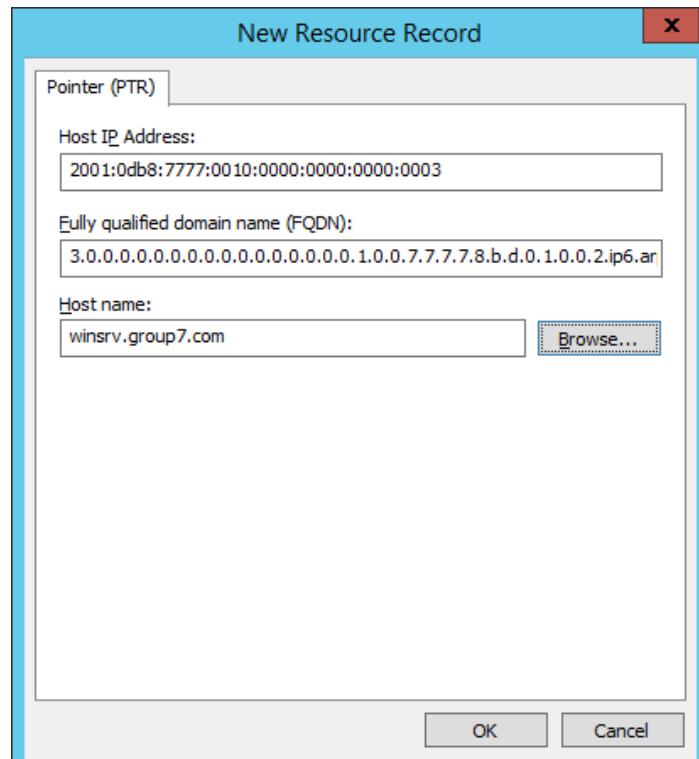


Figure 5. 30 Enter the Host IP Address and Host name

Step 12: Click on winsrv.group7.com and right click then click on New Host (A or AAAA).

An A and AAAA record are primary DNS records. They associate a domain name with a specific IP address, so that when a user types in a web address, such as "winsrv.group7.com" their browser knows where to go for the actual website. The difference between A and AAAA is this: A is IPv4 and AAAA is the current IPv6 record.

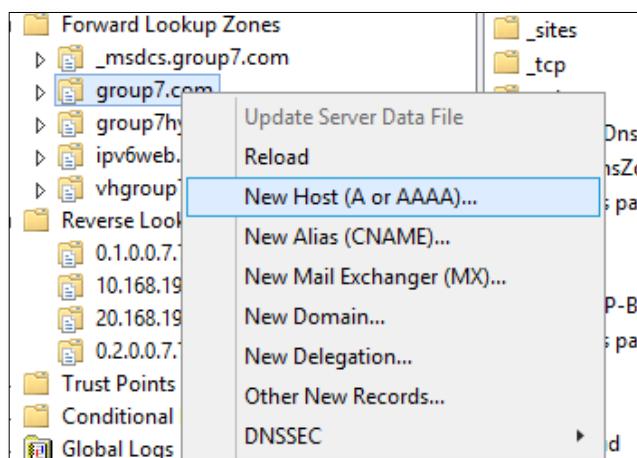


Figure 5. 31: New Host (A or AAAA)

Step 13: Enter the IP address 2001:db8:7777:10::3. Then click Add Host.

We tick create associated pointer (PTR) record because PTR records are mainly used to check if the server name is actually associated with the IP address from where the connection was initiated.

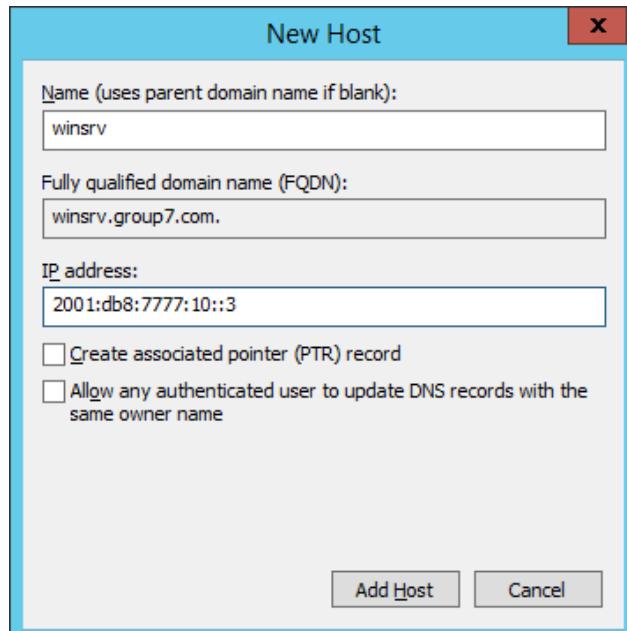


Figure 5. 32: New Host

Secondary DNS - Reverse Lookup Zones (IPv4)

Step 1: Edit ethernet connection 1 in ubuntu to setup the **IP address**.

- IP address : 192.168.20.3
- Netmask : 29
- Default gateway : 192.168.20.1
- Preferred DNS server : 192.168.10.3, 192.168.20.3

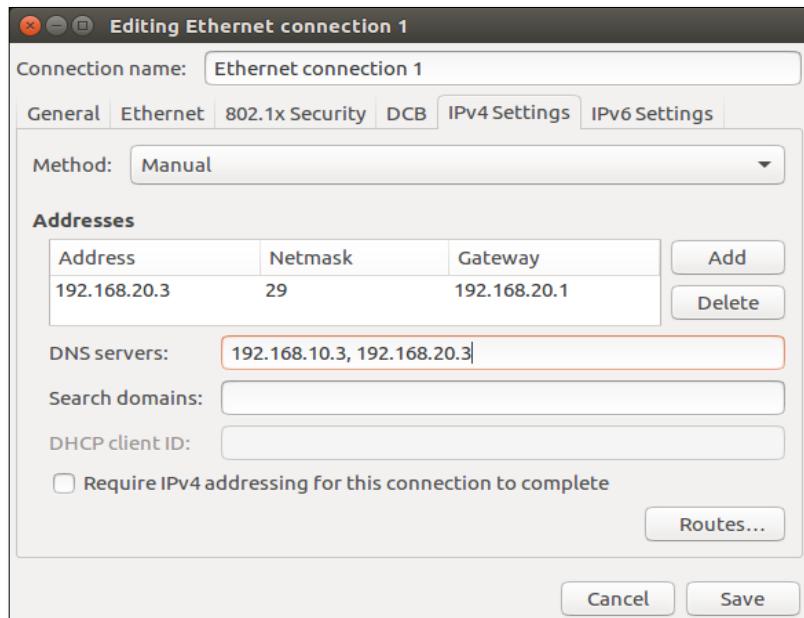


Figure 5. 33: Put correct IP address, Netmask, Default Gateway and Preferred DNS Server

Step 2: Install bind9 in ubuntu server by using *apt-get install bind9*.

```
root@group7:~$ sudo su
[sudo] password for g7:
root@group7:/home/g7# apt-get install bind9
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  linux-headers-4.10.0-28 linux-headers-4.10.0-28-generic
    linux-image-4.10.0-28-generic linux-image-extra-4.10.0-28-generic
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  bind9utils libirs141
Suggested packages:
  bind9-doc
The following NEW packages will be installed:
  bind9 bind9utils libirs141
0 upgraded, 3 newly installed, 0 to remove and 36 not upgraded.
Need to get 592 kB of archives.
After this operation, 2,957 kB of additional disk space will be used.
Do you want to continue? [Y/n] 
```

Figure 5. 34: Install bind9

Step 3: Type `nano /etc/bind/named.conf.default.zones` and add this command at the bottom.

```
root@group7:/home/g7# nano /etc/bind/named.conf.default-zones
root@group7:/home/g7#
```

Figure 5. 35 : Bind9 configuration file path

```
GNU nano 2.5.3                                     File: /etc/bind/named.conf.default-zones

        type master;
        file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};

#This used for forward's DNS
zone "group7.com"{
        type slave;
        masters {192.168.10.3;};
        file "/var/cache/bind/db.group7.com";
};

#This used for reverse DNS
zone "10.168.192.in-addr.arpa" {
        type slave;
        masters {192.168.10.3;};
        file "/var/cache/bind/db.10.168.192";
};

#This used for forward's DNS UBUNTU
zone "20.168.192.in-addr.arpa"{
        type slave;
        masters {192.168.10.3;};
        file "/var/cache/bind/db.20.168.192";
};

#This used for forward's DNS FEDORA
zone "30.168.192.in-addr.arpa"{
        type slave;
        masters {192.168.10.3;};
        file "/var/cache/bind/db.30.168.192";
};
```

Figure 5. 36 : Bind9 configuration file

Step 4: Check the status of the bind9. Make sure the bind9 is running.

```
;; MSG SIZE  rcvd: 296
root@group7:/home/g7# nano /etc/bind/named.conf.default-zones
root@group7:/home/g7# systemctl restart bind9
root@group7:/home/g7# systemctl status bind9
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: en
   Drop-In: /run/systemd/generator/bind9.service.d
             └─50-insserv.conf-$named.conf
     Active: active (running) since Kha 2018-11-29 15:44:26 +08; 6s ago
       Docs: man:named(8)
      Process: 16419 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)
     Main PID: 16424 (named)
        CGroup: /system.slice/bind9.service
                  └─16424 /usr/sbin/named -f -u bind

Nov 29 15:44:26 group7 named[16424]: zone localhost/IN: loaded serial 2
Nov 29 15:44:26 group7 named[16424]: zone 255.in-addr.arpa/IN: loaded serial 1
Nov 29 15:44:26 group7 named[16424]: zone group7.com/IN: loaded serial 4604
Nov 29 15:44:26 group7 named[16424]: zone 10.168.192.in-addr.arpa/IN: loaded ser
Nov 29 15:44:26 group7 named[16424]: all zones loaded
Nov 29 15:44:26 group7 named[16424]: running
Nov 29 15:44:26 group7 named[16424]: zone group7.com/IN: sending notifies (seria
Nov 29 15:44:26 group7 named[16424]: zone 10.168.192.in-addr.arpa/IN: sending no
Nov 29 15:44:26 group7 named[16424]: zone 20.168.192.in-addr.arpa/IN: sending no
Nov 29 15:44:26 group7 named[16424]: zone 30.168.192.in-addr.arpa/IN: refresh: n
lines 1-21... skipping...
```

Figure 5. 37 : Bind9 status

Step 5: Next, we will add new zone for reverse lookup. Right click on Reverse Lookup Zone and click New Zone. Reverse lookup zone is the opposite way of Forward Lookup Zone.

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

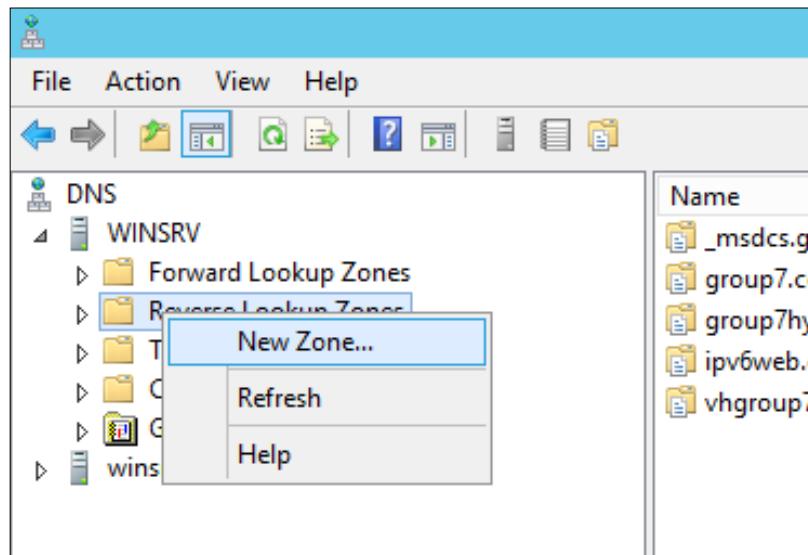


Figure 5. 38: New Zone (Reverse Lookup Zone)

Step 6: Next, we start create the reverse lookup zone.



Figure 5. 39: DNS Server Wizard

Step 7: Next, choose the secondary zone and click next to proceed.

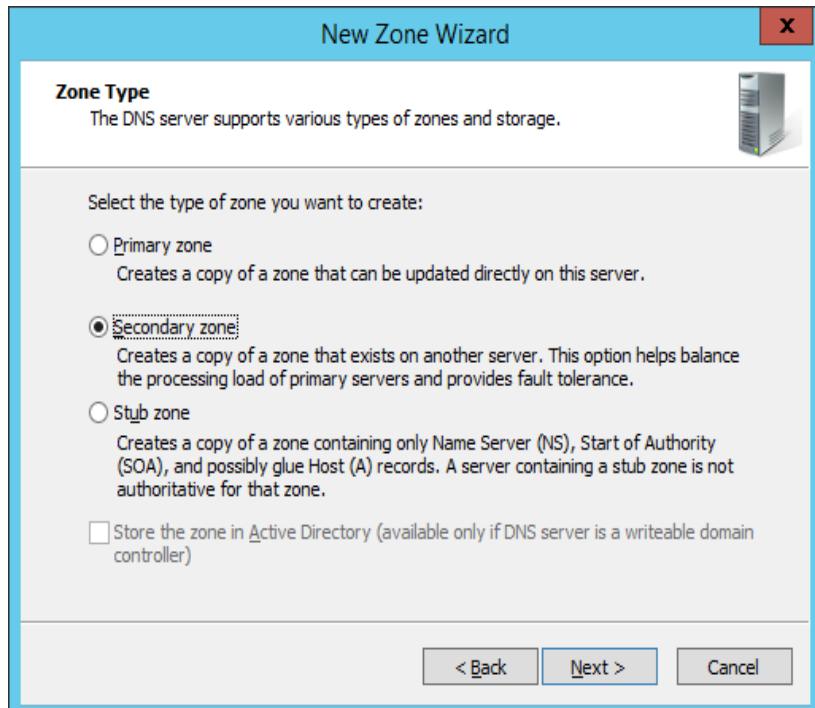


Figure 5. 40: Zone type

Step 8: Next, choose how we want the zone to replicate.

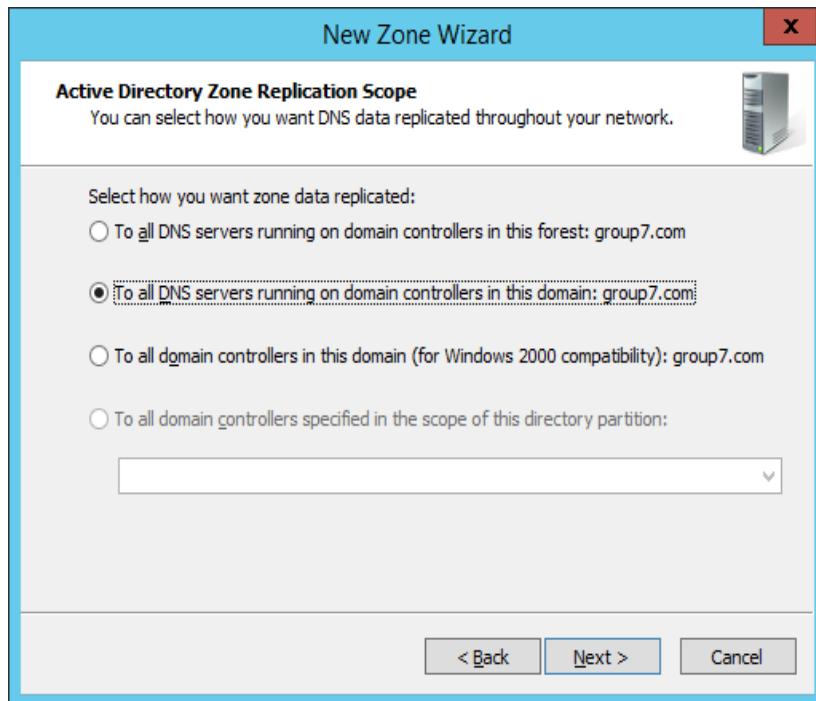


Figure 5. 41: Zone replication

Step 9: Next, we choose for IPv4 Reverse Lookup Zone and click Next>

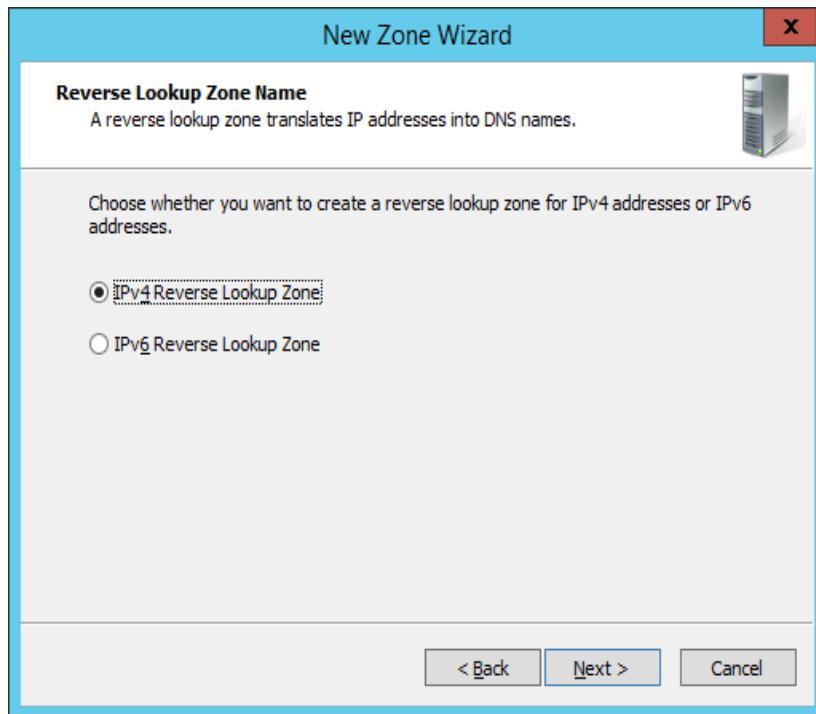


Figure 5. 42: Select IPv4 Reverse Lookup Zone Name (IPv4)

Step 10: Then, we choose Network ID. Group 7's Network ID: 192.168.20.

When you create an IPv4 reverse lookup zone using the DNS Manager, the New Zone Wizard prompts you for a network ID, it is the portion of the IP address range for which the reverse lookup zone is responsible. For example, if the reverse lookup zone covers all addresses that begin with 192 (that is, 192.0.0.0 to 192.255.255.255), you enter 192.

To cover only those addresses in the subnet with an address in the range of 192.168.20.0 to 192.168.20.255, we enter 192.168.20. The wizard then constructs the reverse lookup zone name by reversing the order of the digit blocks and appending the result to the “root” domain name. For example, if we enter 192.168.10 in the wizard, the resulting name of the reverse lookup zone is 20.168.192.in-addr.arpa.

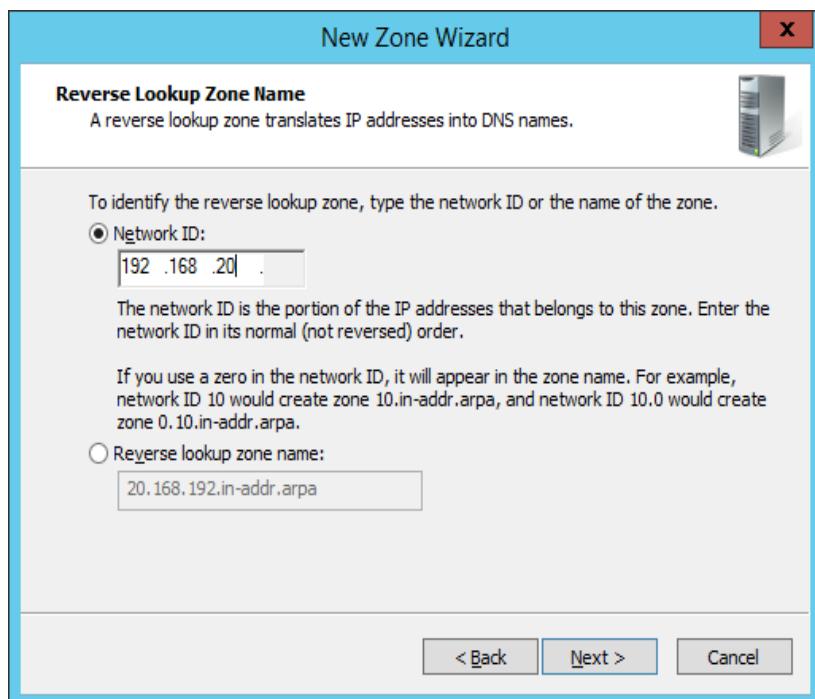


Figure 5. 43: Reverse Lookup Zone Name

Step 11: For Dynamic Update, choose to allow dynamic updates and click Next.

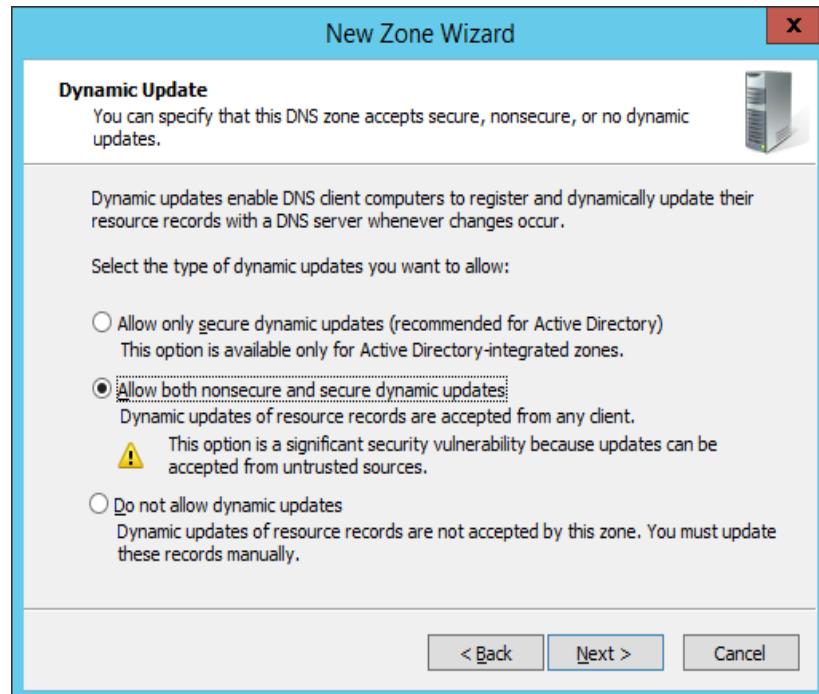


Figure 5. 44: Dynamic Update

Step 12: In Completing the New Zone Wizard it will display the information we have created. Click Finish to end it.

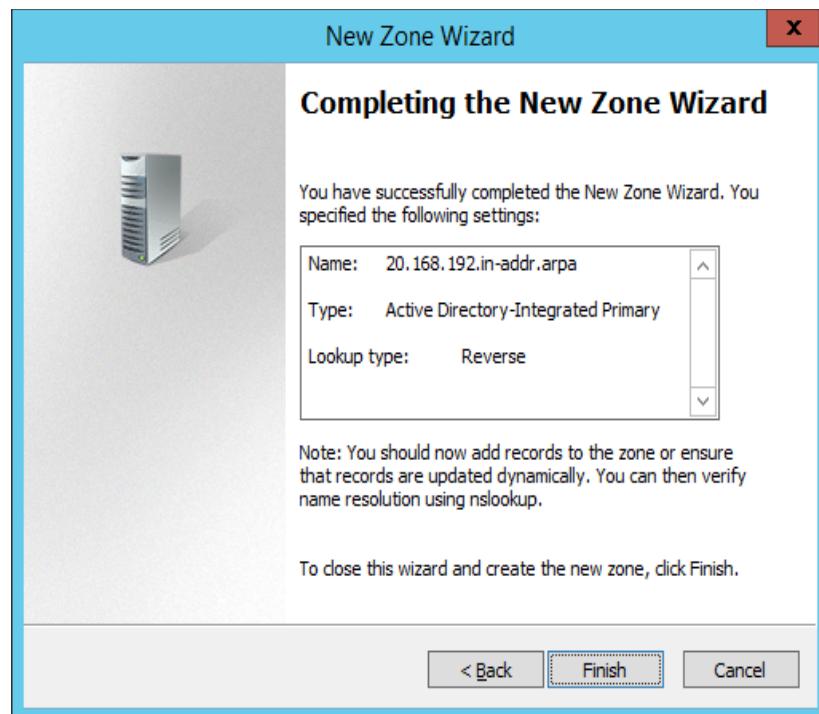


Figure 5. 45: Completing the New Zone Wizard of IPv4 Reverse Lookup Zone

Step 13: Next, right click on IPv6 in Reverse Lookup Zones and click New Pointer (PTR).

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

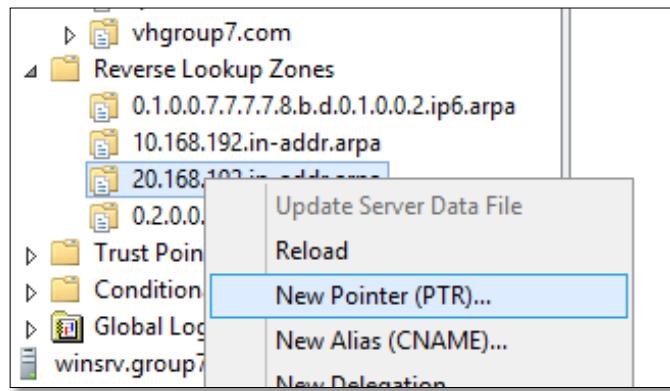


Figure 5. 46: Pointer (PTR)

Step 14: Enter the Host IP Address and host name. Then click OK.

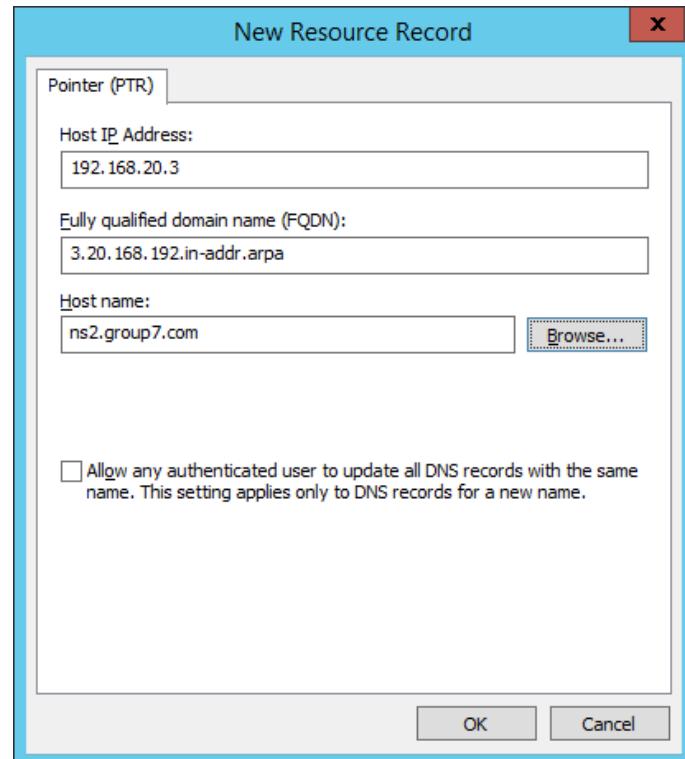


Figure 5. 47: New Resource Record

Step 15: Click on ns2.group7.com and right click then click on New Host (A or AAAA). An A and AAAA record are primary DNS records. They associate a domain name with a specific IP address, so that when a user types in a web address, such as "ns2.group7.com" their browser knows where to go for the actual website. The difference between A and AAAA is this: A is IPv4 and AAAA is the current IPv6 record.

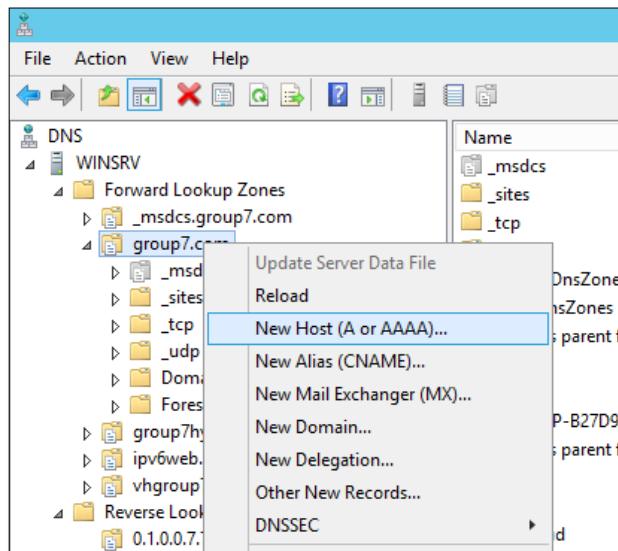


Figure 5. 48: New Host (A or AAAA)

Step 16: Enter the Name ns2 and IP address 192.168.20.3. Then click Add Host.

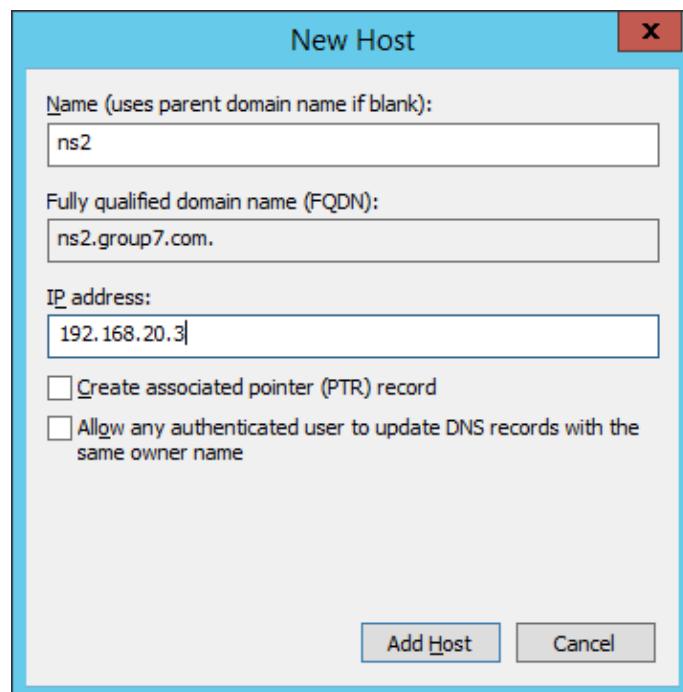


Figure 5. 49: New Host IPv4

Reverse Lookup Zones (IPv6)

Step 1: Double click at Internet Protocol Version 6 (TCP/IPv6) to setup the IP address.

- IP address : 2001:db8:7777:20::3
- Prefix : 64
- Gateway : 2001:db8:7777:20::1
- Preferred DNS server : 2001:db8:7777:10::3, 2001:db8:7777:20::3

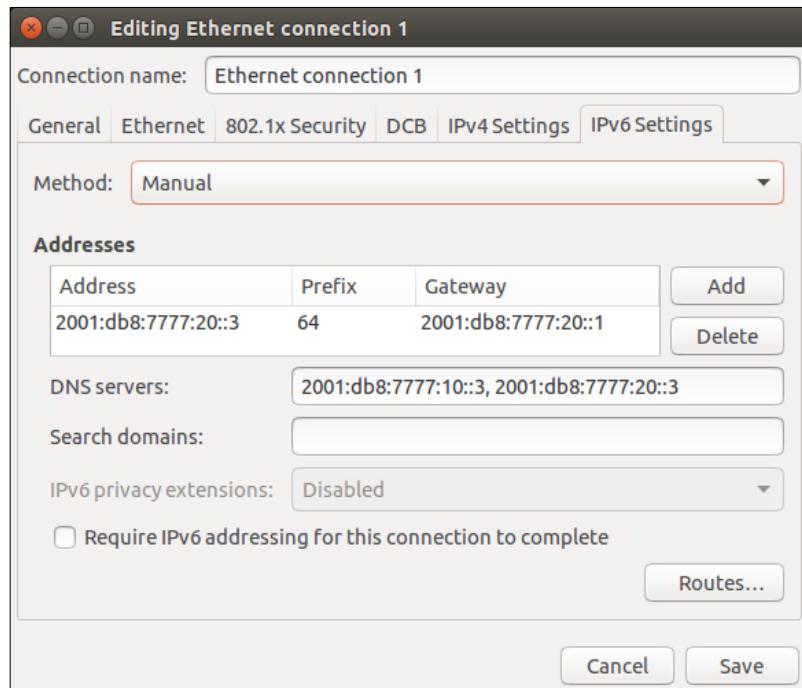


Figure 5. 50: Put correct IP address, Subnet Mask, Default Gateway and Preferred DNS Server

Step 2: Right click on Reverse Lookup Zones and click New Zone.

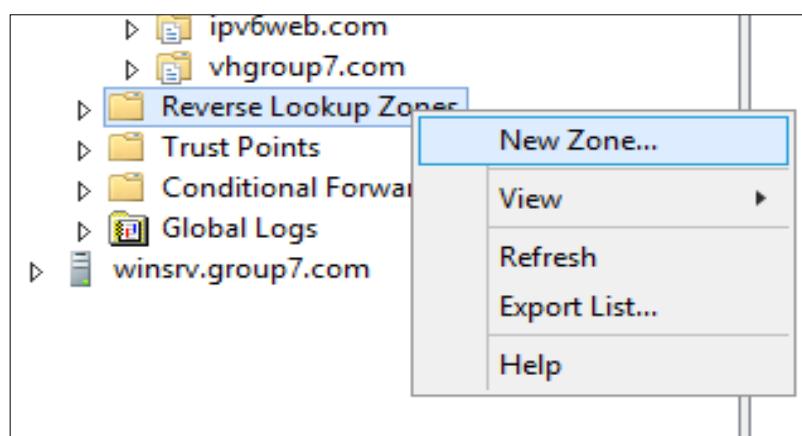


Figure 5. 51: New Zone

Step 3: In Welcome to New Wizard click Next.

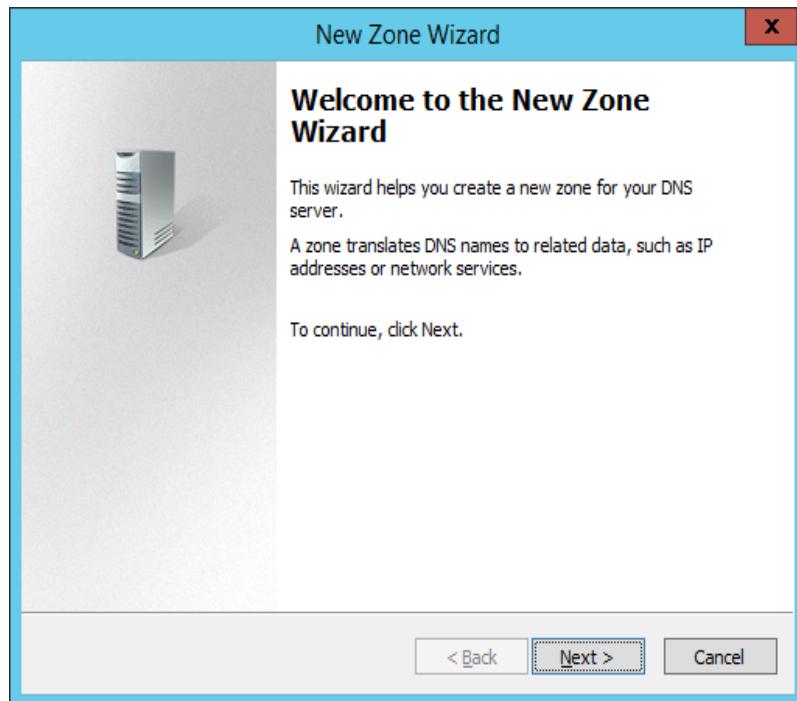


Figure 5. 52: Welcome the New Zone Wizard

Step 4: Then choose Primary zone. Tick on Store the zone in active AD. Then click next.

We tick store the zone in Active Directory because DNS server running on domain controllers can store their zones in Active Directory Domain Services.

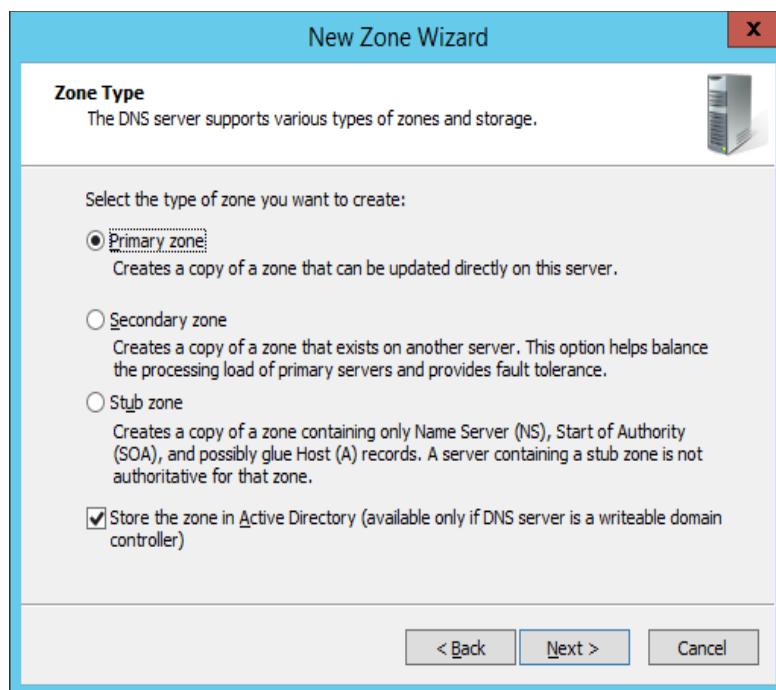


Figure 5. 53: Zone Type

Step 5: Select how we want the zone to replicate and click Next.

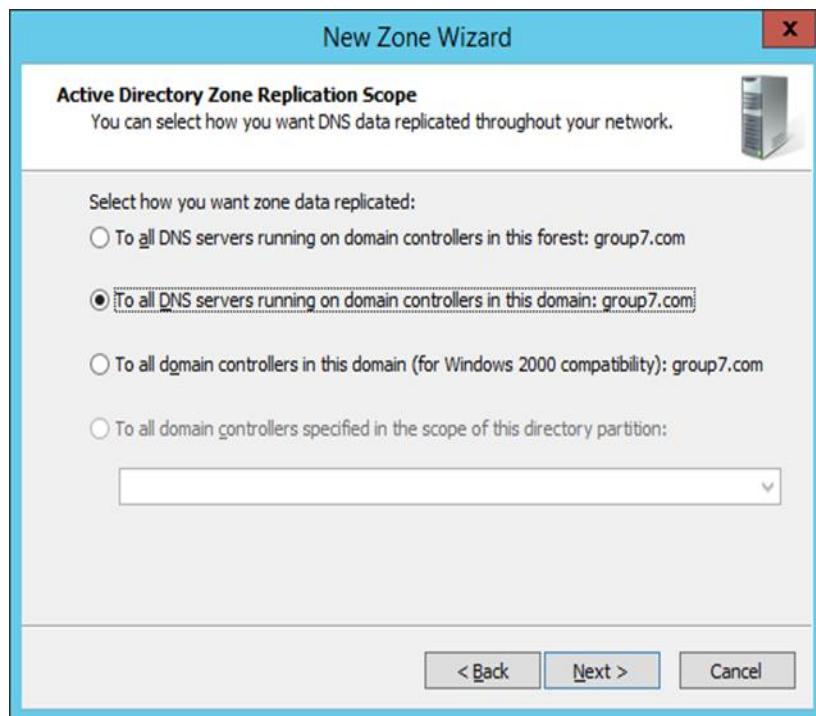


Figure 5. 54: Zone Replication scope

Step 6: Next, choose IPv6 Reverse Lookup Zone.

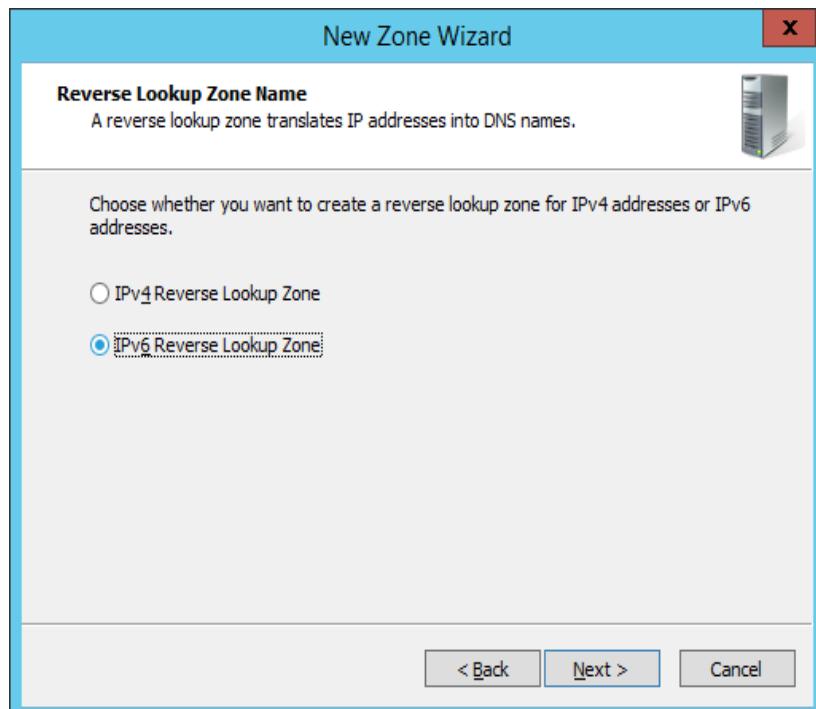


Figure 5. 55: IPv6 Reverse Lookup Zone

Step 7: In IPv6 Address Prefix, we enter 2001:db8:7777:20::/64 and Reverse Lookup Zones will automatically create.

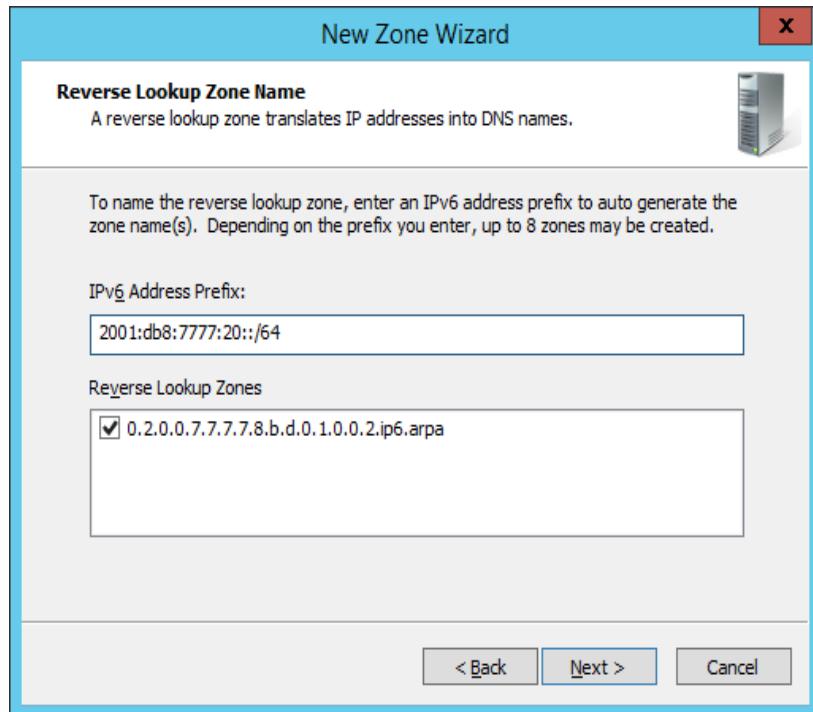


Figure 5. 56: IPv6 Address Prefix

Step 8: Select Allow both nonsecure and secure dynamic updates and click Next.

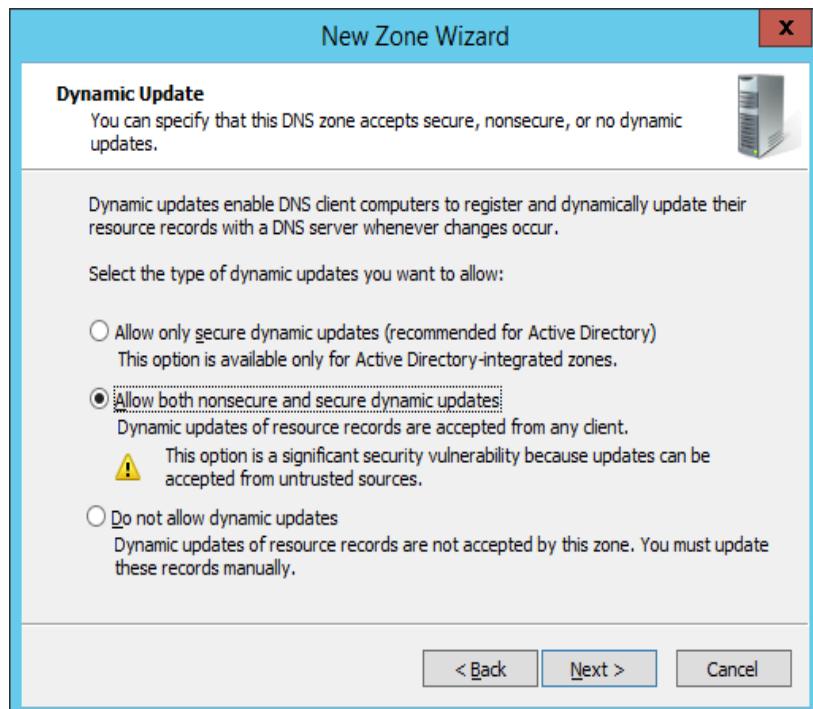


Figure 5. 57: Dynamic Update

Step 9: In Completing the New Zone Wizard click Finish to end it.

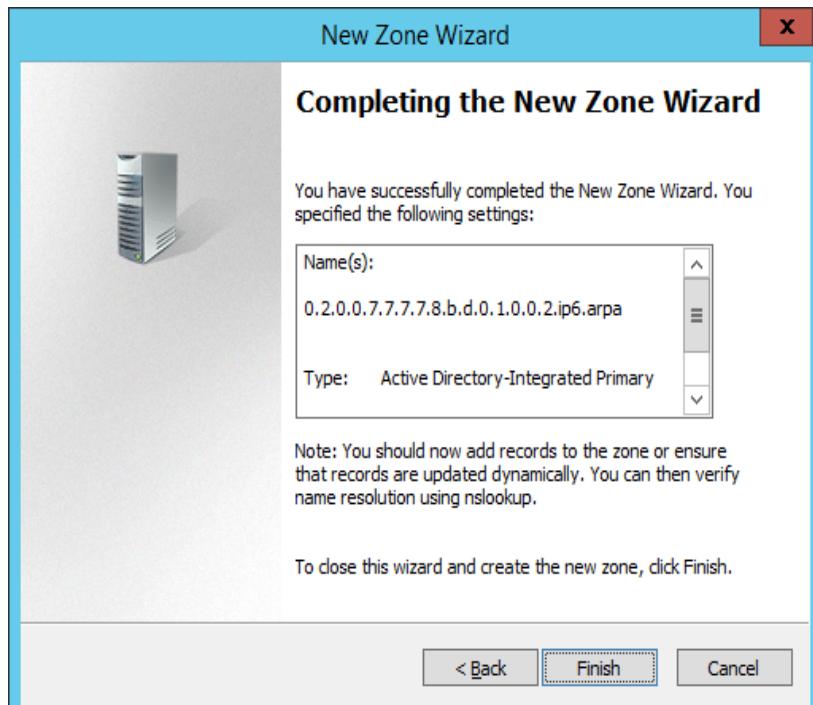


Figure 5. 58 : Completing the New Zone Wizard of IPv6 Reverse Lookup Zone

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

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

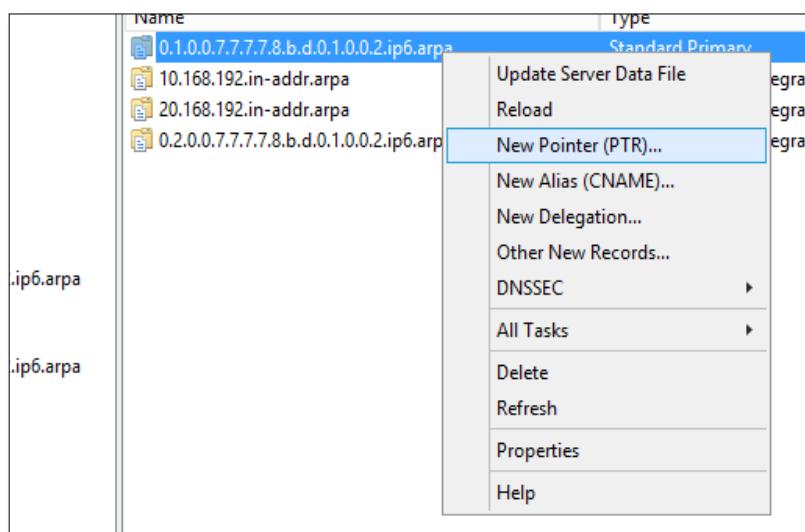


Figure 5. 59: New Pointer (PTR)

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

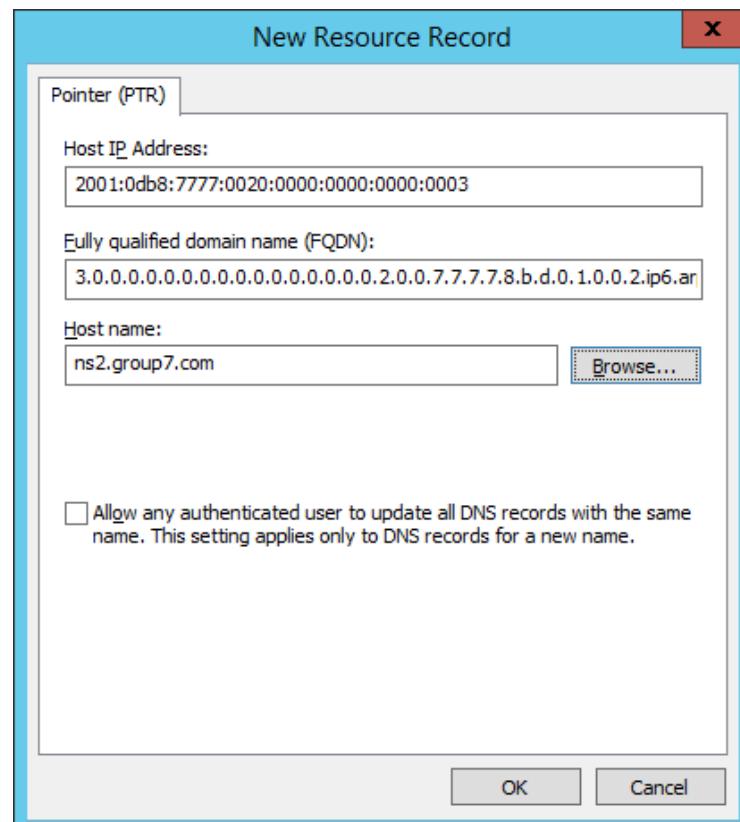


Figure 5. 60: Enter the Host IP Address and Host name

5.2.2 DHCP (IPv4)

Step 1: From Server Manager > Dashboard click on **Add roles and feature**.

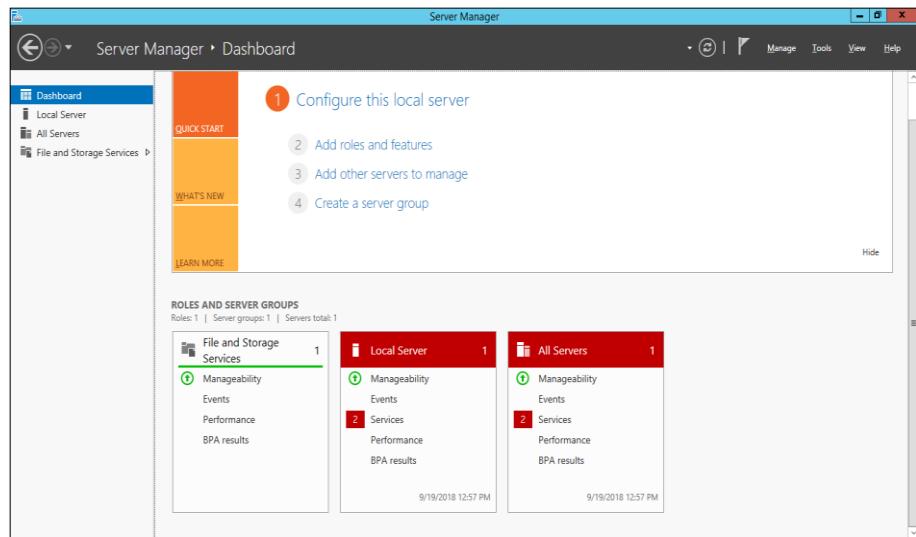


Figure 5. 61 : Server Manager

Step 2: Go to Server Roles and click on **DHCP** then **Add features**.

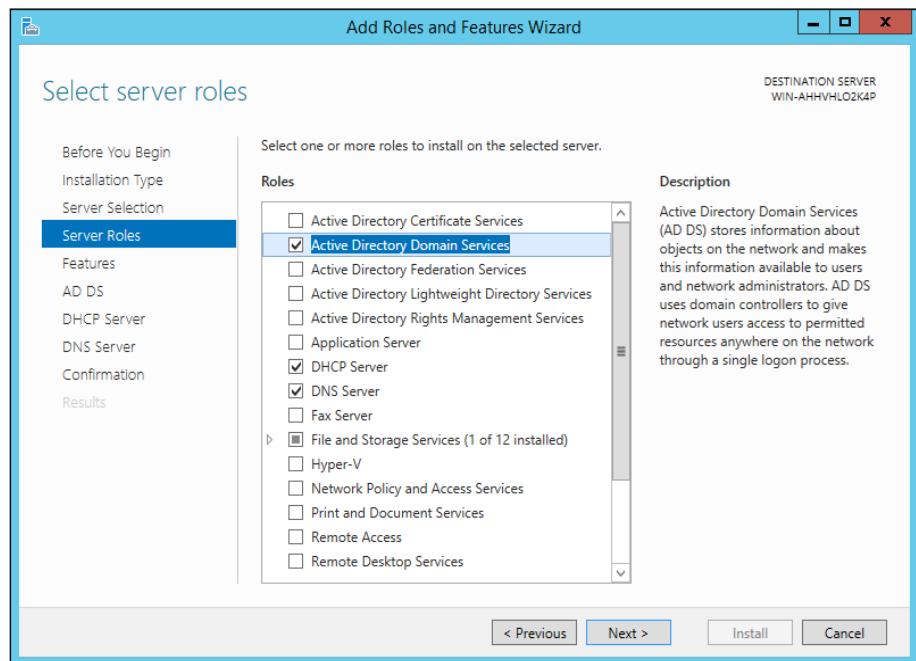


Figure 5. 62 : Server Roles

Step 3: When all the process stated done, just click **Close**.

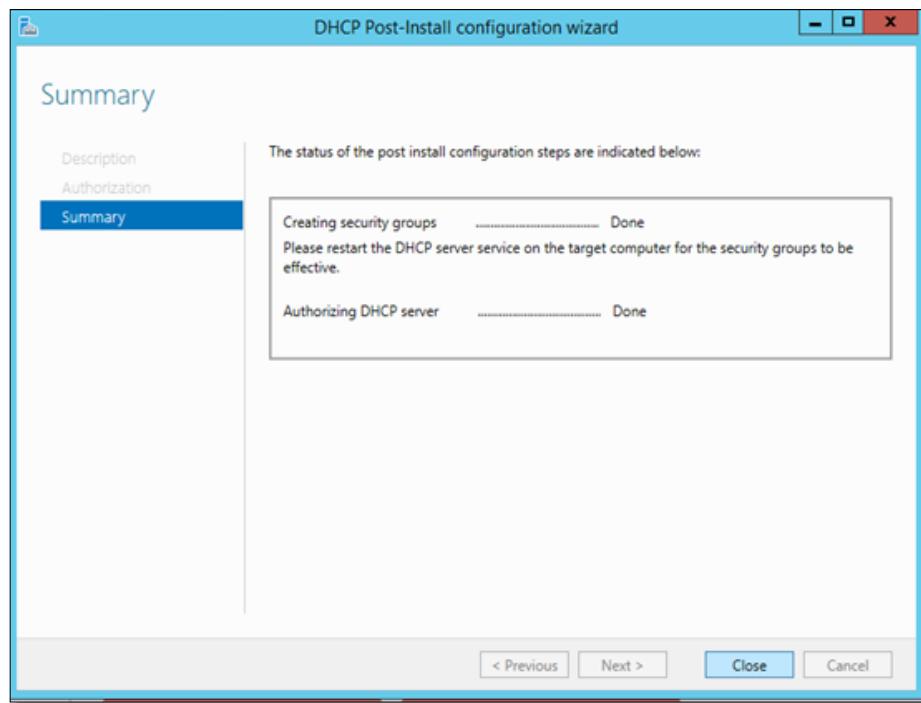


Figure 5. 63: DHCP Summary

Step 4: Under **Server Manager | Tools**, then select **DHCP** to click **DHCP Manager** in order to start configure.

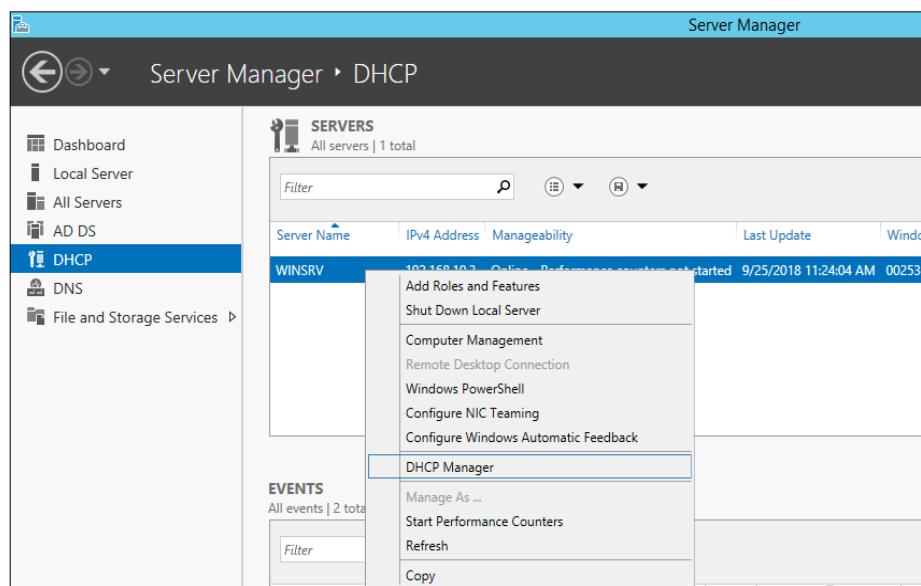


Figure 5. 64: DHCP Manager

Step 5: Under **DHCP** console, right click on **IPv4** in order to create a “**New Scope**”. Then, click **next**.

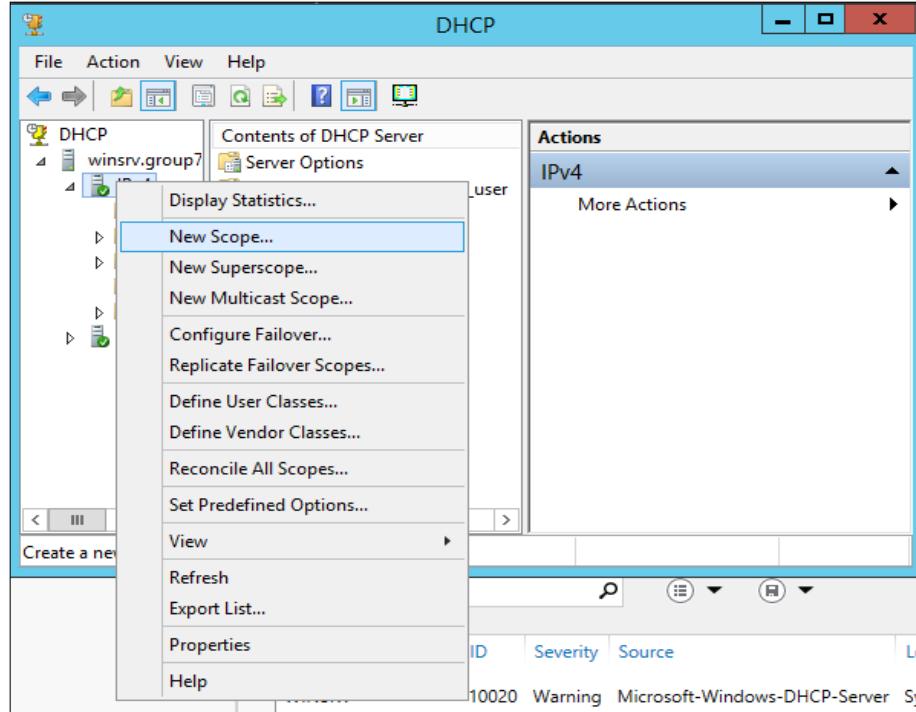


Figure 5. 65: New Scope

Step 6: In **New Scope Wizard**, enter the **Scope Name** “client IPv4” and Description. After that, click **Next** button.

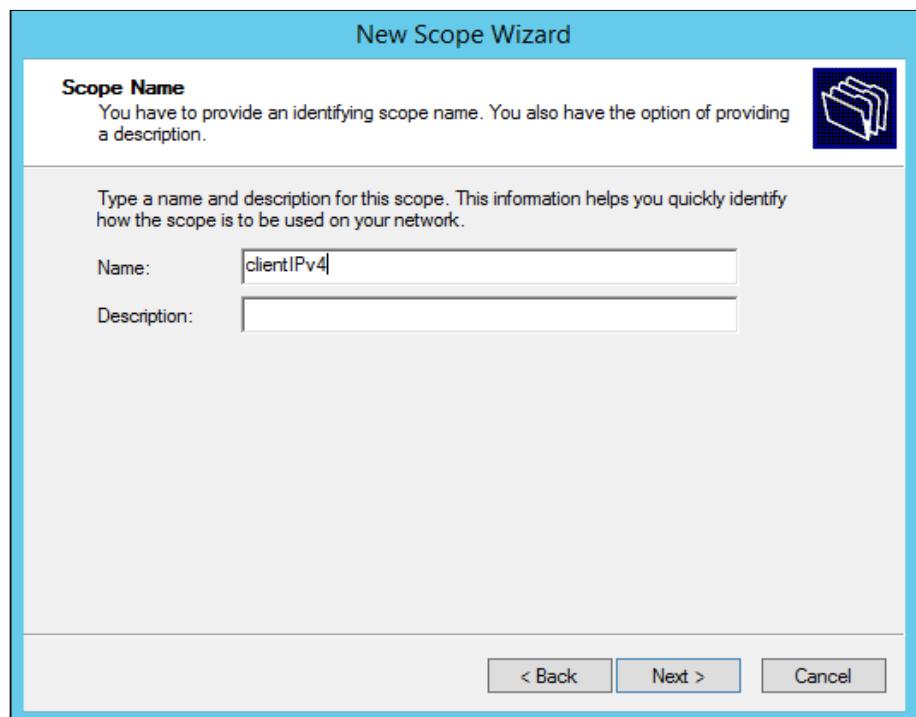


Figure 5. 66: Rename the new scope as clientIPv4

Step 7: Insert IP address **192.168.101.2 - 192.168.101.61** and subnet mask **255.255.255.192** for dhcp IPv4 for client.

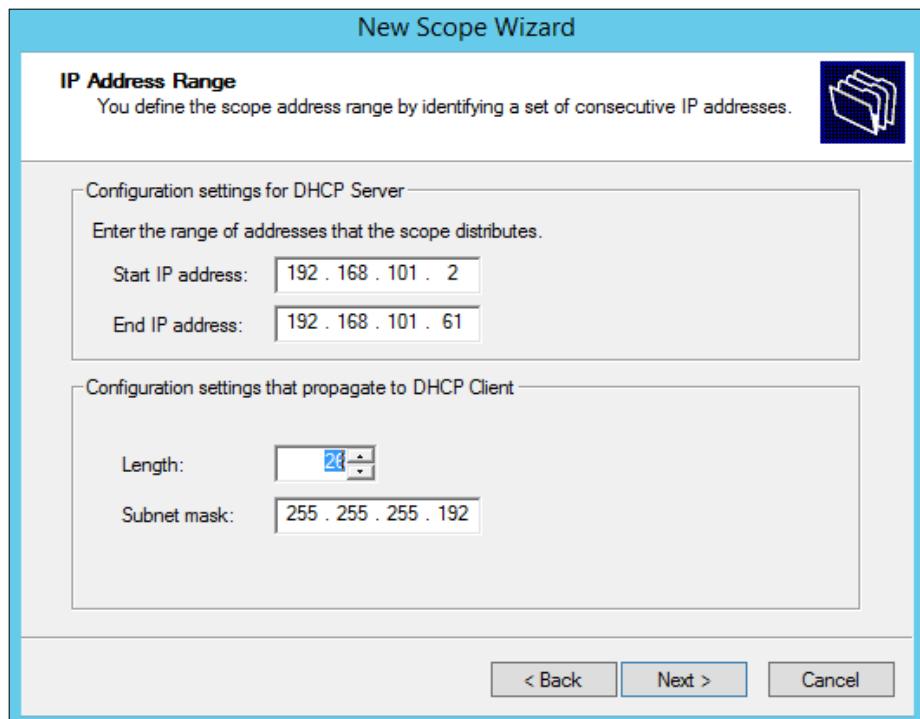


Figure 5. 67: IP Address Range

Step 8: For Add Exclusions and Delay, just click Next button.

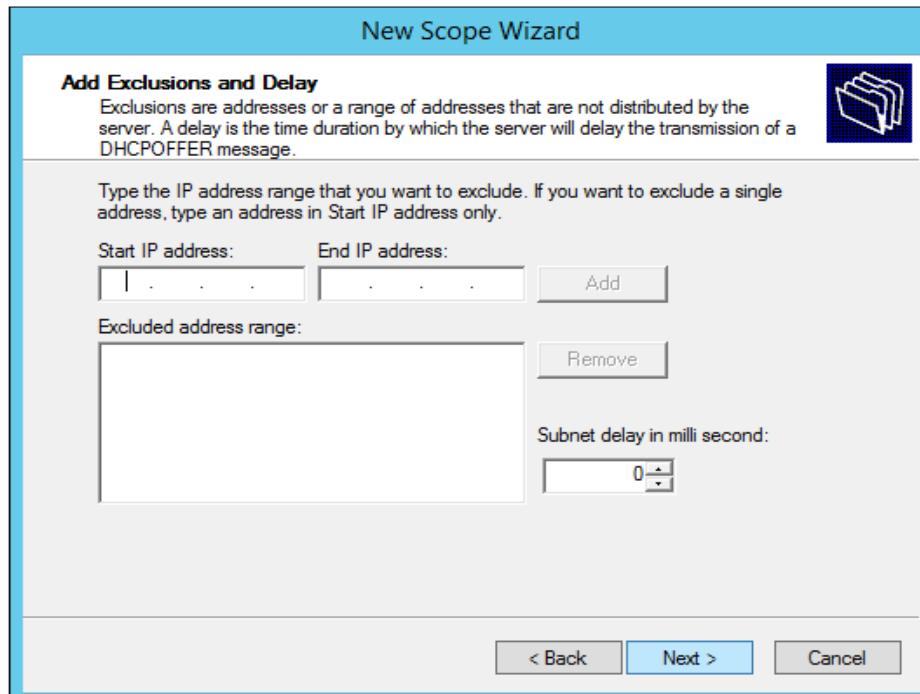


Figure 5. 68: Add Exclusion and Delay

Step 9: For Lease Duration, also click Next.

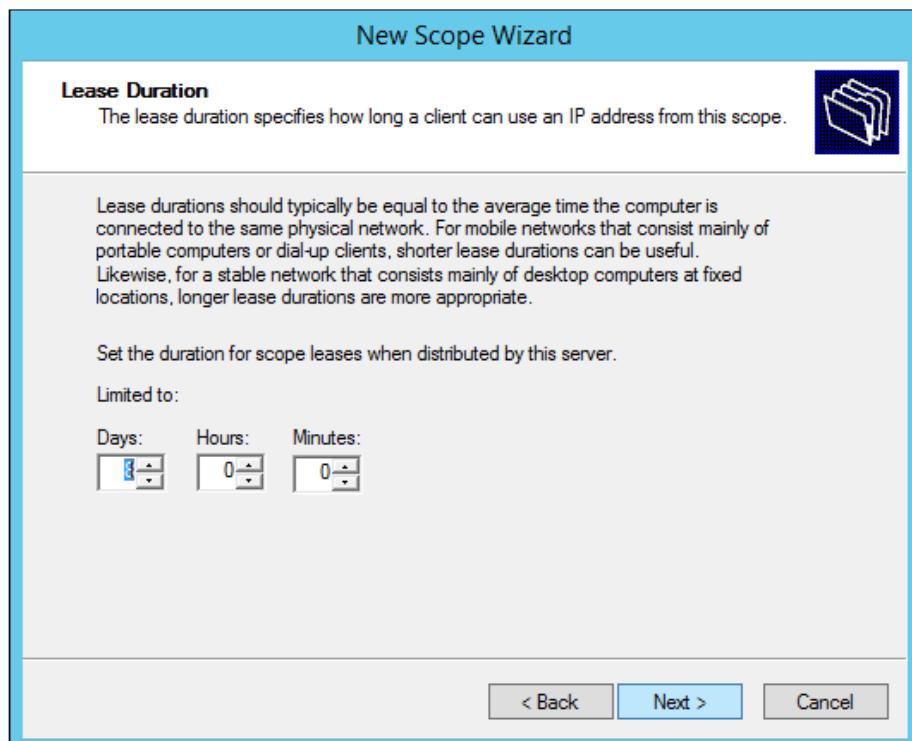


Figure 5. 69: Lease Duration

Step 10: Next, for WINS Servers just click Next.

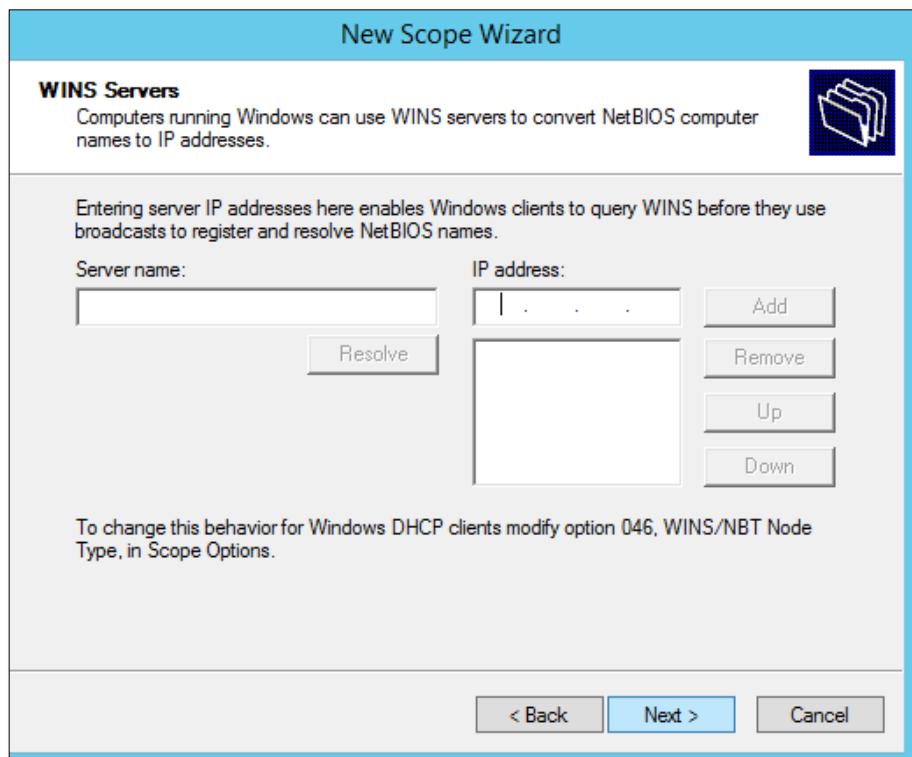


Figure 5. 70: WINS Servers

Step 11: Then, choose “**Yes, I want to configure these options now**” and then, click **next**.

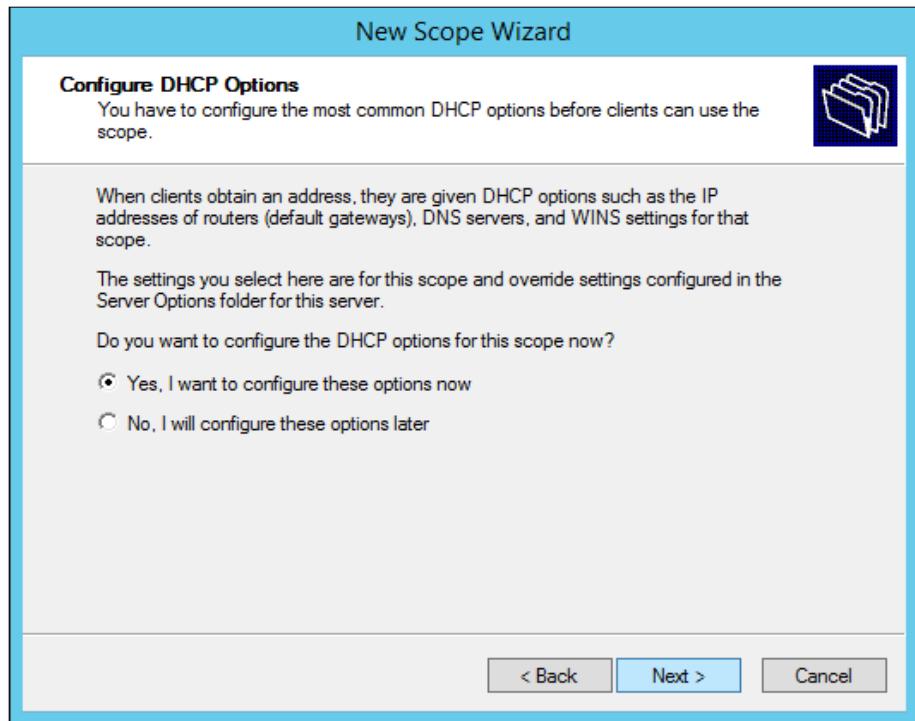


Figure 5. 71: *DHCP Options*

Step 12: Complete configuring the DHCP Server. Click Finish.

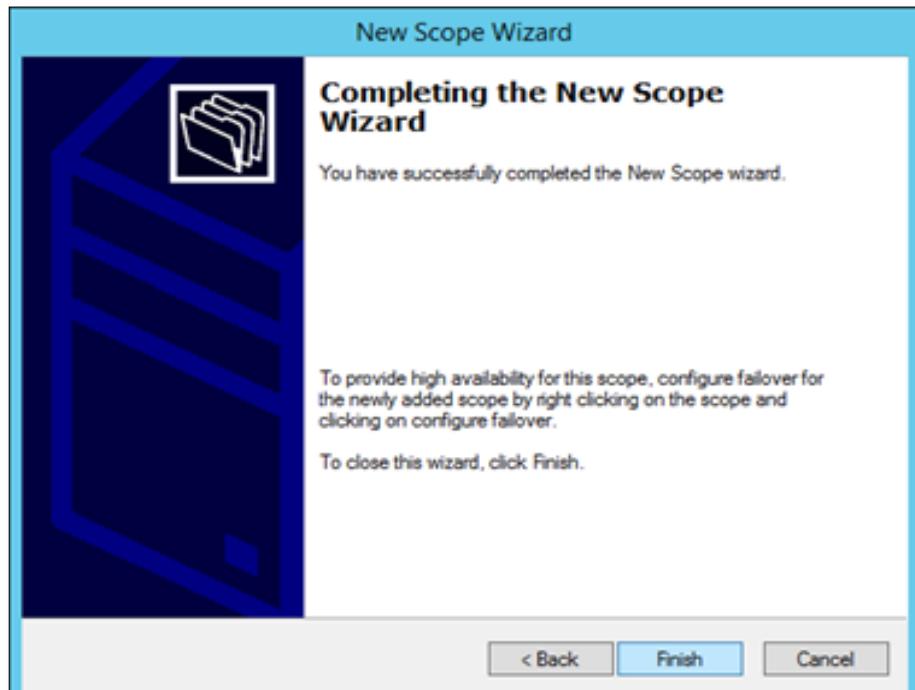


Figure 5. 72: *Complete New Scope*

5.2.3 DHCP (IPv6)

Step 1: First click tools from Server Manager Dashboard then, click DHCP.

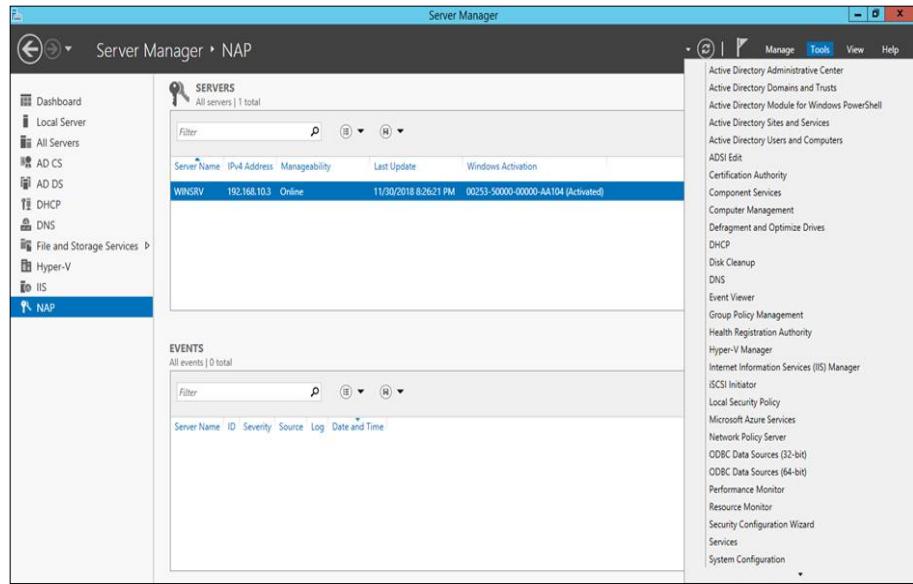


Figure 5. 73: Click tools then click dhcp

Step 2: Right click on IPv6 and click scope.

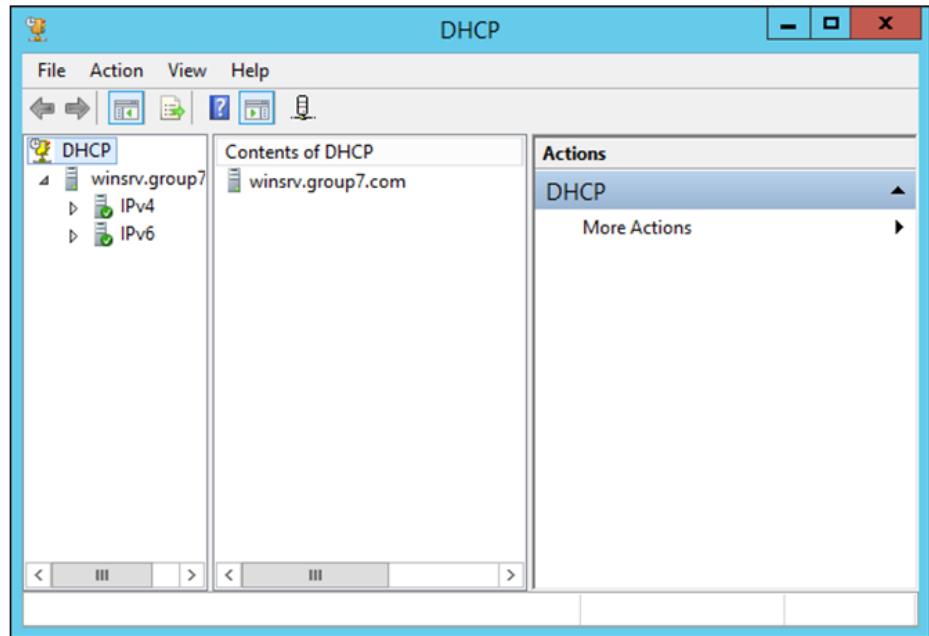


Figure 5. 74: Right click on IPv6 and click scope

Step 3: Once new wizard pop up click Next.

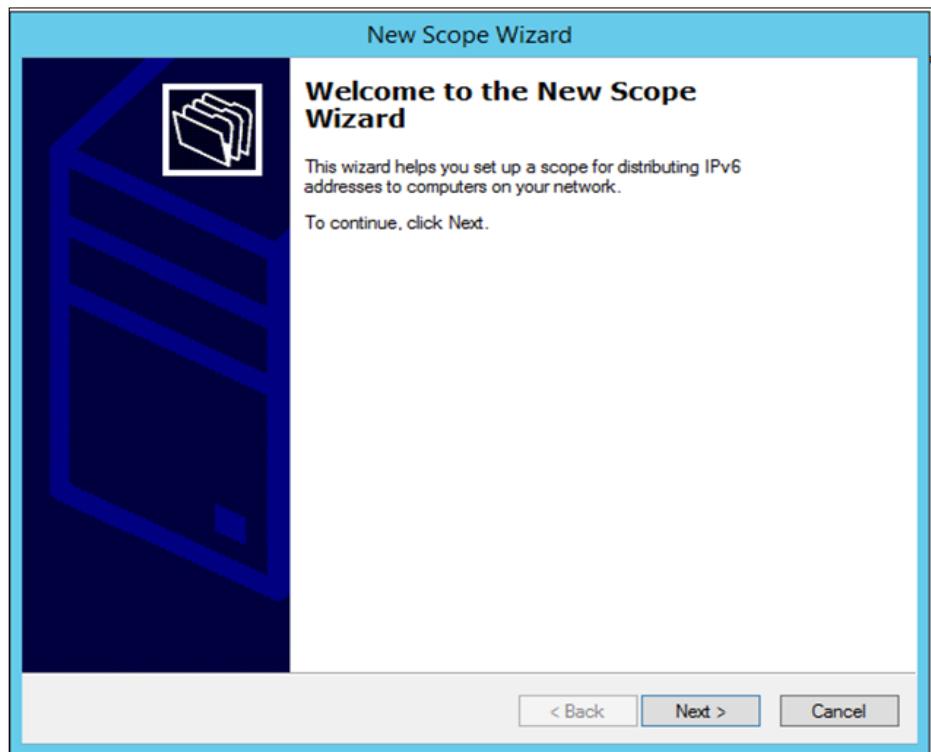


Figure 5. 75: Click next

Step 4: Give a name for the new IPv6 scope then, click next.

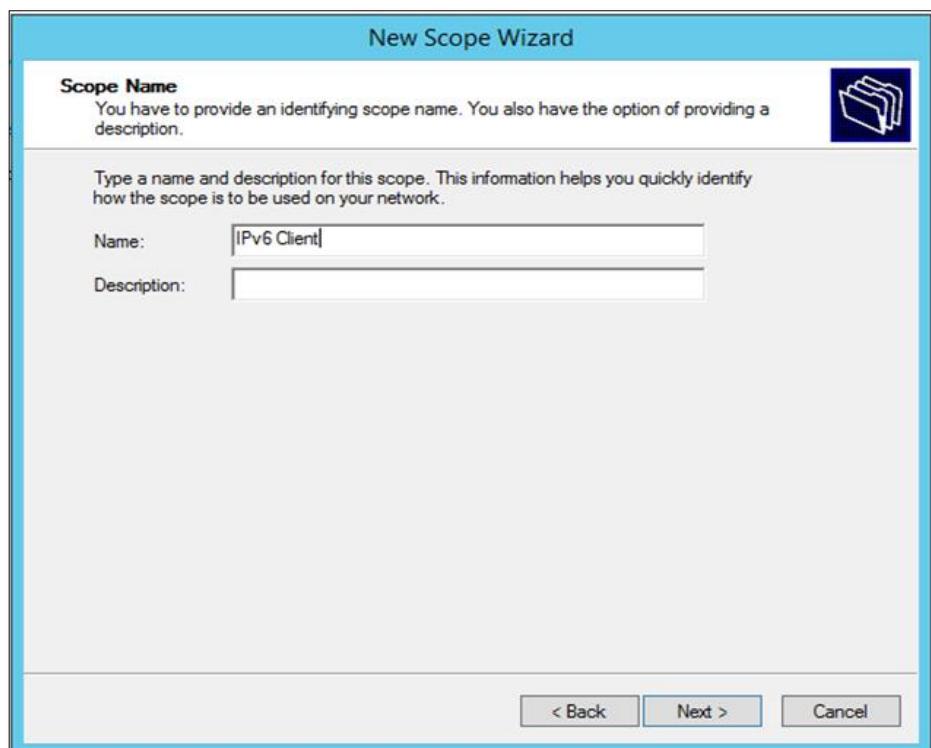


Figure 5. 76: New name for IPv6 scope

Step 5: Set prefix for the IPv6 then click Next.

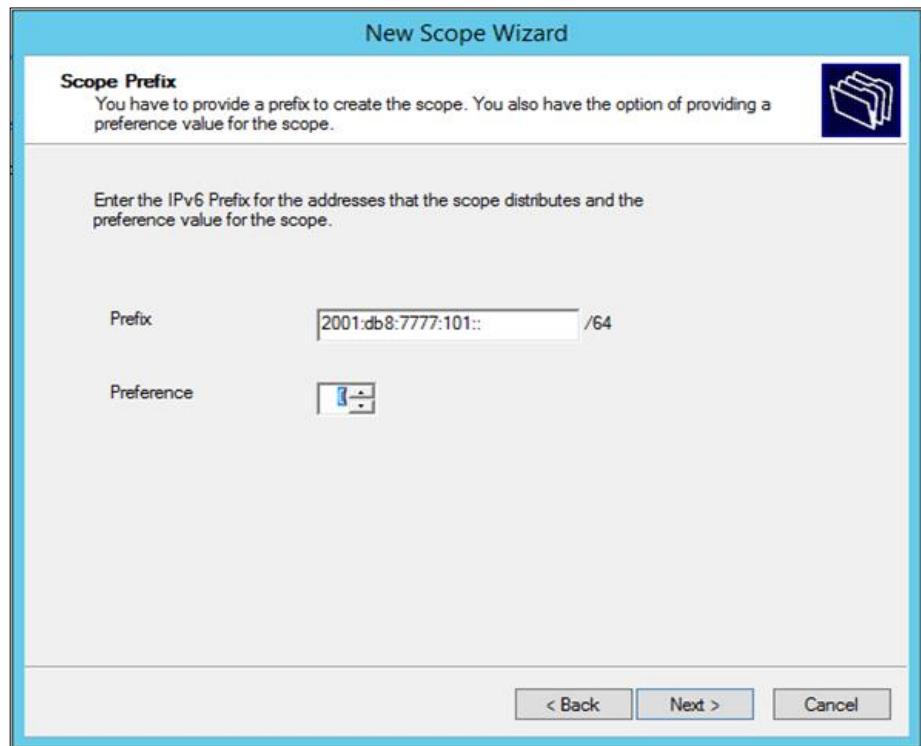


Figure 5. 77: Set IPv6 address

Step 6: Set scope lease time then click next.

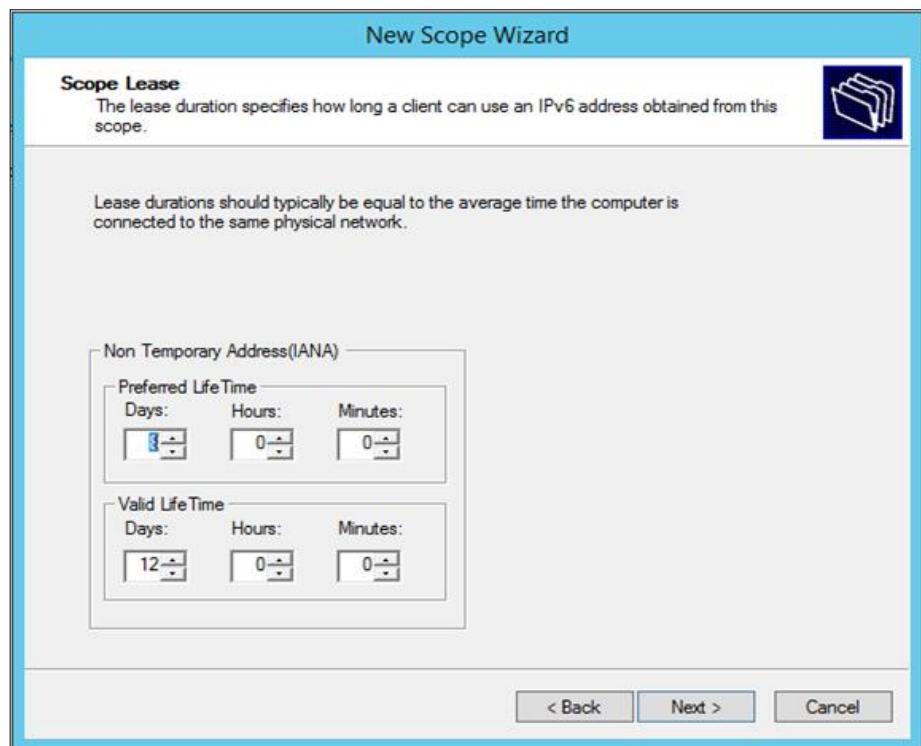


Figure 5. 78: Set scope lease time

Step 7: Once complete click finish.

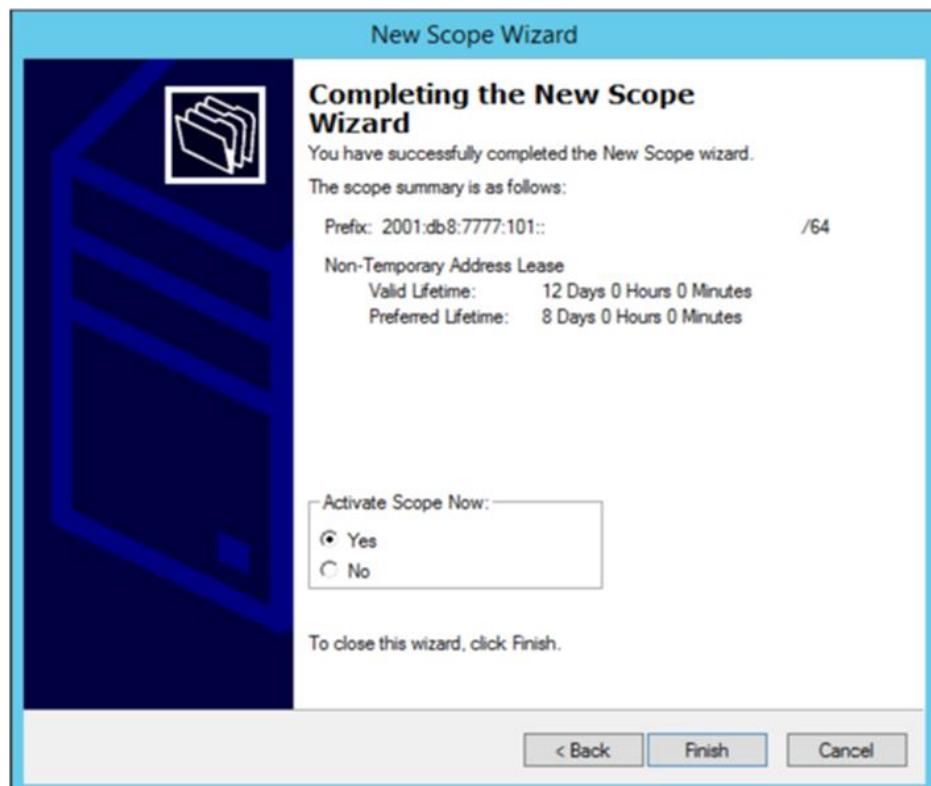


Figure 5. 79: Click finish once done the configuration

5.2.4 Inter VLAN and VLSM addressing

Inter VLAN

Step 1: Set the hostname for the switch.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname group7-SW
```

Figure 5. 80: Labelling switch name.

Step 2: Select the VLAN and label.

```
group7-SW(config)#vlan 5
group7-SW(config-vlan)#name Trunk
```

Figure 5. 81: Assign name for ‘vlan 5’

```
group7-SW(config-vlan)#vlan 10
group7-SW(config-vlan)#name WinServer
```

Figure 5. 82: Assign name for ‘vlan 10’

```
group7-SW(config-vlan)#vlan 20
group7-SW(config-vlan)#name UbuServer
```

Figure 5. 83: Assign name for ‘vlan 20’

```
group7-SW(config-vlan)#vlan 30
group7-SW(config-vlan)#name FedoServer
```

Figure 5. 84: Assign name for ‘vlan 30’

```
group7-SW(config)#vlan 101
group7-SW(config-vlan)#name Client
```

Figure 5. 85: Assign name for ‘vlan 101’

```
group7-SW(config-vlan)#vlan 102
group7-SW(config-vlan)#name AP
```

Figure 5. 86: Assign name for ‘vlan 102’

Step 3: Save the configuration.

```
group7-SW(config-vlan)#do copy r s
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 2823 bytes to 1498 bytes[OK]
group7-SW(config-vlan)#

```

Figure 5. 87: Execution of *copy run start*.

Step 4: Assign available port to the VLAN group and save the configuration.

```
group7-SW(config)#int range gi 1/0/19-21
group7-SW(config-if-range)#sw mo ac
group7-SW(config-if-range)#sw ac vl 101
group7-SW(config-if-range)#no shut

```

Figure 5. 88: Assign port 19 to 21 for *vlan Client*.

```
group7-SW(config-if-range)#int range gi 1/0/16-18
group7-SW(config-if-range)#sw ac vl 102
group7-SW(config-if-range)#sw mo ac
group7-SW(config-if-range)#no shut

```

Figure 5. 89: Assign port 16 to 18 for *vlan AP*.

```
group7-SW(config-if-range)#int range gi 1/0/4-6
group7-SW(config-if-range)#sw mo ac
group7-SW(config-if-range)#sw ac vl 10
group7-SW(config-if-range)#no shut

```

Figure 5. 90: Assign port 4 to 6 for *vlan WinServer*.

```
group7-SW(config-if-range)#int range gi 1/0/7-9
group7-SW(config-if-range)#sw mo ac
group7-SW(config-if-range)#sw ac vl 20
group7-SW(config-if-range)#no shut

```

Figure 5. 91: Assign port 7 to 9 for *vlan UbuServer*

```
group7-SW(config-if-range)#int range gi 1/0/10-12
group7-SW(config-if-range)#sw mo ac
group7-SW(config-if-range)#sw ac vl 30
group7-SW(config-if-range)#
group7-SW(config-if-range)#no shut

```

Figure 5. 92: Assign port 10 to 12 for *vlan FedoServer*.

```

group7-SW(config-if-range)#int range gi 1/0/23-24
group7-SW(config-if-range)#sw mo ac
group7-SW(config-if-range)#sw mo tr
group7-SW(config-if-range)#sw tr na vl 5
group7-SW(config-if-range)#no sw mo ac
group7-SW(config-if-range)#no shut

```

Figure 5. 93: Assign port 23 and 24 for vlan Trunk.

Configure VLAN on Router

Step 1: Configure every inter-Vlan with their own respective IPv4 default gateway.

```

Group7-RT(config)#int g0/0.101
Group7-RT(config-subif)#en dot1q 101
Group7-RT(config-subif)#ip add 192.168.101.1
% Incomplete command.

Group7-RT(config-subif)#ip add 192.168.101.1 255.255.255.192

```

Figure 5. 94: Interface G0/0.101 (Client).

```

Group7-RT(config-subif)#int g0/0.102
Group7-RT(config-subif)#en dot1q 102
Group7-RT(config-subif)#ip add 192.168.102.1 255.255.255.192

```

Figure 5. 95: Interface G0/0.102 (AP).

```

Group7-RT(config-subif)#int g0/0.10
Group7-RT(config-subif)#en dot1q 10
Group7-RT(config-subif)#ip add 192.168.10.1 255.255.255.248

```

Figure 5. 96: Interface G0/0.10 (WinServer).

```

Group7-RT(config-subif)#int g0/0.20
Group7-RT(config-subif)#en dot1q 20
Group7-RT(config-subif)#ip add 192.168.20.1 255.255.255.248

```

Figure 5. 97: Interface G0/0.20 (UbuServer).

```

Group7-RT(config-subif)#int g0/0.30
Group7-RT(config-subif)#en dot1q 30
Group7-RT(config-subif)#ip add 192.168.30.1 255.255.255.248

```

Figure 5. 98: Interface G0/0.30 (FedoServer).

```

Group7-RT(config-subif)#int g0/0.5
Group7-RT(config-subif)#en dot1q 5
Group7-RT(config-subif)#ip add 192.168.5.1 255.255.255.248

```

Figure 5. 99: Interface G0/0.5 (Trunk).

Step 2: Configure IP-Helper on Client and Access Point Interface.

```
Group7-RT(config)#int gigabitEthernet 0/0.101
Group7-RT(config-subif)#ip helper-address 192.168.10.3
Group7-RT(config-subif) #
```

Figure 5. 100: IP-Helper on G0/0.101 (Client).

```
Group7-RT(config)#int gigabitEthernet 0/0.102
Group7-RT(config-subif)#ip h
Group7-RT(config-subif)#ip helper-address 192.168.10.3
Group7-RT(config-subif) #
```

Figure 5. 101: IP-Helper on G0/0.102 (AP).

VLSM

VLAN	Network Address	Usable IP Address	Broadcast Address	IP Server/Client	Default Gateway	Subnet Mask	Prefix
5	192.168.5.0	192.168.5.1-192.168.5.6	192.168.5.7	192.168.5.1	192.168.5.1	255.255.255.248	/29
10	192.168.10.0	192.168.10.1-192.168.10.6	192.168.10.7	192.168.10.3	192.168.10.1	255.255.255.248	/29
20	192.168.20.0	192.168.20.1-192.168.20.6	192.168.20.7	192.168.20.3	192.168.20.1	255.255.255.248	/29
30	192.168.30.0	192.168.30.1-192.168.30.6	192.168.30.7	192.168.30.3	192.168.30.1	255.255.255.248	/29
101	192.168.101.0	192.168.101.1-192.168.101.62	192.168.101.63	Within Range	192.168.101.1	255.255.255.192	/26
102	192.168.102.0	192.168.102.1-192.168.102.62	192.168.102.63	Within Range	192.168.102.1	255.255.255.192	/26

Table 4 : IP Addressing

VLAN	Name	Port Range	IPv4 Address	Sub-Interface	Device Designated	Connected Port
5	Trunk	int range fa0/24	192.168.5.1	Fa0/0.5	Cisco Integrated Router	int fa0/24
10	Windows	int range fa0/4-fa0/6	192.168.10.1	Fa0/0.10	Windows Server	int fa0/4
20	Linux	int range fa0/7-fa0/9	192.168.20.1	Fa0/0.20	Ubuntu Server	int fa0/8
30	Fedora	int range fa0/10-fa0/12	192.168.30.1	Fa0/0.30	Fedora Server	int fa0/12
101	Client	int range fa0/19-fa0/21	Within range	Fa0/0.101	Client	int fa0/18
102	Access Point	int fa0/21-23	Within range	Fa0/0.102	AP	int fa0/22

Table 5 : Port Range

5.2.5 Routing & NAT

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

```
#ip nat inside source static 192.168.10.3 200.200.201.4  
#ip nat inside source static 192.168.20.3 200.200.201.5  
#ip nat inside source static 192.168.30.3 200.200.201.6  
  
#int g0/1  
#ip address 200.200.201.7 255.255.255.240  
#ip nat outside  
  
#access-list 1 permit 192.168.101.0 0.0.0.63  
#access-list 1 permit 192.168.102.0 0.0.0.63  
  
#ip nat inside source list 1 pool G7-Pool  
#ip nat pool G7-Pool 200.200.201.1 200.200.201.7 netmask 255.255.255.240  
  
#router ospf 1  
#router-id 2.2.2.2
```

Figure 5. 102: Configuration of NAT.

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

```
interface GigabitEthernet0/1  
ip address 200.200.201.7 255.255.255.240  
ip nat outside  
ip virtual-reassembly in  
duplex auto  
speed auto
```

Figure 5. 103: List of configuration.

```
ip nat pool G7-Pool 200.200.201.1 200.200.201.7 netmask 255.255.255.240
ip nat inside source list 1 pool G7-Pool overload
ip nat inside source list 10 interface GigabitEthernet0/1 overload
ip nat inside source static 192.168.10.3 200.200.201.4
ip nat inside source static 192.168.20.3 200.200.201.5
ip nat inside source static 192.168.30.3 200.200.201.6
ip ssh version 2
!
ipv6 route 2000:FEEE:AAAA::/48 Tunnel0
ipv6 route 2018:FEEE:AAAA:F035::/64 Tunnel0
ipv6 route 2018:FEEE:AAAA:F045::/64 Tunnel0
ipv6 route 2018:FEEE:AAAA:F055::/64 Tunnel0
ipv6 route 2018:FEEE:AAAA:F100::/64 Tunnel0
ipv6 router ospf 2
  router-id 2.2.2.2
  redistribute static
!
!
!
snmp-server community public RO
snmp-server community private RW
snmp-server community umum RO
snmp-server host 192.168.101.3 public
snmp-server host 192.168.20.3 version 2c public
snmp-server host 192.168.20.3 umum
access-list 1 permit 192.168.101.0 0.0.0.63
access-list 1 permit 192.168.102.0 0.0.0.63
access-list 10 permit 192.168.0.0 0.0.127.255
access-list 10 deny  any
radius-server host 192.168.10.3 key Group7123Admin
```

Figure 5. 104: List of configuration.

5.2.6 Active Directory

AD Installation

Step 1: open Server Manager

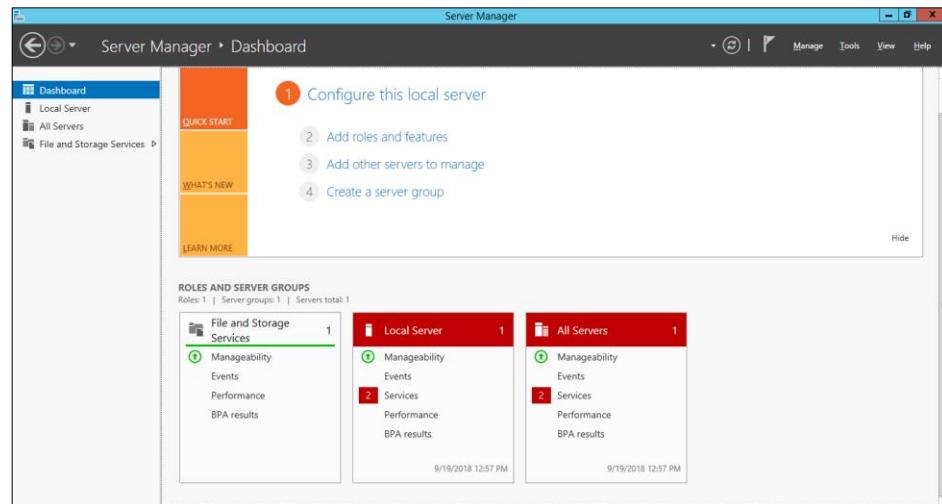


Figure 5. 105: Click Add roles and feature from server manager

Step 2: From Server Manager click on Add roles and feature

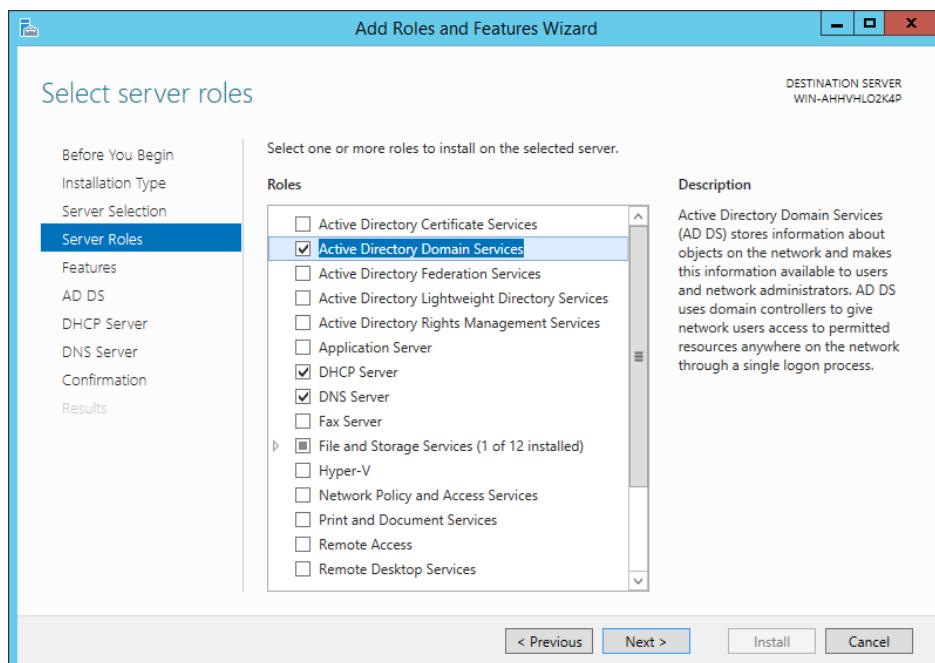


Figure 5. 106: Check on Active Directory Domain Services from Server Roles

Step 3: Then go to Server Roles and click on **Active Directory Domain Services** then **Add features**.

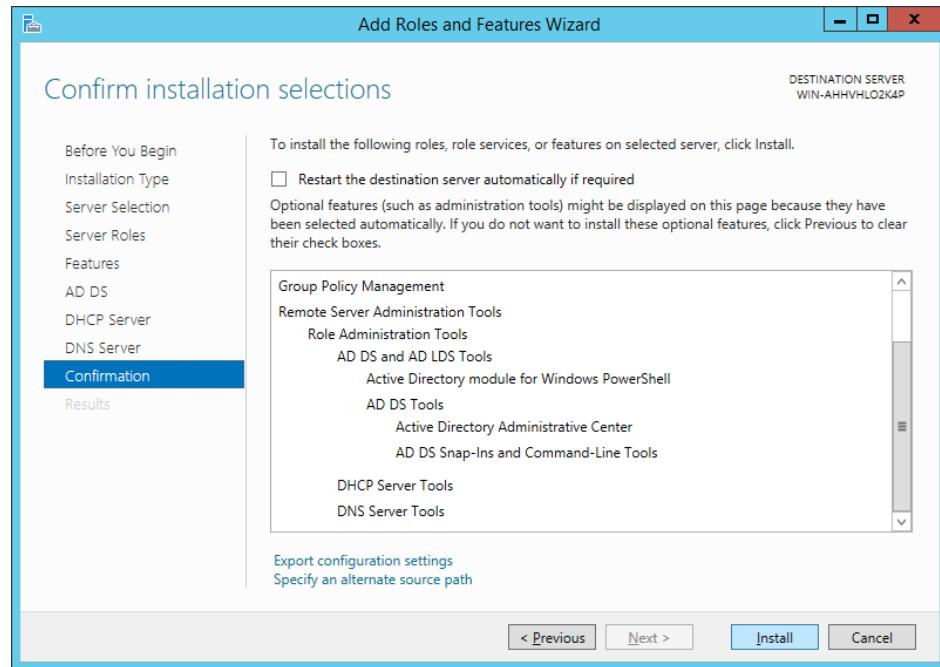


Figure 5. 107: Click on Install on the confirmation window.

Step 4: After install the services, we click flag the click on **Post-deployment Configuration** for AD domain service

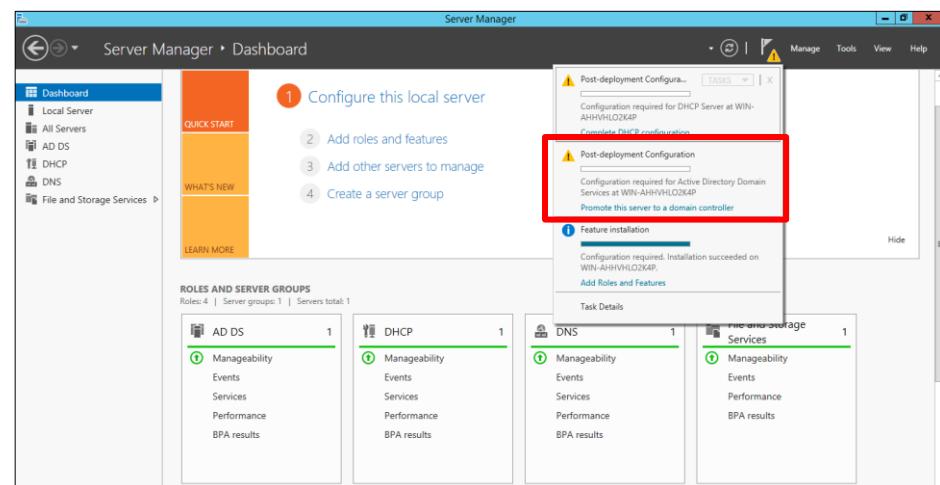


Figure 5. 108: Click on Post-deployment Configuration

Step 5: Click **add a new forest** then specify our root domain name as group7.com, then we click **next**

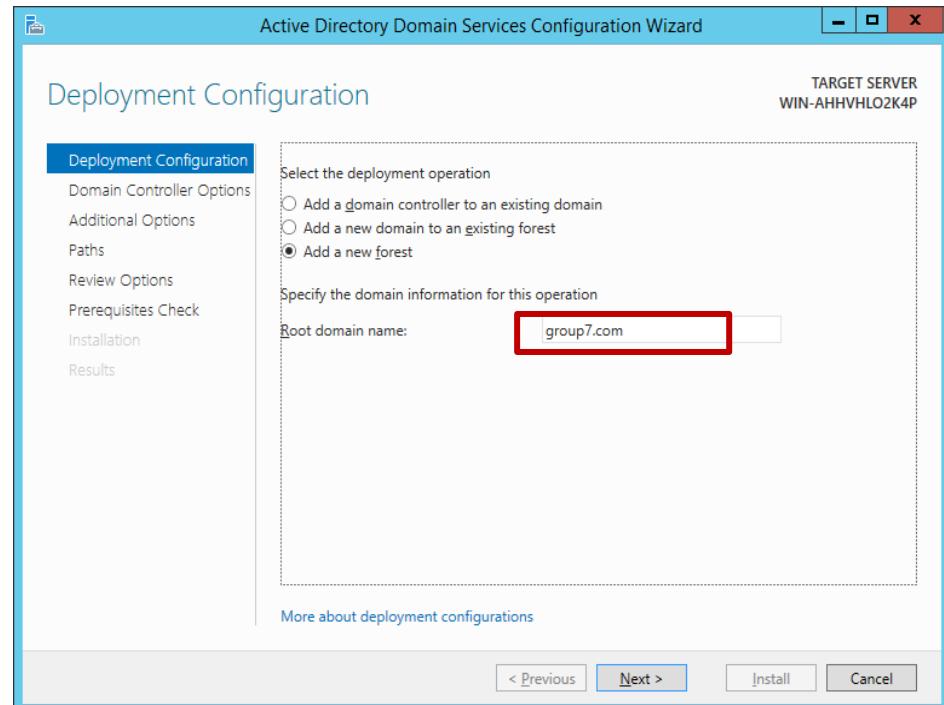


Figure 5. 109: Specify the foot domain name as group7.com

Step 6: password and confirm password. Then we click next

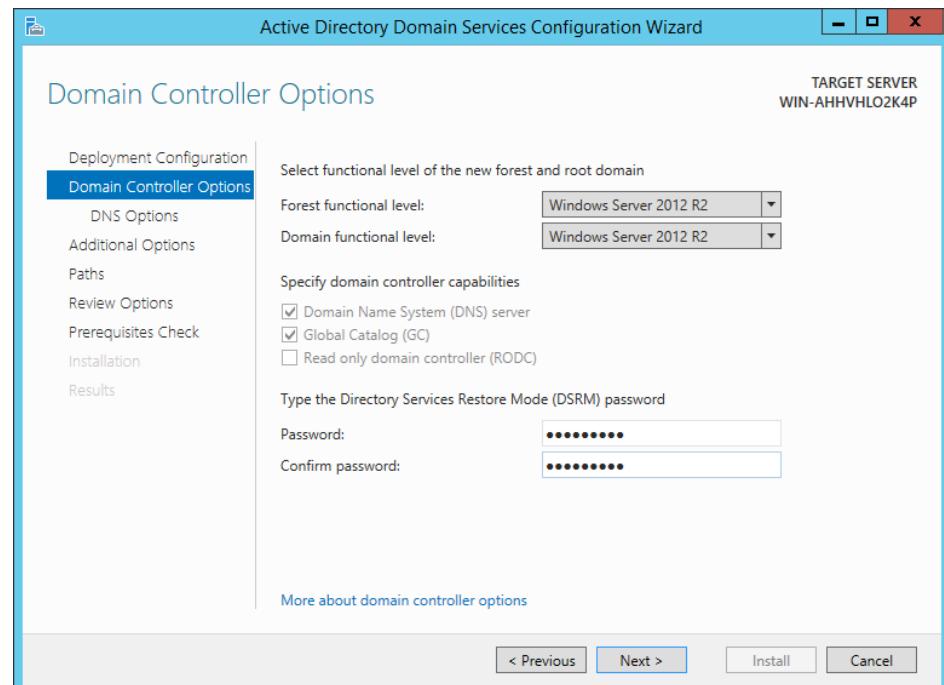


Figure 5. 110: Assign Password for the Directory

Step 7: Form DNS Options click on Next.

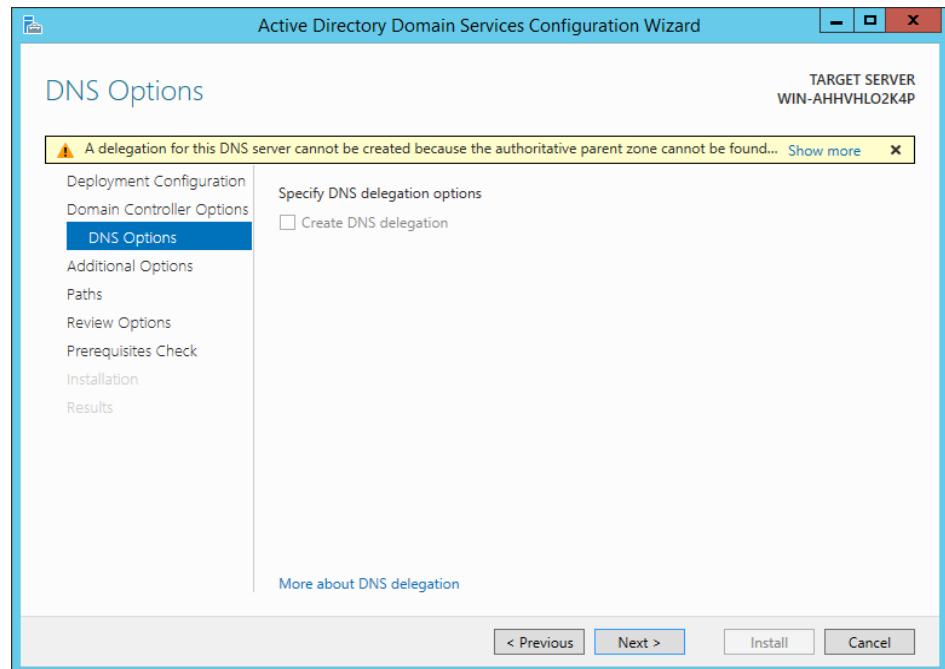


Figure 5. 111 : DNS Options

Step 8: Go to Additional Options insert our domain name GOURP7 and click next

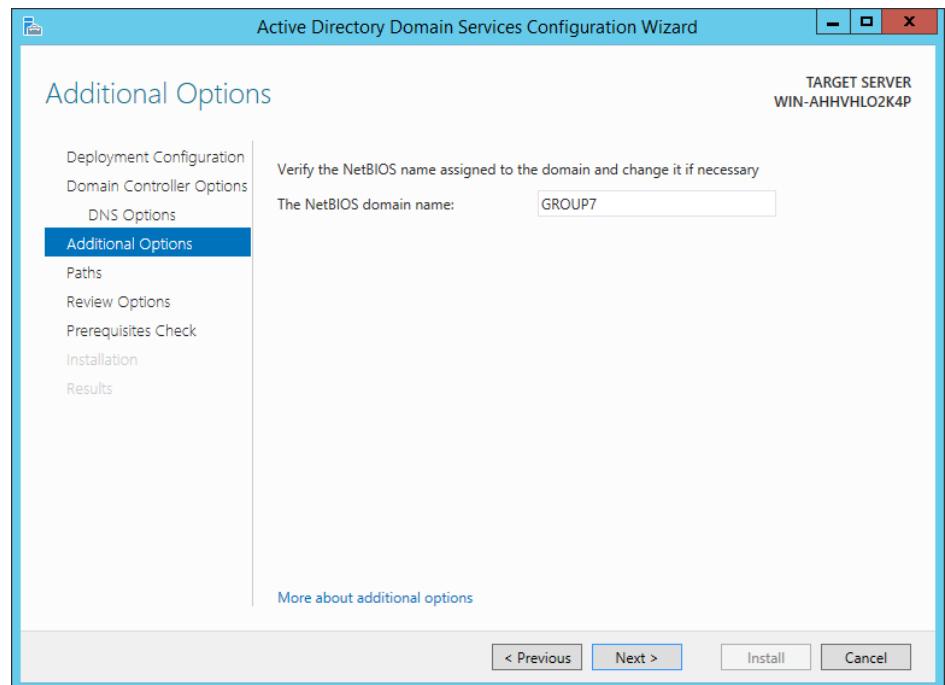


Figure 5. 112 : Active Directory (Additional Options)

Step 9: After All Prerequisites Check passed successfully click **Install**

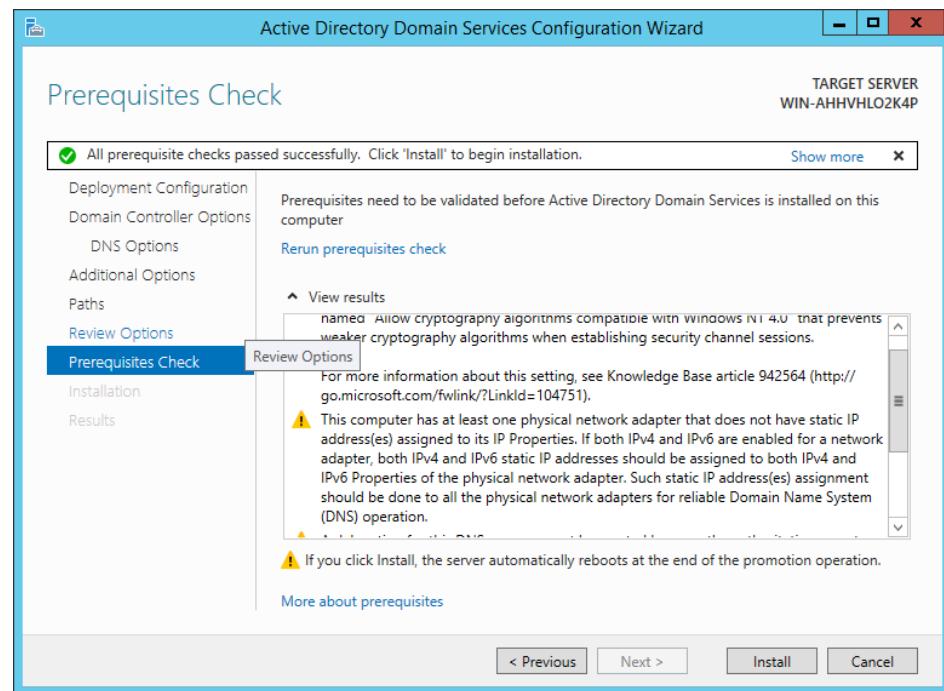


Figure 5. 113 : All Prerequisites Check

Configuration of Active Directory Users and Computers

Step 1: After restart Windows server, From Server Manager click **Tools** then **Active Directory Users and Computers**

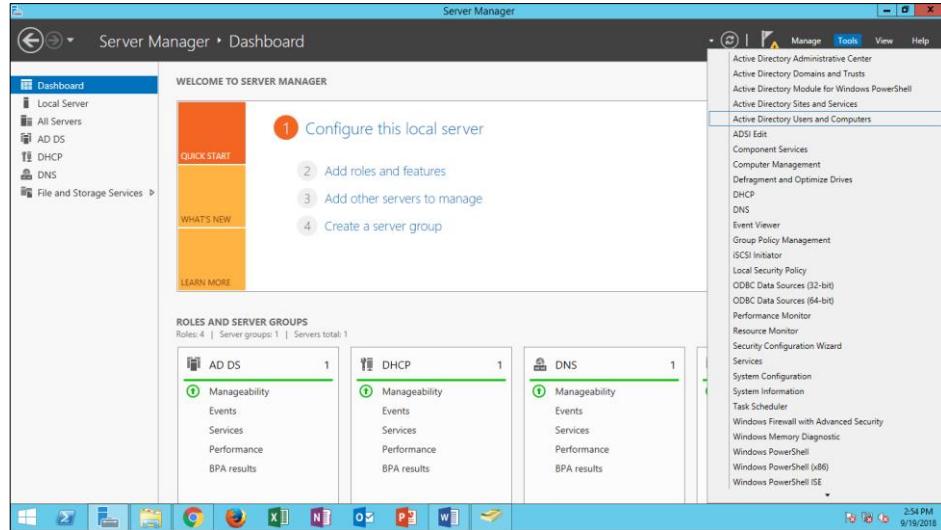


Figure 5. 114: Open Active Directory Users and Computers

Step 2: From **group7.com/Managed Service Accounts/ Users**, Click on the right and click **new** then **computer**

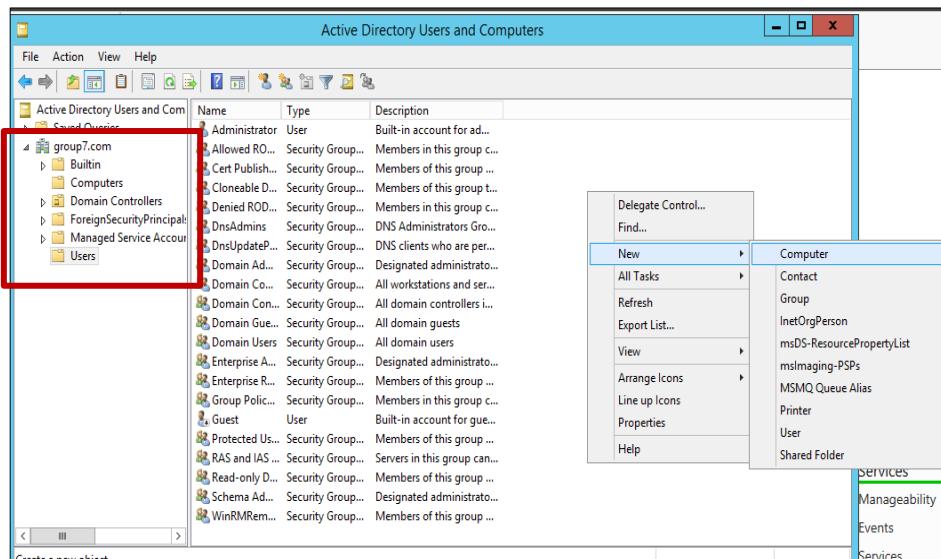


Figure 5. 115: Adding a computer to our domain controller

Step 3: Now, we create a new organizational Unit and called is as **Group7**

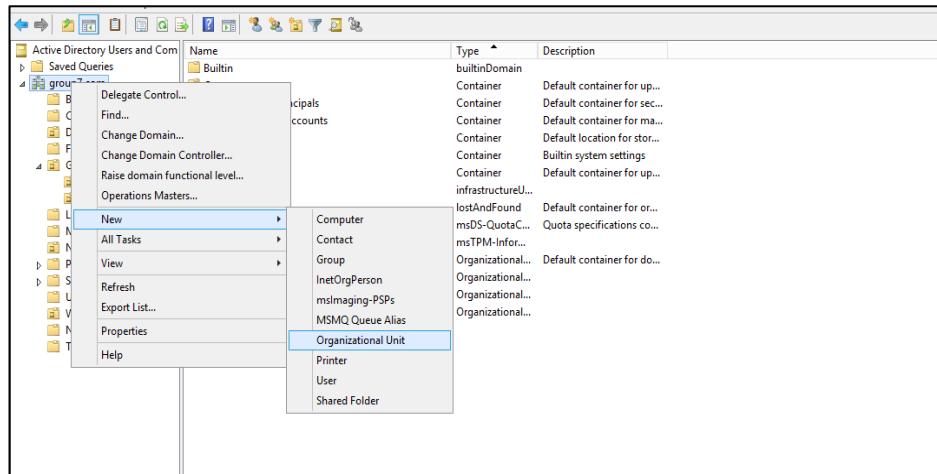


Figure 5. 116 : Creating Group7 organizational Unit.

Step 4: Click right and choose New then User

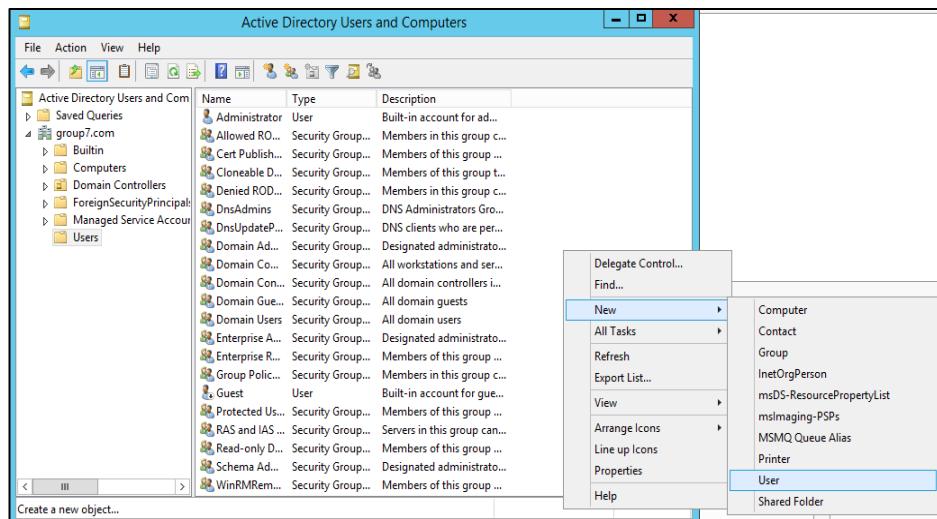


Figure 5. 117 : Adding User to our domain controller

Step 5: After that, a pop-up will appear as follow. In the First name column enter our user name group7admin follow by the User logon name, which is the same. Then, click Next.

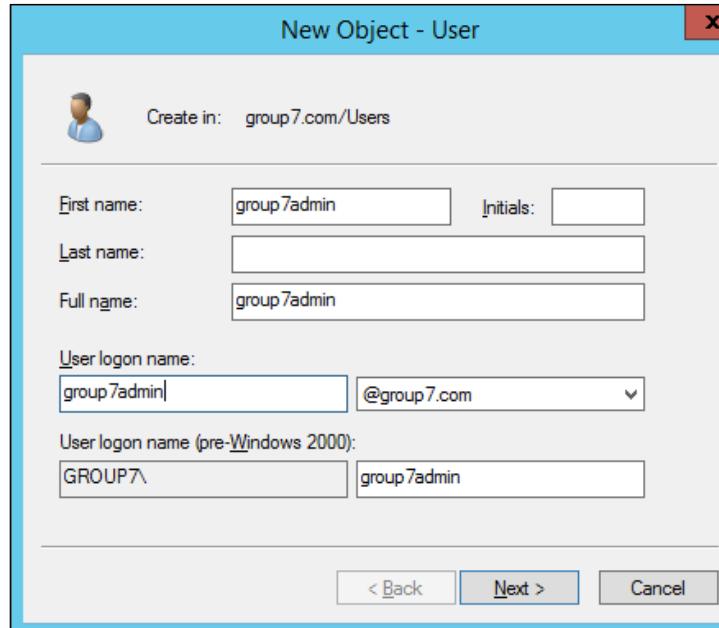


Figure 5. 118 : Setup the information

Step 6: In the next section, enter the Password and tick the Password never expires check box for easy access in each time you wish to login. Then, click Next

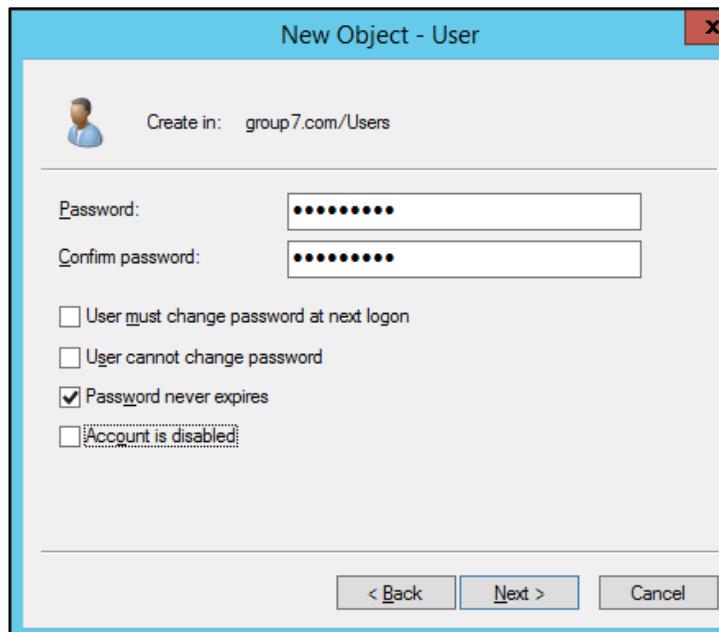


Figure 5. 119 : Setup password of the New User

Step 7: Now, we will Add each and every user of group Follow the step from Figure Creating Group7 until Figure Adding User After seven. There will be RAHMAN, SYDIDA, NISA, DAUS, AZMI, RAIHAN, FAHMY users.

Name	Type
Rahman	User
Azmi	User
Daus	User
Nisa	User
Raihan	User
Syida	User
Fahmy	User

Figure 5. 120 : Show all created users.

Step 8: Enter the Group name and click OK. The first group name would be BITC, follow by BITZ.

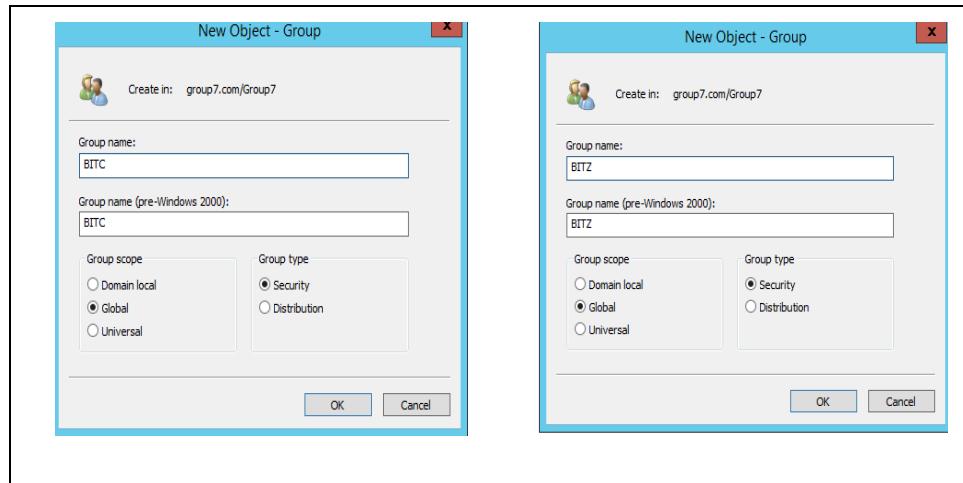


Figure 5. 121 : Create other Group

Step 9: Now, we will create new groups for all the new users. Right-click in the Users and Select New Group.

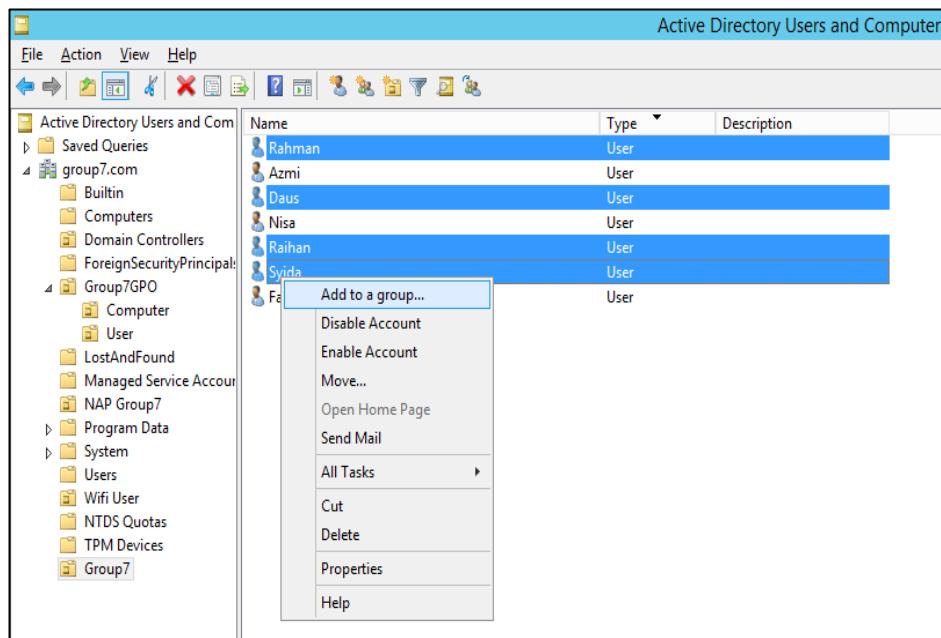


Figure 5. 122 : Navigate to Group and then New.

Step 10: Enter any short-form of our newly created group, for this one would be BITC (for BITC) and Click Check Names.

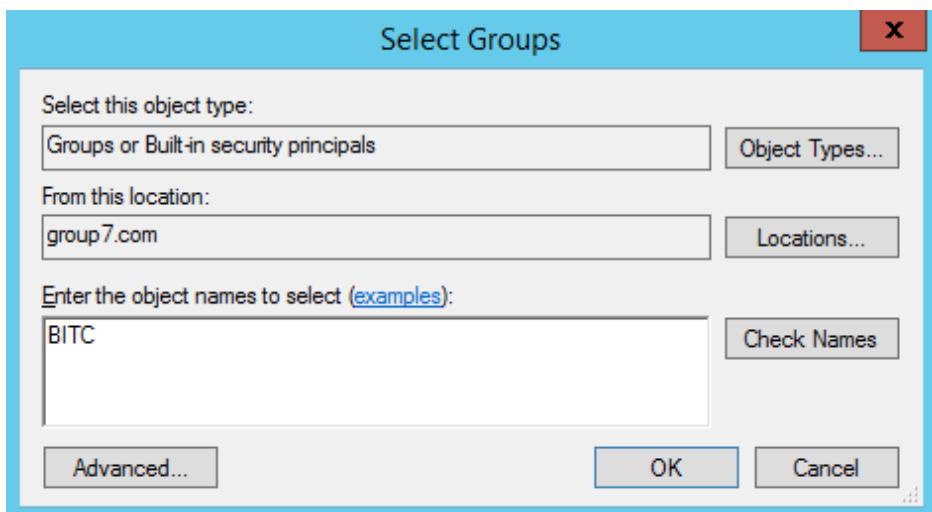


Figure 5. 123 : Select then click OK to continue.

Step 11: Highlighting the selected users again. Right-click and go to Add to a group.

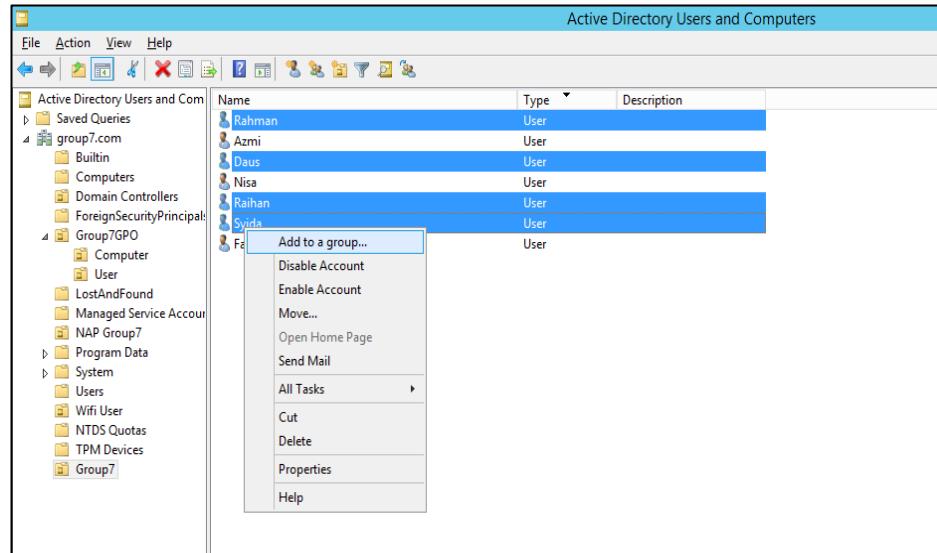


Figure 5. 124 : Add another user to Group.

Step 12: There will appear **BITZ** in the selected available list. Choose it and click **OK**.

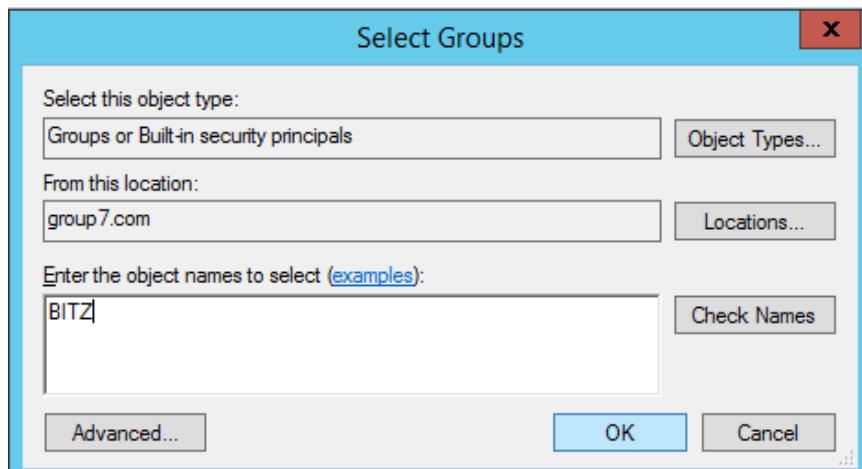


Figure 5. 125 : Select then click OK to continue.

Step 13: Now, we need to Create a new folder that can store each and every users profile. The folder is created in Local Disk (C :) and named SharedFolderProfile. Another new folder will be created together with it, which is SharedFolderHome for the home directory

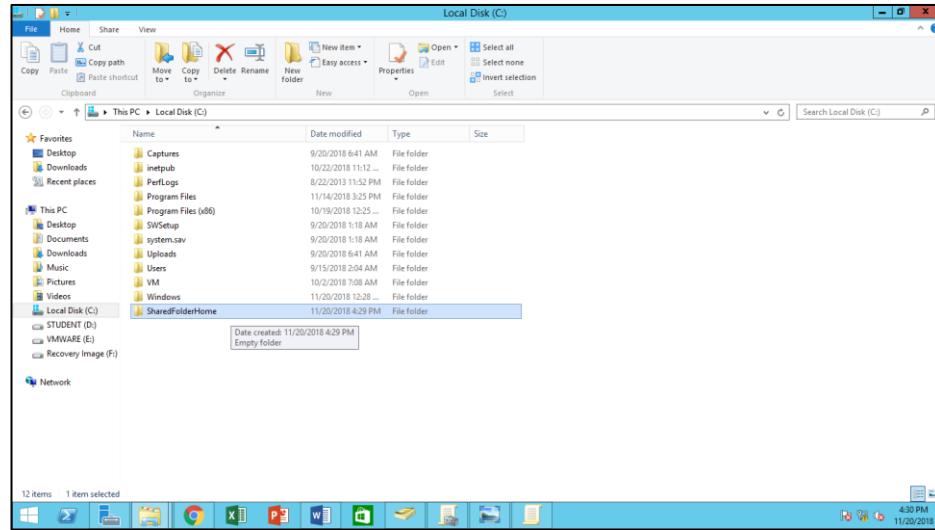


Figure 5. 126 : Show a new folder that can store SharedFolderHome.

Also Should SharedFolderProfile also near be created same SharedFolderHome.

Step 14: To Share the sharedFolderHome directory, Right-click and select Properties.

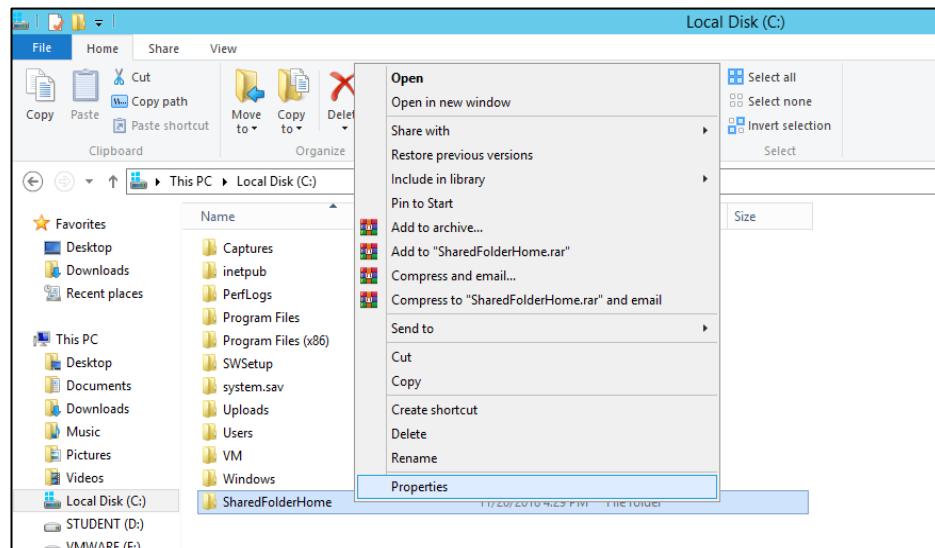


Figure 5. 127 : Navigate to Properties.

Step 15: Choose the Sharing tab and click on Share.

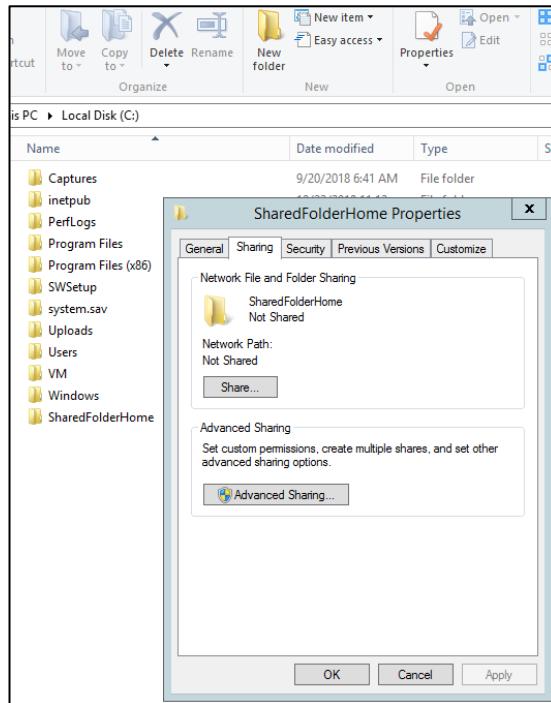


Figure 5. 128 : Navigate to Sharing tab and click on Share

Step 16: In the name column, Click on the arrow and choose **Everyone**. Click AND Permission Level to read and write.
Repeat from Step 13 until Step 16 for the shared Folder Profile directory which we had created just now

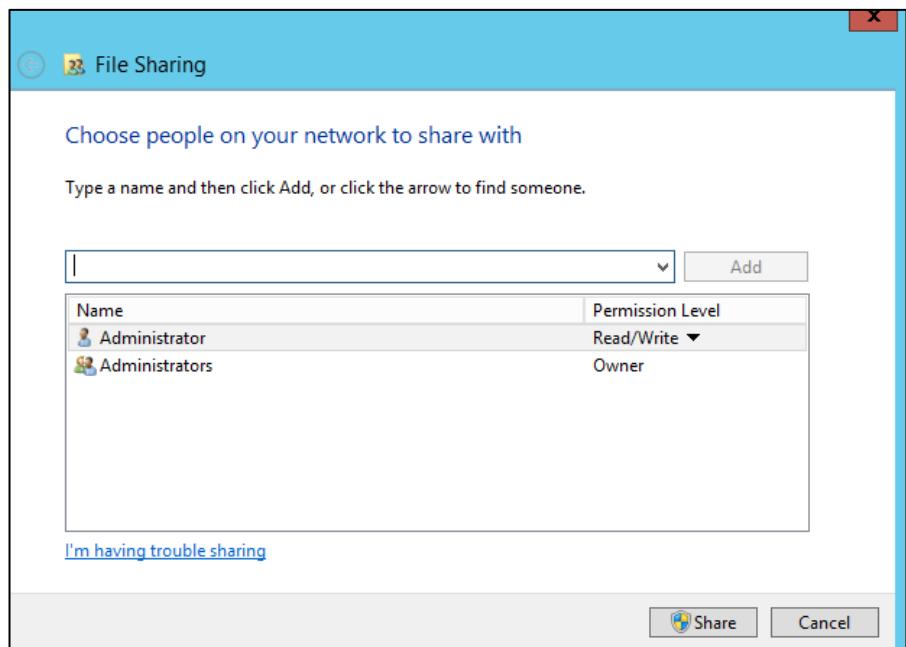


Figure 5. 129 : Click on the arrow and choose **Everyone** and to read and write for permission level

Step 17: Go back to the Active Directory Users and Computers and highlight all the new users that had been created which are RAHMAN, SYDIDA, NISA, DAUS, AZMI, RAIHAN, and FAHMY. Go to the Profile tab and Tick at the Profile path: Then, Enter \\winser\sharedFolderProfile%\username% for the path. Tick another box below which is the Home folder. Select the Connect radio button and enter \\winser\sharedFolderHome%\username% for its path. After that, click Apply.

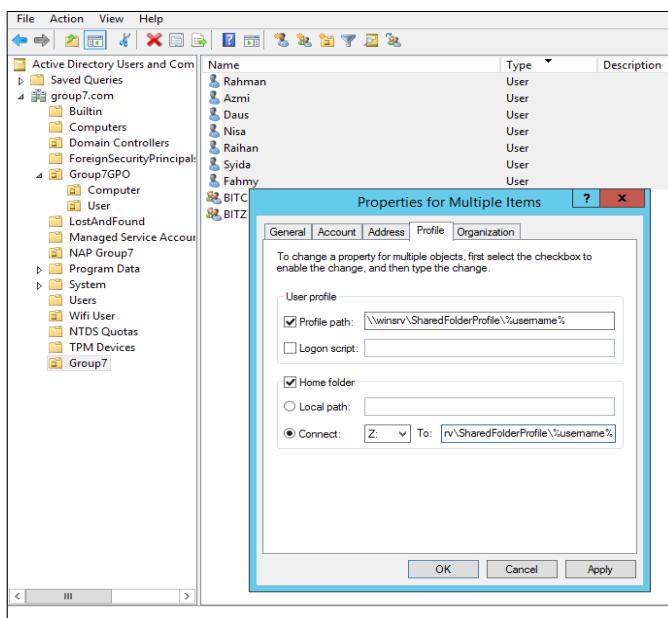


Figure 5. 130 : Go to the Profile tab and tick at the Profile path.

Step 18: To check the result after specifying the path in the profile properties, go to the location where the sharedFolderHome have been created. Doubleclick on the folder and all of the users names will appear in it.

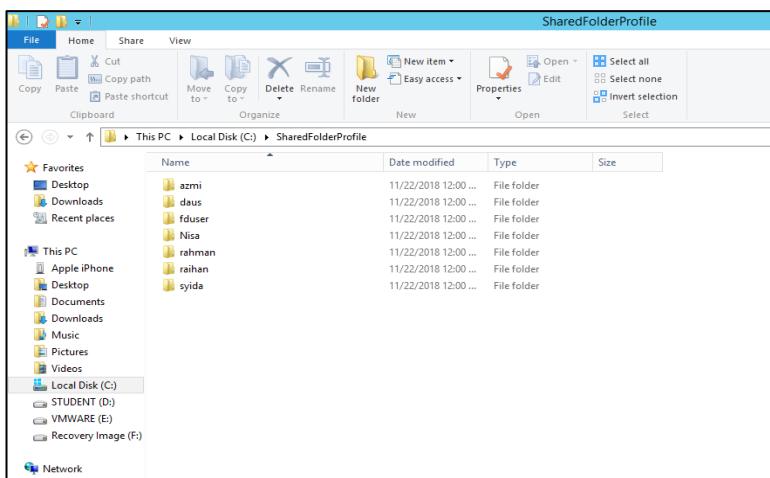


Figure 5. 131 : Check the result after specifying the

path in the profile properties
GPO (Group Police for network.)

Step 1: Open group Policy window create new group Policy click on Create a GPO in this domain.... BITC_GPO and other one is BITZ_GPO.

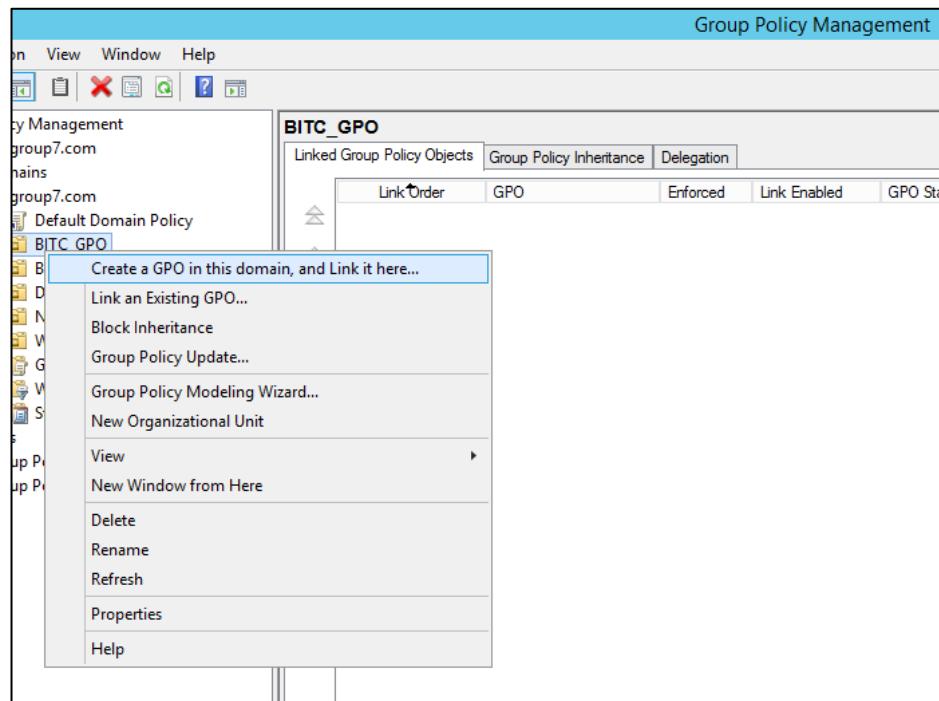


Figure 5. 132 : Create a new group policy

Step 2: We create our first group policy for BITC_GPO for BITC group and with same way we created BITZ_GPO.

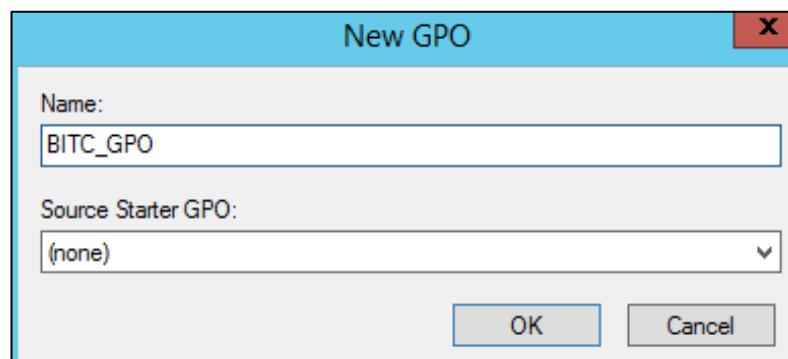


Figure 5. 133 : Create group policy for BITC

Step 3: Then we linked Our BITC_GPO with BITC Organizational Unit.

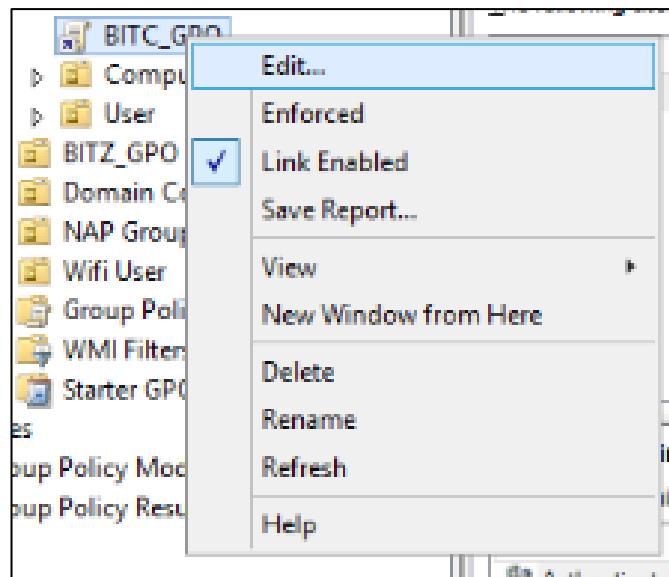


Figure 5. 134 : Show that BITC_GPO is linked

Step 4: Then we linked Our BITZ_GPO with BITC Organizational Unit

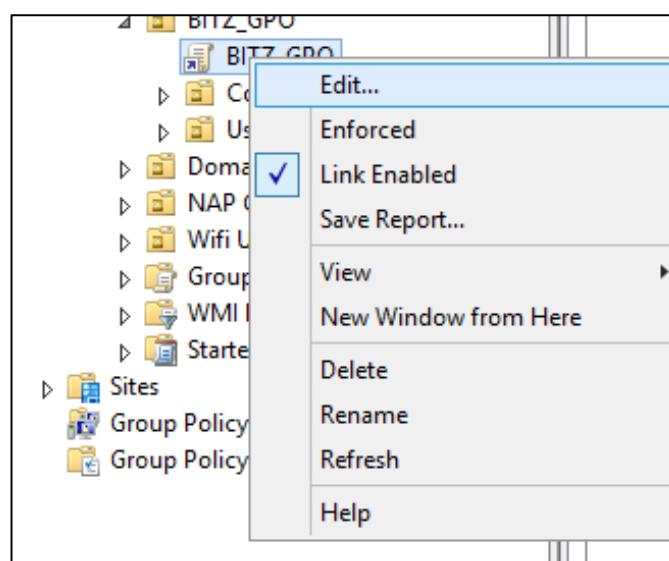


Figure 5. 135 : Show that BITZ_GPO is linked

Step 5: First we start with BITC_GPO, we made our policy for BITC users to not be able to use any storage device, editing the BITC_GPO

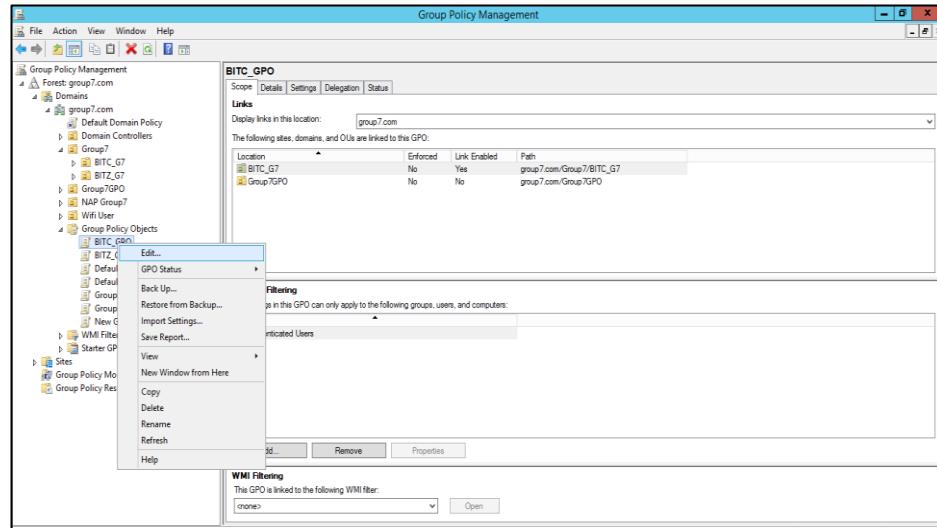


Figure 5. 136 : Editing BITC_GPO file.

Step 6: We enable the All Removable Storage Classes Deny all access.

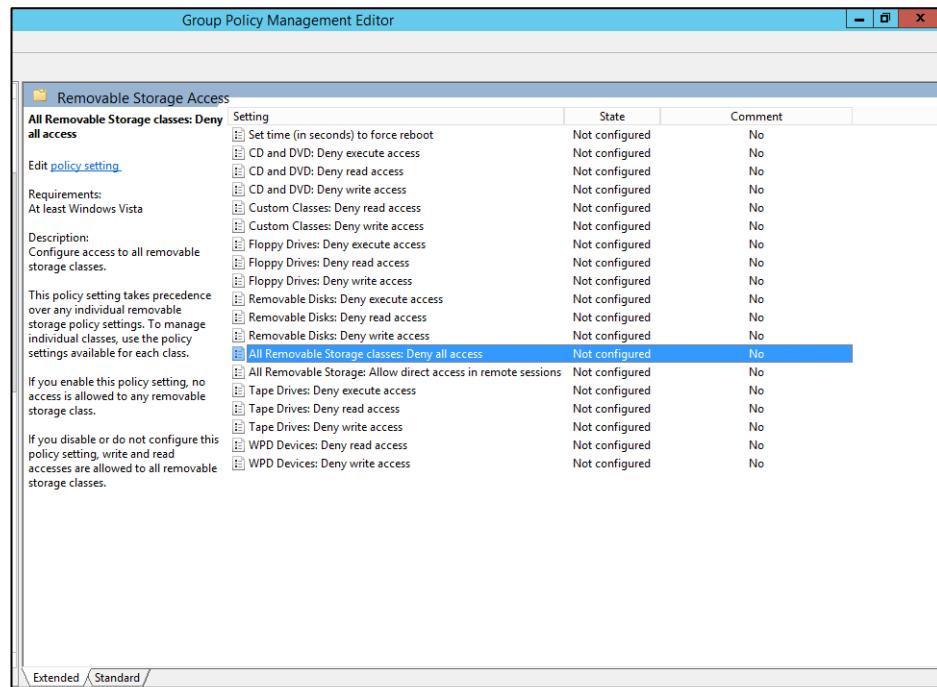


Figure 5. 137 : Click on All Removable Storage classes Deny all access.

Step 7: In the All Removable Storage etc. window, we select on **Enabled** an then **OK**

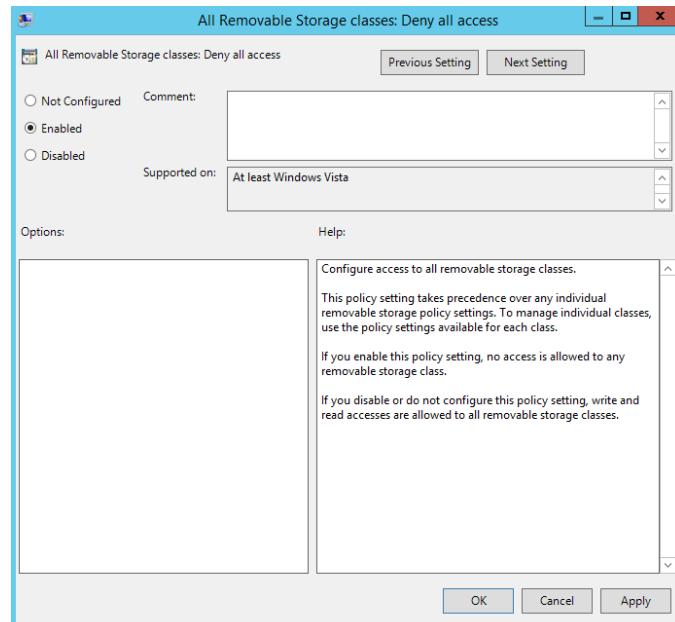


Figure 5. 138 : Enabled denying all removable devices.

Step 8: Second policy for **BITC B** is to not allow password to be saved for more security for make the network more secure.

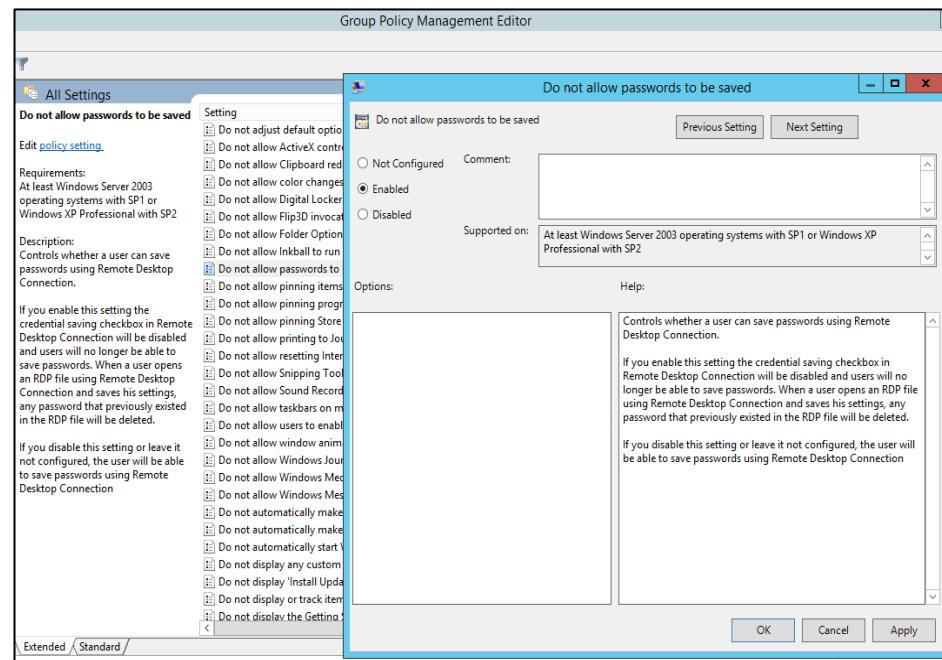


Figure 5. 139 : Enabling the policy to not allow password to be saved.

Step 9: Now for BITZ user we have created two policy, the first is not allowing the access of storage device and maximum the password age to 40 days.

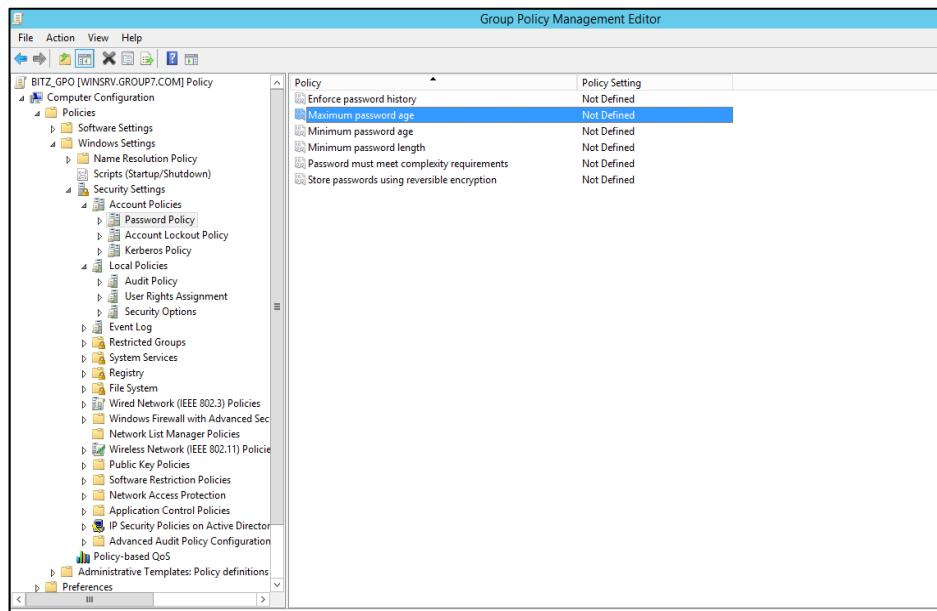
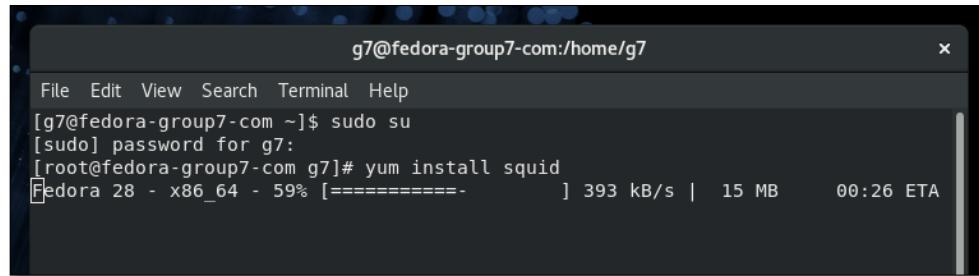


Figure 5. 140 : Maximum the password age for BITZ users.

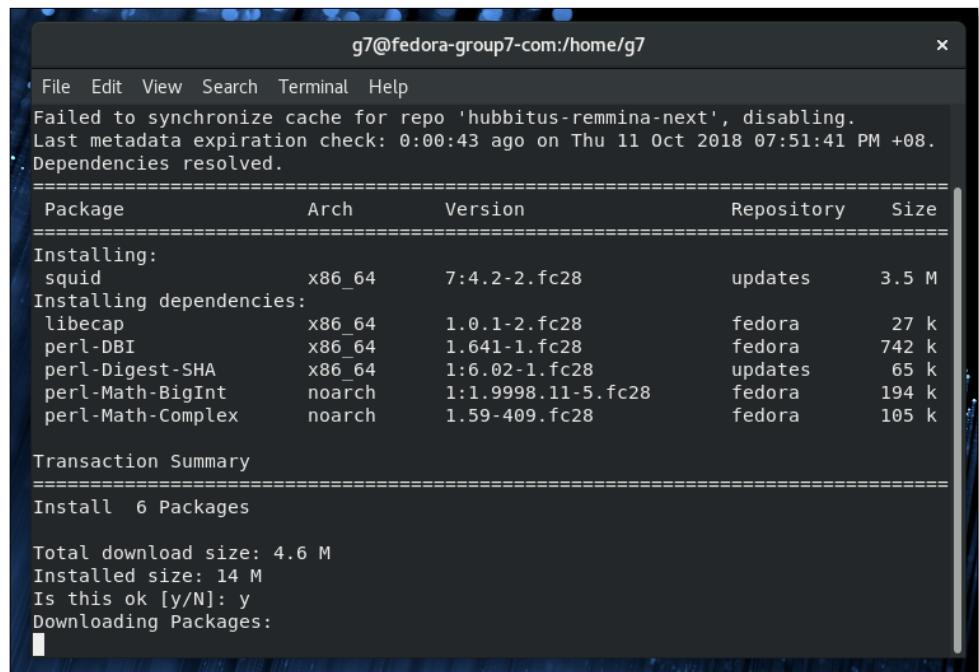
5.2.7 Proxy Server

Step 1: Open the terminal in Fedora, and then **install** squid packages with command “**yum install squid**”, then click Enter. “Is this ok?” type **y**.



```
g7@fedora-group7-com:/home/g7
File Edit View Search Terminal Help
[g7@fedora-group7-com ~]$ sudo su
[sudo] password for g7:
[root@fedora-group7-com g7]# yum install squid
Fedora 28 - x86_64 - 59% [=====] 393 kB/s | 15 MB      00:26 ETA
```

Figure 5. 141 : Install Squid



```
g7@fedora-group7-com:/home/g7
File Edit View Search Terminal Help
Failed to synchronize cache for repo 'hubbitus-remmina-next', disabling.
Last metadata expiration check: 0:00:43 ago on Thu 11 Oct 2018 07:51:41 PM +08.
Dependencies resolved.
=====
Package          Arch    Version       Repository   Size
=====
Installing:
squid           x86_64  7:4.2-2.fc28     updates      3.5 M
Installing dependencies:
libcap           x86_64  1.0.1-2.fc28     fedora      27 k
perl-DBI         x86_64  1.641-1.fc28    fedora     742 k
perl-Digest-SHA x86_64  1:6.02-1.fc28   updates      65 k
perl-Math-BigInt noarch   1:1.9998.11-5.fc28 fedora     194 k
perl-Math-Complex noarch   1.59-409.fc28   fedora     105 k
Transaction Summary
=====
Install 6 Packages

Total download size: 4.6 M
Installed size: 14 M
Is this ok [y/N]: y
Downloading Packages:
```

Figure 5. 142 : Downloading package

Step 2: Edit squid configuration file, insert the squid directory with command “**cd /etc/squid**”. After that, copy the file squid configuration as the backup with other name “**cp squid.conf squid.conf_ori**”. Edit the configuration with command “**vi squid.conf**”.

```

g7@fedora-group7-com:/etc/squid
File Edit View Search Terminal Help
Installing      : libecap-1.0.1-2.fc28.x86_64          5/6
Running scriptlet: libecap-1.0.1-2.fc28.x86_64          5/6
Running scriptlet: squid-7:4.2-2.fc28.x86_64          6/6
Installing      : squid-7:4.2-2.fc28.x86_64          6/6
Running scriptlet: squid-7:4.2-2.fc28.x86_64          6/6
Verifying       : squid-7:4.2-2.fc28.x86_64          1/6
Verifying       : libecap-1.0.1-2.fc28.x86_64          2/6
Verifying       : perl-DBI-1.641-1.fc28.x86_64          3/6
Verifying       : perl-Math-BigInt-1:1.9998.11-5.fc28.noarch 4/6
Verifying       : perl-Math-Complex-1.59-409.fc28.noarch 5/6
Verifying       : perl-Digest-SHA-1:6.02-1.fc28.x86_64          6/6

Installed:
squid.x86_64 7:4.2-2.fc28
libecap.x86_64 1.0.1-2.fc28
perl-DBI.x86_64 1.641-1.fc28
perl-Digest-SHA.x86_64 1:6.02-1.fc28
perl-Math-BigInt.noarch 1:1.9998.11-5.fc28
perl-Math-Complex.noarch 1.59-409.fc28

Complete!
[root@fedora-group7-com g7]# cd /etc/squid
[root@fedora-group7-com squid]# cp squid.conf squid.conf_ori
[root@fedora-group7-com squid]# vi squid.conf

```

Figure 5. 143 : Edit squid configuration

Step 3: Edit squid configuration file. Run command #vi squid.conf. Change http access deny all to http access allow all. Then, start the squid service.

```

g7@fedora-group7-com:/etc/squid
File Edit View Search Terminal Help
acl blockdomains dstdomain "/etc/squid/block.domain.acl"
http_access deny blockdomains

acl blockurl url_regex "/etc/squid/block.keywords.acl"
http_access deny blockurl

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localnet
http_access allow localhost

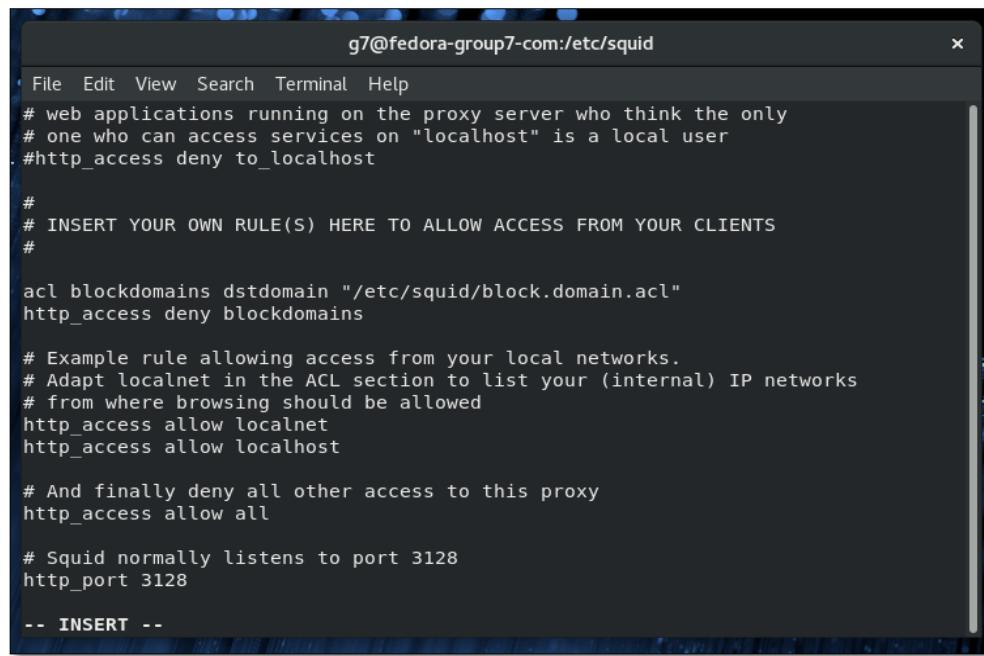
# And finally deny all other access to this proxy
http_access deny all

# Squid normally listens to port 3128
http_port 3128
#
# Uncomment and adjust the following to add a disk cache directory.
#cache_dir ufs /var/spool/squid 100 16 256

# Leave core dumps in the first cache dir
coredump_dir /var/spool/squid

```

Figure 5. 144 : File of squid configuration



The screenshot shows a terminal window titled "g7@fedora-group7-com:/etc/squid". The window contains the squid configuration file (squid.conf). The file includes comments about web applications running on the proxy server, rules for access control (allowing localhost and specific local networks while denying others), and port settings (listening on port 3128). A section at the bottom is labeled "-- INSERT --".

```
File Edit View Search Terminal Help
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#

acl blockdomains dstdomain "/etc/squid/block.domain.acl"
http_access deny blockdomains

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localnet
http_access allow localhost

# And finally deny all other access to this proxy
http_access allow all

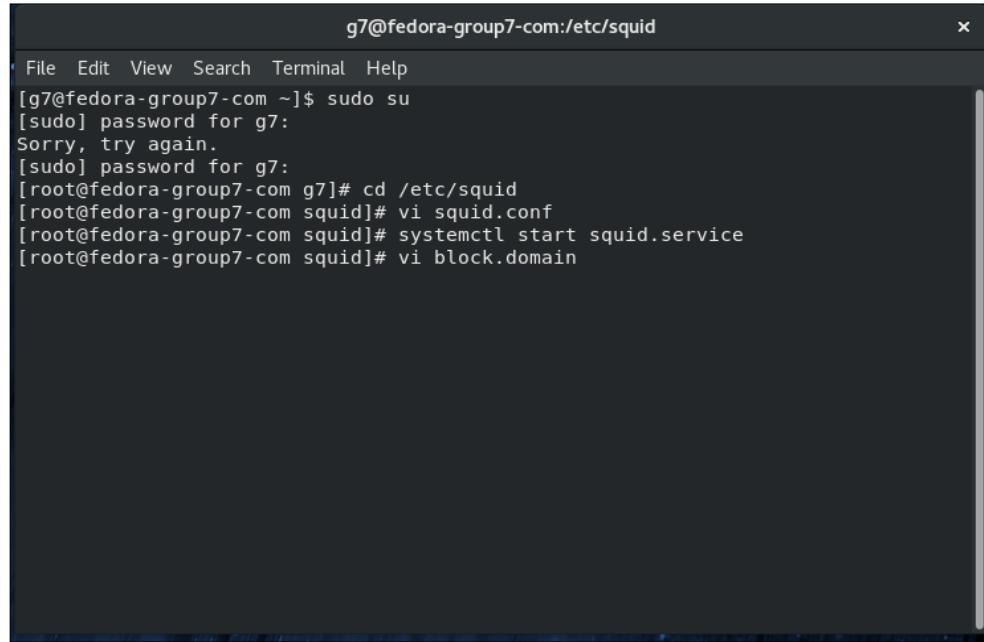
# Squid normally listens to port 3128
http_port 3128

-- INSERT --
```

Figure 5. 145 : Http port

Step 4: Restart the services run command “**systemctl start squid.service**”.

Then, edit block.domain with command “**vi block.domain**”.

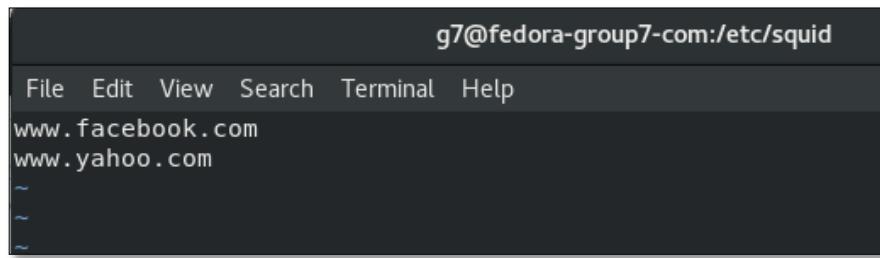


The screenshot shows a terminal window titled "g7@fedora-group7-com:/etc/squid". The window displays a command-line session where the user runs "sudo su" to become root, changes directory to /etc/squid, edits the squid configuration file ("squid.conf") with "vi", starts the squid service using "systemctl start squid.service", and then edits the "block.domain" file with "vi".

```
File Edit View Search Terminal Help
[g7@fedora-group7-com ~]$ sudo su
[sudo] password for g7:
Sorry, try again.
[sudo] password for g7:
[root@fedora-group7-com g7]# cd /etc/squid
[root@fedora-group7-com squid]# vi squid.conf
[root@fedora-group7-com squid]# systemctl start squid.service
[root@fedora-group7-com squid]# vi block.domain
```

Figure 5. 146 : Edit block domain

Step 5: Add the websites.

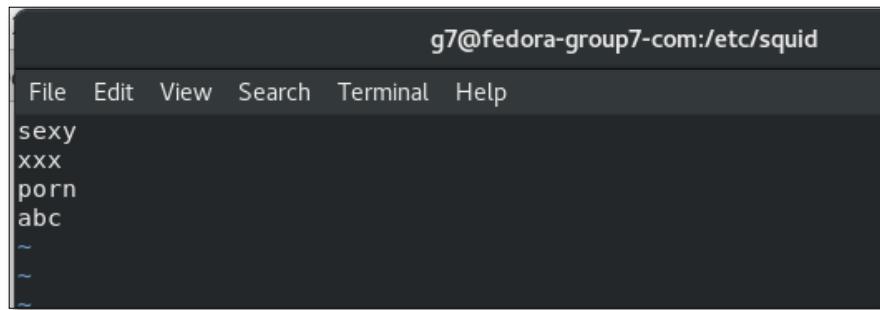


g7@fedora-group7-com:/etc/squid

```
File Edit View Search Terminal Help
www.facebook.com
www.yahoo.com
~
```

Figure 5. 147 : Websites

Step 6: To add keywords, run command “**vi keywords.acl**”. Then, insert keywords.

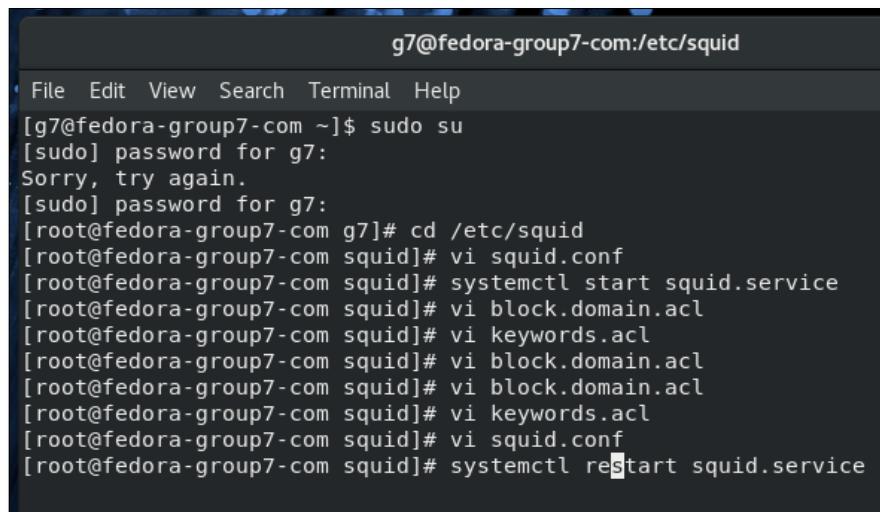


g7@fedora-group7-com:/etc/squid

```
File Edit View Search Terminal Help
sexy
xxx
porn
abc
~
```

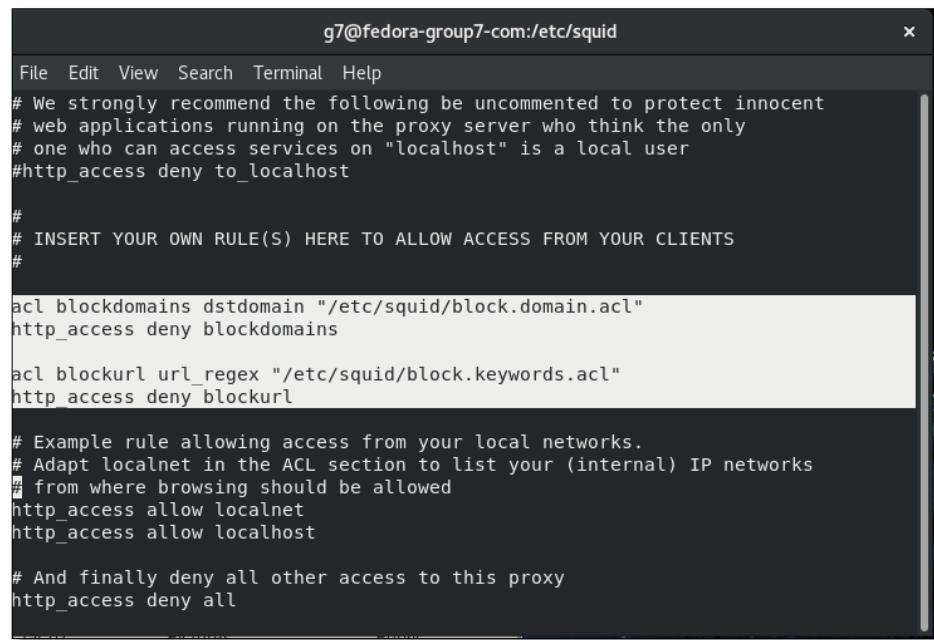
Figure 5. 148 : Keywords

Step 7: If you have a long list of domain names, create a file “**vi squid.conf**” and put domain name one per line and add below rule in squid configuration file. After making changing, let’s restart Squid service to reload the configuration changes run command “**systemctl restart squid.service**”.



```
g7@fedora-group7-com:/etc/squid
File Edit View Search Terminal Help
[g7@fedora-group7-com ~]$ sudo su
[sudo] password for g7:
Sorry, try again.
[sudo] password for g7:
[root@fedora-group7-com g7]# cd /etc/squid
[root@fedora-group7-com squid]# vi squid.conf
[root@fedora-group7-com squid]# systemctl start squid.service
[root@fedora-group7-com squid]# vi block.domain.acl
[root@fedora-group7-com squid]# vi keywords.acl
[root@fedora-group7-com squid]# vi block.domain.acl
[root@fedora-group7-com squid]# vi block.domain.acl
[root@fedora-group7-com squid]# vi keywords.acl
[root@fedora-group7-com squid]# vi squid.conf
[root@fedora-group7-com squid]# systemctl restart squid.service
```

Figure 5. 149 : Restart service



The screenshot shows a terminal window titled "g7@fedora-group7-com:/etc/squid". The window contains the configuration file for the Squid proxy server. The code is as follows:

```
File Edit View Search Terminal Help
# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#

acl blockdomains dstdomain "/etc/squid/block.domain.acl"
http_access deny blockdomains

acl blockurl url_regex "/etc/squid/block.keywords.acl"
http_access deny blockurl

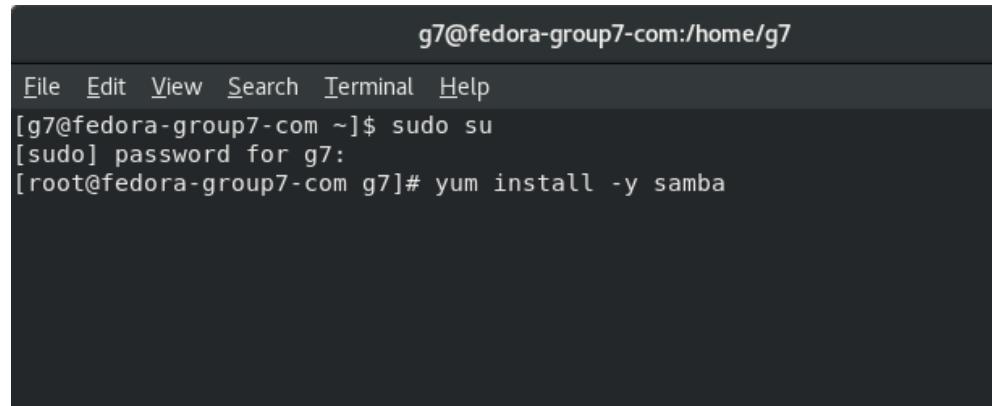
# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localnet
http_access allow localhost

# And finally deny all other access to this proxy
http_access deny all
```

Figure 5. 150 : File of squid configuration

5.2.8 Samba

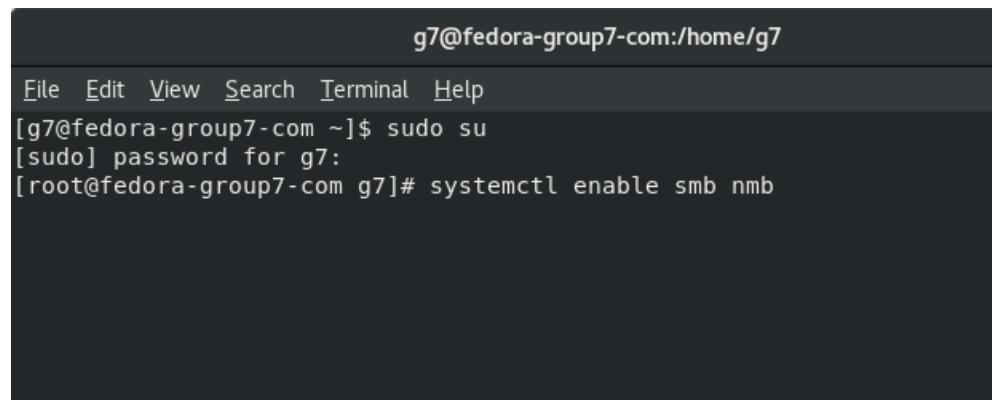
Step 1: First, use yum to install samba package



```
g7@fedora-group7-com:/home/g7
File Edit View Search Terminal Help
[g7@fedora-group7-com ~]$ sudo su
[sudo] password for g7:
[root@fedora-group7-com g7]# yum install -y samba
```

Figure 5. 151 : Install samba

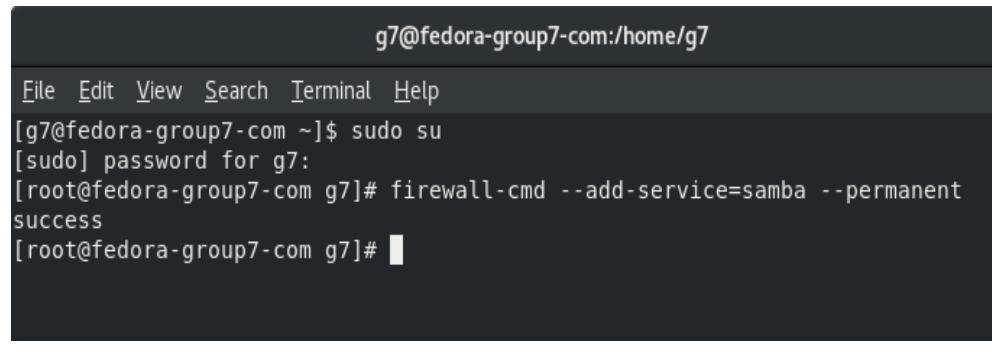
Step 2: Enable the Samba and Netbios Nameservices



```
g7@fedora-group7-com:/home/g7
File Edit View Search Terminal Help
[g7@fedora-group7-com ~]$ sudo su
[sudo] password for g7:
[root@fedora-group7-com g7]# systemctl enable smb nmb
```

Figure 5. 152 : Enable smb

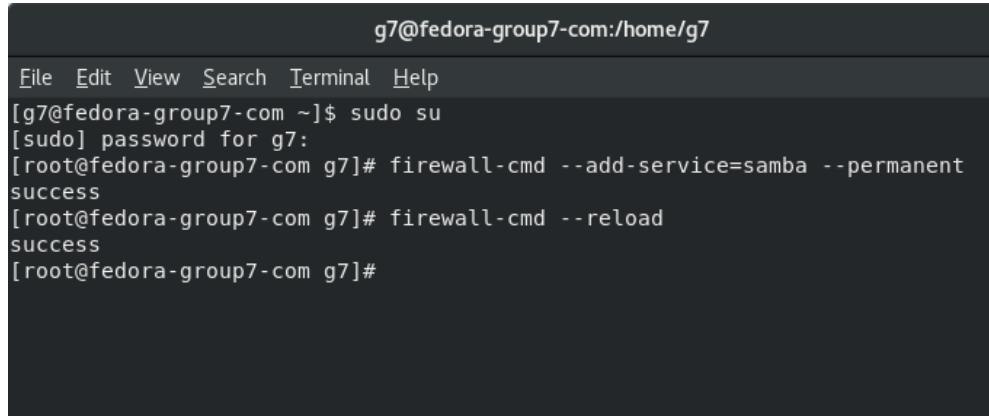
Step 3: Set the firewall to allow samba to work



```
g7@fedora-group7-com:/home/g7
File Edit View Search Terminal Help
[g7@fedora-group7-com ~]$ sudo su
[sudo] password for g7:
[root@fedora-group7-com g7]# firewall-cmd --add-service=samba --permanent
success
[root@fedora-group7-com g7]# █
```

Figure 5. 153 : Allow samba to work

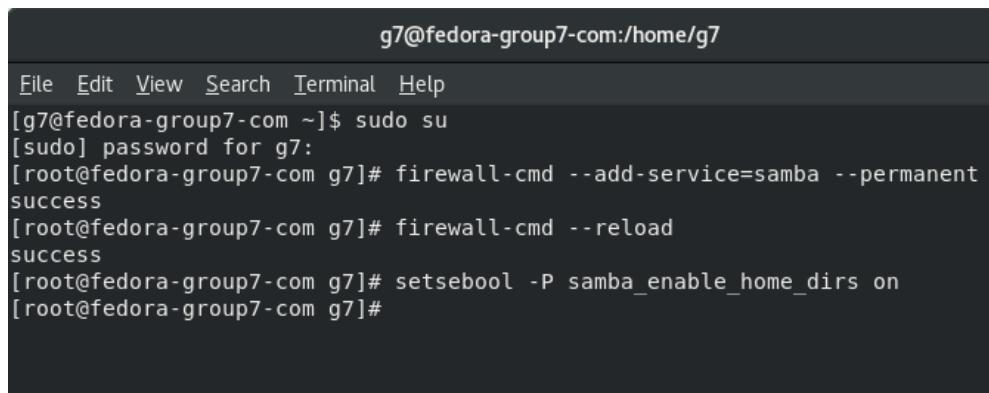
Step 4: Open port with using service file of firewall-cmd



```
g7@fedora-group7-com:/home/g7
File Edit View Search Terminal Help
[g7@fedora-group7-com ~]$ sudo su
[sudo] password for g7:
[root@fedora-group7-com g7]# firewall-cmd --add-service=samba --permanent
success
[root@fedora-group7-com g7]# firewall-cmd --reload
success
[root@fedora-group7-com g7]#
```

Figure 5. 154 : Open port

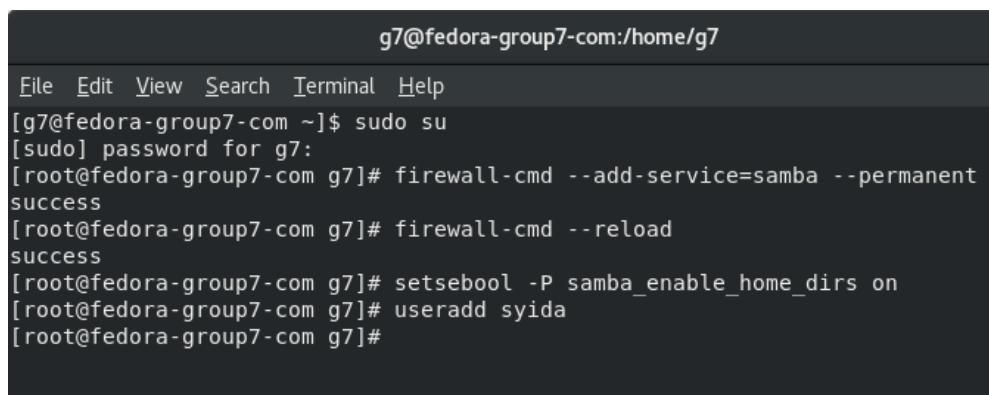
Step 5: Enable access to home directory without samba_share_t labelA



```
g7@fedora-group7-com:/home/g7
File Edit View Search Terminal Help
[g7@fedora-group7-com ~]$ sudo su
[sudo] password for g7:
[root@fedora-group7-com g7]# firewall-cmd --add-service=samba --permanent
success
[root@fedora-group7-com g7]# firewall-cmd --reload
success
[root@fedora-group7-com g7]# setsebool -P samba_enable_home_dirs on
[root@fedora-group7-com g7]#
```

Figure 5. 155 : Home directory

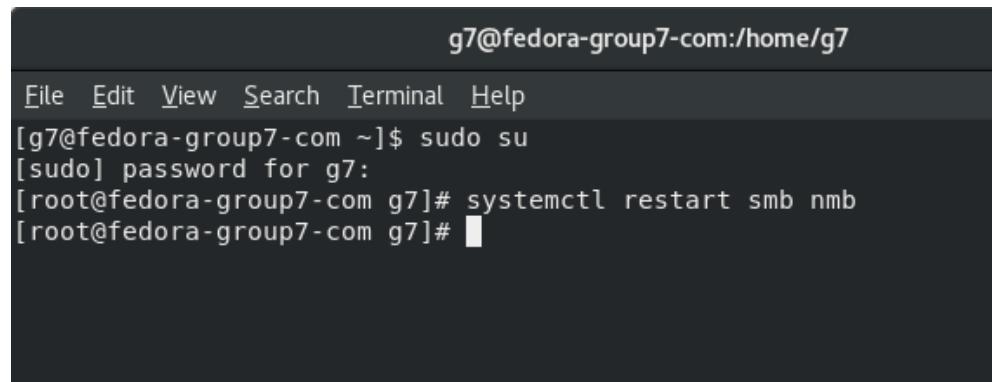
Step 6: Add user that access to samba



```
g7@fedora-group7-com:/home/g7
File Edit View Search Terminal Help
[g7@fedora-group7-com ~]$ sudo su
[sudo] password for g7:
[root@fedora-group7-com g7]# firewall-cmd --add-service=samba --permanent
success
[root@fedora-group7-com g7]# firewall-cmd --reload
success
[root@fedora-group7-com g7]# setsebool -P samba_enable_home_dirs on
[root@fedora-group7-com g7]# useradd syida
[root@fedora-group7-com g7]#
```

Figure 5. 156 : Add user

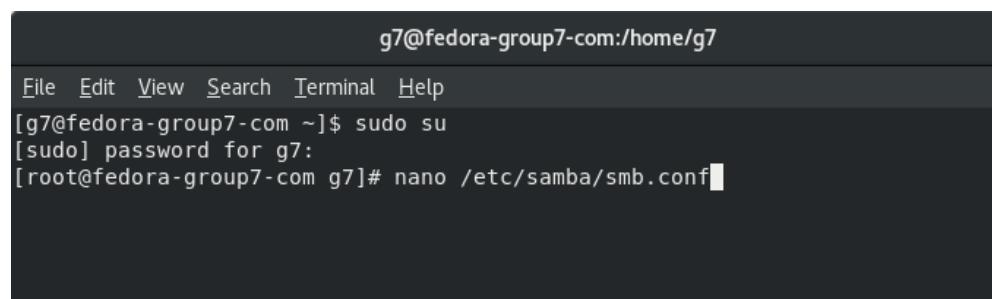
Step 7: Reboot smb and nmb after add user to samba



```
g7@fedora-group7-com:/home/g7
File Edit View Search Terminal Help
[g7@fedora-group7-com ~]$ sudo su
[sudo] password for g7:
[root@fedora-group7-com g7]# systemctl restart smb nmb
[root@fedora-group7-com g7]#
```

Figure 5. 157 : Restart samba

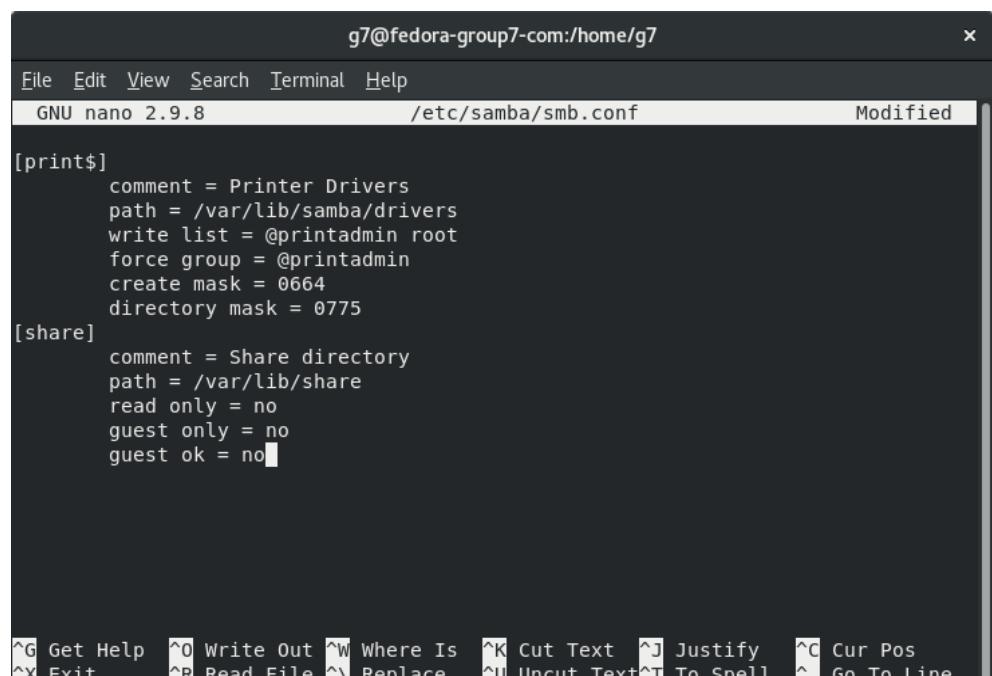
Step 8: The configuration file for Samba is located at /etc/samba/smb.conf.
Add the new directory as a share.



```
g7@fedora-group7-com:/home/g7
File Edit View Search Terminal Help
[g7@fedora-group7-com ~]$ sudo su
[sudo] password for g7:
[root@fedora-group7-com g7]# nano /etc/samba/smb.conf
```

Figure 5. 158 : Add new directory

Step 9: Next, modify the directive settings to share a folder. Share permission 0777 directory.



```
g7@fedora-group7-com:/home/g7
File Edit View Search Terminal Help
GNU nano 2.9.8          /etc/samba/smb.conf      Modified
[x]
[print$]
comment = Printer Drivers
path = /var/lib/samba/drivers
write list = @printadmin root
force group = @printadmin
create mask = 0664
directory mask = 0775
[share]
comment = Share directory
path = /var/lib/share
read only = no
guest only = no
guest ok = no
```

Figure 5. 159 : Samba configuration

Step 10: The configuration file for Samba is located at /etc/samba/smb.conf

```
g7@fedora-group7-com:/home/g7
File Edit View Search Terminal Help
[g7@fedora-group7-com ~]$ sudo su
[sudo] password for g7:
[root@fedora-group7-com g7]# nano /etc/samba/smb.conf
[root@fedora-group7-com g7]# mkdir /var/lib/share
[root@fedora-group7-com g7]# █
```

Figure 5. 160 : File located

Step 11: Change /var/lib/share's permission to 0777

```
g7@fedora-group7-com:/home/g7
File Edit View Search Terminal Help
[g7@fedora-group7-com ~]$ sudo su
[sudo] password for g7:
[root@fedora-group7-com g7]# nano /etc/samba/smb.conf
[root@fedora-group7-com g7]# mkdir /var/lib/share
[root@fedora-group7-com g7]# chmod 0777 /var/lib/share
[root@fedora-group7-com g7]# █
```

Figure 5. 161 : File permission

Step 12: Add samba_share_t label to /var/lib/share

```
g7@fedora-group7-com:/home/g7
File Edit View Search Terminal Help
[g7@fedora-group7-com ~]$ sudo su
[sudo] password for g7:
[root@fedora-group7-com g7]# nano /etc/samba/smb.conf
[root@fedora-group7-com g7]# mkdir /var/lib/share
[root@fedora-group7-com g7]# chmod 0777 /var/lib/share
[root@fedora-group7-com g7]# chcon -R -t samba_share_t /var/lib/share
[root@fedora-group7-com g7]# █
```

Figure 5. 162 : Label file

5.2.9 Network Management System

Step 1: Check if there is any update.

```
g7@group7:~$ sudo su  
[sudo] password for g7:  
root@group7:/home/g7# apt-get update
```

Figure 5. 163 : Update Ubuntu

Step 2: Download Apache web server and utilities.

```
root@group7:/home/g7# apt-get install -y build-essential apache2 apache2-utils sendmail daemon
```

Figure 5. 164 : Installing package.

Step 3: Installing Apache web server

```
root@group7:/home/g7# apt-get install apache2
```

Figure 5. 165 : Extract Apache to server.

Step 4: Adding new user. ‘useradd <username>’.

```
root@group7:/home/g7# useradd newnagios
```

Figure 5. 166 : User ‘newnagios’ been added.

Step 5: Create a new group. ‘groupadd <groupname>’.

```
root@group7:/home/g7# groupadd newnagios
```

Figure 5. 167 : Group ‘newnagios’ added.

Step 6: Setup user mode and assign user to the group.

```
root@group7:/home/g7# usermod -a -G newnagios newnagios
```

Figure 5. 168 : Permission and grouping.

Step 7: Configuration for grouping in nagios.

```
root@group7:/home/g7/Downloads/nagios-4.4.2# ./configure --with-nagios-group=newnagios --with-command-group=newnagios --with-mail=/usr/bin/sendmail --with-httpd-conf=/etc/apache2/sites-enabled
```

Figure 5. 169 : Group the new user to a group.

Step 8: Installing Nagios.

```
root@group7:/home/g7/Downloads/nagios-4.4.2# make all
```

Figure 5. 170 : Installing Nagios.

Step 9: Initiate the installer.

```
root@group7:/home/g7/Downloads/nagios-4.4.2# make install
```

Figure 5. 171 : Installer setup.

Step 10: Install the boot configuration.

```
root@group7:/home/g7/Downloads/nagios-4.4.2# make install-init
```

Figure 5. 172 : Installing boot configuration.

Step 11: Installing the command mode.

```
root@group7:/home/g7/Downloads/nagios-4.4.2# make install-commandmode
```

Figure 5. 173 : Command mode installation.

Step 12: Install configuration files.

```
g7@group7:~/Downloads/nagios-4.4.2$ sudo make install-commandmode  
/usr/bin/install -c -m 775 -o nagios -g newnagios -d /usr/local/nagios/var/rw  
chmod g+s /usr/local/nagios/var/rw
```

Figure 5. 174 : Install other configuration files for Nagios.

Step 13: Installing web configuration.

```
g7@group7:~/Downloads/nagios-4.4.2$ sudo make install-webconf  
/usr/bin/install -c -m 644 sample-config/httpd.conf /etc/apache2/sites-enabled/n  
agios.conf
```

Figure 5. 175 : Web configure installation.

Step 14: Copy the eventhandler directory to the nagios directory.

```
g7@group7:~/Downloads/nagios-4.4.2$ sudo cp -R contrib/eventhandlers/ /usr/local/  
/nagios/libexec/
```

Figure 5. 176 : Copy the eventhandler.

Step 15: Set the permission for nagios directory.

```
g7@group7:~/Downloads/nagios-4.4.2$ sudo chown -R nagios:nagios /usr/local/nagio  
s/libexec/eventhandlers
```

Figure 5. 177 : Give permission to read in nagios directory.

Step 16: Configure the ‘nagios.cfg’ files.

```
g7@group7:~/Downloads/nagios-4.4.2$ sudo /usr/local/nagios/bin/nagios -v /usr/lo  
cal/nagios/etc/nagios.cfg
```

Figure 5. 178: ‘Nagios.cfg’ file setting.

Step 17: Start nagios in Ubuntu Server.

```
g7@group7:~/Downloads/nagios-4.4.2$ sudo systemctl start nagios
```

Figure 5. 179 : Set nagios tu running state.

Step 18: Set password for login to nagios.

```
g7@group7:~/Downloads/nagios-4.4.2$ sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

Figure 5. 180 : Set the password.

Step 19: Checking for nagios configuration.

```
g7@group7:~/Downloads/nagios-plugins-2.2.1$ sudo ./configure --with-nagios-user=nagios --with-nagios-group=nagios
```

Figure 5. 181 : Nagios configuration checking.

Step 20: Enable the Nagios configuration files.

```
g7@group7:~/Downloads/nagios-plugins-2.2.1$ sudo ln -s /etc/init.d/nagios /etc/rc5.d/S99nagios
```

Figure 5. 182 : Nagios configuration enabling.

Step 21: Allowing port 80 been use for Nagios.

```
g7@group7:~/Downloads/nagios-plugins-2.2.1$ sudo iptables -I INPUT -p tcp --destination-port 80 -j ACCEPT
```

Figure 5. 183 : Allowing selected port.

Step 22: Get installer for IP table.

```
g7@group7:~/Downloads/nagios-plugins-2.2.1$ sudo apt-get install -y iptables-persistent
```

Figure 5. 184 : Installation of ip table persistent.

Step 23: Start the nagios application.

```
g7@group7:~/Downloads/nagios-4.4.2$ sudo systemctl start nagios
```

Figure 5. 185 : Execute nagios application.

Step 24: Enable module for nagios.

```
g7@group7:~/Downloads/nagios-plugins-2.2.1$ sudo a2enmod
```

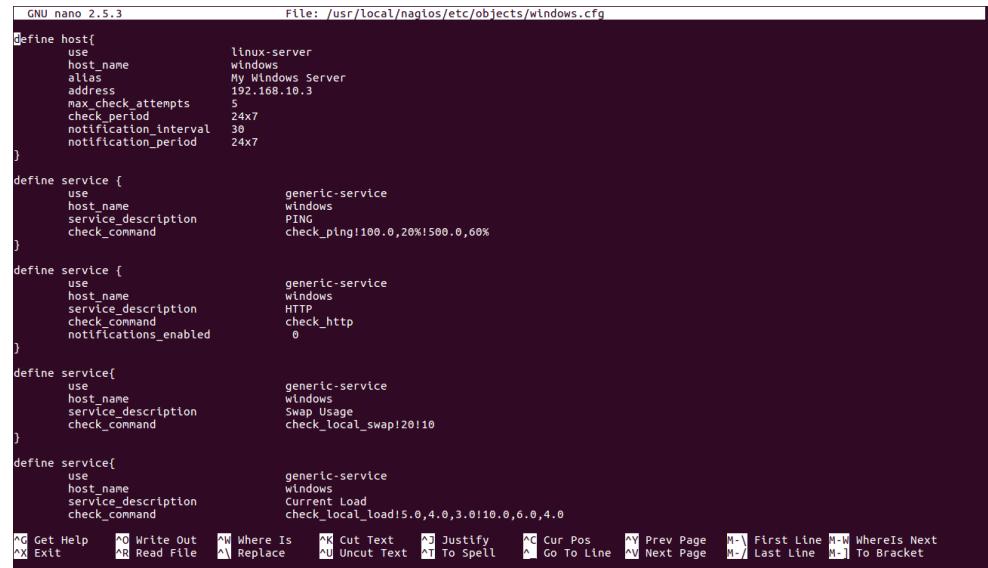
Figure 5. 186 : Nagios module enabling

Step 25: Enabling cgi module.

```
g7@group7:~/Downloads/nagios-plugins-2.2.1$ sudo a2enmod cgi  
Enabling module cgi.  
To activate the new configuration, you need to run:  
    service apache2 restart
```

Figure 5. 187 : CGI module enabled.

Step 26: Edit windows.cfg files for windows configuration for host and service definition.



```
GNU nano 2.5.3          File: /usr/local/nagios/etc/objects/windows.cfg

define host{
    use           linux-server
    host_name     windows
    alias         My WIndows Server
    address       192.168.10.3
    max_check_attempts 5
    check_period   24x7
    notification_interval 30
    notification_period 24x7
}

define service {
    use           generic-service
    host_name     windows
    service_description PING
    check_command  check_ping!100.0,20%!500.0,60%
}

define service {
    use           generic-service
    host_name     windows
    service_description HTTP
    check_command  check_http
    notifications_enabled 0
}

define service{
    use           generic-service
    host_name     windows
    service_description Swap Usage
    check_command  check_local_swap!20!10
}

define service{
    use           generic-service
    host_name     windows
    service_description Current Load
    check_command  check_local_load!5.0,4.0,3.0!10.0,6.0,4.0
}

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos  ^Y Prev Page  M-] First Line  M-W WhereIs Next
^X Exit      ^R Read File  ^A Replace  ^U Uncut Text  ^T To Spell  ^H Go To Line  ^N Next Page  M-[ Last Line  M-] To Bracket
```

Figure 5. 188 : Windows configuration for services and host.

5.2.10 Server Virtualization

Step 1 : First, install hyperv inside server manager

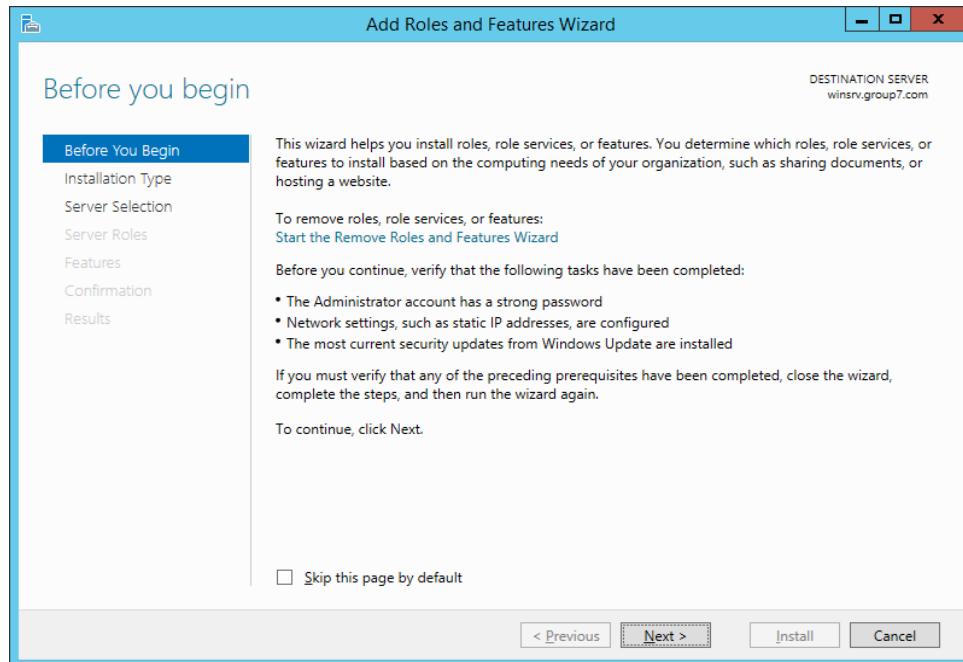


Figure 5. 189 : Install hyperv

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

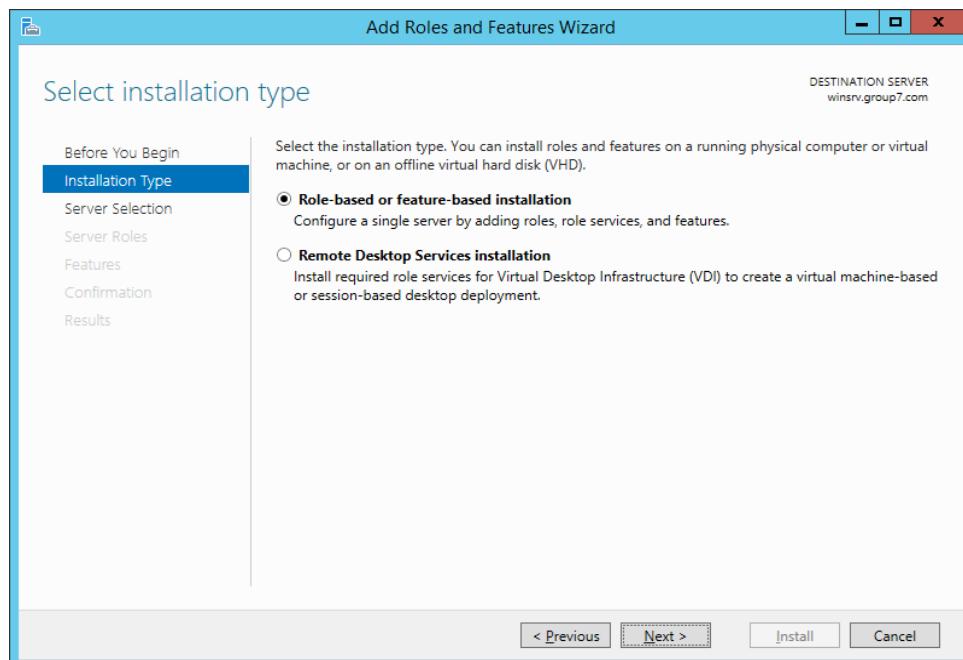


Figure 5. 190 : Installation type

Step 3 : For server selection, click on select a server from the server pool

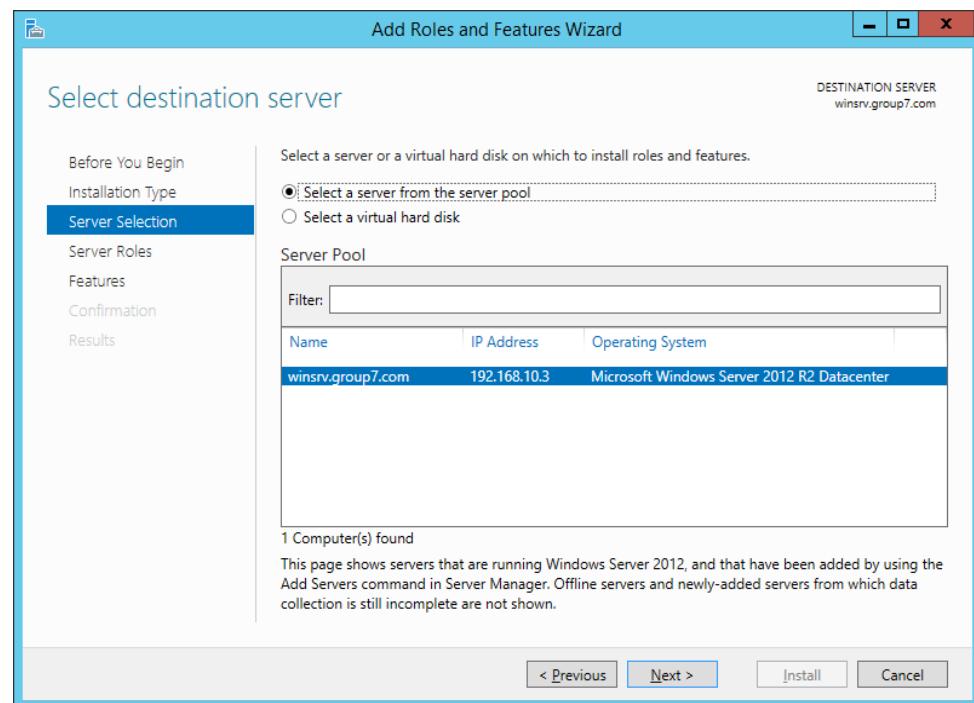


Figure 5. 191 : Server selection

Step 4: Click on add features to add features for Hyper-V

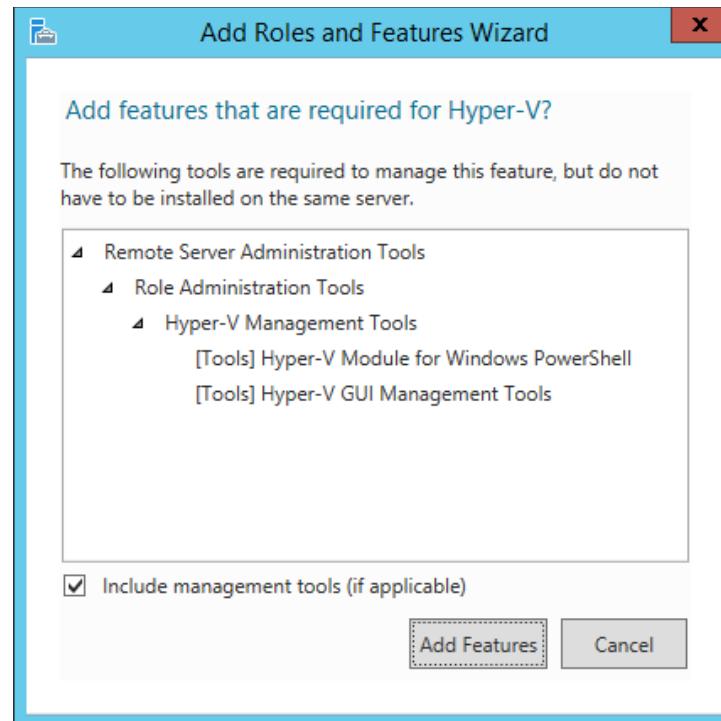


Figure 5. 192 : Add features

Step 5: Tick the check box for Hyper-V installation then click next

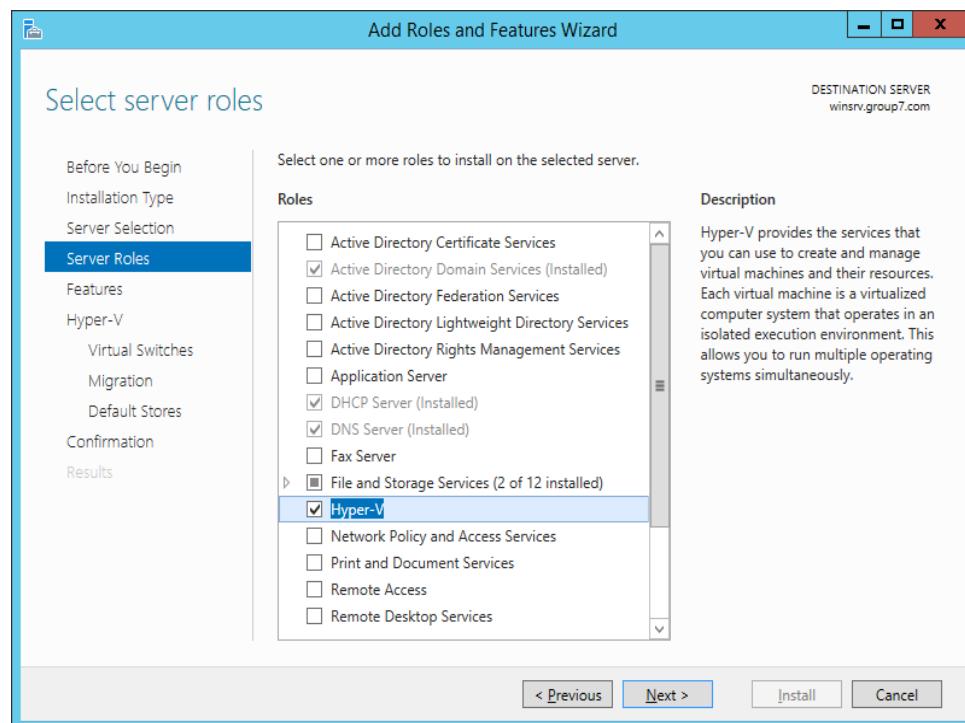


Figure 5. 193 : Server roles

Step 6: Then, choose NET Framework 4.5 features and click next

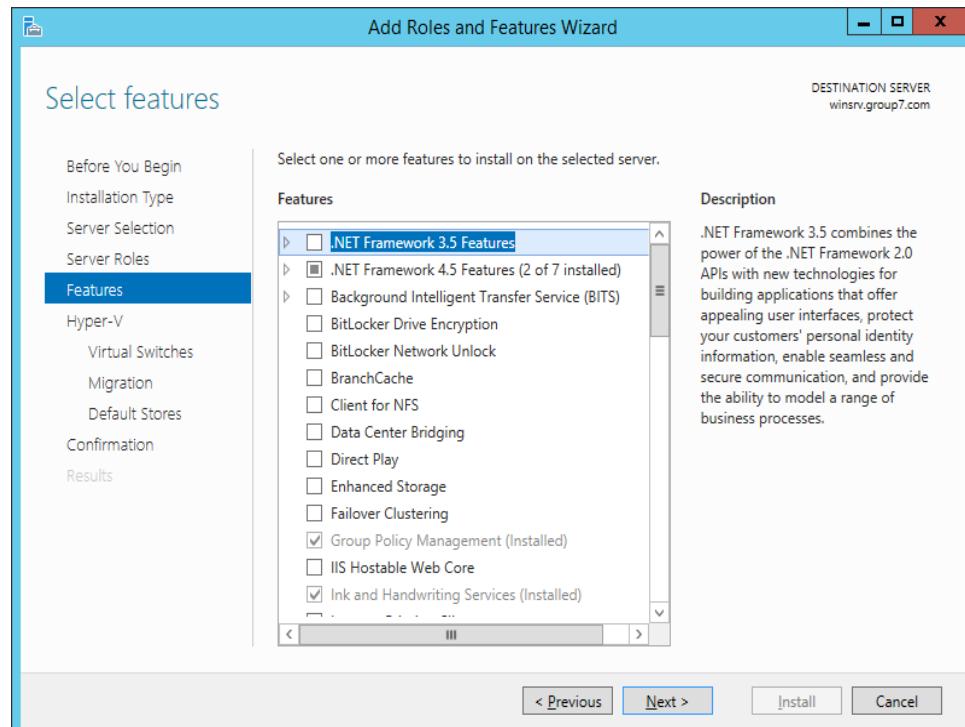


Figure 5. 194 : Features

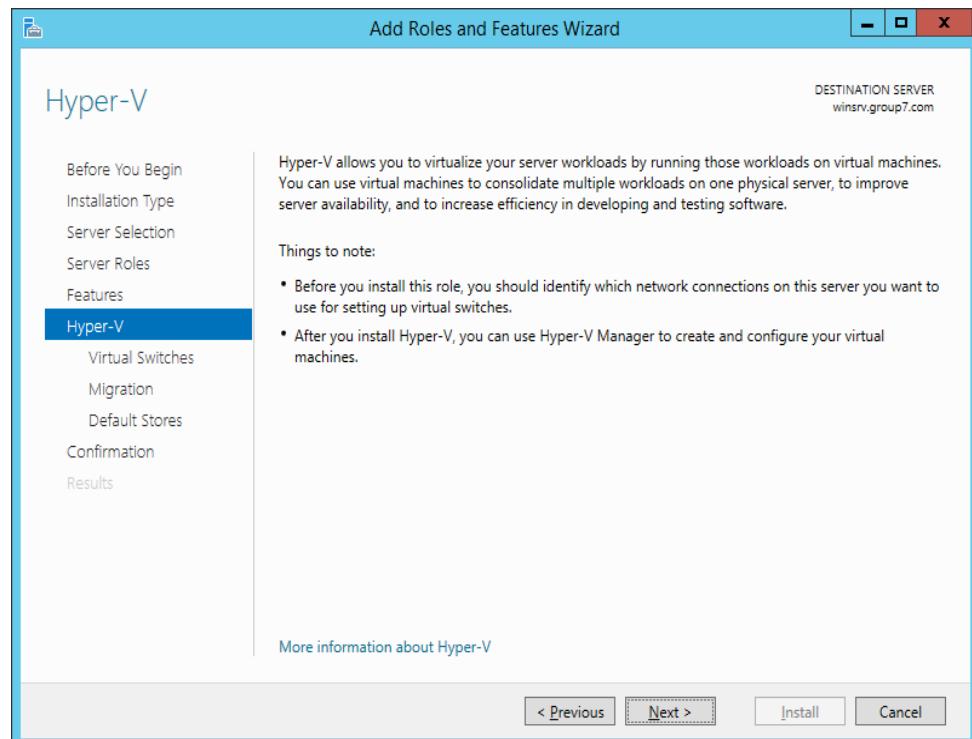


Figure 5. 195 : hyperv installation

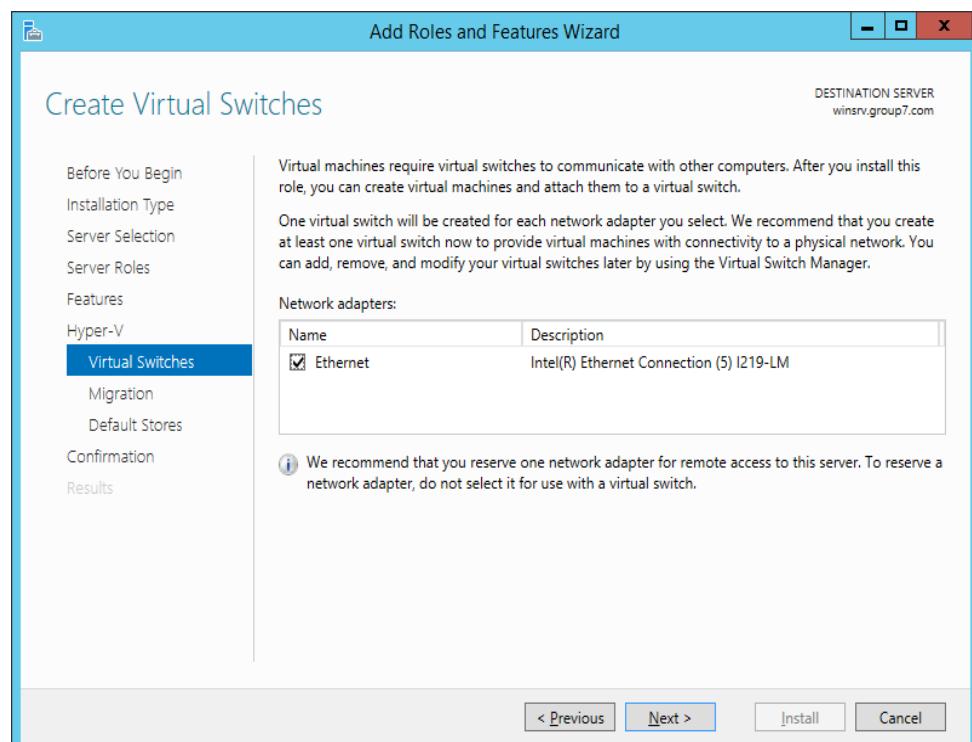


Figure 5. 196 : Virtual switch manager

Step 7: Click Use Credential Security Support Provider (CredSSP) for authentication protocol and then click next

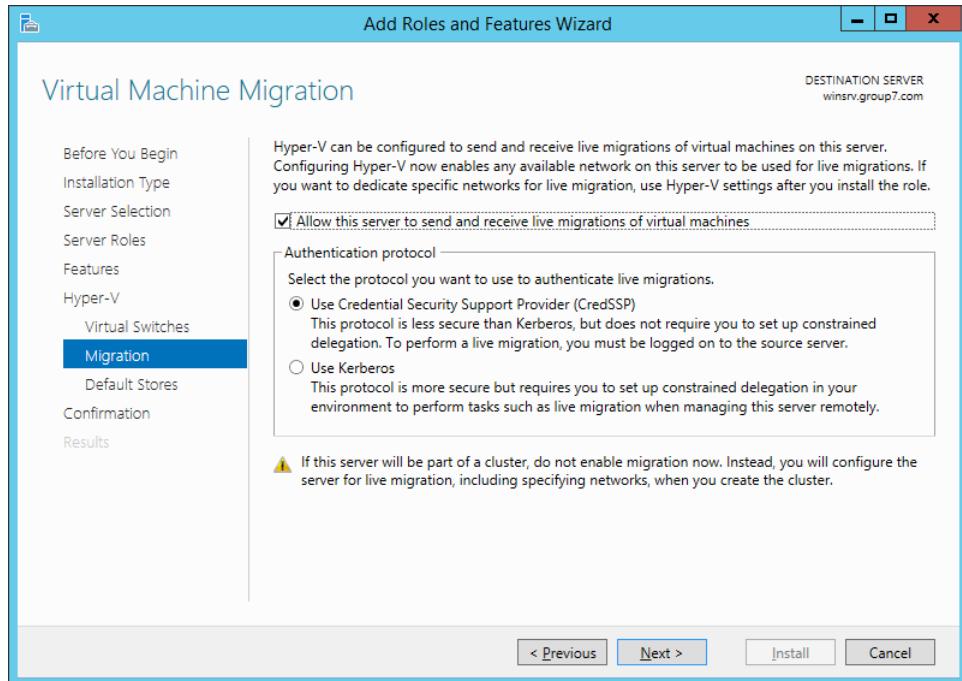


Figure 5. 197 : Authentication protocol

Step 8: Browse the default location for virtual hard disk files and virtual machine configuration files.

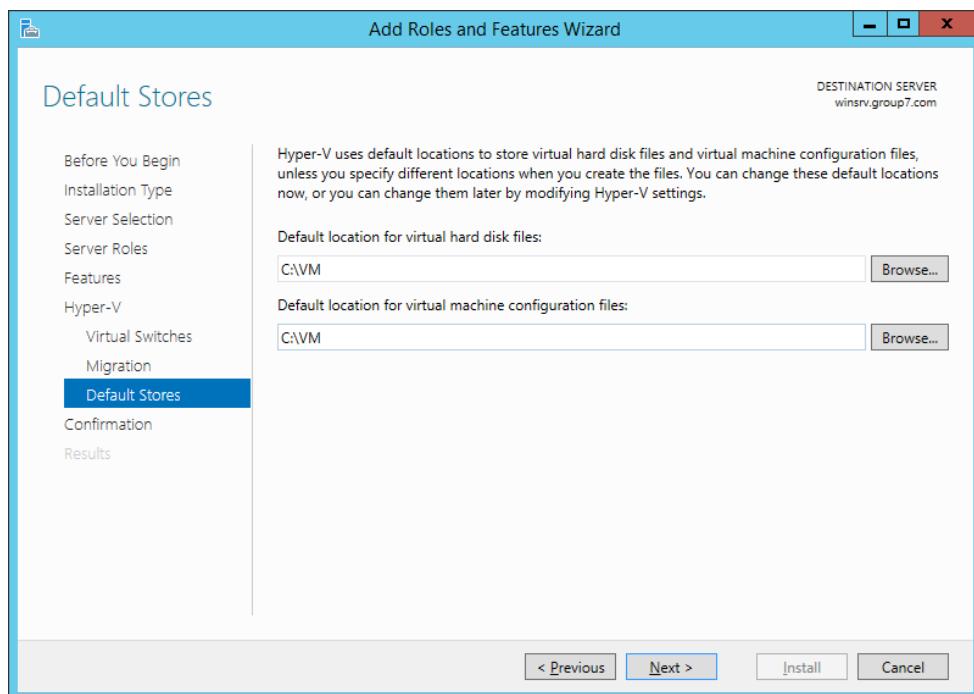


Figure 5. 198 : Default location for hard disk files

Step 9: Click install to install roles and features Hyper-V

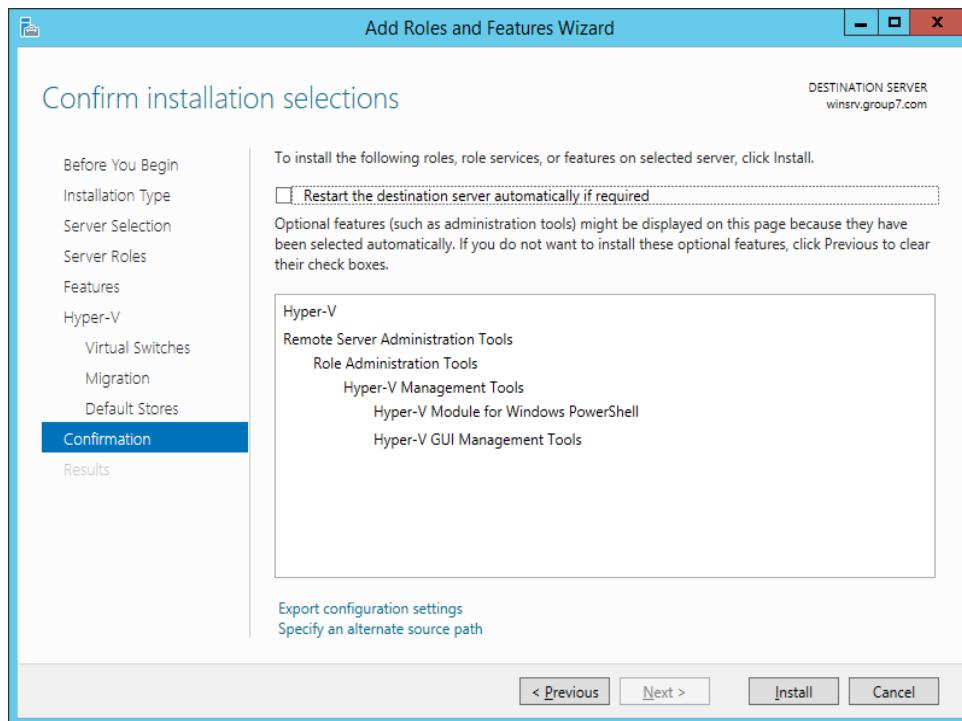


Figure 5. 199 : Confirm installation hyperv

Step 10: Hyper-V successfully installed

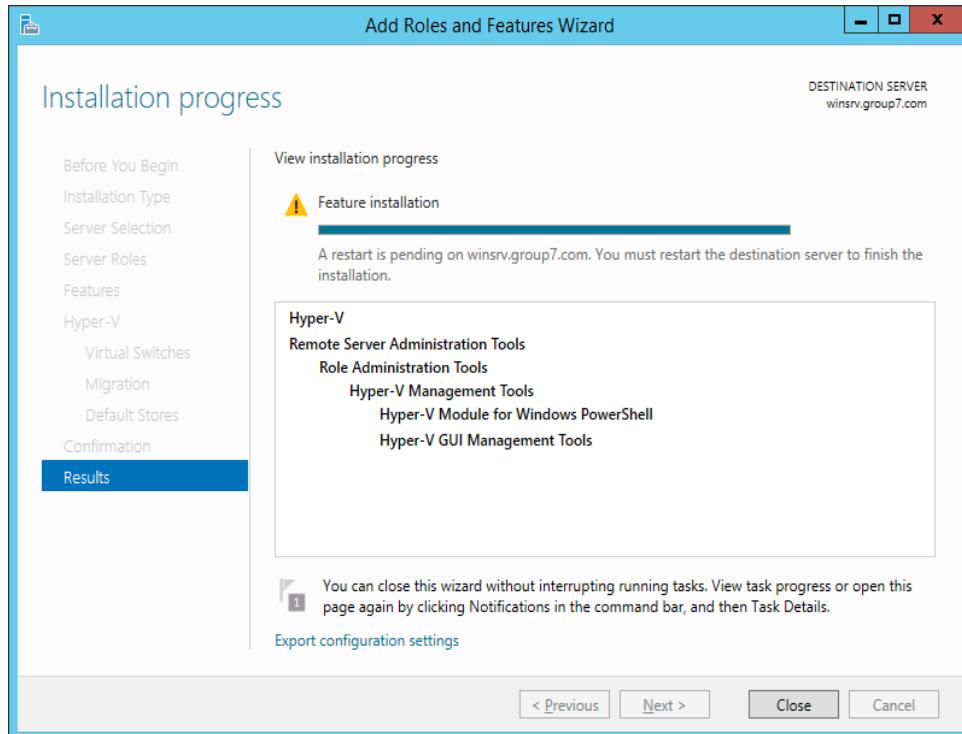


Figure 5. 200 : hyperv installed

Step 11: After HyperV was installed, install a new virtual machine inside hyperV manager

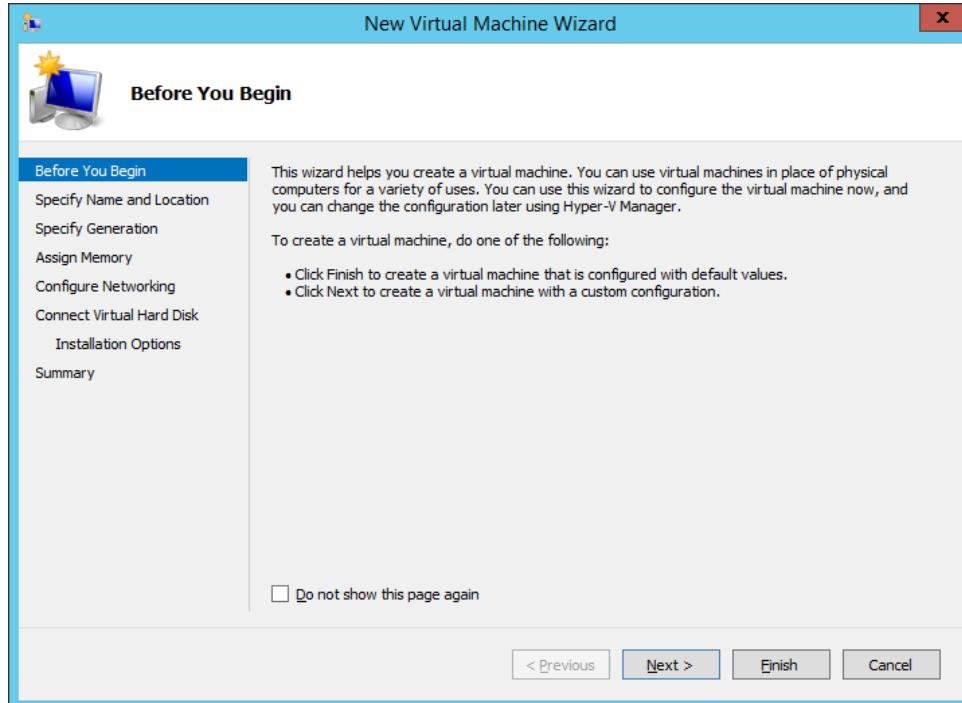


Figure 5. 201 : Install virtual machine

Step 12: Choose a name and location for the virtual machine. The name will display in Hyper-V manager

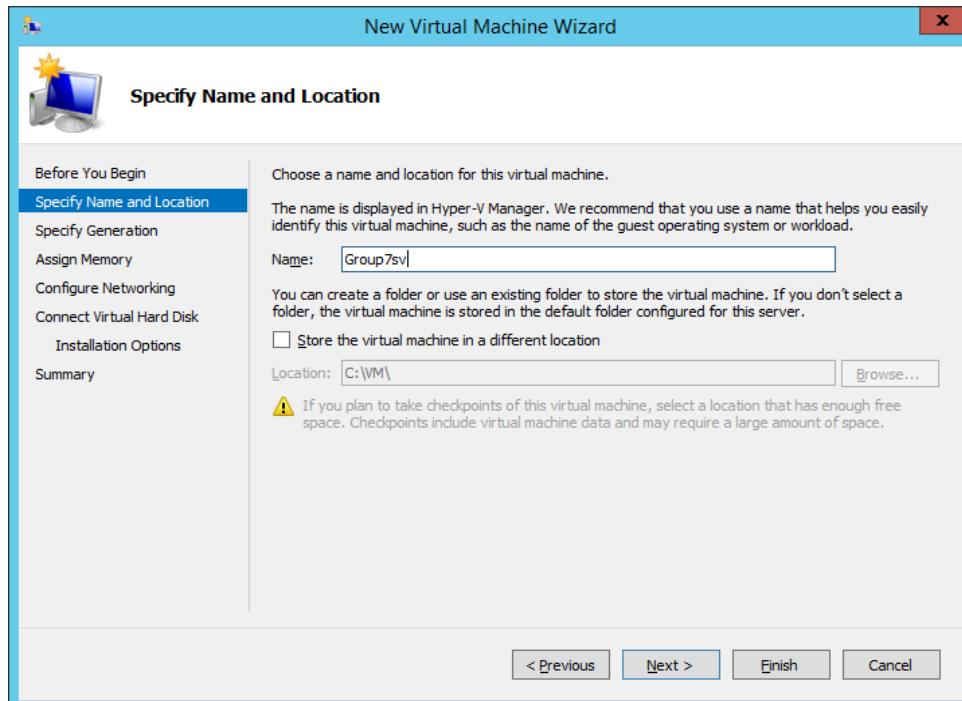


Figure 5. 202 : Name and location virtual machine

Step 13: Click generation 1 of the virtual machine that provides same virtual hardware to the virtual machine and then click next

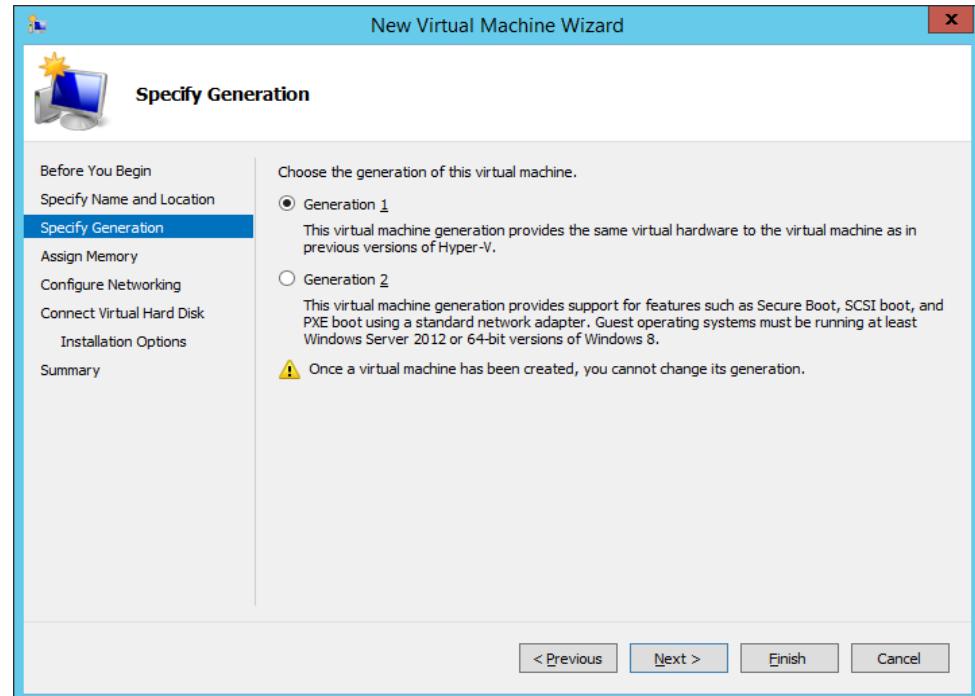


Figure 5. 203 : Specify generation

Step 14: Assign the memory to 8096 MB to improve the performance of the virtual machine

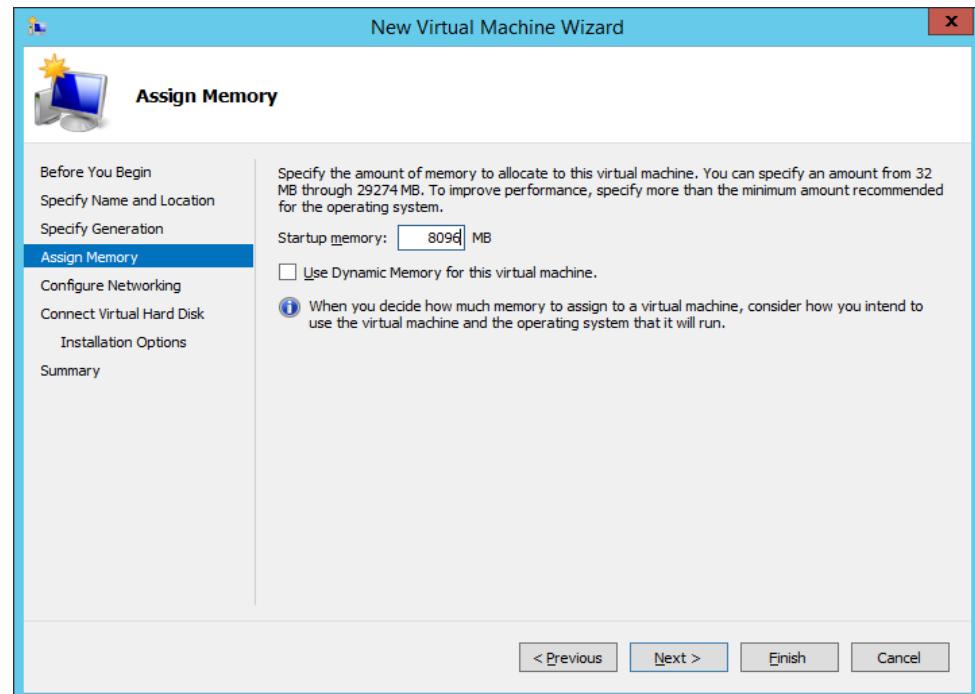


Figure 5. 204 : Assign memory

Step 15: Choose virtual switch for the connection then click next

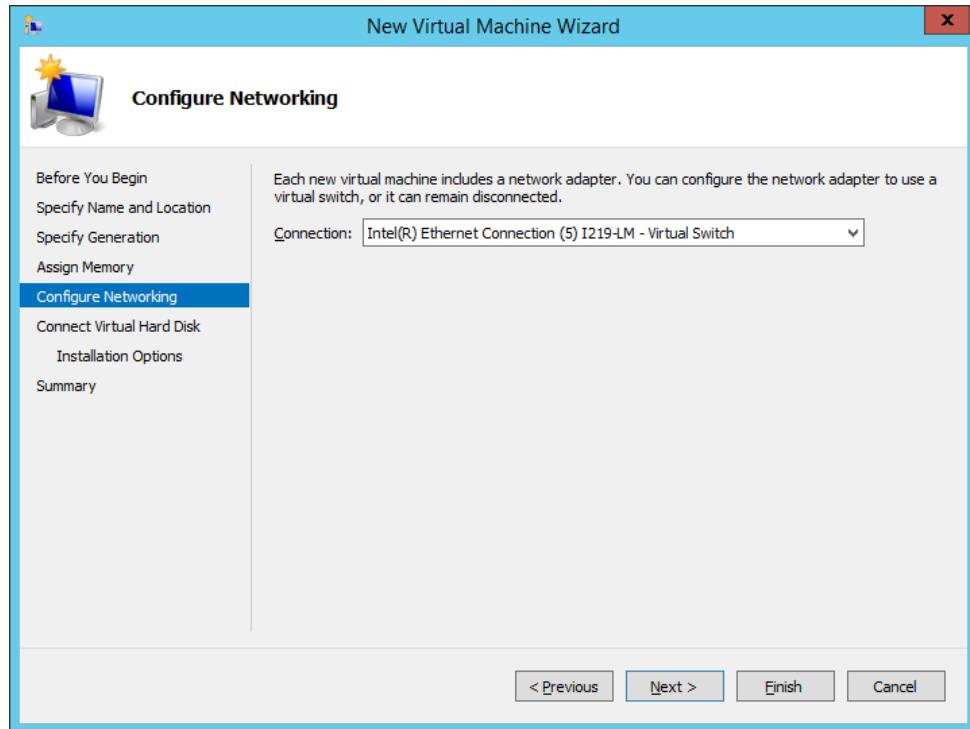


Figure 5. 205 : Assign connection

Step 16: Click on create a virtual hard disk then click next to continue

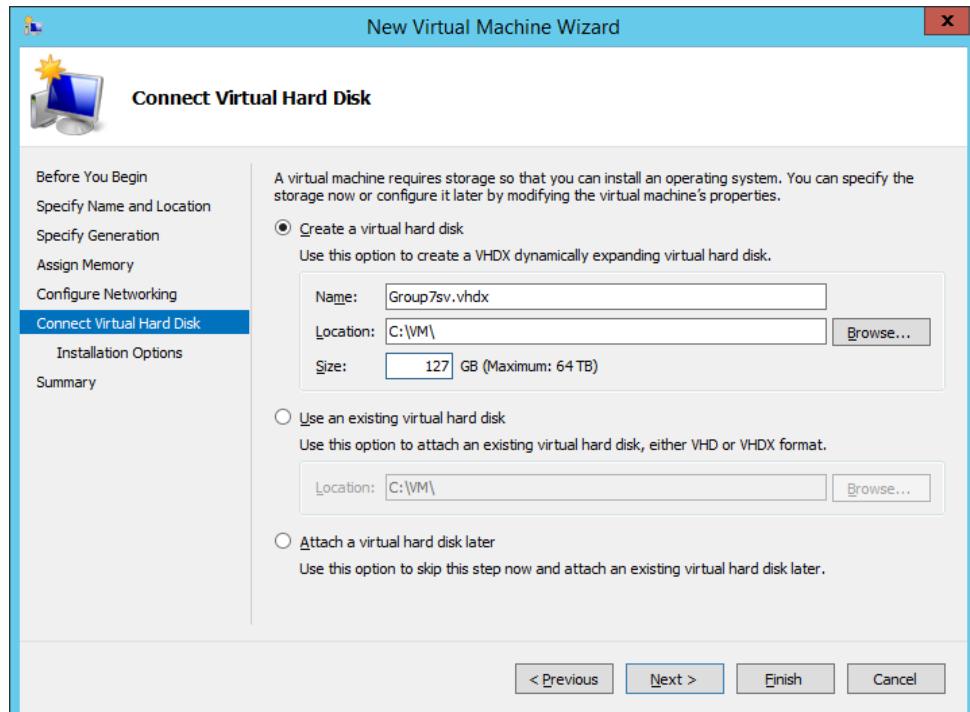


Figure 5. 206 : Create virtual hard disk

Step 17: Install an operating system and browse Ubuntu 16.04 installer in image file

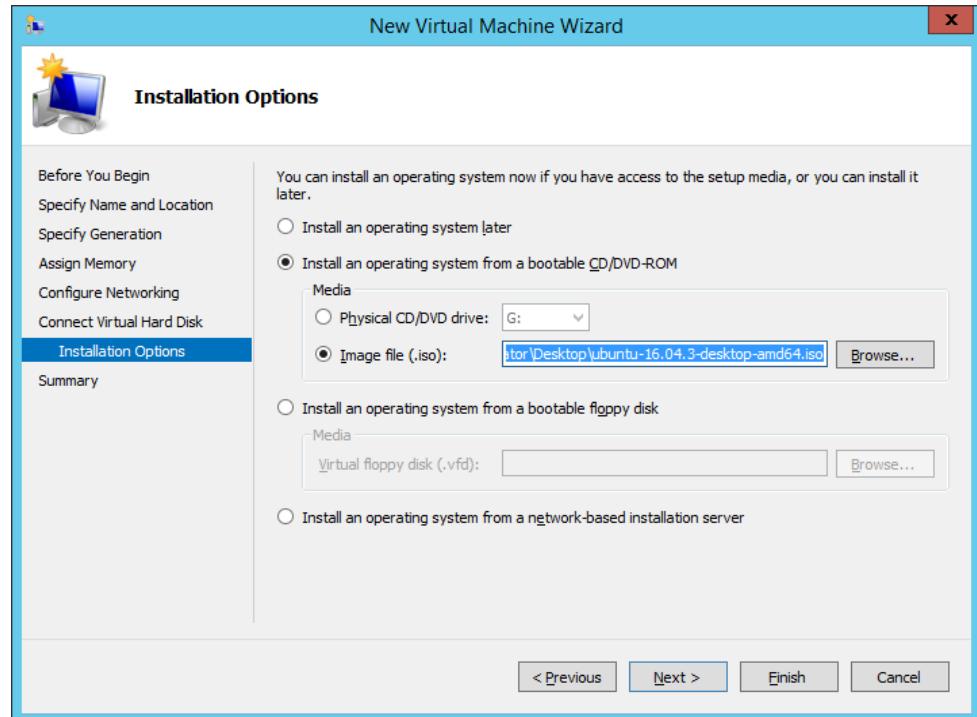


Figure 5. 207 : Installation operating system

Step 18: After Ubuntu successfully installed in HyperV then click finish

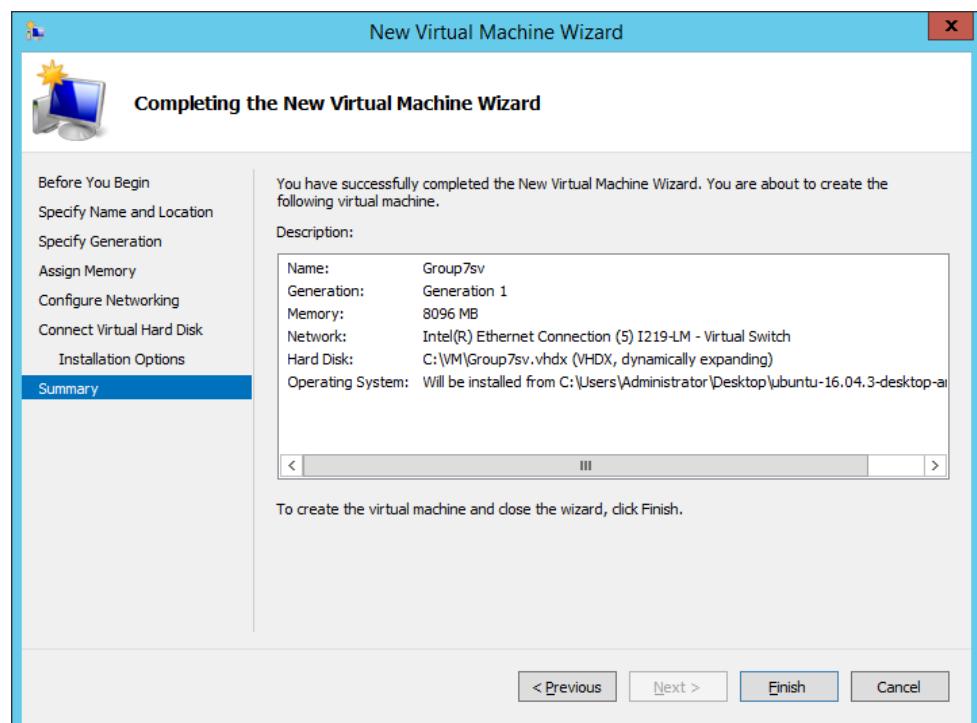


Figure 5. 208 : Ubuntu installed

Configure FTP in Ubuntu

Step 1: Firstly, create a folder in home directory name it as “ftp-files” and create a document outside the ftp-files and name it as “download-test.txt”.

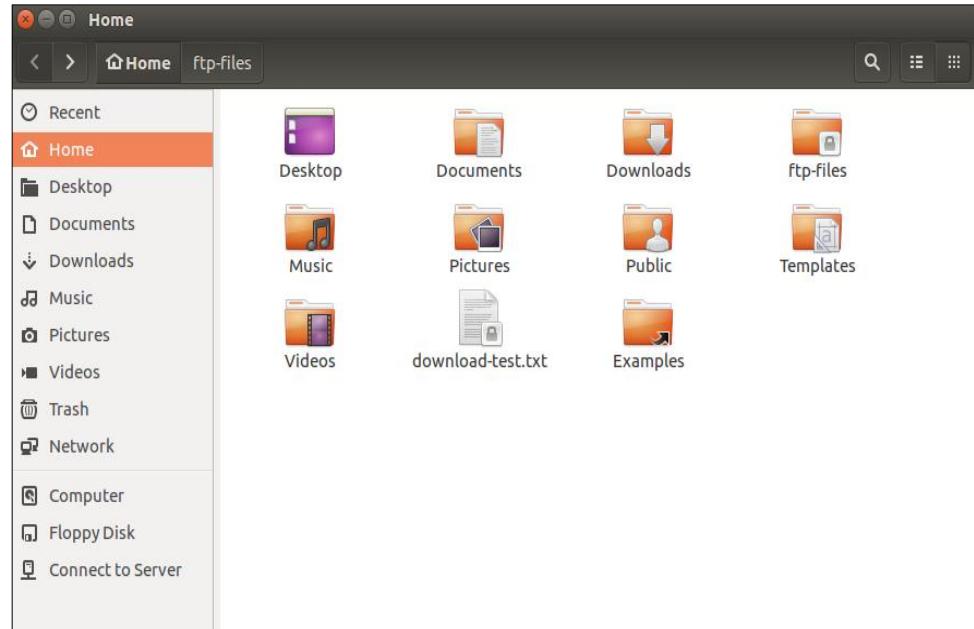


Figure 5. 209 : Create a ftp file and text file

Step 2: Next, inside ftp-files create a folder and a document name it as “upload-test.txt”.

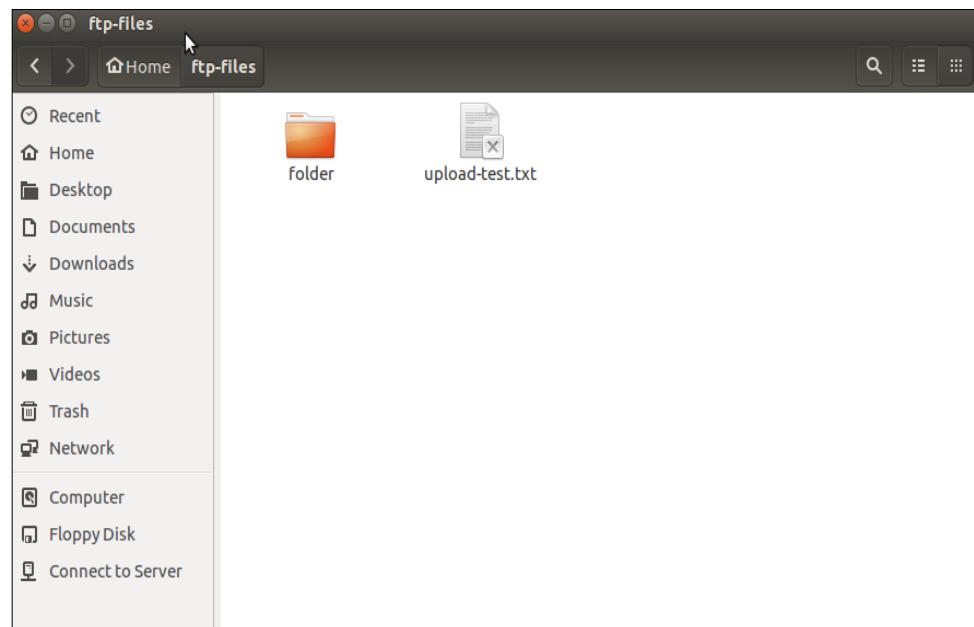
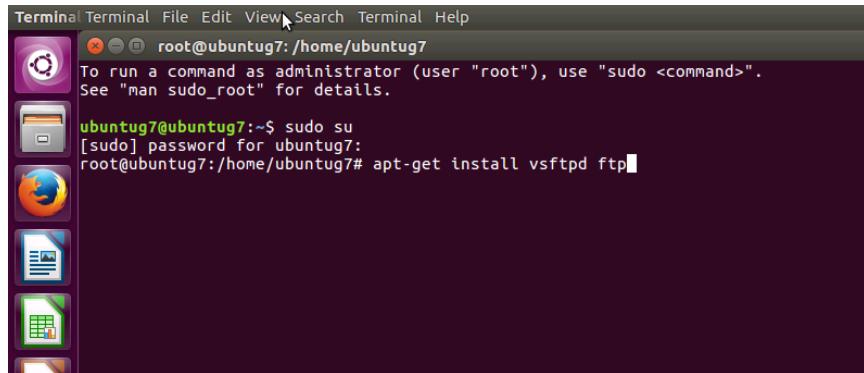


Figure 5. 210 : Create a folder in ftp file and text file

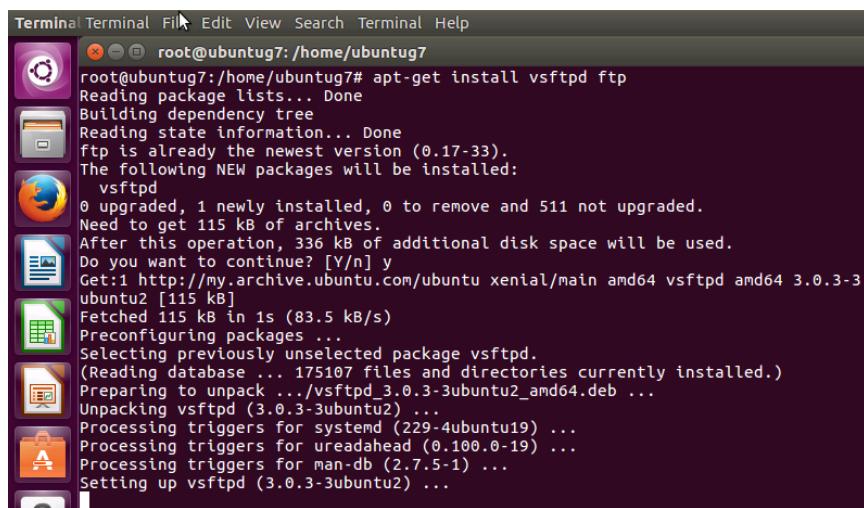
Step 3: Install vsftpd by using command “apt-get install vsftpd ftp”



```
Terminal Terminal File Edit View Search Terminal Help
root@ubuntug7:/home/ubuntug7
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntug7@ubuntug7:~$ sudo su
[sudo] password for ubuntug7:
root@ubuntug7:/home/ubuntug7# apt-get install vsftpd ftp
```

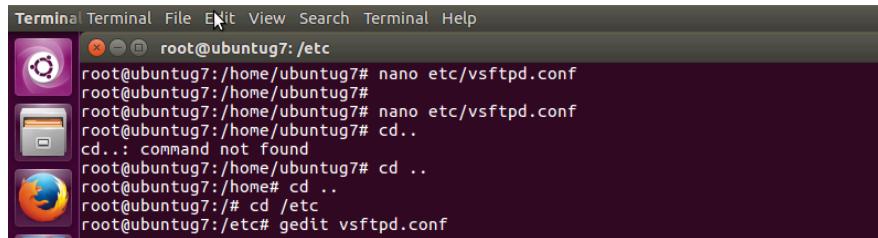
Figure 5. 211 : install vsftpd



```
Terminal Terminal File Edit View Search Terminal Help
root@ubuntug7:/home/ubuntug7
root@ubuntug7:/home/ubuntug7# apt-get install vsftpd ftp
Reading package lists... Done
Building dependency tree
Reading state information... Done
ftp is already the newest version (0.17-33).
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 511 not upgraded.
Need to get 115 kB of archives.
After this operation, 336 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://my.archive.ubuntu.com/ubuntu xenial/main amd64 vsftpd amd64 3.0.3-3
ubuntu2 [115 kB]
Fetched 115 kB in 1s (83.5 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 175107 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-3ubuntu2_amd64.deb ...
Unpacking vsftpd (3.0.3-3ubuntu2) ...
Processing triggers for systemd (229-4ubuntu19) ...
Processing triggers for ureadahead (0.100.0-19) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up vsftpd (3.0.3-3ubuntu2) ...
```

Figure 5. 212 : vsftpd installed

Step 4: Open the config file to verify that the settings in configuration by using command “nano etc/vsftpd.conf” or command “gedit etc/vsftpd.conf”.

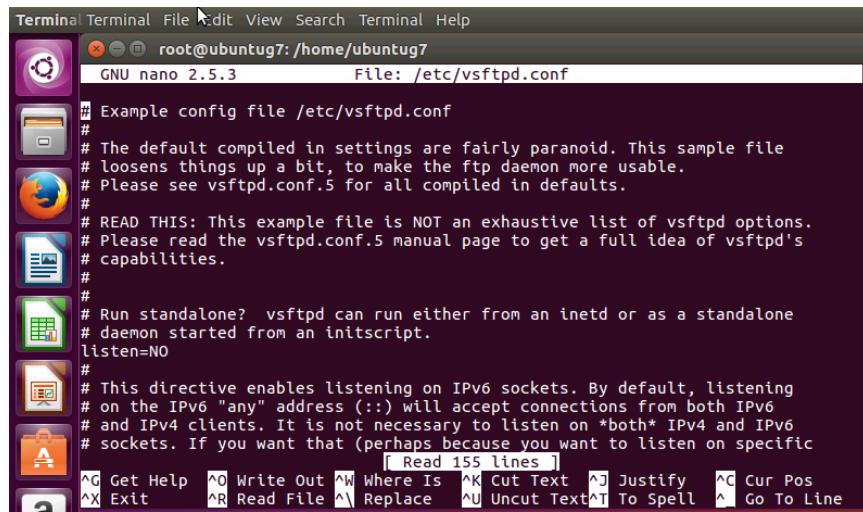


```
Terminal Terminal File Edit View Search Terminal Help
root@ubuntug7:/etc
root@ubuntug7:/home/ubuntug7# nano etc/vsftpd.conf
root@ubuntug7:/home/ubuntug7#
root@ubuntug7:/home/ubuntug7# nano etc/vsftpd.conf
root@ubuntug7:/home/ubuntug7# cd ..
cd...: command not found
root@ubuntug7:/home/ubuntug7# cd ..
root@ubuntug7:/home# cd ..
root@ubuntug7:/# cd /etc
root@ubuntug7:/etc# gedit vsftpd.conf
```

Figure 5. 213 : Open config file

Step 5: Edit the config file in several things:

- Uncomment annoynymous _enable=NO
- Uncomment local_enable=YES to allow local users to log in
- Uncomment write_enable=YES

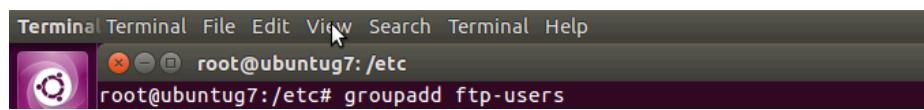


```
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Run standalone?  vsftpd can run either from an inetc or as a standalone
# daemon started from an initscript.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPV4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
[ Read 155 lines ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^L Replace ^U Uncut Text ^T To Spell ^L Go To Line
```

Figure 5. 214 : config file

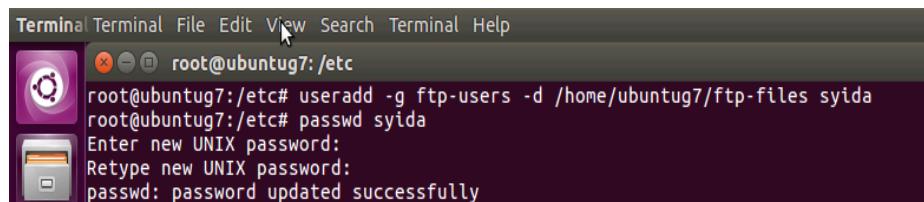
Step 6: Uncomment ftpd_banner and change it to “ftpd_banner= Welcome to Group7 FTP Service”.

Step 7 : Add group ftp user and add user into ftp user by using command “useradd -g ftp-users -d /home/ubuntug7/ftp-files syida” then set the password for the user.



```
root@ubuntug7: /etc
root@ubuntug7:/etc# groupadd ftp-users
```

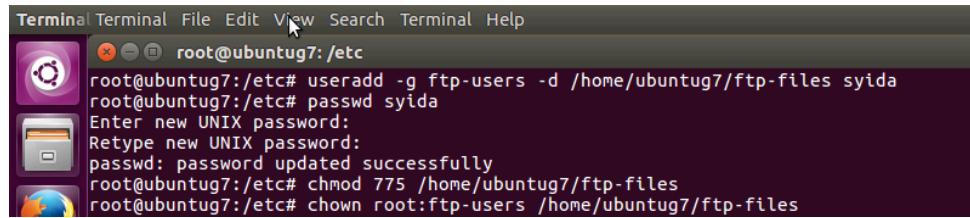
Figure 5. 215 : Add group ftp user



```
root@ubuntug7: /etc
root@ubuntug7:/etc# useradd -g ftp-users -d /home/ubuntug7/ftp-files syida
root@ubuntug7:/etc# passwd syida
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Figure 5. 216 : Add user into group ftp user

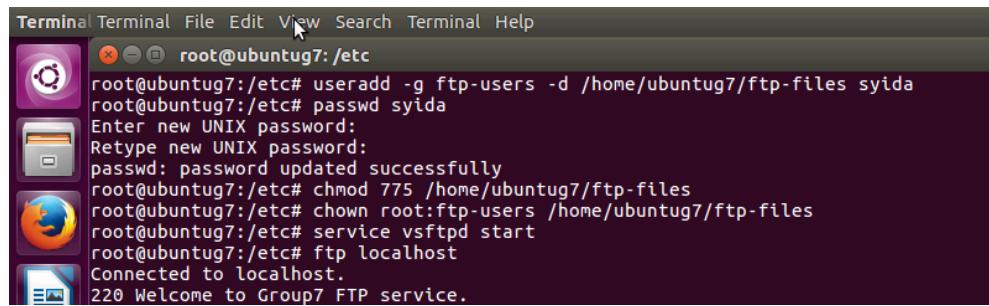
Step 8: Change mode permission for ftp user accessibility to “chmod 775” and change owner from root to ftp-users by using command “chown root:ftp-users”



```
Terminal Terminal File Edit View Search Terminal Help
root@ubuntug7: /etc
root@ubuntug7:/etc# useradd -g ftp-users -d /home/ubuntug7/ftp-files syida
root@ubuntug7:/etc# passwd syida
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@ubuntug7:/etc# chmod 775 /home/ubuntug7/ftp-files
root@ubuntug7:/etc# chown root:ftp-users /home/ubuntug7/ftp-files
```

Figure 5. 217 : Change mode permission and change owner directory

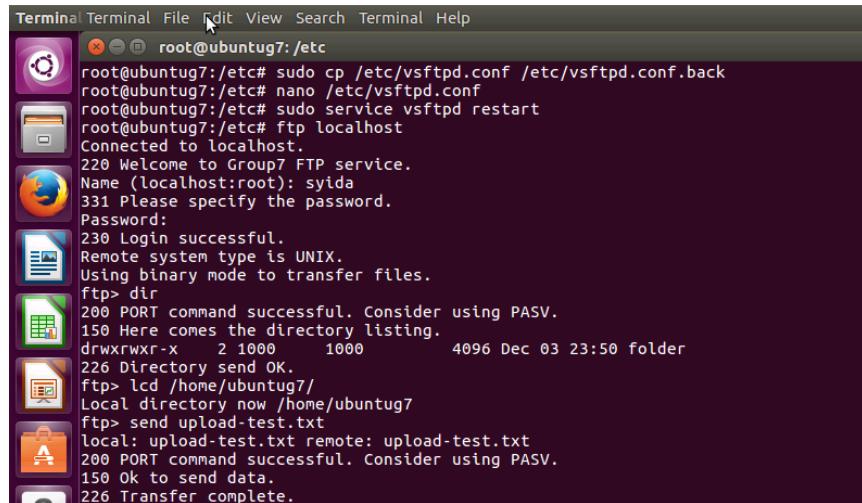
Step 9: Restart vsftpd by using command “service vsftpd start” and then enter “ftp localhost”. The output will be appear “Welcome to Group7 FTP service”



```
Terminal Terminal File Edit View Search Terminal Help
root@ubuntug7: /etc
root@ubuntug7:/etc# useradd -g ftp-users -d /home/ubuntug7/ftp-files syida
root@ubuntug7:/etc# passwd syida
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@ubuntug7:/etc# chmod 775 /home/ubuntug7/ftp-files
root@ubuntug7:/etc# chown root:ftp-users /home/ubuntug7/ftp-files
root@ubuntug7:/etc# service vsftpd start
root@ubuntug7:/etc# ftp localhost
Connected to localhost.
220 Welcome to Group7 FTP service.
```

Figure 5. 218 : Restart vsftpd and access ftp localhost

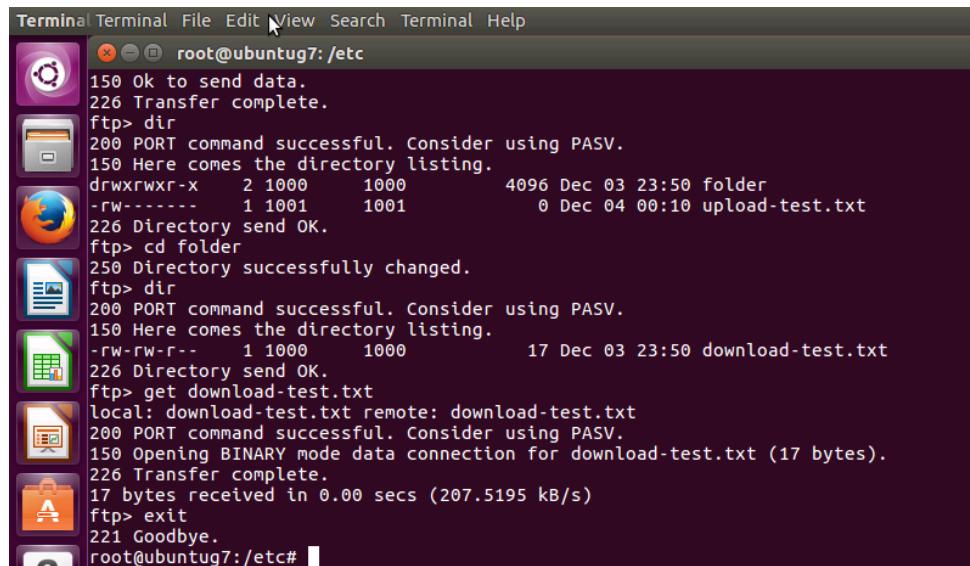
Step 10: After ftp user successfully login, enter home directory by using command “lcd /home/ubuntug7” and then send the document text file.



```
Terminal Terminal File Edit View Search Terminal Help
root@ubuntug7: /etc
root@ubuntug7:/etc# sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.back
root@ubuntug7:/etc# nano /etc/vsftpd.conf
root@ubuntug7:/etc# sudo service vsftpd restart
root@ubuntug7:/etc# ftp localhost
Connected to localhost.
220 Welcome to Group7 FTP service.
Name (localhost:root): syida
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxr-x 2 1000 1000 4096 Dec 03 23:50 folder
226 Directory send OK.
ftp> lcd /home/ubuntug7/
Local directory now /home/ubuntug7
ftp> send upload-test.txt
local: upload-test.txt remote: upload-test.txt
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
```

Figure 5. 219 : Send document text file

Step 11: Next, enter home directory and then get the document text file.



```
Terminal Terminal File Edit View Search Terminal Help
root@ubuntug7:/etc
150 Ok to send data.
226 Transfer complete.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxr-x 2 1000 1000 4096 Dec 03 23:50 folder
-rw----- 1 1001 1001 0 Dec 04 00:10 upload-test.txt
226 Directory send OK.
ftp> cd folder
250 Directory successfully changed.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r-- 1 1000 1000 17 Dec 03 23:50 download-test.txt
226 Directory send OK.
ftp> get download-test.txt
local: download-test.txt remote: download-test.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for download-test.txt (17 bytes).
226 Transfer complete.
17 bytes received in 0.00 secs (207.5195 kB/s)
ftp> exit
221 Goodbye.
root@ubuntug7:/etc#
```

Figure 5. 220 : Get document text file

Step 12: In home directory, you will see the document text file inside ftp-files folder transfer to home directory which means the send file transfer was successful.

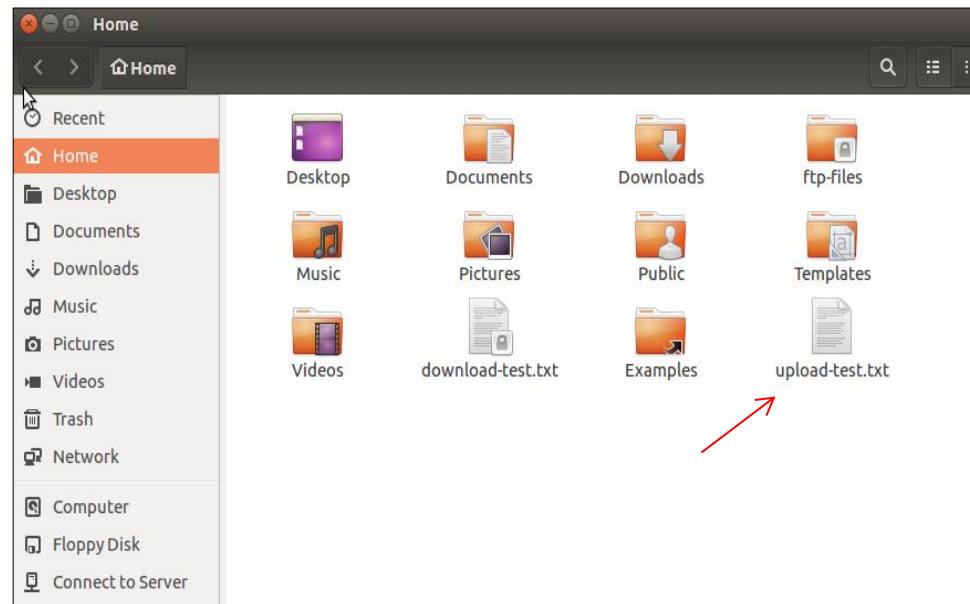


Figure 5. 221 : Files in home directory

Step 13: In ftp files that you have created at the beginning, you will see the document text file inside the folder in ftp-files folder in home directory which means the get file transfer was successful.

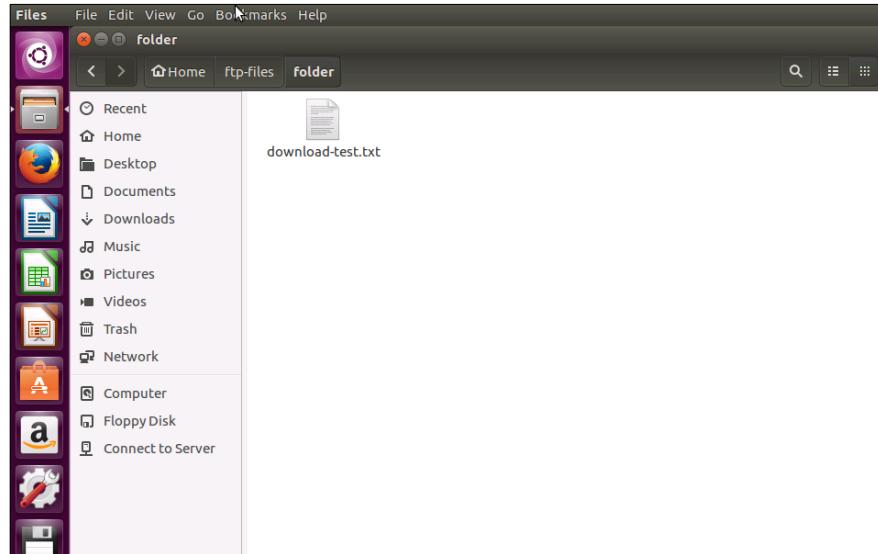


Figure 5. 222 : File text in folder in ftp file

Step 14: Restart vsftpd using command “systemctl restart vsftpd”

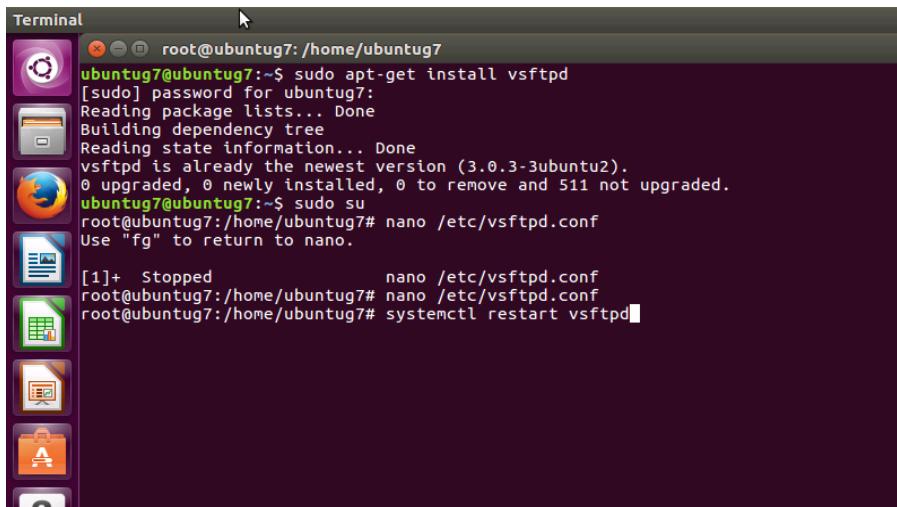


Figure 5. 223 : Restart vsftpd

Step 15: Testing ftp by enter “ftp://192.168.10.4” in Mozilla Firefox. The output as below:

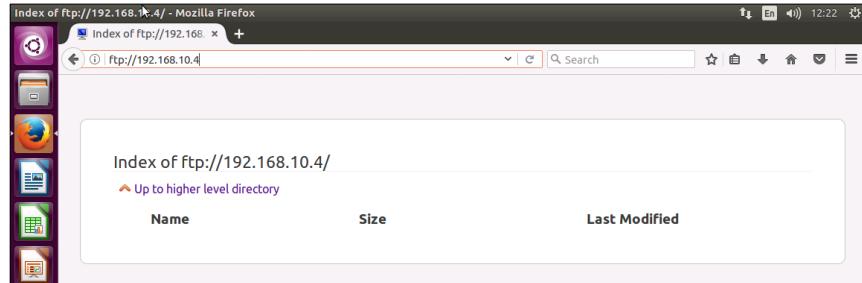


Figure 5. 224 : Testing ftp

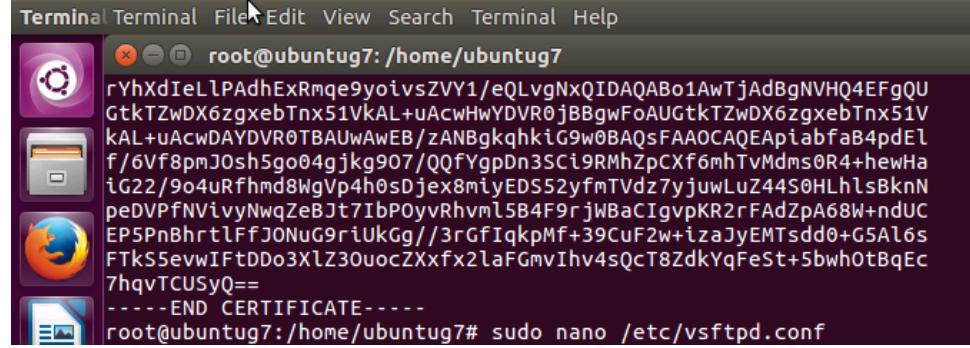
Configure Secure FTP

Step 1: Create the SSL certificates for use with vsftpd since FTP does *not* encrypt any data in transit, including user credentials, need to enable TLS/SSL to provide that encryption. Use `openssl` to create a new certificate and use the `-days` flag to make it valid for one year. Then by setting both the `-keyout` and `-out` flags to the same value, the private key and the certificate will be located in the same file.

A screenshot of a terminal window on a Linux system. The title bar says "Terminal". The command entered is "root@ubuntug7:~\$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.pem". The terminal then prompts for certificate information, asking for fields like Country Name, State or Province Name, Locality Name, Organization Name, Organizational Unit Name, Common Name, and Email Address. The user inputs values such as "US" for Country Name, "NY" for State or Province Name, "New York City" for Locality Name, "Internet Widgits Pty Ltd" for Organization Name, and "192.168.10.4" for Common Name.

Figure 5. 225 : Create ssl certificates vsftpd

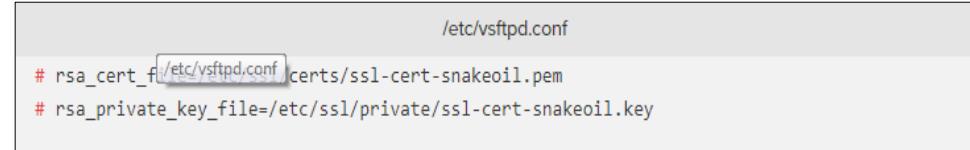
Step 2: Once have created the certificates, open the vsftpd configuration file again



```
rYHxDiElPAhExRmqe9yoivsZVY1/eQLvgNxQIDAQABo1AwTjAdBgNVHQ4EFgQU  
GtkTzWDX6zgxebTx51VkJAL+uAcwHwYDVR0jBBgwFoAUGtKTzWDX6zgxebTx51V  
kAL+uAcwDAYDVR0TBBAUwAwEB/zANBqkqhkiG9w0BAQsFAAOCAQEApiabfaB4pdEl  
f/6Vf8pmJ0sh5go04gjkg907/QQfYgpDn3SCi9RMhZpCXf6mhTvMdms0R4+hewHa  
iG22/9o4uRfhmd8WgVp4h0sDjex8miyEDS52yfmrTVdz7yjuwLuZ44S0HLhlsBknN  
peDVpfNVivynWqZeBJt7IbPOyvRhvm15B4F9rjWBaCIgvKR2rFAdZpA68W+ndUC  
EP5PnPBrtrLFfJ0NuG9riUkGg//3rGFIqkpMf+39CuF2w+izaJyEMTsdd0+G5Al6s  
FTks5evwIFtDDo3XlZ30uocZXxfx2laFGmvIhv4sQcT8ZdkYqFeSt+5bwh0tBqEc  
7hqvTCUSyQ==  
-----END CERTIFICATE-----  
root@ubuntug7: /home/ubuntug7# sudo nano /etc/vsftpd.conf
```

Figure 5. 226 : open vsftpd configuration file

Step 3: Toward the bottom of the file, noticed two lines that begin with rsa_. Comment them out.



```
/etc/vsftpd.conf  
# rsa_cert_file=/etc/vsftpd.conf certs/ssl-cert-snakeoil.pem  
# rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
```

Figure 5. 227 : comment command

Step 4: Below them, add the following lines which point to the certificate and private key we just created.



```
/etc/vsftpd.conf  
rsa_cert_file=/etc/ssl/private/vsftpd.pem  
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
```

Figure 5. 228 : Add command point to certificate

Step 5: After that, we will force the use of SSL, which will prevent clients that can't deal with TLS from connecting. This is necessary in order to ensure all traffic is encrypted but may force your FTP user to change clients. Change ssl_enable to YES.



```
/etc/vsftpd.conf  
ssl_enable=YES
```

Figure 5. 229 : Command force use of SSL

Step 6: After that, add the following lines to explicitly deny anonymous connections over SSL and to require SSL for both data transfer and logins

```
/etc/vsftpd.conf  
allow_anon_ssl=NO  
force_local_data_ssl=YES  
force_local_logins_ssl=YES
```

Figure 5. 230 : Add command to deny annoynomous over SSL

Step 7: After this, configure the server to use TLS, the preferred successor to SSL by adding the following line.

```
/etc/vsftpd.conf  
ssl_tlsv1=YES  
ssl_ss1v2=NO  
ssl_ss1v3=NO
```

Figure 5. 231 : Add command ssl_tlsv1 only

Step 8: Finally, add two more options. First, will not require SSL reuse because it can break many FTP clients and second will require "high" encryption cipher suites, which currently means key lengths equal to or greater than 128 bits.

```
/etc/vsftpd.conf  
require_ssl_reuse=NO  
ssl_ciphers=HIGH
```

Figure 5. 232 : Command allow ftp client without SSL

Step 9: When everything done, save and close the file and next need to restart the server for the changes to take effect.

```
Terminal Terminal File Edit View Search Terminal Help  
root@ubuntug7: /home/ubuntug7  
root@ubuntug7:/home/ubuntug7# sudo systemctl restart vsftpd
```

Figure 5. 233 : Command restart vsftpd

5.2.11 AAA (Authentication, Authorization, and Accounting) using Radius

Step 1: Click Start and then click **Server Manager > Dashboard**. Next, right click on **Add Roles and Features**.

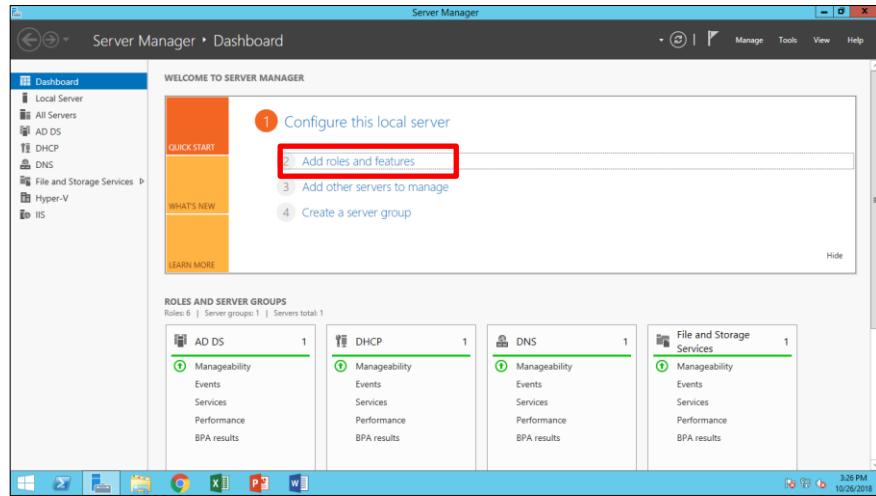


Figure 5. 234 : Server Manager

Step 2: In the **Add Roles and Features Wizard**, if the page Before You Begin appears, click **next**. On the before you begin page, verify that our destination server and network environment are prepared for the role and feature we want to install. Then, click **next**.

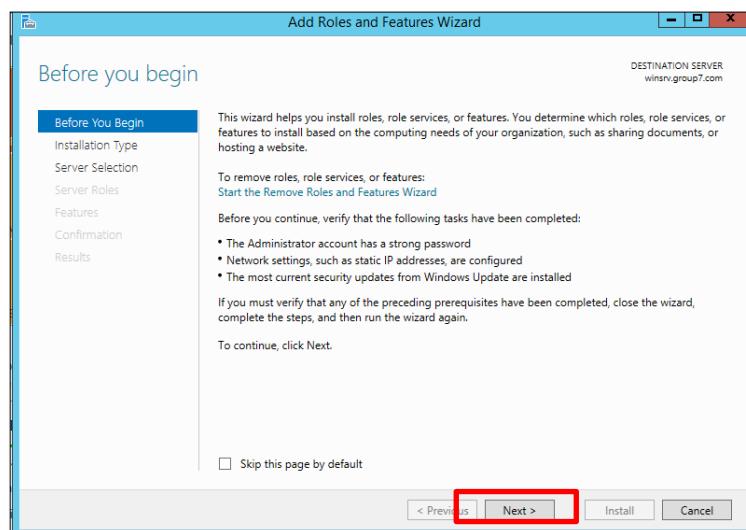


Figure 5. 235 : Add Roles and Features

Step 3: In the Roles list, click **Network Policy and Access Services**, and then click **next**. Network Policy and Access Services (NPAS) allows you to provide local and remote network access and to define and enforce policies for network access authentication, authorization, and client health.

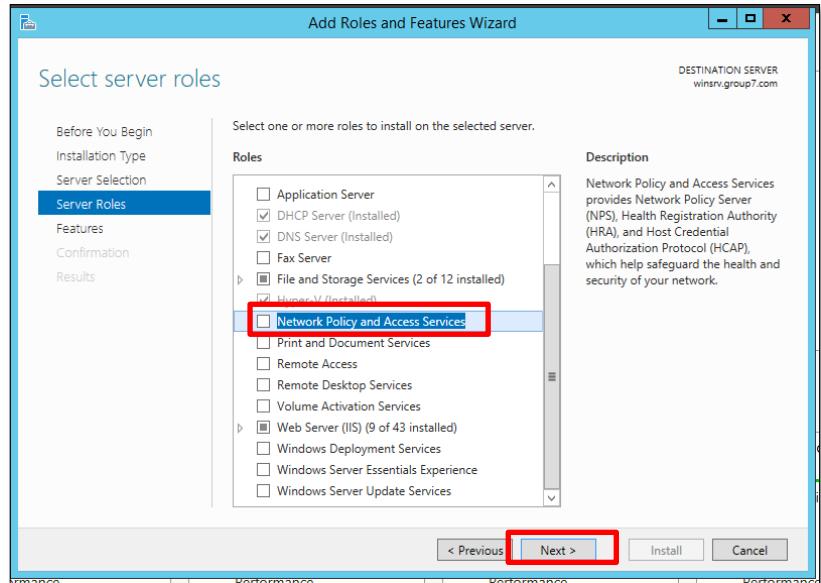


Figure 5. 236 : Select server roles

Step 4: Wait until the features **Network Policy and Access Services** installation done, and then click **Close**.

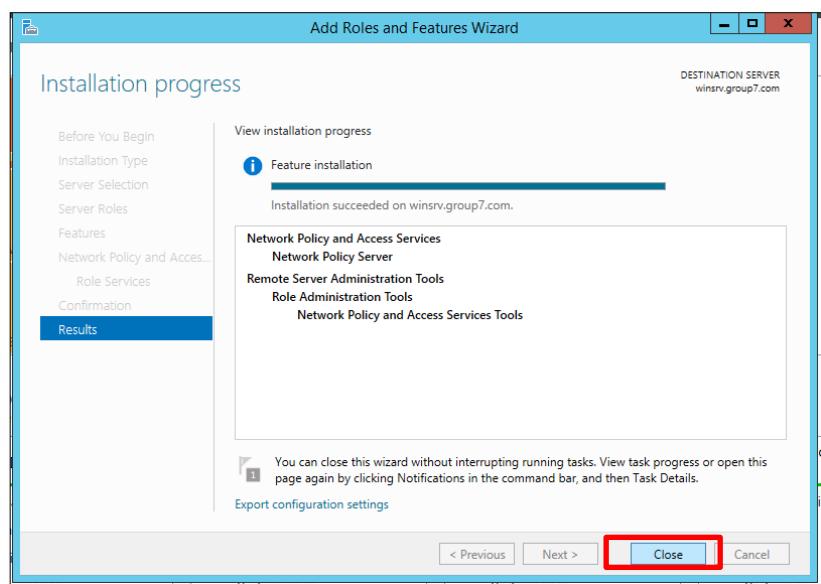


Figure 5. 237 : Installation progress

Step 5: Right click on **NAP**, and then click **Network Policy Server**, then click to **register server in Active Directory**. When Network Policy Server (NPS) is a member of an Active Directory Domain Services (AD DS) domain, NPS performs authentication by comparing user credentials that it receives from network access servers with the credentials that are stored for the user account in AD DS. In addition, NPS authorizes connection requests by using network policy and by checking user account in AD DS.

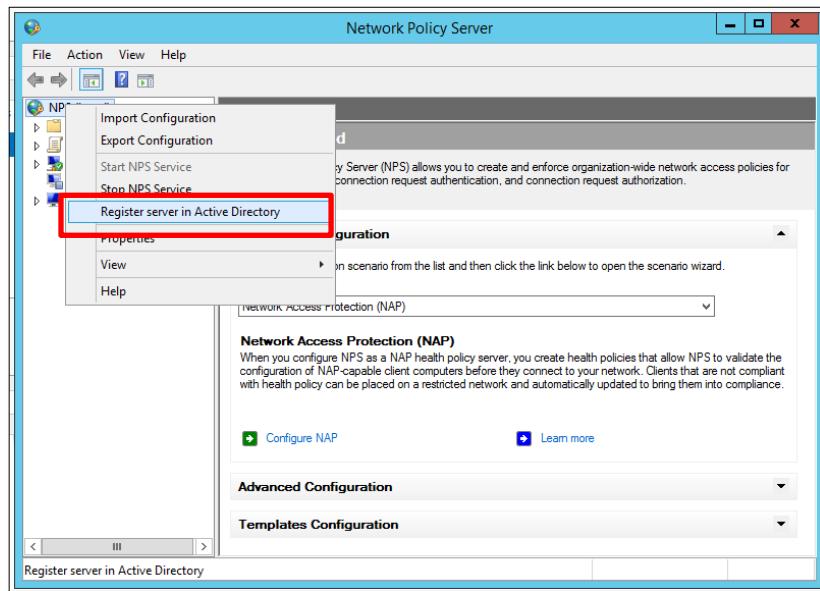


Figure 5. 238 : Network Policy Server

Step 6: Network Policy Server will prompt this window. Then click **OK**.

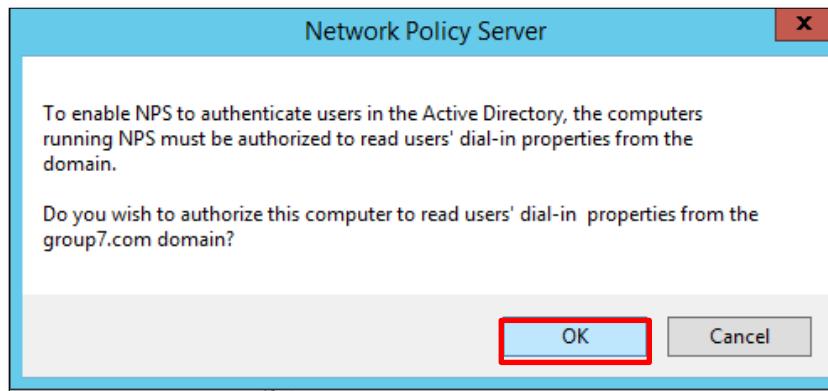


Figure 5. 239 : Enable NPS

Step 7: Right click on **RADIUS Client**, and then **New RADIUS Client**.

A network access server (NAS) is a device that provides some level of access to a larger network. A NAS using a RADIUS infrastructure is also a RADIUS client, sending connection requests and accounting messages to a RADIUS server for authentication, authorization, and accounting.

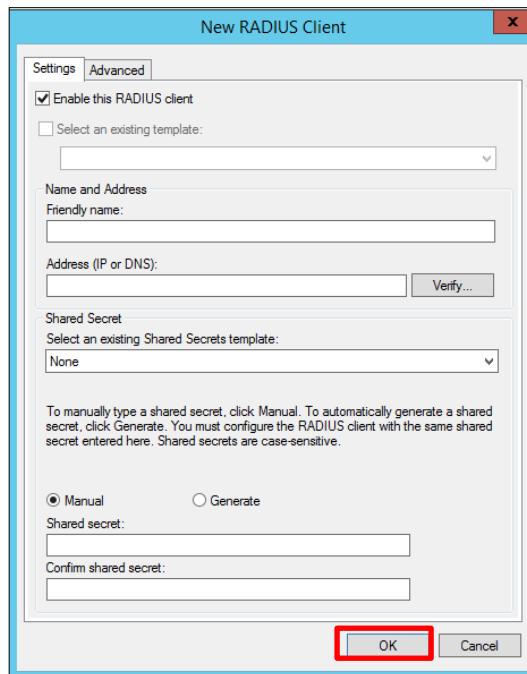


Figure 5. 240 : New radius client

Step 8: Enter Friendly **Name and IP address** (default IP gateway for your router). Tick manual secret and enter the Shared secret. Then, clicks apply and **OK**.

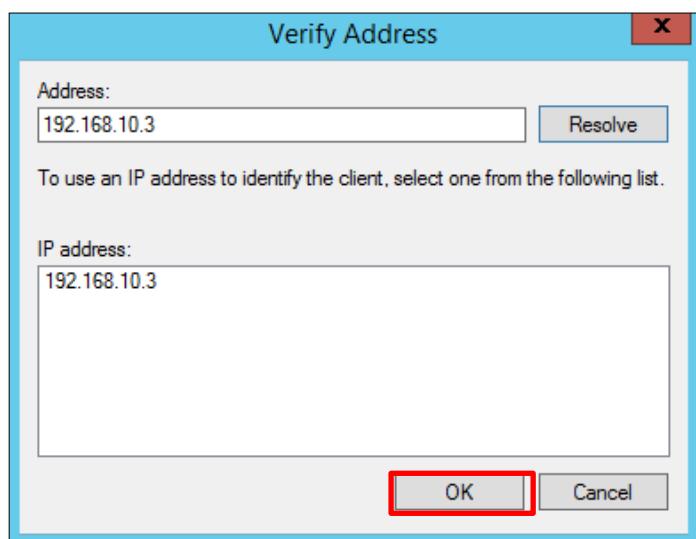


Figure 5. 241 : Verify Address

Step 9: Next we need to **create new network policies**. To do that, go to the **network policies** and then right click on it, after that click **New**. Network policies are sets of conditions, constraints, and settings that allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect. When you deploy Network Access Protection (NAP), health policy is added to the network policy configuration so that Network Policy Server (NPS) performs client health checks during the authorization process.

When processing connection requests as a Remote Authentication Dial-In User Service (RADIUS) server, NPS performs both authentication and authorization for the connection request. During the authentication process, NPS verifies the identity of the user or computer that is connecting to the network. During the authorization process, NPS determines whether the user or computer is allowed to access the network.

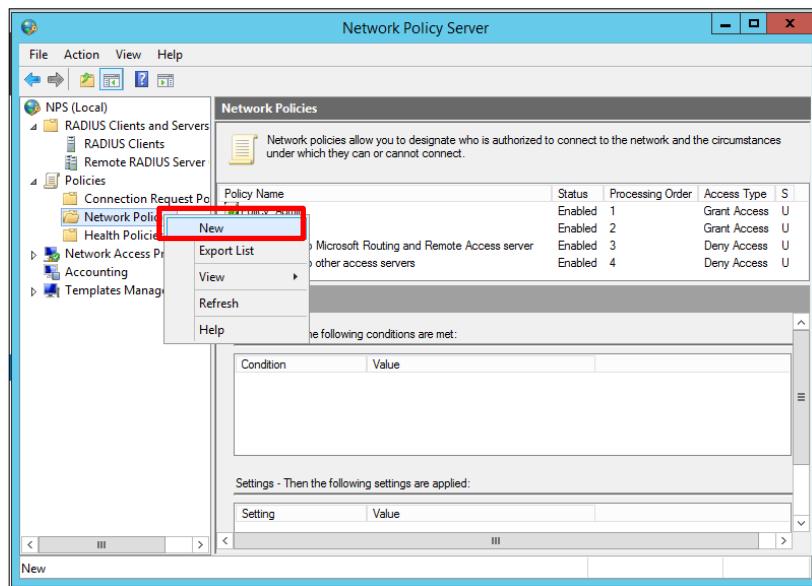


Figure 5. 242 : New network policies

Step 10: Enter the Policy Name and click **next**.

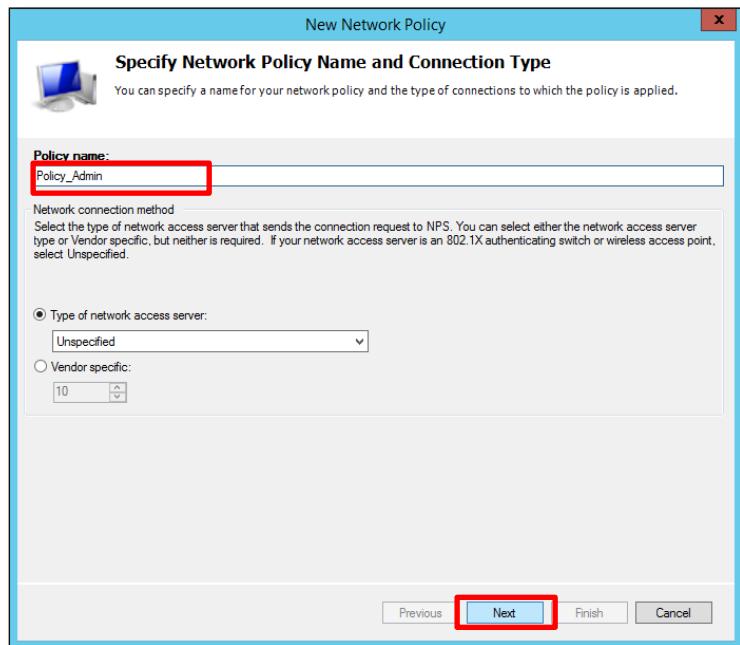


Figure 5. 243 : Policy Name

Step 11: Select the **condition > User Groups**, the click **Add**.

You can use this procedure to create a user or computer group in Active Directory Domain Services (AD DS) and then add the group as a condition in a Network Policy Server (NPS) network policy. Membership in Domain Users, or equivalent, is the minimum required to complete this procedure.

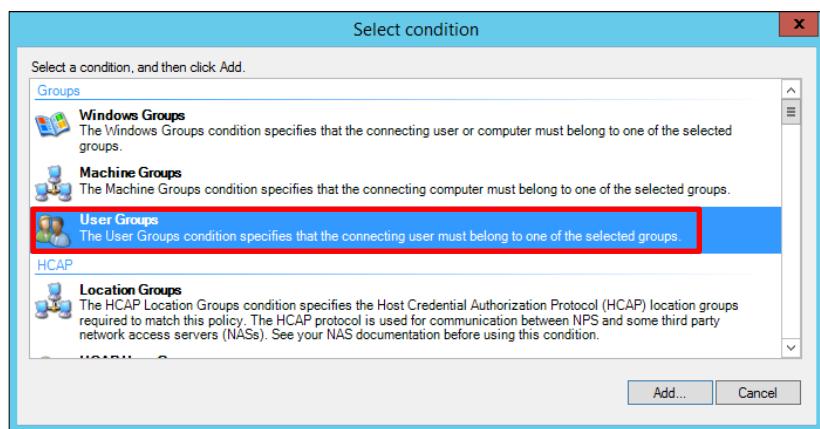


Figure 5. 244 : Specify Condition

Step 12: In User Groups page, click Add Groups.

This step is to define which groups that can access the network.

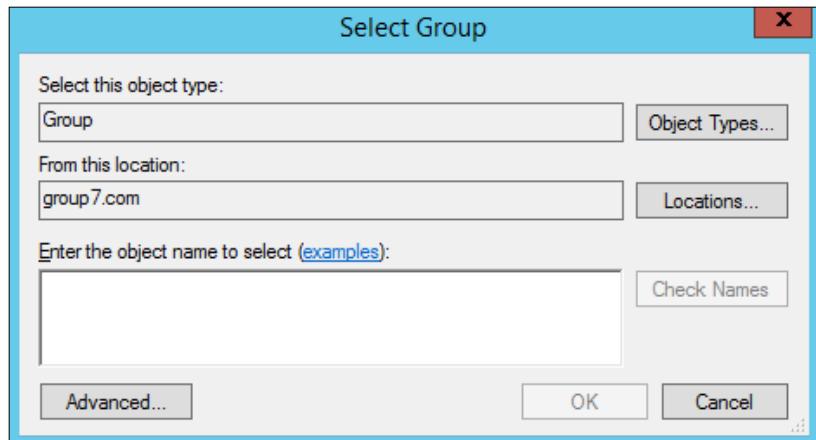


Figure 5. 245 : Select group

Step 13: Enter the object name to select > type “AAA” > click Check Names.

Then, choose **AAAGroup7admin** and click **OK**.

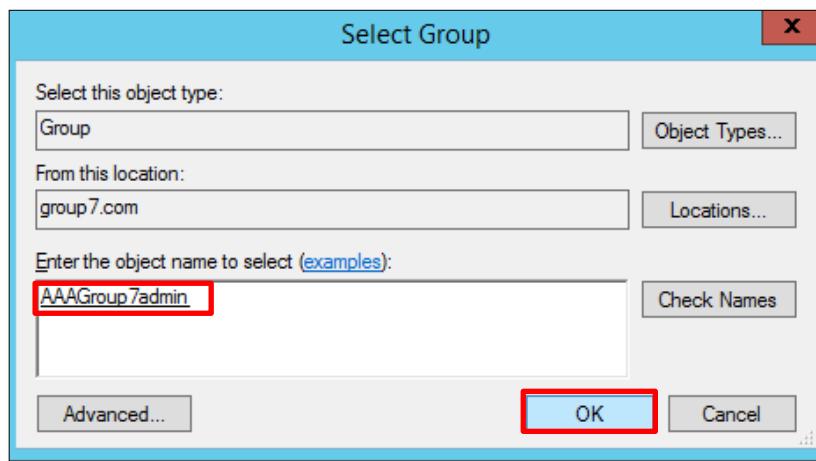


Figure 5. 246 : Check names

Step 14: Proceed to **OK**.

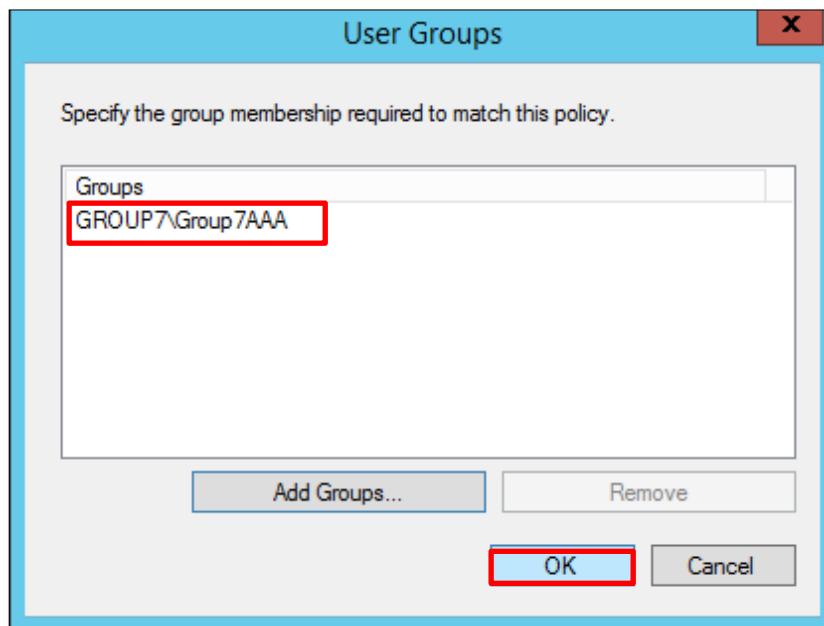


Figure 5. 247 : User groups

Step 15: In **Specify Access Permission**, tick **Access granted**. Proceed to **Next**.

This step is to configure whether you want to grant network access or deny network access if the connection request matches this policy.

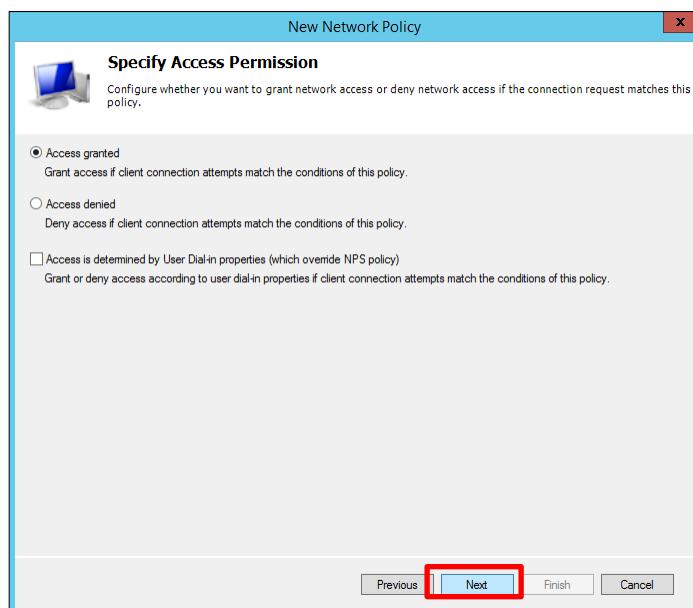


Figure 5. 248 : Access permission

Step 16: On Configuration Authentication Methods, tick on Unencrypted authentication (PAP, SPAP), and Encrypted authentication. Proceed to Next. When Connection Request Policy windows appear, click **no**.

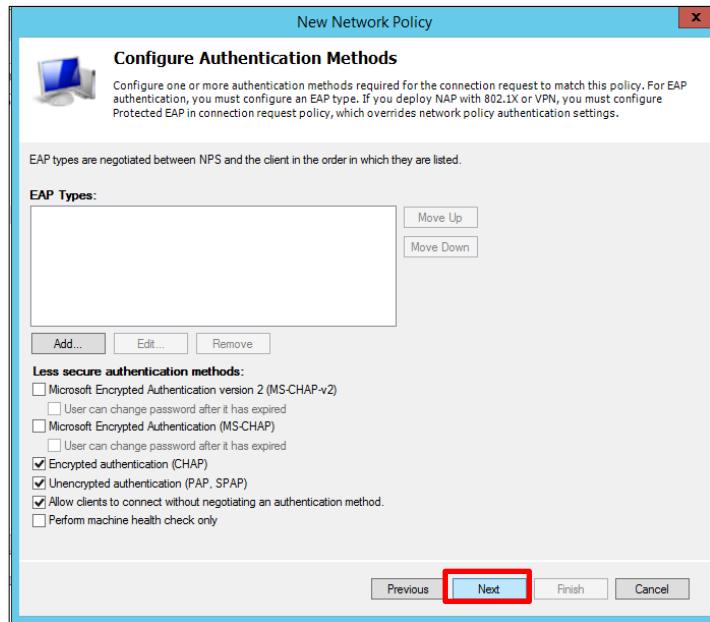


Figure 5. 249 : Authentication method

Step 17: Configure Constraint page, proceed to Next.

Constraint are additional parameters of the network policy that are required to match the connection request.

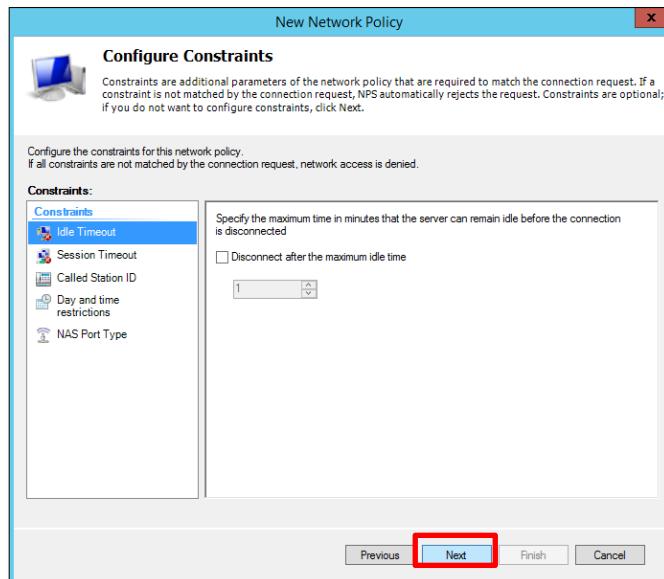


Figure 5. 250 : Configure constraint

Step 18: In Standard, remove **Framed-Protocol** and edit Service -Type attributes.

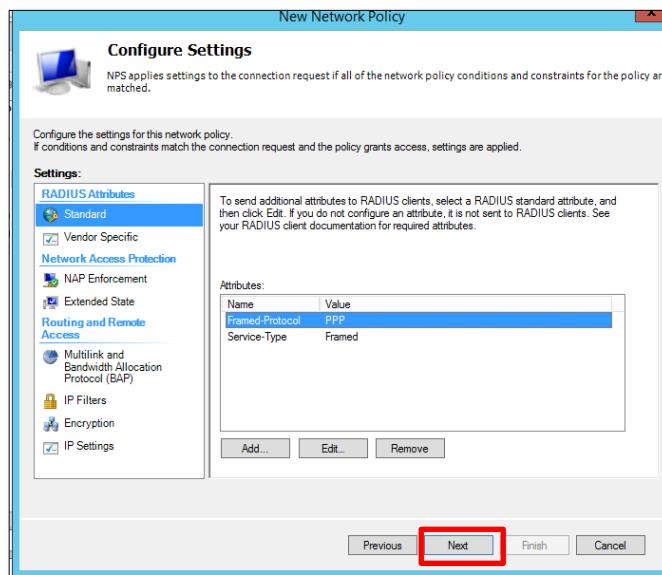


Figure 5. 251 : Configure settings

Step 19: Then, select **others** > pick **Login**. After that, click **OK**.

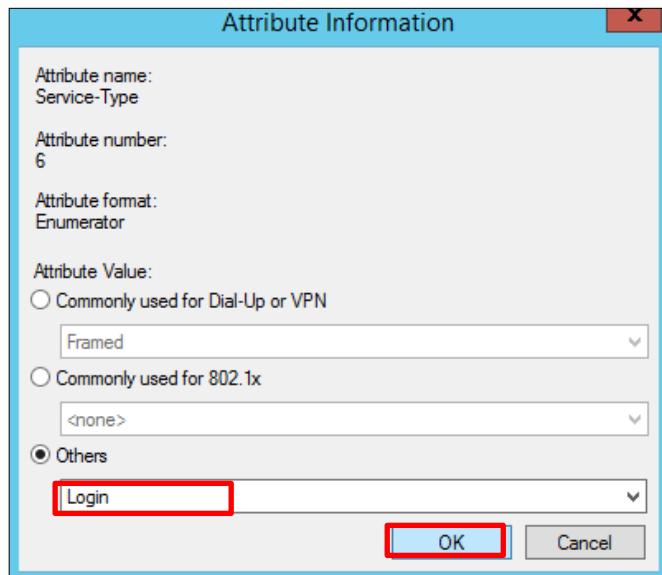


Figure 5. 252 : Attribute information

Step 20: In Vendor Specific, click Add.

Vendor-Specific Attributes (VSA) is a method for communicating vendor-specific information between NASs and RADIUS servers. Attribute 26 encapsulates vendor specific attributes, thereby, allowing vendors to support their own extended attributes otherwise not suitable for general use.

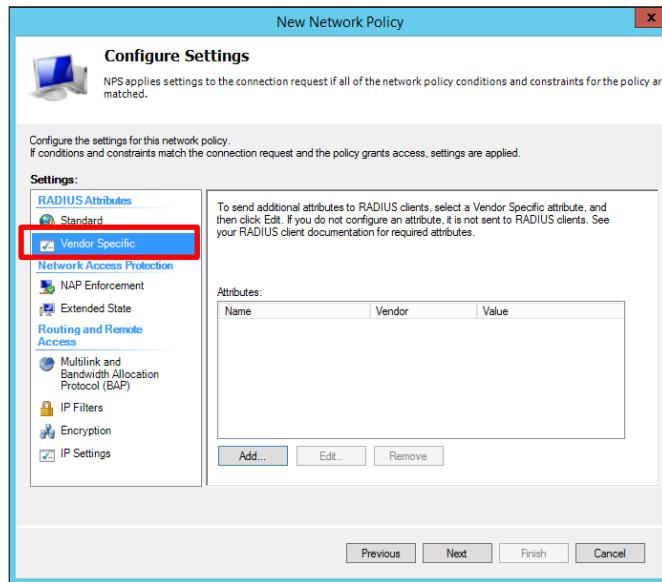


Figure 5. 253 : Vendor specific

Step 21: Add attributes name **Cisco-AV-Pair**, vendor Cisco and value **shell:priv lvl=15**.

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

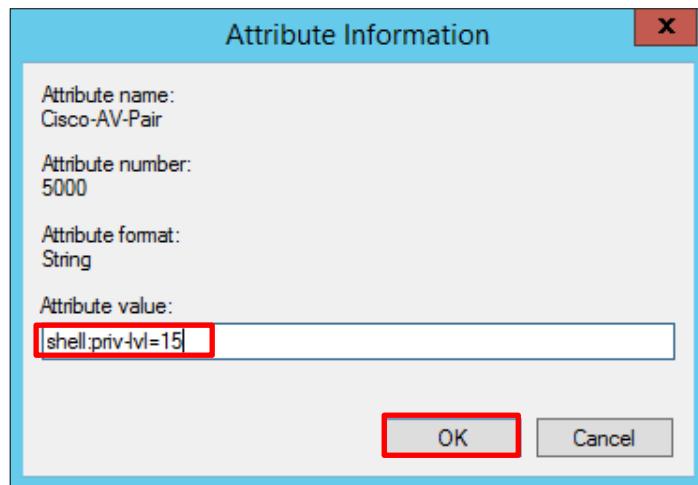


Figure 5. 254: Attribute value

Step 22: In **Completing New Network Policy**, it will displays that successfully created the network policy, Click **Finish**. Then your network policy is created.

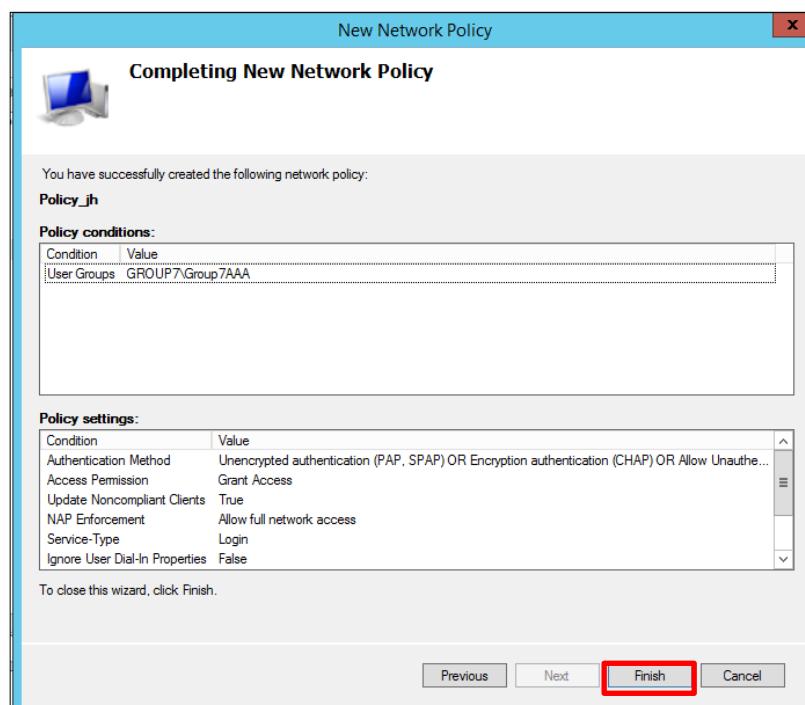


Figure 5. 255 Successful created network policy

Step 23: On the Accounting tab, click on Configure Accounting.

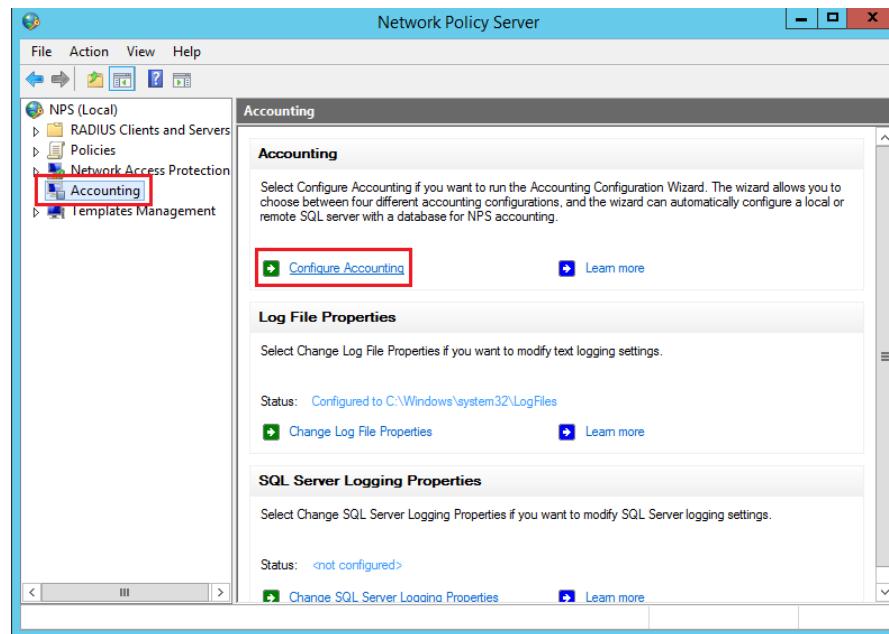


Figure 5. 256 : Accounting in Network Policy Server

Step 24: Click next on the Introduction page of the Accounting Configuration Wizard.

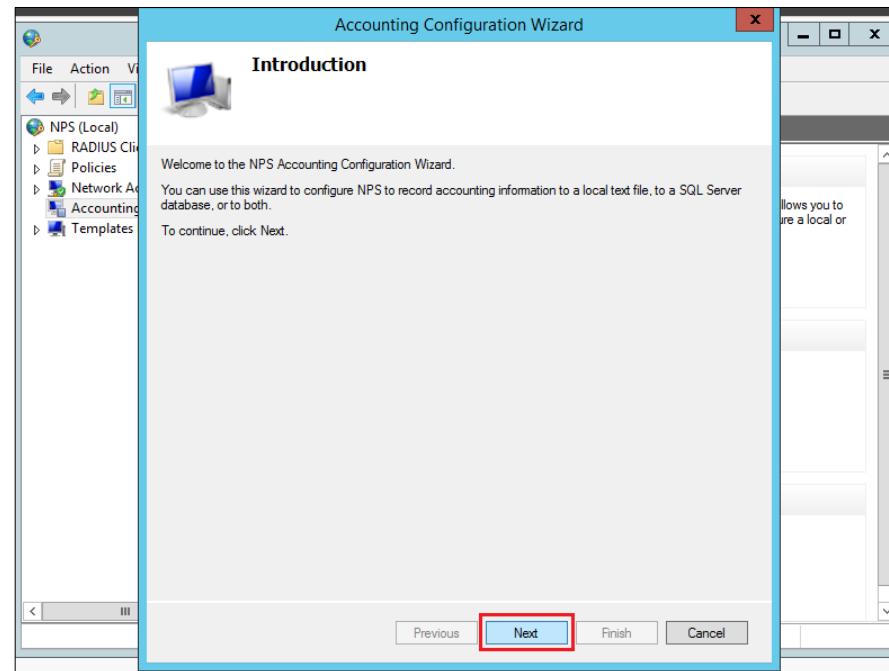


Figure 5. 257: Introduction in accounting configuration

Step 24: Select Accounting Options, pick Log to a text file on the local computer. Then, click next.

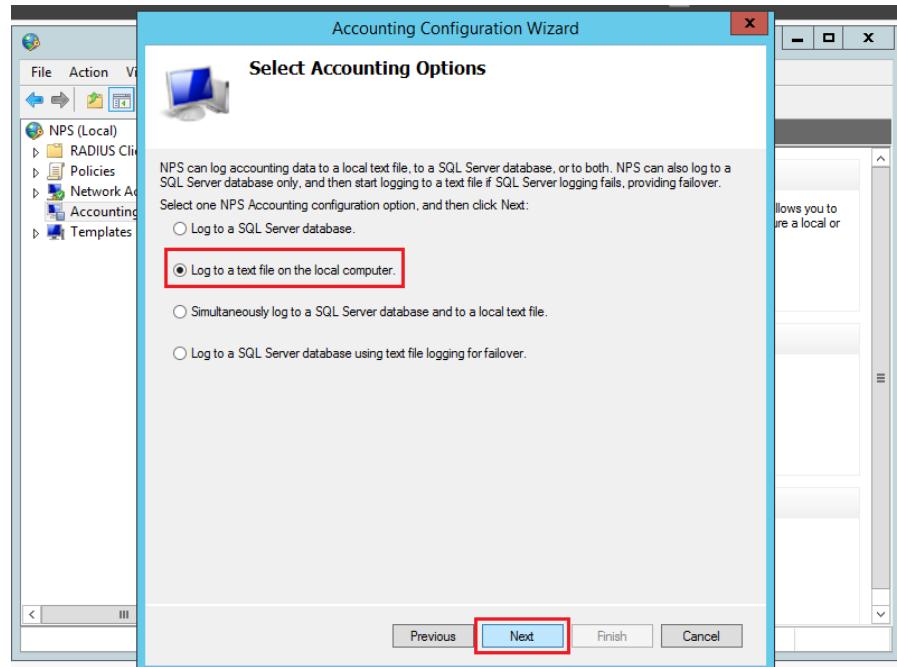


Figure 5. 258 : Select accounting option

Step 25: Pick all the highlighted option for Logging Information. Then, specify a location for the log file. Mark the options to discard connection requests if logging fails. Then, click next.

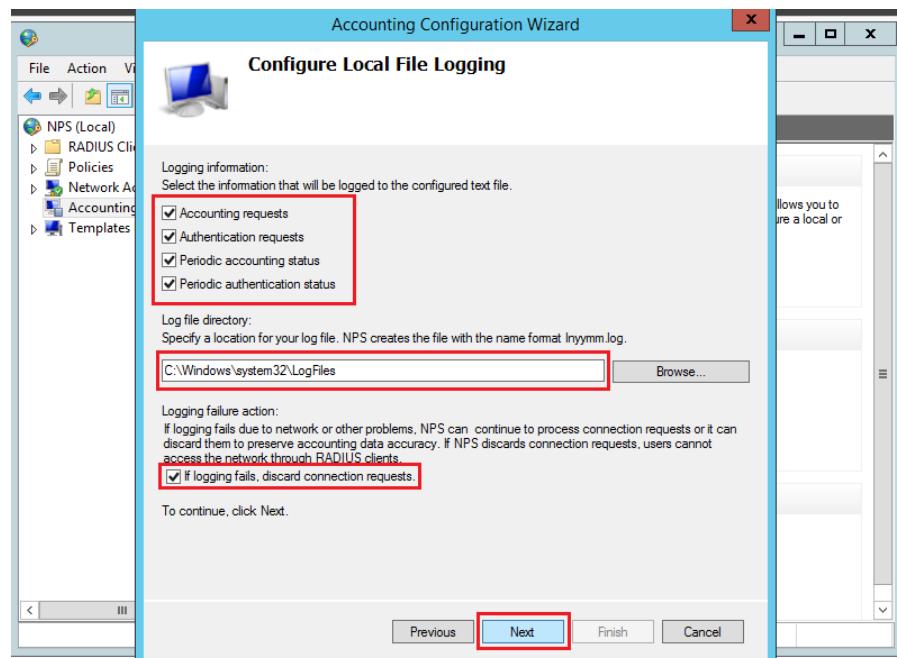


Figure 5. 259: Configure file logging

Step 26: In the Conclusion page, click Close.

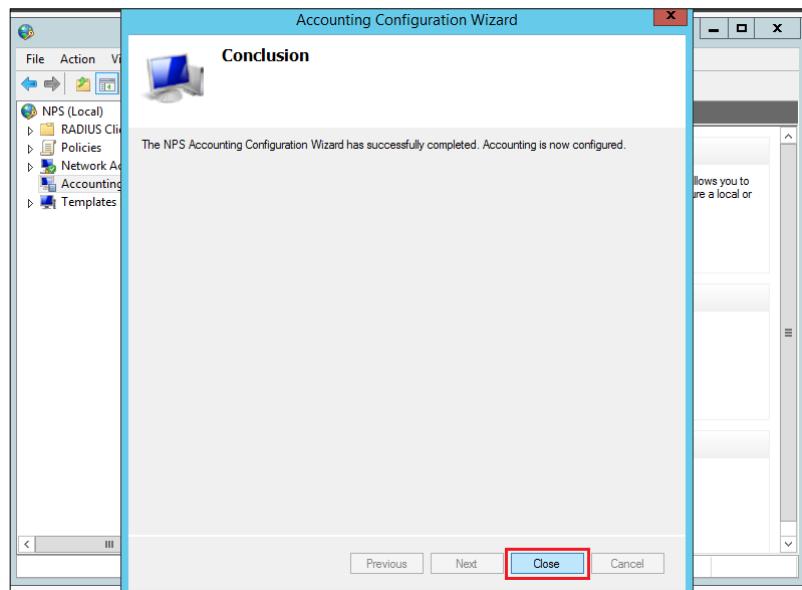
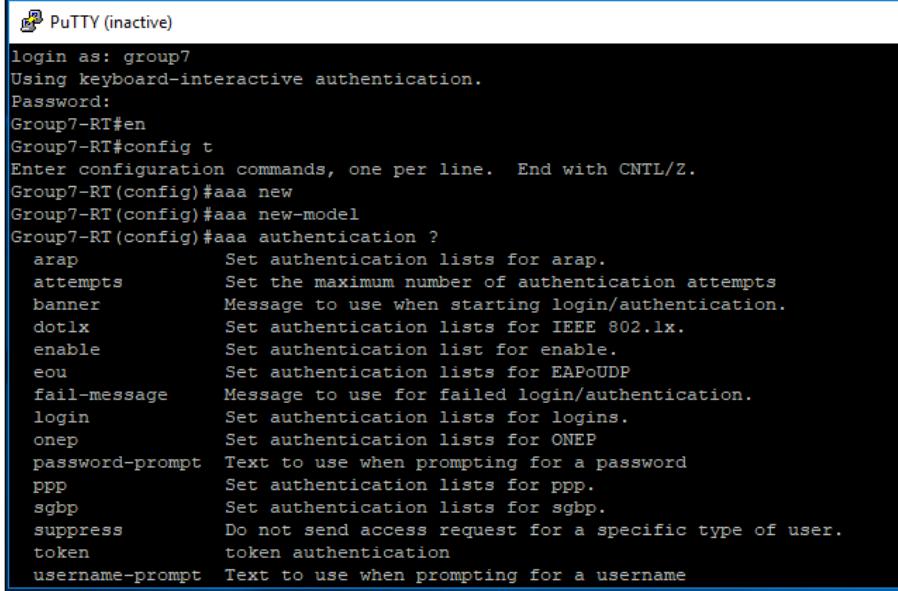


Figure 5. 260 : Conclusion

AUTHENTICATION USING RADIUS SERVER

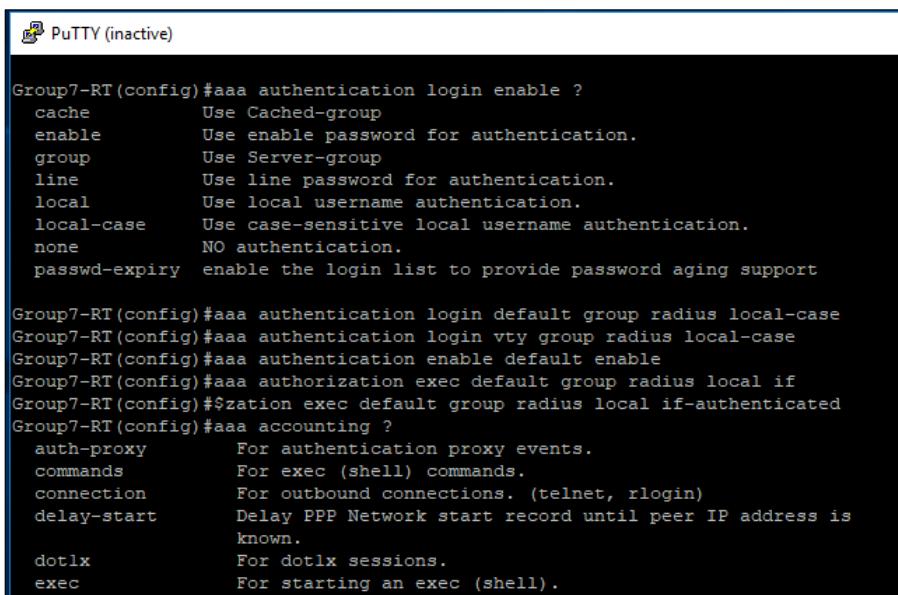
Step 1: Open Putty, then get into your router configuration and enter this command:

```
Router(config)# config t  
  
Router(config)# aaa new-model  
  
Router(config)# aaa group server radius RAD  
  
Router(config-in-rad)# server-private 192.168.10.3 auth-port 1645 acct-port  
1646 key Group7123Admin  
  
Router(config-in-rad)# exit  
  
Router(config)# aaa authentication login default group RAD local  
  
Router(config)# aaa authorization exec default group RAD local if-  
authenticated  
  
Router(config)# aaa authorization console  
  
Router(config)# exit
```



```
PuTTY (inactive)
login as: group7
Using keyboard-interactive authentication.
Password:
Group7-RT#en
Group7-RT#config t
Enter configuration commands, one per line. End with CNTL/Z.
Group7-RT(config)#aaa new
Group7-RT(config)#aaa new-model
Group7-RT(config)#aaa authentication ?
  arap      Set authentication lists for arap.
  attempts  Set the maximum number of authentication attempts
  banner    Message to use when starting login/authentication.
  dot1x    Set authentication lists for IEEE 802.lx.
  enable    Set authentication list for enable.
  eou       Set authentication lists for EAPoUDP
  fail-message Message to use for failed login/authentication.
  login     Set authentication lists for logins.
  onep     Set authentication lists for ONEP
  password-prompt Text to use when prompting for a password
  ppp       Set authentication lists for ppp.
  sgbp     Set authentication lists for sgbp.
  suppress  Do not send access request for a specific type of user.
  token    token authentication
  username-prompt Text to use when prompting for a username
```

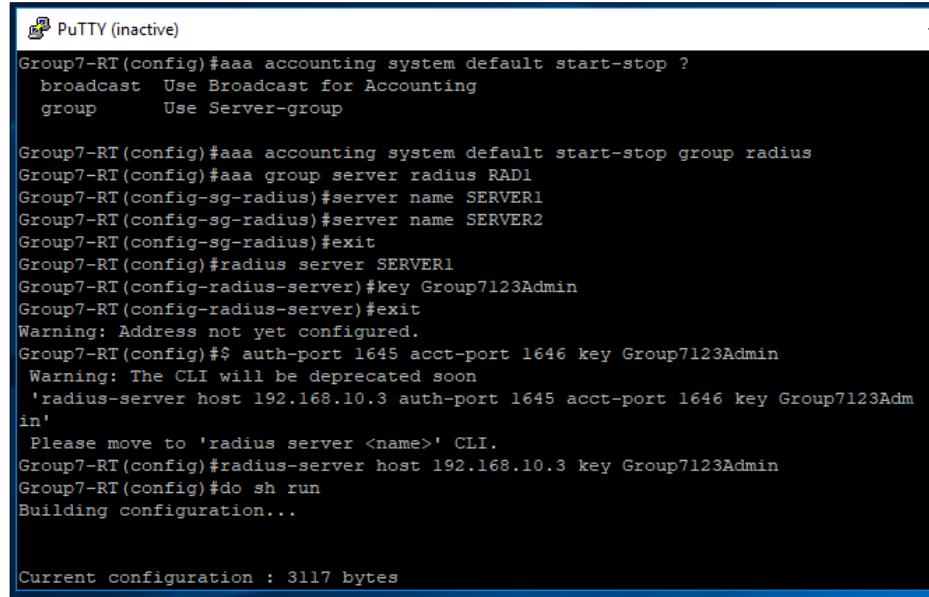
Figure 5. 261 : Configuration in putty for aaa new model



```
PuTTY (inactive)
Group7-RT(config)#aaa authentication login enable ?
  cache      Use Cached-group
  enable     Use enable password for authentication.
  group      Use Server-group
  line       Use line password for authentication.
  local      Use local username authentication.
  local-case Use case-sensitive local username authentication.
  none       NO authentication.
  passwd-expiry enable the login list to provide password aging support

Group7-RT(config)#aaa authentication login default group radius local-case
Group7-RT(config)#aaa authentication login vty group radius local-case
Group7-RT(config)#aaa authentication enable default enable
Group7-RT(config)#aaa authorization exec default group radius local if
Group7-RT(config)#$zation exec default group radius local if-authenticated
Group7-RT(config)#aaa accounting ?
  auth-proxy   For authentication proxy events.
  commands    For exec (shell) commands.
  connection  For outbound connections. (telnet, rlogin)
  delay-start Delay PPP Network start record until peer IP address is
               known.
  dot1x      For dot1x sessions.
  exec       For starting an exec (shell).
```

Figure 5. 262: Configuration in putty for authentication



```
PuTTY (inactive)
Group7-RT(config)#aaa accounting system default start-stop ?
  broadcast  Use Broadcast for Accounting
  group      Use Server-group

Group7-RT(config)#aaa accounting system default start-stop group radius
Group7-RT(config)#aaa group server radius RAD1
Group7-RT(config-sg-radius)#server name SERVER1
Group7-RT(config-sg-radius)#server name SERVER2
Group7-RT(config-sg-radius)#exit
Group7-RT(config)#radius server SERVER1
Group7-RT(config-radius-server)#key Group7123Admin
Group7-RT(config-radius-server)#exit
Warning: Address not yet configured.
Group7-RT(config)#${ auth-port 1645 acct-port 1646 key Group7123Admin
  Warning: The CLI will be deprecated soon
  'radius-server host 192.168.10.3 auth-port 1645 acct-port 1646 key Group7123Adm
in'
  Please move to 'radius server <name>' CLI.
Group7-RT(config)#radius-server host 192.168.10.3 key Group7123Admin
Group7-RT(config)#do sh run
Building configuration...

Current configuration : 3117 bytes
```

Figure 5. 263 : Configuration in putty for server name

Step 2: Then type “show run” to make sure you have done all of the command.



```
:
hostname Group7-RT
!
boot-start-marker
boot-end-marker
!
!
!
!
aaa new-model
!
!
aaa group server radius RAD1
  server name SERVER1
  server name SERVER2
!
aaa authentication login default group radius local-case
aaa authentication login vty group radius local-case
aaa authentication enable default enable
aaa authorization exec default group radius local if-authenticated
aaa accounting system default start-stop group radius
!
```

Figure 5. 264 : Show run in putty

5.2.12 Access Control List (ACL)

Step 1: Configure ACL (Access Control List) at router, our access-list was numbered as 122.

First we will deny any access from outside our network to reach https that is in windows server with **200.200.201.4** public IP address.

Second we will deny any outside ip address to reach both ftp and ftpts which is in Fedora server with **200.200.201.6** public ip address.

Lastly, we permit all other ip.

```
Group7-RT#config t
Enter configuration commands, one per line. End with CNTL/Z.
Group7-RT(config)#acce
Group7-RT(config)#access-list 122 deny tcp any host 200.200.201.4 eq 443
Group7-RT(config)#access-list 122 deny tcp any host 200.200.201.6 eq 20
Group7-RT(config)#access-list 122 deny tcp any host 200.200.201.6 eq 21
Group7-RT(config)#int
Group7-RT(config)#interface G0/1
Group7-RT(config-if)#ip acce
Group7-RT(config-if)#ip access-group 122 in
Group7-RT(config-if)#exit
Group7-RT(config)#end
```

Figure 5. 265: ACL Configuration

Step 2: Save ACL configuration

We use **copy run start** to save the configuration.

```
Group7-RT#copy run start
Destination filename [startup-config]?
Building configuration...

[OK]
Group7-RT#
```

Figure 5. 266: Save ACL Configuration

Step 3: Show ACL configuration

```
access-list 1 permit 192.168.100.0 0.0.0.15
access-list 122 deny    tcp any host 200.200.200.4 eq 443
access-list 122 deny    tcp any host 200.200.200.6. eq ftp-data
access-list 122 deny    tcp any host 200.200.200.6. eq ftp
access-list 122 permit ip any any
```

Figure 5. 267: Show ACL configuration

5.2.13 Secured FTP

Step 1: Entering root by “sudo su”, and add group followed by name of the group “groupadd <group name>”.

```
[g7@fedora-group7-com ~]$ sudo su  
[sudo] password for g7:  
[root@fedora-group7-com g7]# groupadd G7sftp
```

Figure 5. 268: Create group by the name “G7sftp”

Step 2: Create new user that will be add in the group that has been created.

```
[root@fedora-group7-com g7]# adduser sftp7 -g G7sftp -s /sbin/nologin
```

Figure 5. 269: Create and add new user to G7sftp with permission.

Step 3: Set the password to access SFTP.

```
[root@fedora-group7-com g7]# passwd sftp7  
Changing password for user sftp7.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.
```

Figure 5. 270: Set password for user “sftp7”.

Step 4: Create directory for folder that will be share.

```
[root@fedora-group7-com g7]# mkdir /home/shareSFTP/
```

Figure 5. 271: Directory named “shareSFTP” has been created.

Step 5: Change permission on directory that we just created.

```
[root@fedora-group7-com g7]# chmod g+rx /home/shareSFTP/
```

Figure 5. 272: Read and execute has been allowed on ‘/home/shareSFTP’.

Step 6: Create subfolder in share folder and give same permission.

```
[root@fedora-group7-com g7]# mkdir -p /home/shareSFTP/file  
[root@fedora-group7-com g7]# chmod g+rwx /home/shareSFTP/file/
```

Figure 5. 273: Create ‘file’ folder and give permission read, write and execute.

Step 7: After that, assign group to SFTP share file.

```
[root@fedora-group7-com g7]# chgrp -R G7sftp /home/shareSFTP/
```

Figure 5. 274: Assign ‘G7sftp’ which is group, to share directory.

Step 8: Configure the ‘sshd_config’.

```
[root@fedora-group7-com g7]# nano /etc/ssh/sshd_config
```

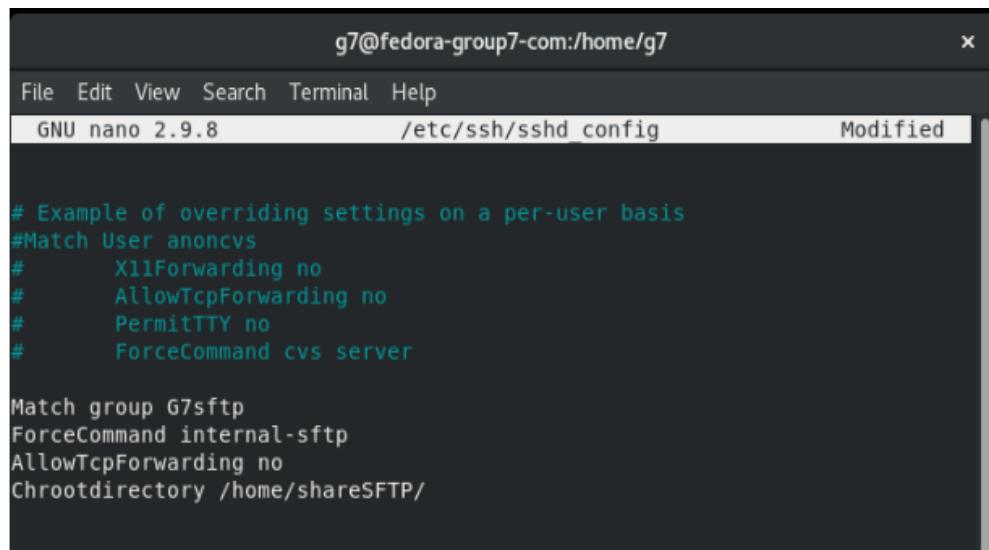
Figure 5. 275 : Access the configuration file.

Step 9: On ‘sshd_config’ file, alter this line to internal sftp.

```
#Subsystem sftp /usr/lib/openssh/sftp-server
Subsystem sftp internal-sftp
```

Figure 5. 276 : Changing the subsystem SFTP to internal only.

Step 10: After that, add this command line below, for declaration of group, shared root directory, disabling TCP Forwarding and force the SFTP to operate internal.



```
# Example of overriding settings on a per-user basis
#Match User anoncvs
#     X11Forwarding no
#     AllowTcpForwarding no
#     PermitTTY no
#     ForceCommand cvs server

Match group G7sftp
ForceCommand internal-sftp
AllowTcpForwarding no
Chrootdirectory /home/shareSFTP/
```

Figure 5. 277: Declare the variable

5.2.14 Web, SSL & Virtual Hosting Linux Email Server

Web

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

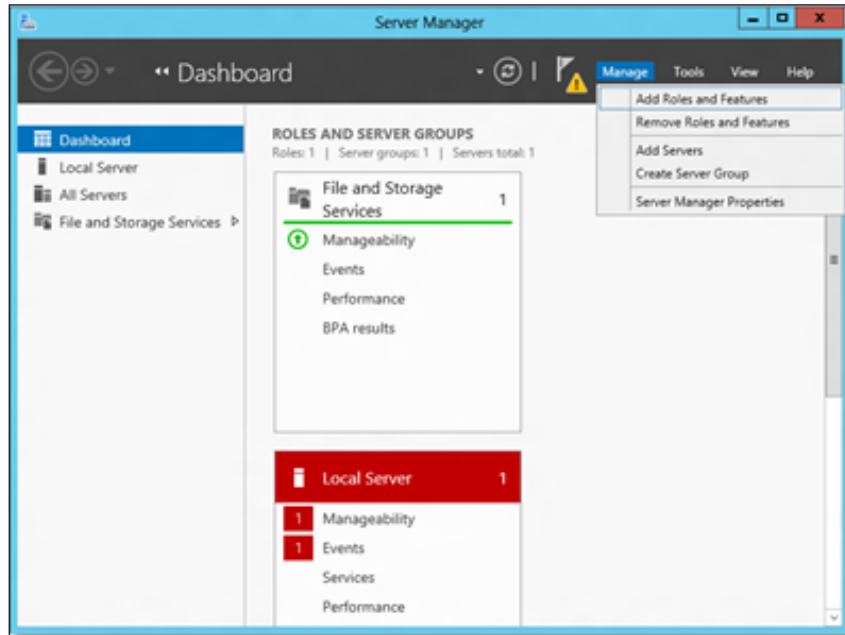


Figure 5. 278: Add role in server

Step 2: Select **Role-based or Feature-based Installation**

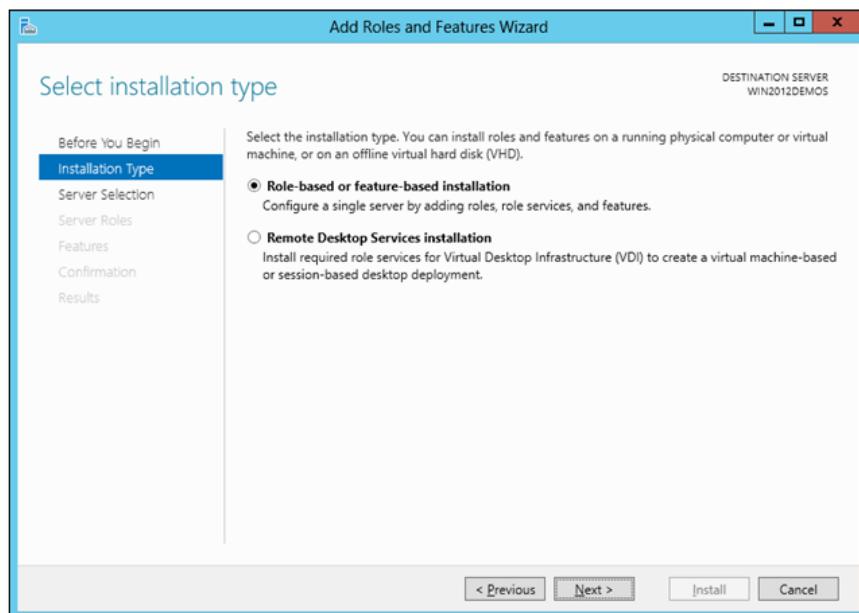


Figure 5. 279: Select Role-based or Feature-based Installation

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

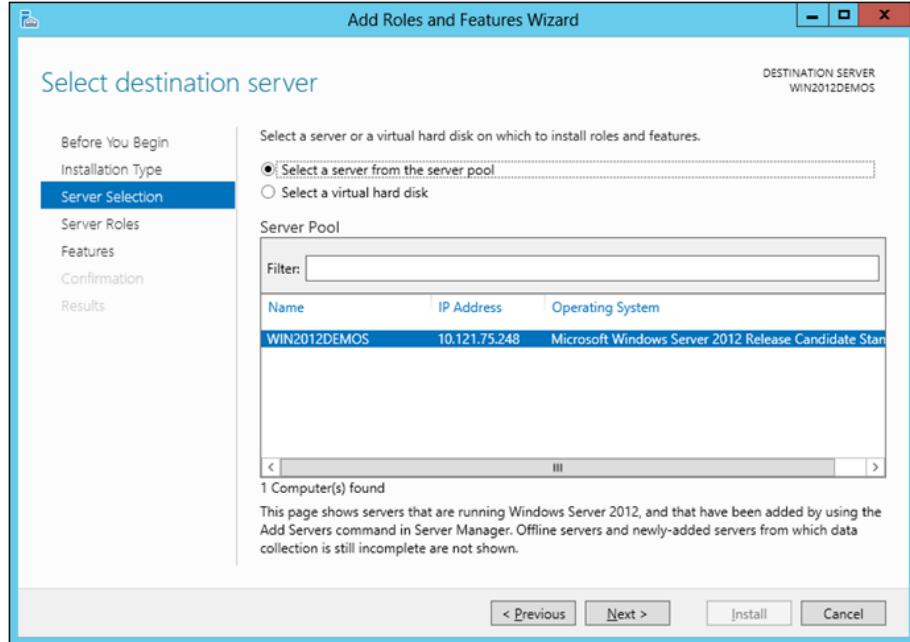


Figure 5. 280: Select Role-based or Feature-based Installation

Step 4: Select Web Server (IIS)

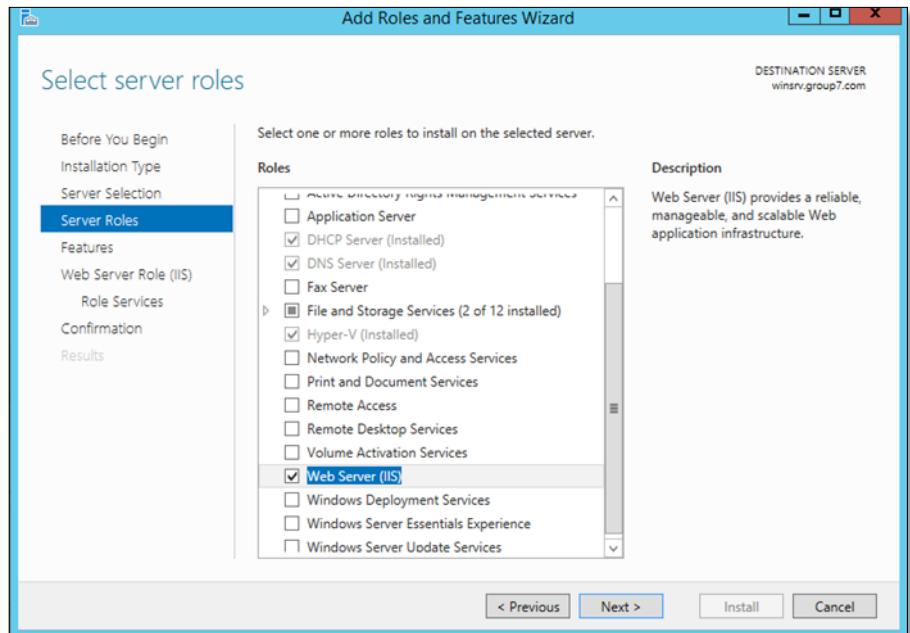


Figure 5. 281: Select Web Server (IIS)

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

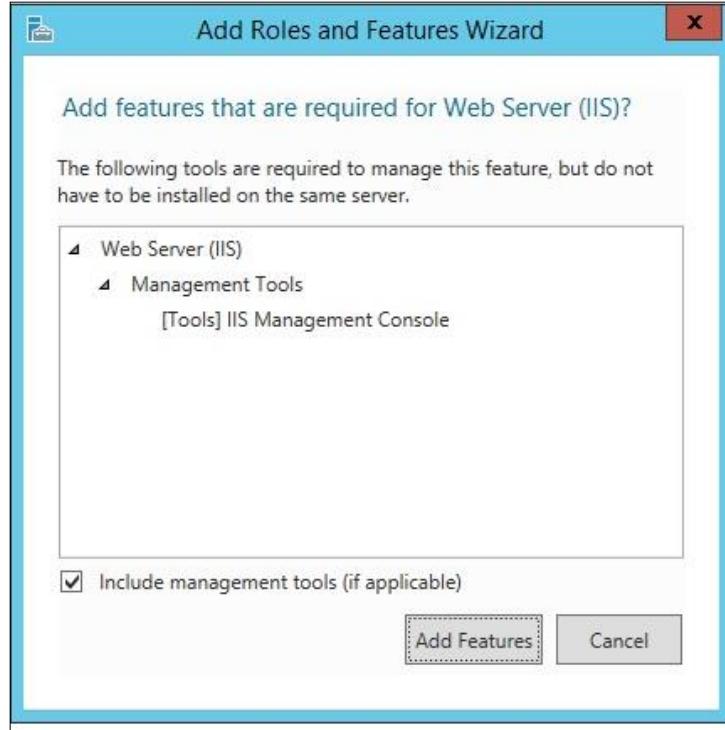


Figure 5. 282: Add Roles and Features wizard

Step 6: Keeping click next until to reach confirmation page

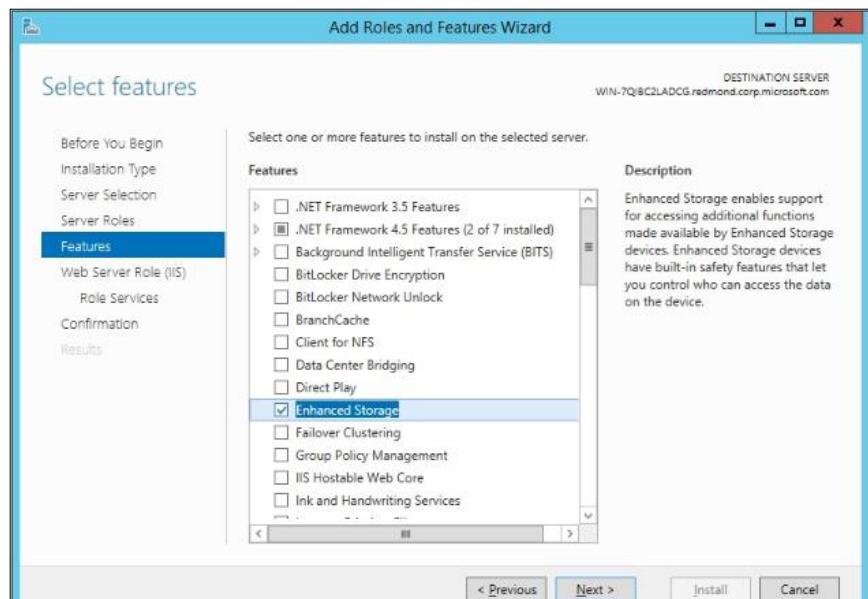


Figure 5. 283: Keep clicking next until reaching to confirmation page

Step 7: In conformation page click **Install** to start installing

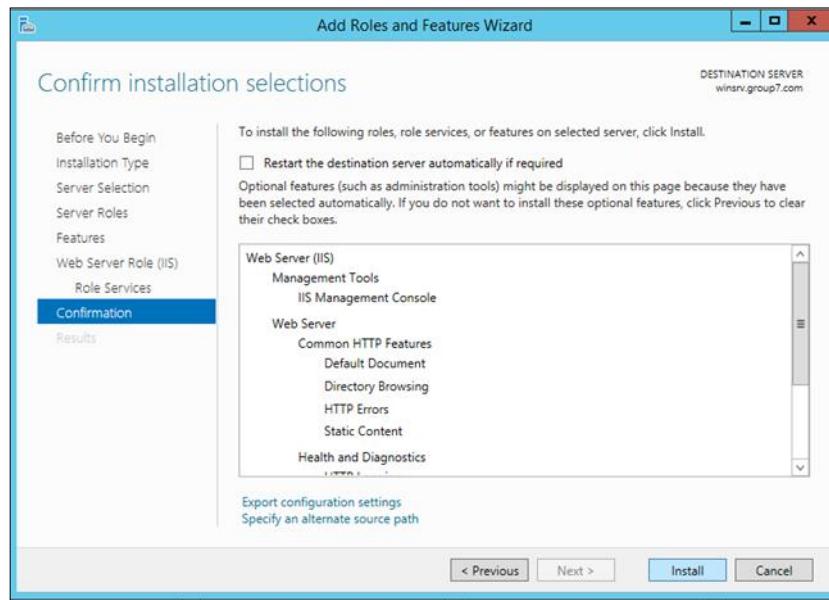


Figure 5. 284: Installing conformation

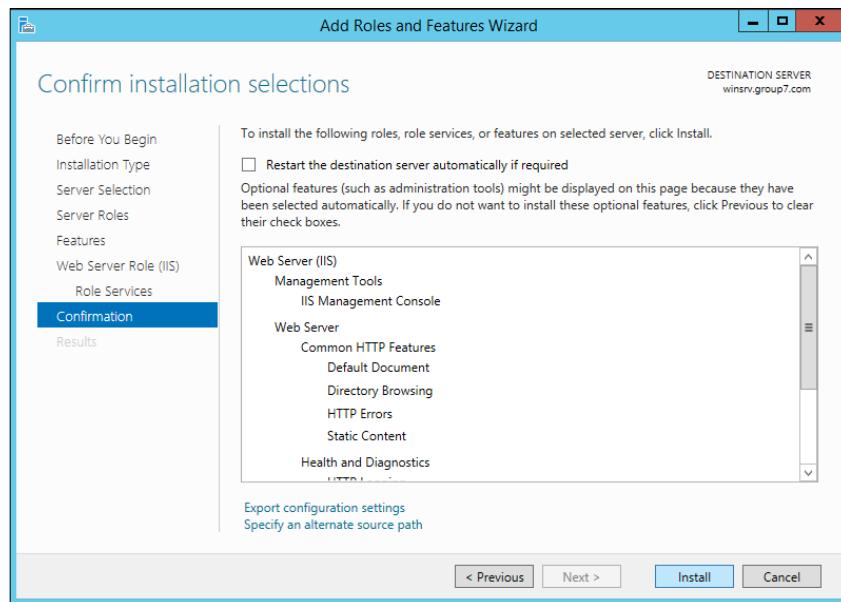


Figure 5. 285: Installing progress

Step 8: After finishing the installation, Go to **Administrator** tools and click Internet

Information Service (IIS). Right click at **Sites** and choose Add website to add a new website

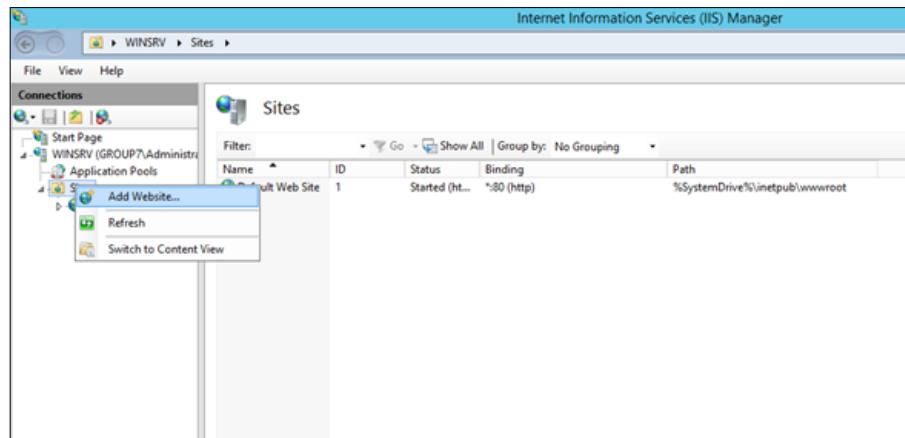


Figure 5. 286: IIS manager to adding new web

Step 9: Right Click at Sites and click Add New Site. Fill all the details for the website including the web path and click OK to finish

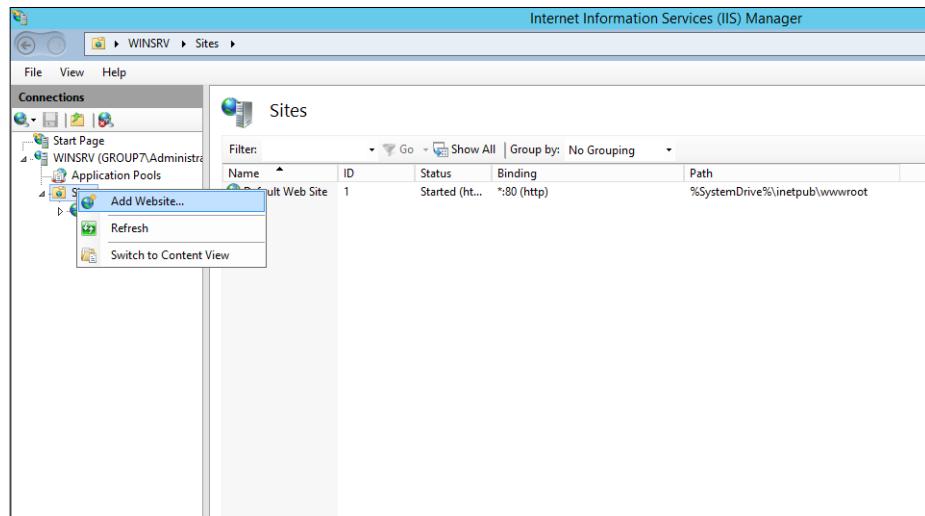


Figure 5. 287: IIS manager to adding new web

Step 10: Right Click at sites and click add new site. Fill all the details for the website including the web path and click OK to finish.

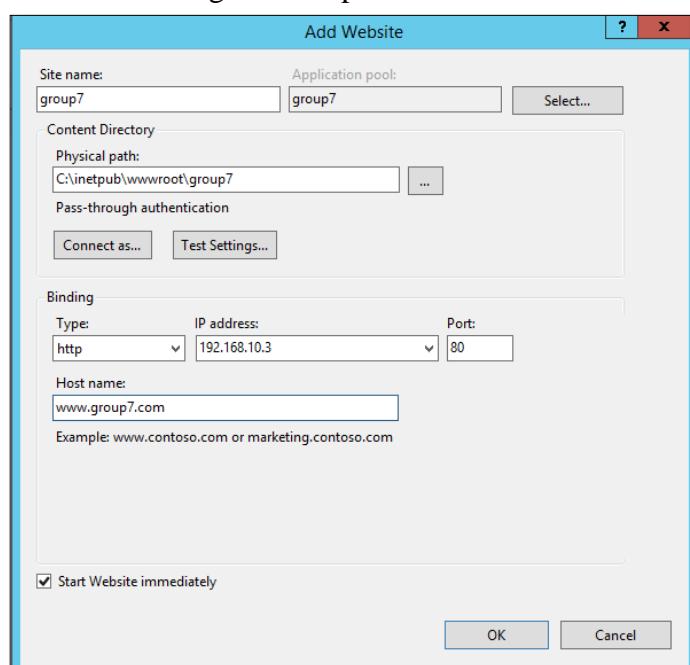


Figure 5. 288: Installing progress

Secure Socket Layer (SSL)

Step 1: Go to IIS Manager. Choose Server Certificates

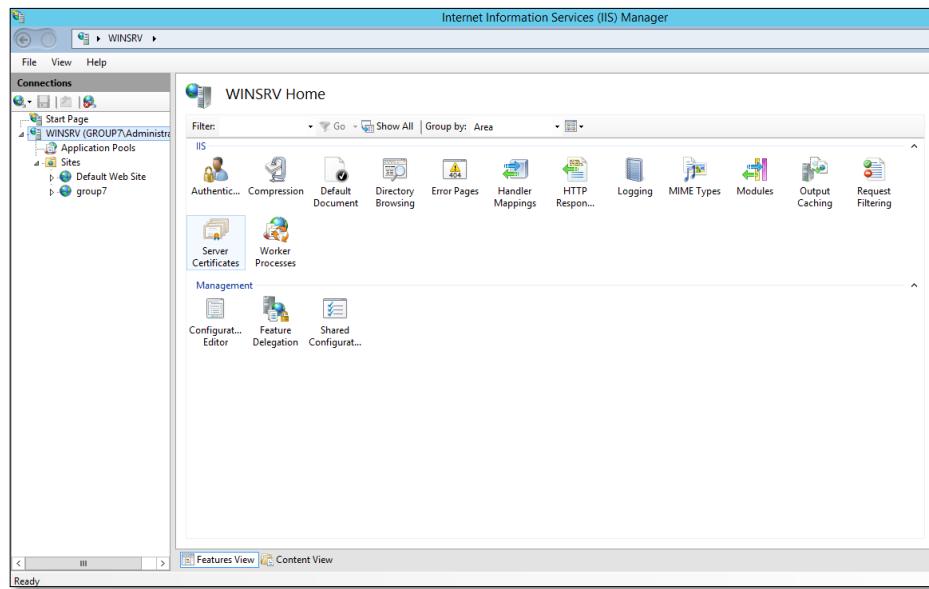


Figure 5. 289 : Server Certificates

Step 2: Type in the name for the certificate and click OK

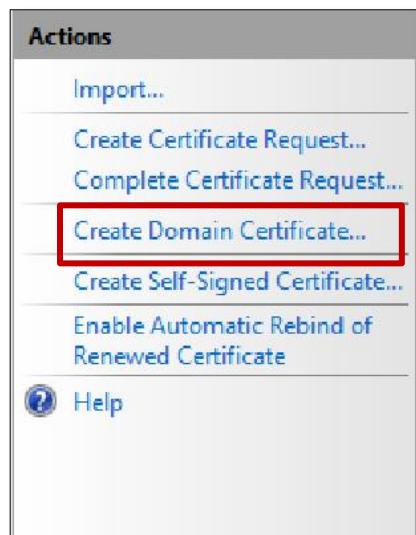


Figure 5. 290: Server Certificates

Step 3: Type in the name for the certificate and click OK

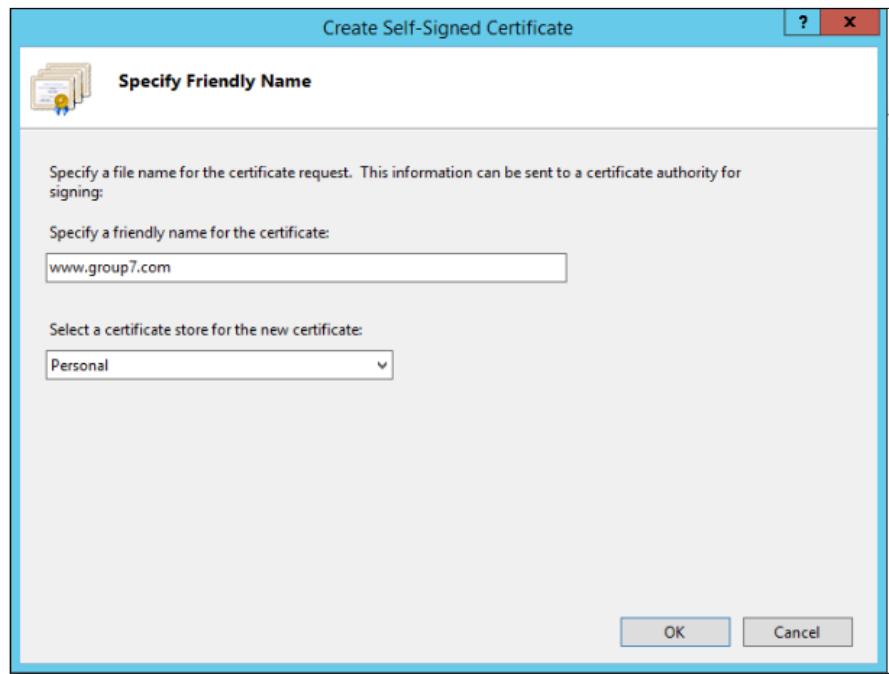


Figure 5. 291: Specify name for certificate

Step 4: The certificate is created and can be used.

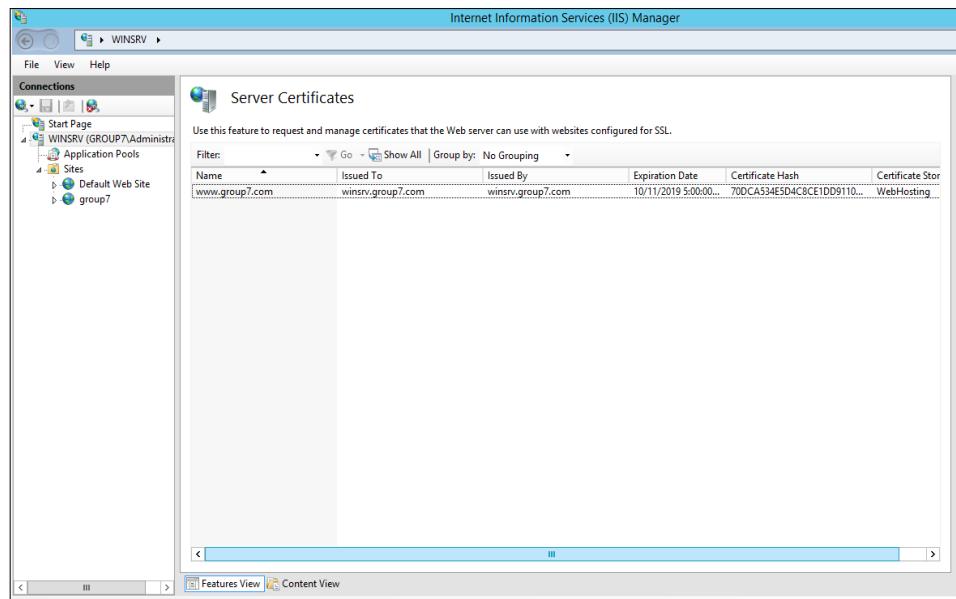


Figure 5. 292 : List of Certificate

Step 5: Add Site **Binding** and choose type **https** for SSL. Choose SSL Certificate that had created before.

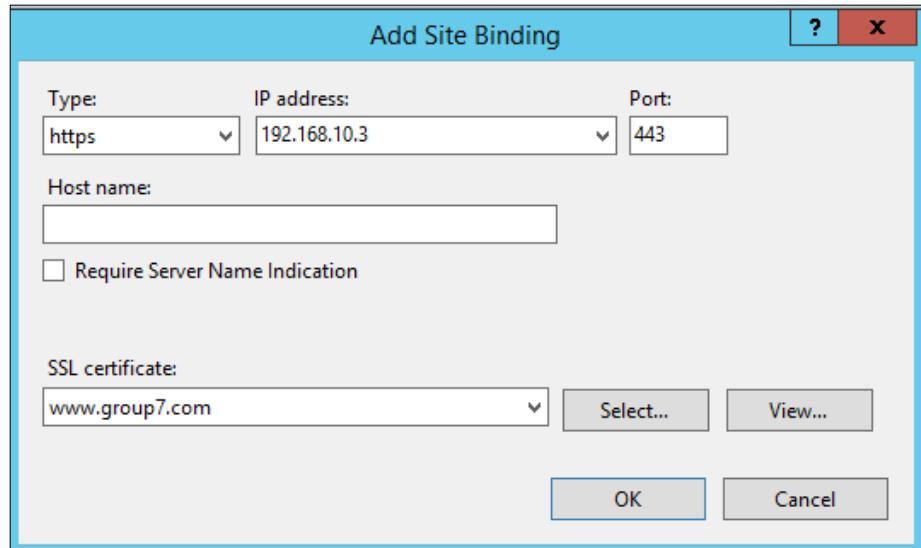


Figure 5. 293: Add site binding for SSL

Step 6: Go to SSL Setting to change SSL setting,

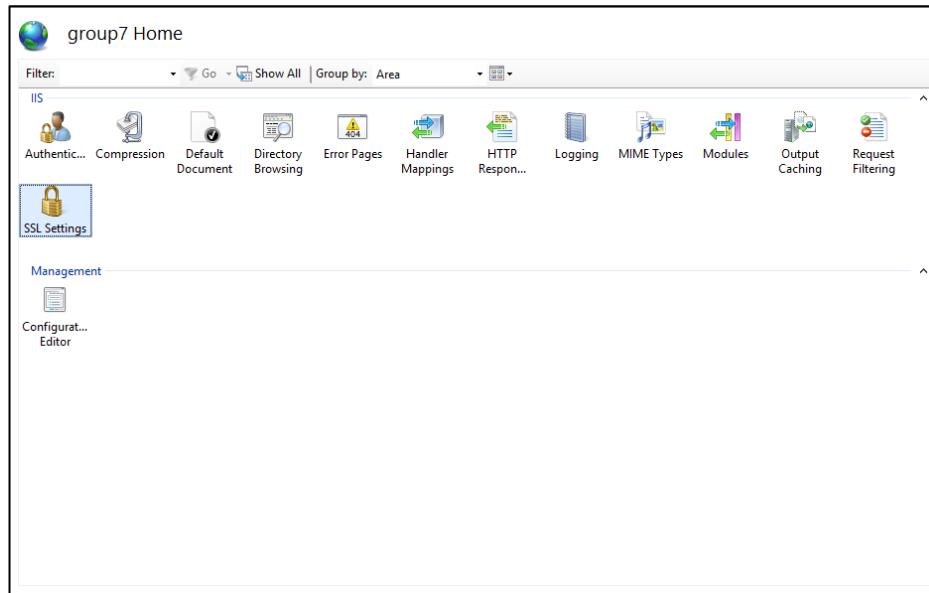


Figure 5. 294: SSL setting

Step 7: Tick Require SSL and Accept client certificate, Next Apply the Changed.

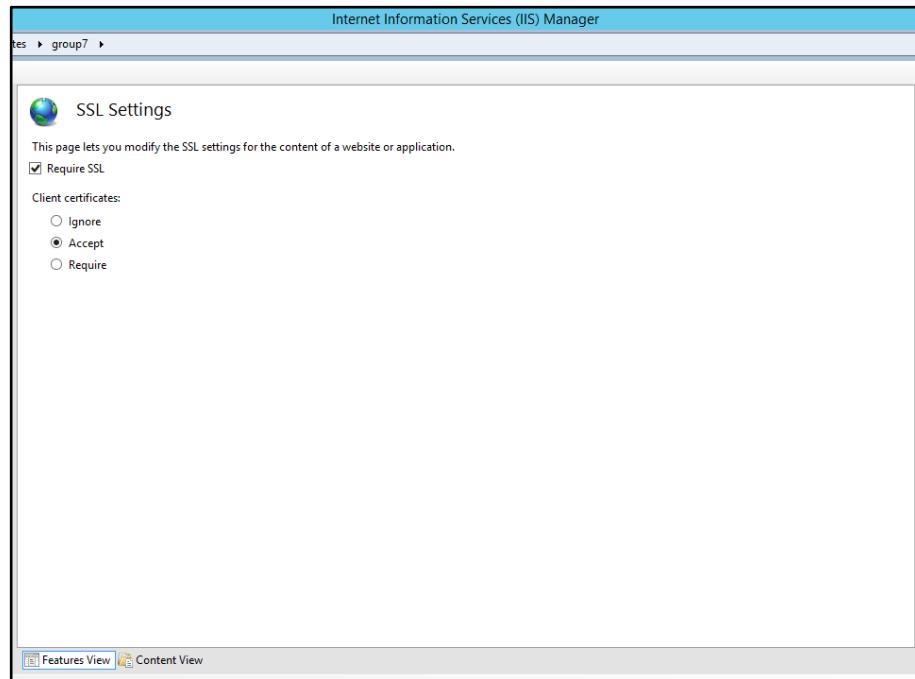


Figure 5. 295: Change SSL setting

Virtual Hosting

Step 1: Add a new website in IIS manager. Fill the site name with virtual hosting name and all the detail required.

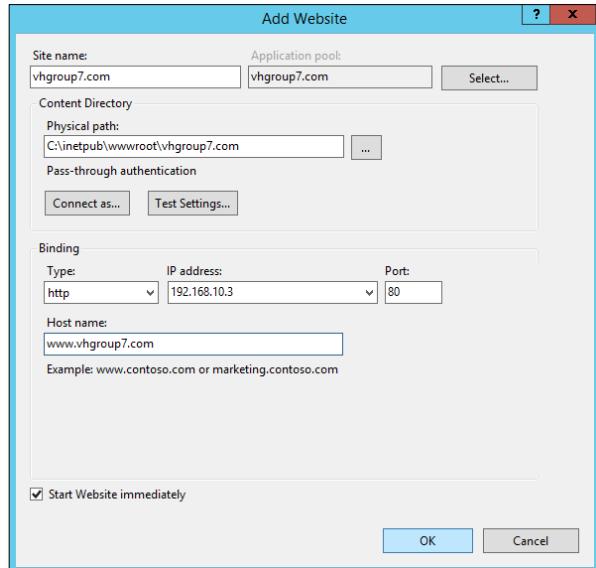


Figure 5. 296 : Add new website

Step 2: Add a Default document for the website by click at Default Document.

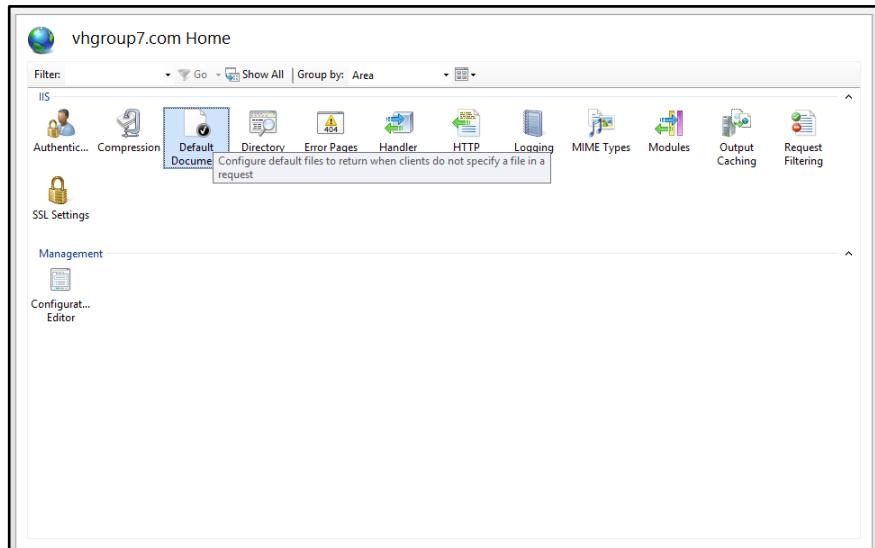


Figure 5. 297 : Add new Default Document

Step 3: Add new html file in default document by type the file name and click **OK**.

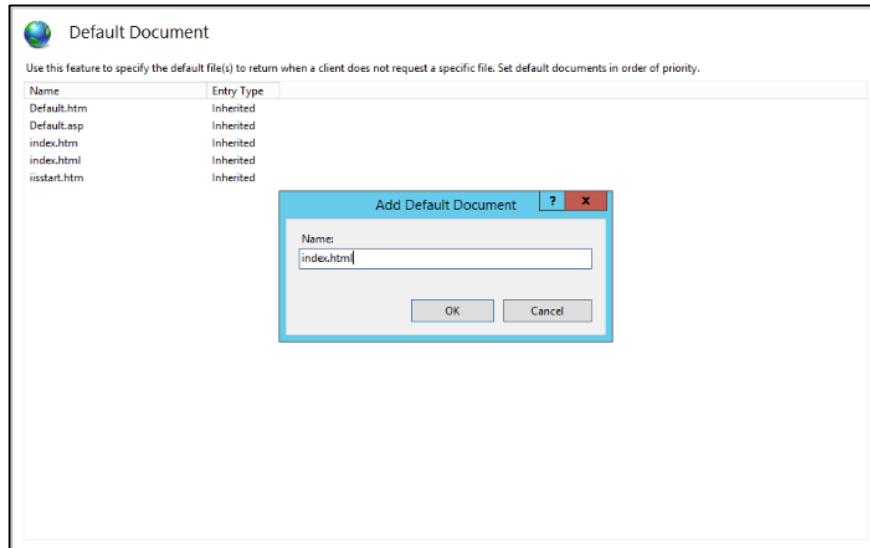


Figure 5. 298 : New html File

Step 4: Create a **New Zone** for the website at DNS.



Figure 5. 299: Create a new zone

Step 5: Choose a zone type for website. Tick for Primary zone

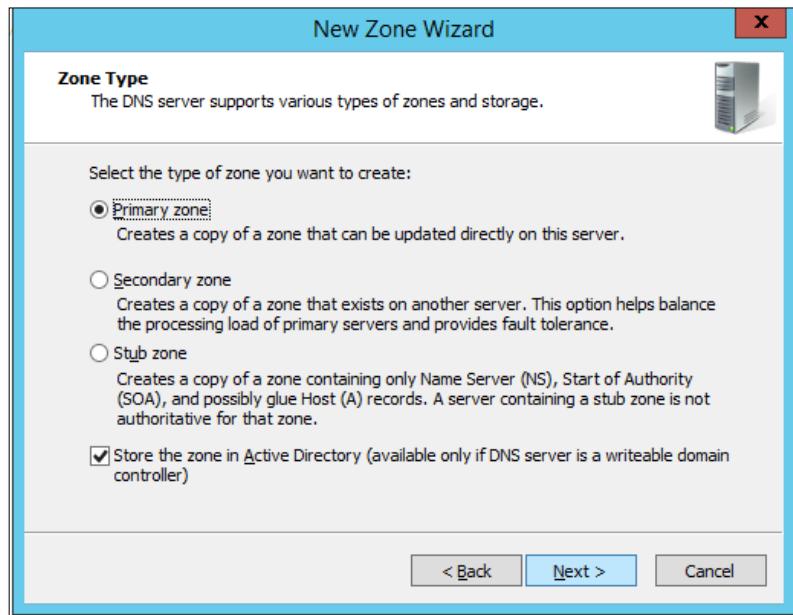


Figure 5. 300: Choose a zone type

Step 6: Choose how zone to replicate the website.

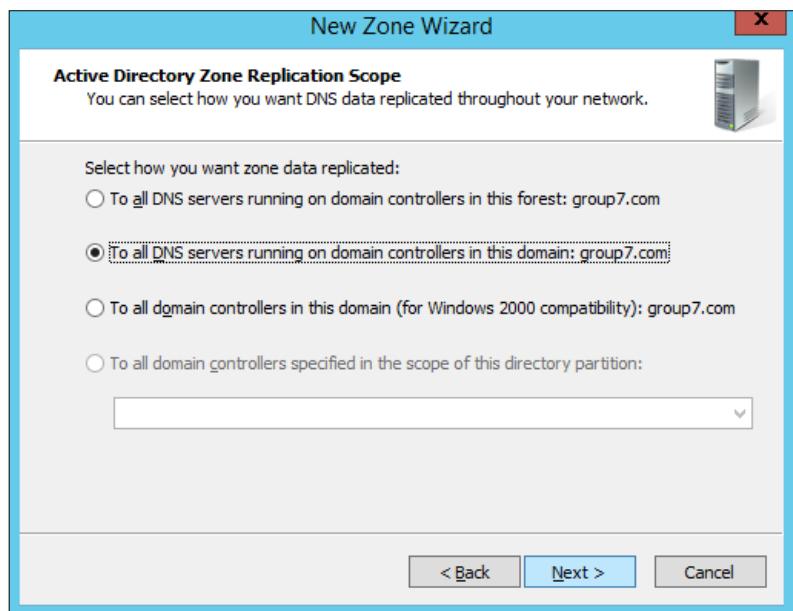


Figure 5. 301: Zone Replication Scope

Step 7: Choose a dynamic update for domain. Tick for **Allow both non-secure and Secure Dynamic Updates**



Figure 5. 302: Dynamic update DNS

Step 8: Completing a New Zone Wizard that had been created.



Figure 5. 303: The New Zone wizard complete

Step 10: Create a New Host in vhgroup3.com. by right click and choose **new host**.

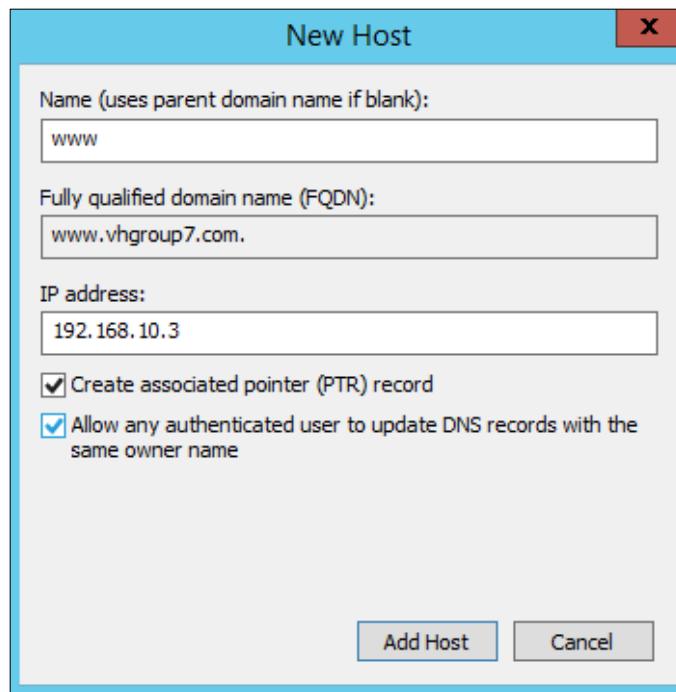


Figure 5. 304: Create a new host

5.2.15 Linux Email Server

Step 1: Install Postfix Mail Server. Postfix is a mail transfer agent (MTA) that is responsible for delivering and receiving emails which is very important element to create a complete mail server.

- I. Choose default file configuration for server.
- II. Then choose “Internet Site” to select type of mail configuration when this interface pops out below.

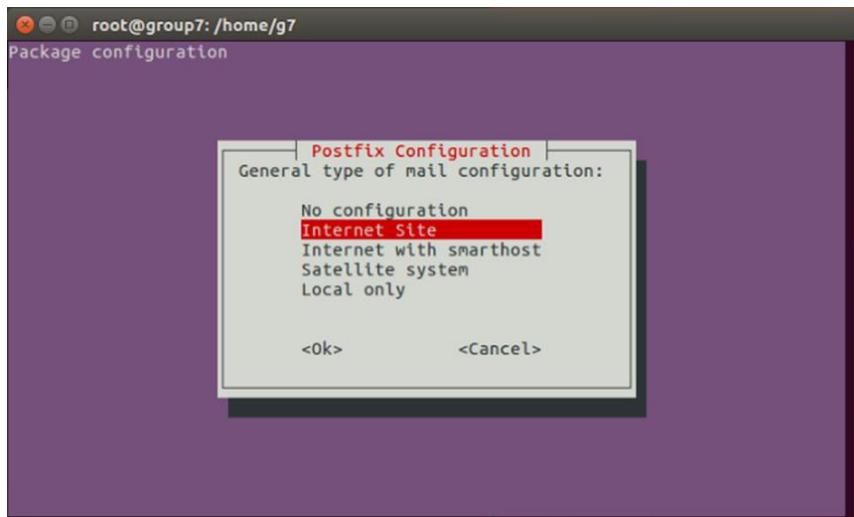


Figure 5. 305: Setting up postfix

- III. At the next Postfix Configuration interface, type in our domain name which is “group7.com”.

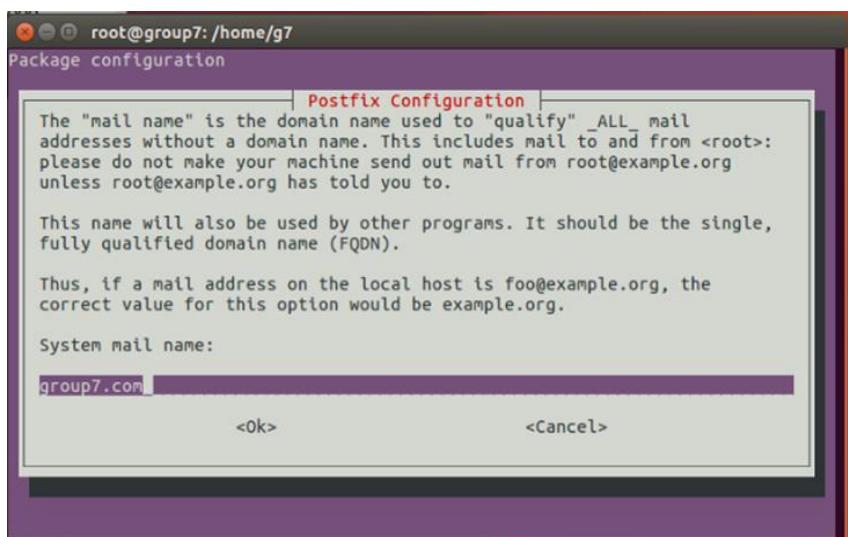


Figure 5. 306: Type in domain name for system mail name

Step 2: Configure the Postfix mail server by using the command as below:

```
vim /etc/postfix/main.cf
```

Edit the “inet_protocols” section from “all” to “ipv4”

Then, add this command line “home_mailbox = Maildir /” below the inet_protocols line.

```
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 = ipv4
home_mailbox = Maildir/
```

Figure 5. 307: Editing configuration of postfix

Step 5: Restart the Postfix by using the following command.

```
systemctl restart postfix
```

Step 6: Install Dovecot package and IMAP package on Ubuntu server

```
sudo apt install dovecot-core dovecot-imapd
```

Step 7: Configure the dovecot configuration file by using the following command line.

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

In the dovecot.conf file, add the following lines as below:

```
GNU nano 2.5.3          File: /etc/dovecot/dovecot.conf      Modif
# 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 pop3
#disable_plaintext_auth = no
mail_location = mbox:~/mail:INBOX=/var/mail/%u
mail_location = maildir:~/Maildir
```

Figure 5. 308: Configuring the dovecot.conf file.

Step 8: Then, restart the dovecot service using the following command.

```
systemctl restart dovecot
```

Step 9: Install Rainloop

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

```
mkdir rainloop
```

Cd into the directory and download the latest RainLoop community edition with the following commands:

```
cd rainloop
```

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

```
g7@group7:~/rainloop$ curl -s http://repository.rainloop.net/installer.php | php
#!/usr/bin/env php

[RainLoop Webmail Installer]

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

* [Success] Installation is finished!
```

Figure 5. 309 : Installing Rainloop

Now set web server user (www-data) as the owner.

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

```
g7@group7:~/rainloop$ cd ..
g7@group7:~$ sudo mv rainloop /var/www/
[sudo] password for g7:
g7@group7:~$ sudo chown www-data:www-data /var/www/rainloop/ -R
g7@group7:~$ █
```

Figure 5. 310 : Set web server user

Step 10: Configure a virtual host for RainLoop

- I. If you like to use Apache web server, then create the virtual host file with the following command

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

The screenshot shows a terminal window titled "g7@group7: ~". The command "GNU nano 2.5.3 File: /etc/apache2/sites-available/rainloop.conf" is displayed at the top. The content of the file is a VirtualHost configuration for port 80, serving the domain mail.group7.com from the directory "/var/www/rainloop/". It includes logs for error and access. The configuration ends with a Directory block and a closing VirtualHost tag. At the bottom of the screen, there is a menu bar with options like "Read 17 lines", "Get Help", "Write Out", "Where Is", "Cut Text", "Justify", "Exit", "Read File", "Replace", "Uncut Text", "To Spell", and "Replace".

Figure 5. 311 : Editing virtual hosting file

- II. Save and close the file. Then enable this virtual host.

- III. Reload Apache2.

```
g7@group7:~$ sudo a2ensite rainloop.conf
Enabling site rainloop.
To activate the new configuration, you need to run:
  service apache2 reload
g7@group7:~$ sudo systemctl reload apache2
g7@group7:~$
```

Figure 5. 312 : Save and reload Apache2

Step 11: Configure RainLoop webmail.

- I. Go to mail.group7.com/?admin. Then login using default username and password.
- II. Once login, go to domain tab to edit the setting.

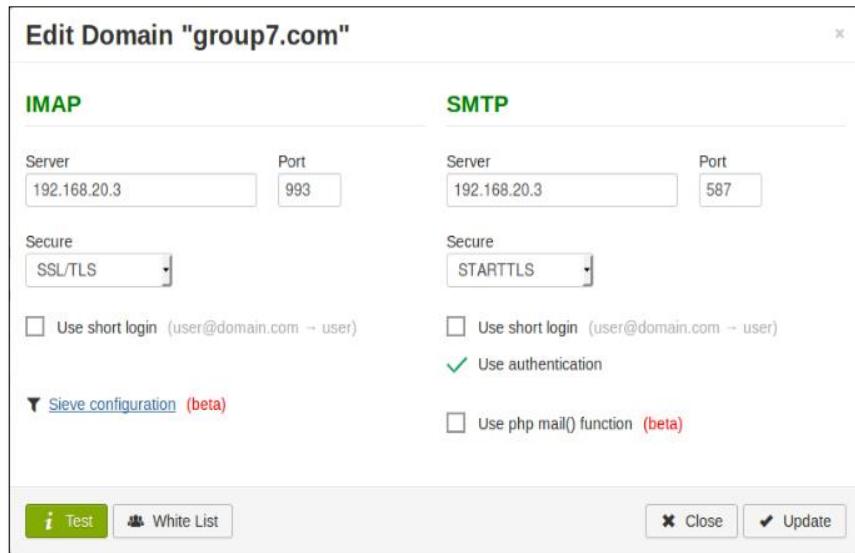


Figure 5. 313 : Editing domain setting

- III. Set up existing Email account.

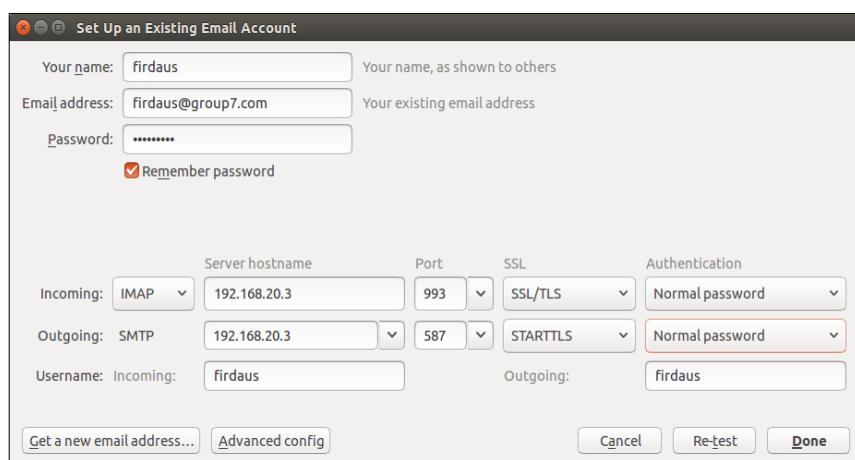


Figure 5. 314: Set up email account

5.2.16 IPv6 Web with IPv6 Tunneling

IPv6 Web

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

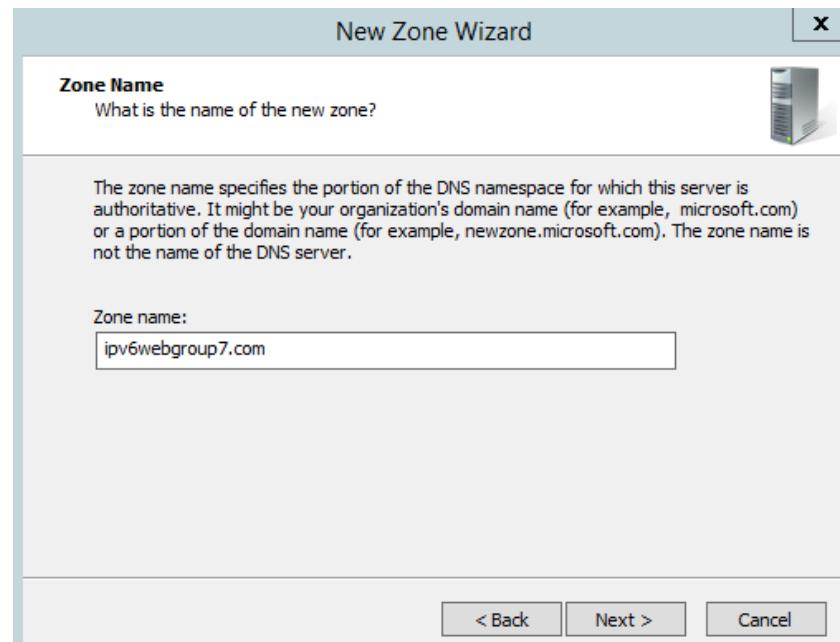


Figure 5. 315: New zone in forward lookup zones

Step 2: Add new host (AAAA) and set ip address to 2001:db8:7777:10::3

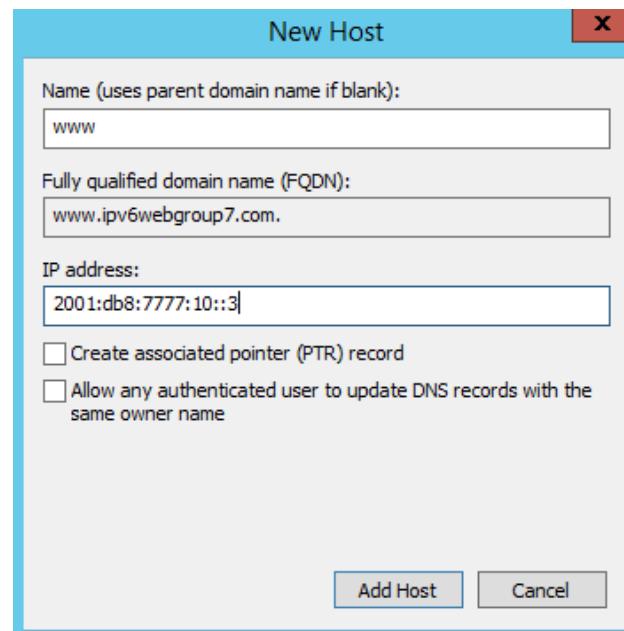


Figure 5. 316: Add new host in
ipv6webgroup7.com

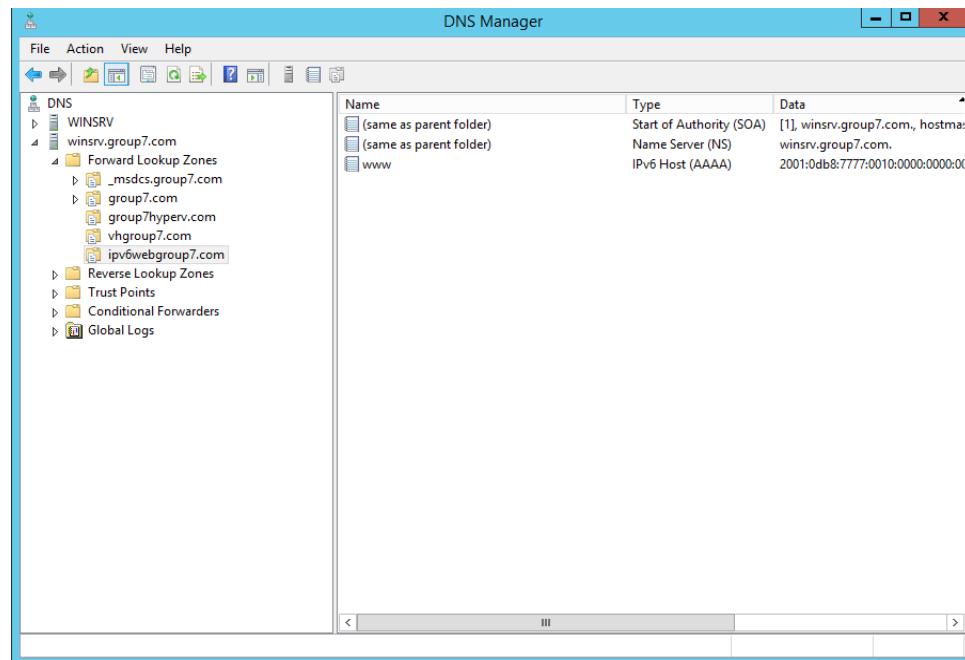


Figure 5. 317 : New host added

Step 3: Create self-signed certificate before configure ssl

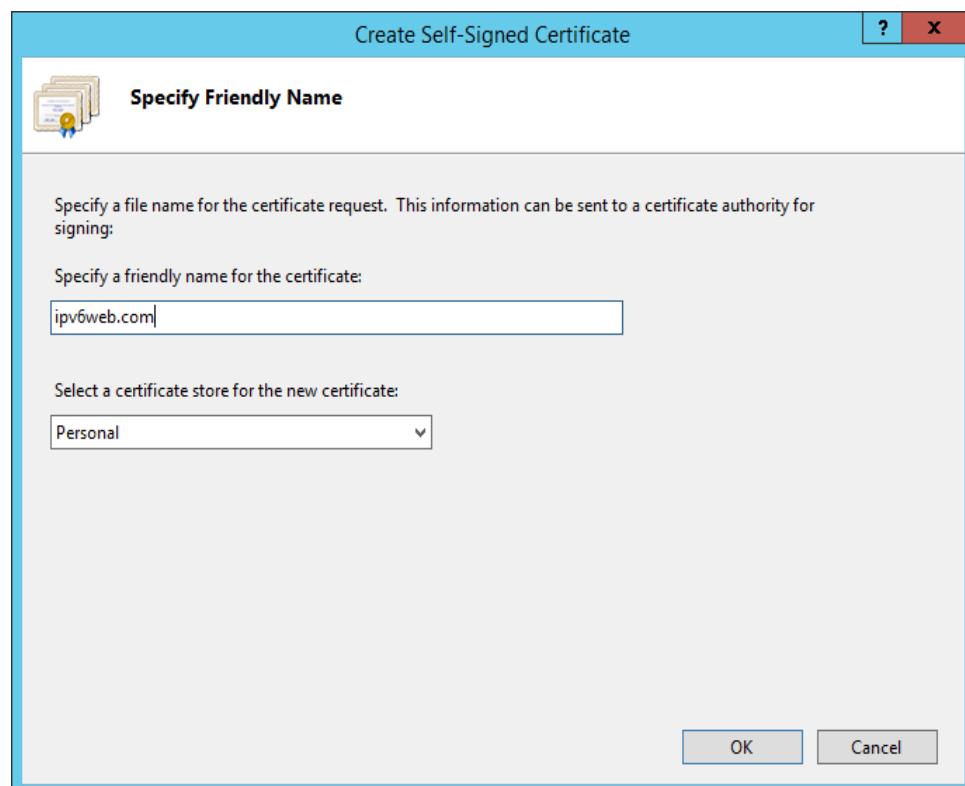


Figure 5. 318: Create personal certificate for ssl

Step 4: Add site binding in website ipv6webgroup7.com

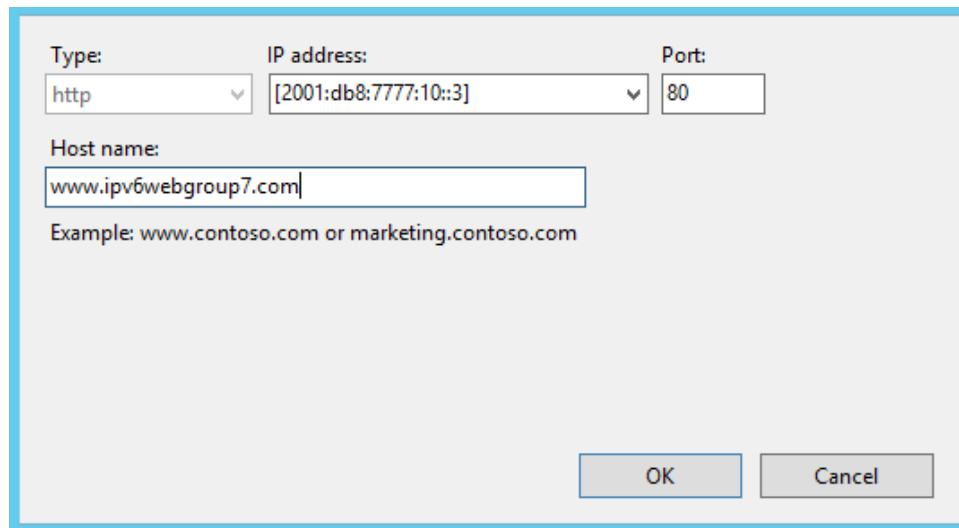


Figure 5. 319: Add site binding for web

Step 5: Add another site binding using ssl certificate that have been created

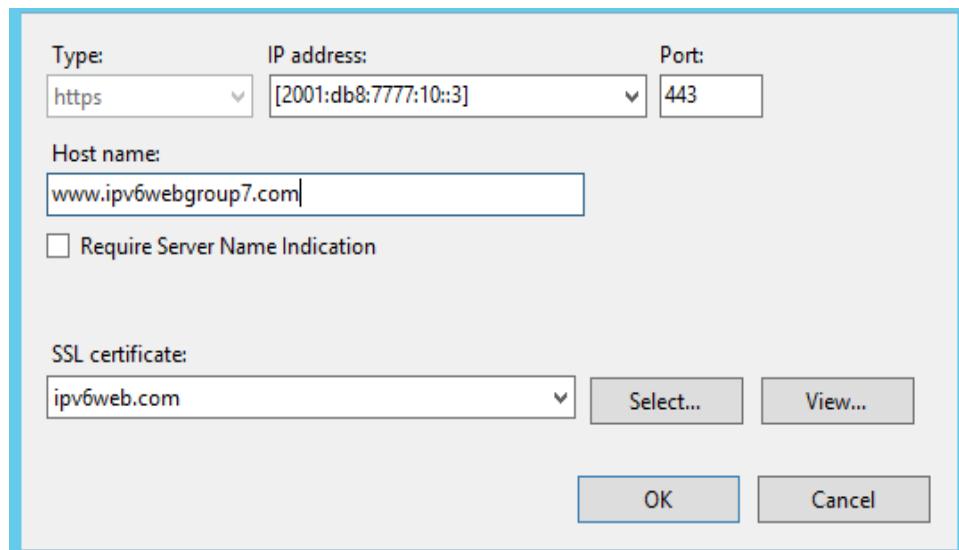


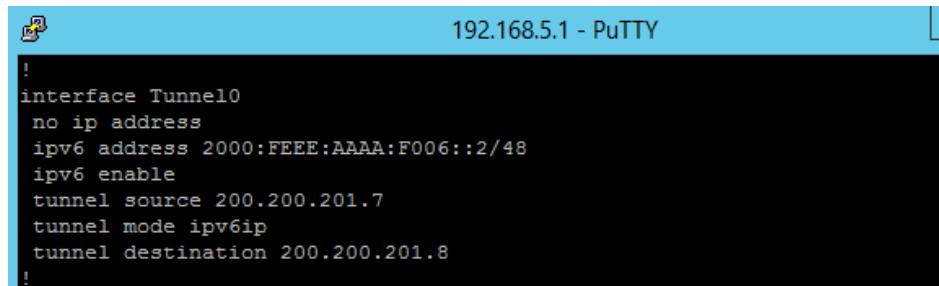
Figure 5. 320 : Add site binding using ssl certificate

IPv6 tunnelling

Step 1: To configure ipv6 tunnelling, first we need to create a tunnel interface on each dual-stack edge router. There are three key components relevant to Ipv6:

- The tunnel mood ipv6ip
- The tunnel source (Ipv4 interface or address)
- The tunnel destination (Ipv4 interface or address for neighbour)

On our router, we create the tunnel interface, configure it as 6to4, and specify its cloud-facing IPv4 interface as the tunnel source.



```
192.168.5.1 - PuTTY

!
interface Tunnel0
no ip address
ipv6 address 2000:FFFF:AAAA:F006::2/48
ipv6 enable
tunnel source 200.200.201.7
tunnel mode ipv6ip
tunnel destination 200.200.201.8
!
```

Figure 5. 321: Interface tunnel0

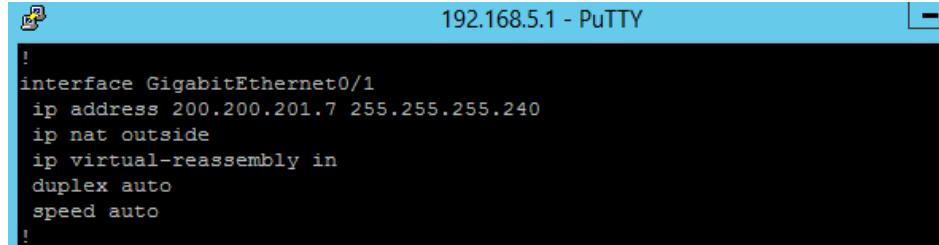
Step 2: To determine the IPv6 address of the tunnel interface, we convert the IPv4 source address to hexadecimal in IPv6 notation.



```
 ipv6 address 2000:FFFF:AAAA:F006::2/48
```

Figure 5. 322: IPv6 address of the tunnel interface

Step 3: Create interface and set public ip address for router

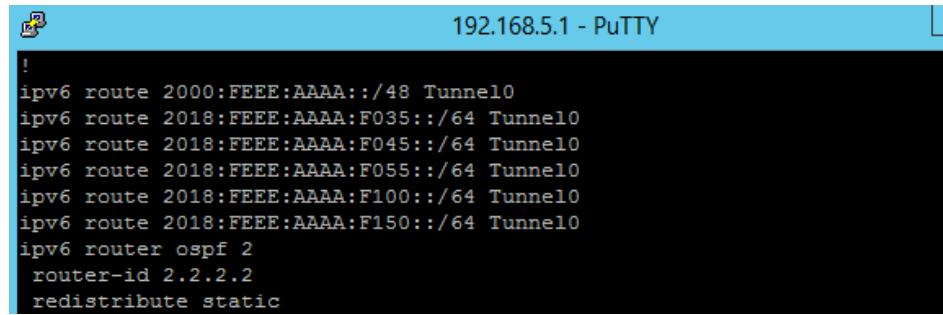


```
192.168.5.1 - PuTTY

!
interface GigabitEthernet0/1
ip address 200.200.201.7 255.255.255.240
ip nat outside
ip virtual-reassembly in
duplex auto
speed auto
!
```

Figure 5. 323: Tunnel interface

Step 4: Now that the 6to4 address of each router is known, add the necessary static routes to achieve IPv6 connectivity between both routers. The first indicates that 2000::/48 is reachable out of interface Tunnel0. The others are routes for the individual /64 prefixes at either of the other sites, which are to be routed via the 6to4 tunnel for neighbour's group. Then, set ipv6 router ospf and router id.



```
192.168.5.1 - PuTTY

!
ipv6 route 2000:FEEE:AAAA::/48 Tunnel0
ipv6 route 2018:FEEE:AAAA:F035::/64 Tunnel0
ipv6 route 2018:FEEE:AAAA:F045::/64 Tunnel0
ipv6 route 2018:FEEE:AAAA:F055::/64 Tunnel0
ipv6 route 2018:FEEE:AAAA:F100::/64 Tunnel0
ipv6 route 2018:FEEE:AAAA:F150::/64 Tunnel0
ipv6 router ospf 2
  router-id 2.2.2.2
  redistribute static
```

Figure 5. 324 Neighbour Ipv6 address

5.2.17 Media streaming server

Step 1: Download Plex Media Streaming Server from “<https://www.plex.tv/media-server-downloads>” website.

Step 2: Choose the platform and distribution.

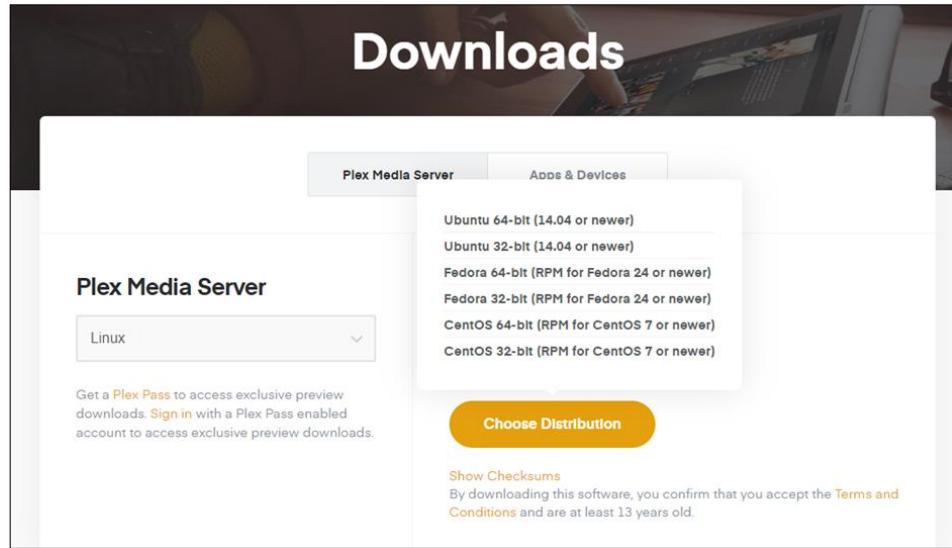


Figure 5. 325: Choose Platform “Linux” and distribution “Ubuntu”.

Step 3: Once download install Plex Media streaming server.

Step 4: Once install enter `http://localhost:8888/web` into your browser to view the Plex web interface, as shown below. Input your Plex account username and password to proceed with the setup process.

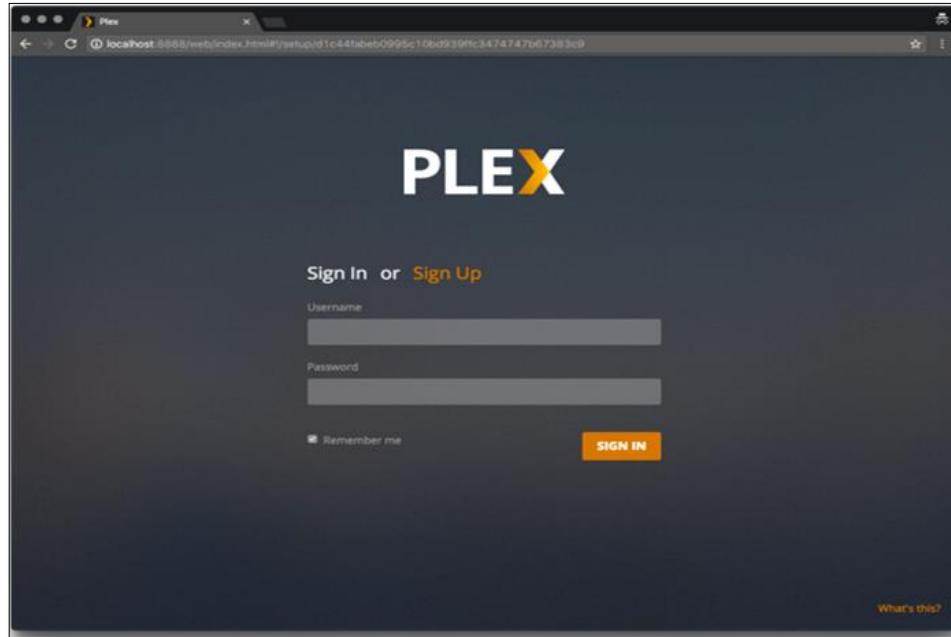


Figure 5. 326 : Show Plex web interface “Login Page”

Step 5: Give your Plex server a name. Be sure to leave the Allow me to access my media outside my home box checked and click **next**.



Figure 5. 327 : Set Plex Server name

Step 6: Now that you've signed into Plex, you should see the following page. Click the Add Library button to start setting up your media libraries.



Figure 5. 328 : Click add library button to add media files

Step 7: Navigate to the corresponding media directory that you created previously, then click **Add**.

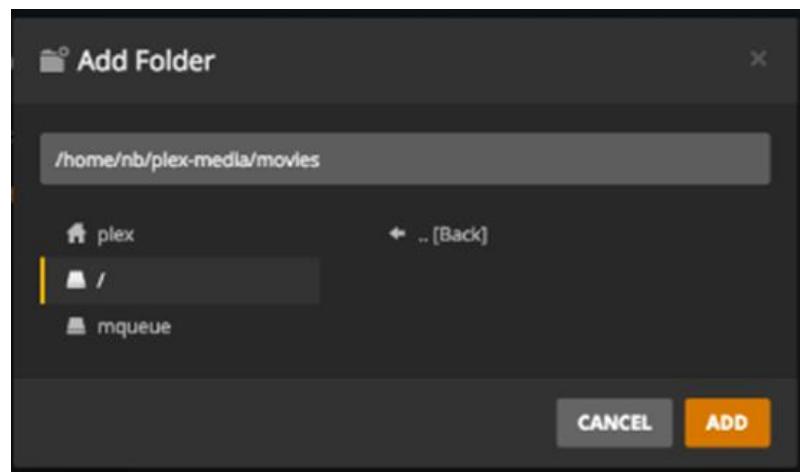


Figure 5. 329 : Add media files to library

Step 8: Once add media file to library click next to redirect to Plex dashboard. Now can see the media files in the Plex dashboard.

5.2.18 Cloud server

Step 1: Go to terminal and login into root.

```
g7@g7:~$ sudo su
root@g7:/home/g7# apt-get install lamp-server^
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'libhttp-message-perl' for task 'lamp-server'
Note, selecting 'libencode-locale-perl' for task 'lamp-server'
```

Figure 5. 330 : Root environment

Step 2: First, we need to install LAMP Server.

```
g7@g7:~$ sudo su
root@g7:/home/g7# apt-get install lamp-server^
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'libhttp-message-perl' for task 'lamp-server'
Note, selecting 'libencode-locale-perl' for task 'lamp-server'
```

Figure 5. 331 : Install LAMP Server

Step 3: Then, Install PHP Extension.

```
root@g7:/home/g7# apt-get install libapache2-mod-php7.0 php7.0-mbstring php7.0-c
url php7.0-gd php7.0-mysql php7.0-mcrypt
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

Figure 5. 332 : Download Nextcoud

Step 5: After that, we need to move Nexcloud file into html folder.

```
root@g7:/home/g7# mv nextcloud /var/www/html/
```

Figure 5. 333 : Move the file

Step 6: Change the permission of the file

```
root@g7:/home/g7# chown -R www-data:www-data /var/www/html/nextcloud
root@g7:/home/g7#
```

Figure 5. 334 : Change the permission

Step 7: Configure the MariaDB for Nextcloud.

```
root@g7:/home/g7# mysql_secure_installation
Securing the MySQL server deployment.
```

Figure 5. 335 : Mysql

```

By default, MySQL comes with a database named 'test' that
anyone can access. This is also intended only for testing,
and should be removed before moving into a production
environment.

Remove test database and access to it? (Press y|Y for Yes, any other key for No)
: y
- Dropping test database...
Success.

- Removing privileges on test database...
Success.

Reloading the privilege tables will ensure that all changes
made so far will take effect immediately.

Reload privilege tables now? (Press y|Y for Yes, any other key for No) : y
Success.

All done!

```

Figure 5. 336 : Configure MariaDB

Step 8: Create the Nextcloud database.

```

root@g7:/home/g7# mysql -u root -p
Enter password: 
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 5.7.23-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> GRANT ALL PRIVILEGES ON nextcloud.* TO 'nextcloud'@'localhost' IDENTIFIED
BY 'group7';
Query OK, 0 rows affected, 1 warning (0.00 sec)

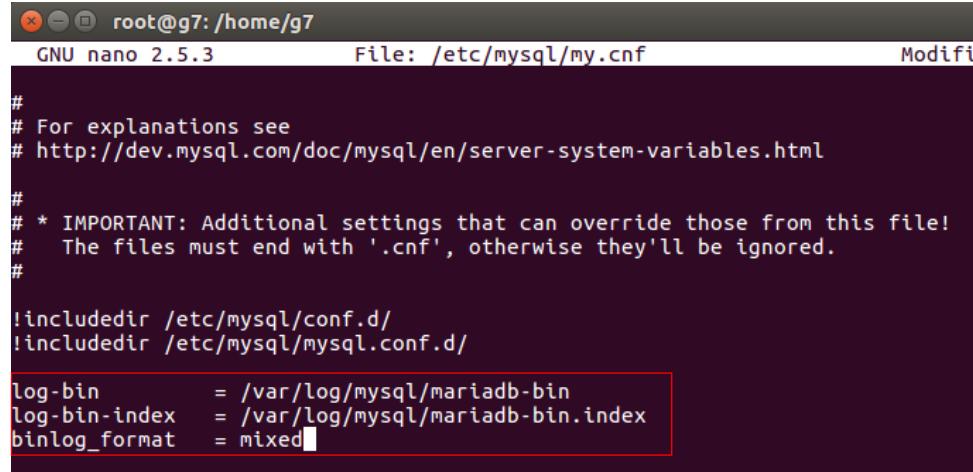
mysql> FLUSH PRIVILEGES
-> ;
Query OK, 0 rows affected (0.01 sec)

mysql>

```

Figure 5. 337 : Create Nextcoud Database

Step 9: Disable MariaDB binary logging by enter the `nano /etc/mysql/my.cnf` and add the 3 lines code.



```
root@g7:/home/g7# nano /etc/mysql/my.cnf
GNU nano 2.5.3           File: /etc/mysql/my.cnf           Modified

#
# For explanations see
# http://dev.mysql.com/doc/mysql/en/server-system-variables.html

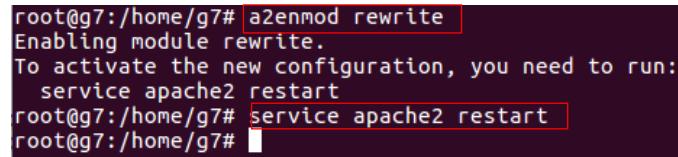
#
# * IMPORTANT: Additional settings that can override those from this file!
#   The files must end with '.cnf', otherwise they'll be ignored.
#

!includedir /etc/mysql/conf.d/
!includedir /etc/mysql/mysql.conf.d/

log-bin      = /var/log/mysql/mariadb-bin
log-bin-index = /var/log/mysql/mariadb-bin.index
binlog_format = mixed
```

Figure 5. 338 : Disable the MariaDB

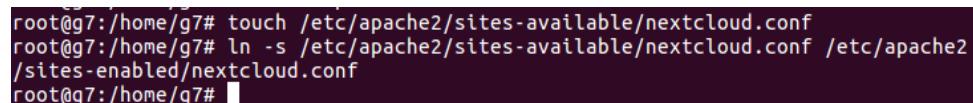
Step 10: Configure the Apache Web Server. Run the `a2enmod rewrite` command and restart the apache web server.



```
root@g7:/home/g7# a2enmod rewrite
Enabling module rewrite.
To activate the new configuration, you need to run:
  service apache2 restart
root@g7:/home/g7# service apache2 restart
root@g7:/home/g7#
```

Figure 5. 339 : Configure apache server

Step 11: Create the nextcloud.conf file and continue configure the web server.



```
root@g7:/home/g7# touch /etc/apache2/sites-available/nextcloud.conf
root@g7:/home/g7# ln -s /etc/apache2/sites-available/nextcloud.conf /etc/apache2/sites-enabled/nextcloud.conf
root@g7:/home/g7#
```

Figure 5. 340 : Create the nextcloud.conf file

Step 12: Create the file the nextcloud.conf by using nano /etc/apache2/sites-available/nextcloud.conf and write all this command.

```
root@g7: /home/g7
GNU nano 2.5.3  File: /etc/apache2/sites-available/nextcloud.conf  Modified

<VirtualHost *:80>
ServerAdmin admin@ubuntu
DocumentRoot "/var/www/html/nextcloud/"
ServerName 192.168.20.3
ServerAlias ubuntu
<Directory "/var/www/html/nextcloud/">
Options FollowSymLinks
AllowOverride All
Order allow,deny
allow from all
</Directory>
ErrorLog /var/log/apache2/you-domain.com-error_log
CustomLog /var/log/apache2/your-domain.com-access_log common
</VirtualHost>
```

Figure 5. 341: Create the nextcloud.conf file

Step 13: Restart the apache server after change the configuration.

```
root@g7:/home/g7# nano /etc/apache2/sites-available/nextcloud.conf
root@g7:/home/g7# nano /etc/apache2/sites-available/nextcloud.conf
root@g7:/home/g7# nano /etc/apache2/sites-available/nextcloud.conf
root@g7:/home/g7# systemctl restart apache2.service
root@g7:/home/g7#
```

Figure 5. 342 : Restart apache server

Step 14: Open the web browser and type the ip address for the Nextcloud. Then, login as admin and enter the password.

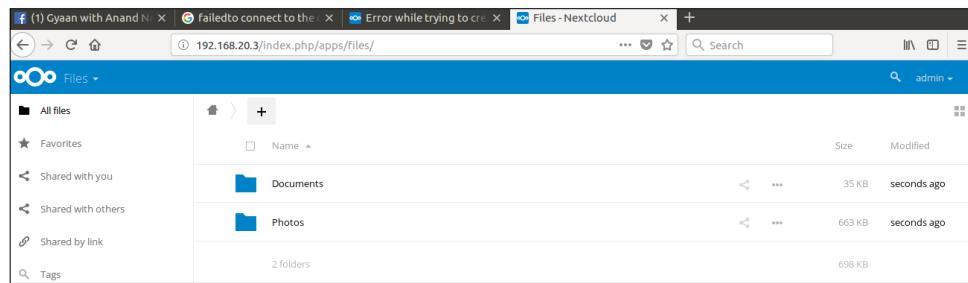


Figure 5. 343 : Nextcloud User Interface

5.2.19 VLAN Security

Step 1: To prevent switch spoofing, disable DTP by using command switchport nonegotiate on g1/0/24.

```
group7-SW#config t
Enter configuration commands, one per line. End with CNTL/Z.
group7-SW(config)#int g1/0/24
group7-SW(config-if)#switchport nonegotiate
group7-SW(config-if)#end

```

Figure 5. 344 : Switchport nonegotiate

Step 2: To prevent double tagging, DO NOT put any host on native VLAN 5.

```
group7-SW#sh vlan
VLAN Name          Status    Ports
---   -----
1    default        active    Gi1/0/1, Gi1/0/2, Gi1/0/3
                           Gi1/0/13, Gi1/0/14, Gi1/0/15
                           Gi1/0/22, Gi1/0/23, Gi1/1/1
                           Gi1/1/2, Gi1/1/3, Gi1/1/4
5    Trunk          active
10   WinServer      active    Gi1/0/4, Gi1/0/5, Gi1/0/6
20   UbuServer      active    Gi1/0/7, Gi1/0/8, Gi1/0/9
30   vlan FedoServer active    Gi1/0/10, Gi1/0/11, Gi1/0/12
101  Client         active    Gi1/0/16, Gi1/0/17, Gi1/0/18
102  AP             active    Gi1/0/19, Gi1/0/20, Gi1/0/21
1002 fddi-default  act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default  act/unsup
```

Figure 5. 345 : Show vlan

Step 3: Create a VLAN 60 to place all unused ports and suspend it so that there is no communication between VLAN 60 and other VLANs.

```
group7-SW(config)#vlan 60
group7-SW(config-vlan)#name unusedPorts
group7-SW(config-vlan)#end
```

Figure 5. 346 : Create VLAN 60 named unusedPorts

```
group7-SW(config)#vlan 60
group7-SW(config-vlan)#state suspend
group7-SW(config-vlan)#end
```

Figure 5. 347 : Suspend VLAN 60

Step 4: Put all unused port into VLAN 60.

```
group7-SW(config)#int rang g1/0/1-3,g1/0/13-15
group7-SW(config-if-range)#switchport mode access
group7-SW(config-if-range)#switchport access vlan 60
group7-SW(config-if-range)#end
```

Figure 5. 348 : Assign all unused port into VLAN 60

Step 5: Assign used vlans into trunk port

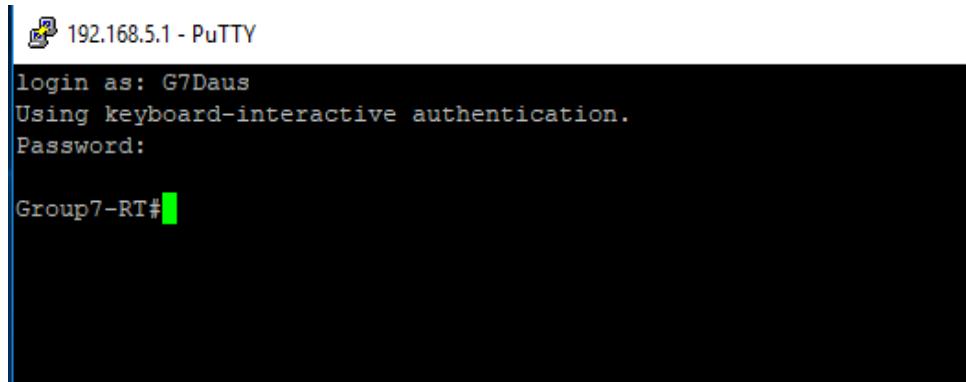
```
group7-SW(config)#int g1/0/24
group7-SW(config-if)#switchport mode trunk
group7-SW(config-if)#switchport trunk allowed vlan 1,5,10,20,30,101,102
group7-SW(config-if)#end
```

Figure 5. 349 : Assign all usable VLANs into trunk ports

5.2.20 Router hardening

Enable Login Banner

Step 1 : Login without banner.



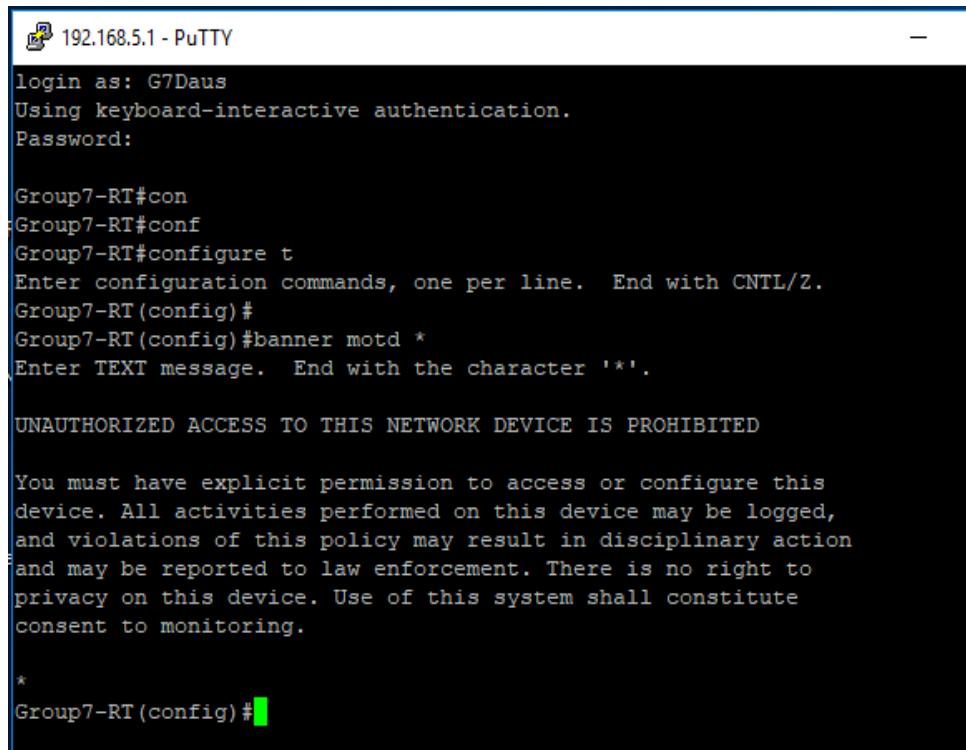
A screenshot of a PuTTY terminal window titled "192.168.5.1 - PuTTY". The session is titled "login as: G7Daus". The text in the window shows the following sequence:

```
login as: G7Daus
Using keyboard-interactive authentication.
Password:

Group7-RT#
```

Figure 5. 350 : Putty

Step 2: To active the banner, use command **banner motd ***. Then, enter the banner message and end with character *.



A screenshot of a PuTTY terminal window titled "192.168.5.1 - PuTTY". The session is titled "login as: G7Daus". The text in the window shows the following sequence:

```
login as: G7Daus
Using keyboard-interactive authentication.
Password:

Group7-RT#con
Group7-RT#conf
Group7-RT#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Group7-RT(config)#
Group7-RT(config)#banner motd *
Enter TEXT message. End with the character '**.

UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED

You must have explicit permission to access or configure this
device. All activities performed on this device may be logged,
and violations of this policy may result in disciplinary action
and may be reported to law enforcement. There is no right to
privacy on this device. Use of this system shall constitute
consent to monitoring.

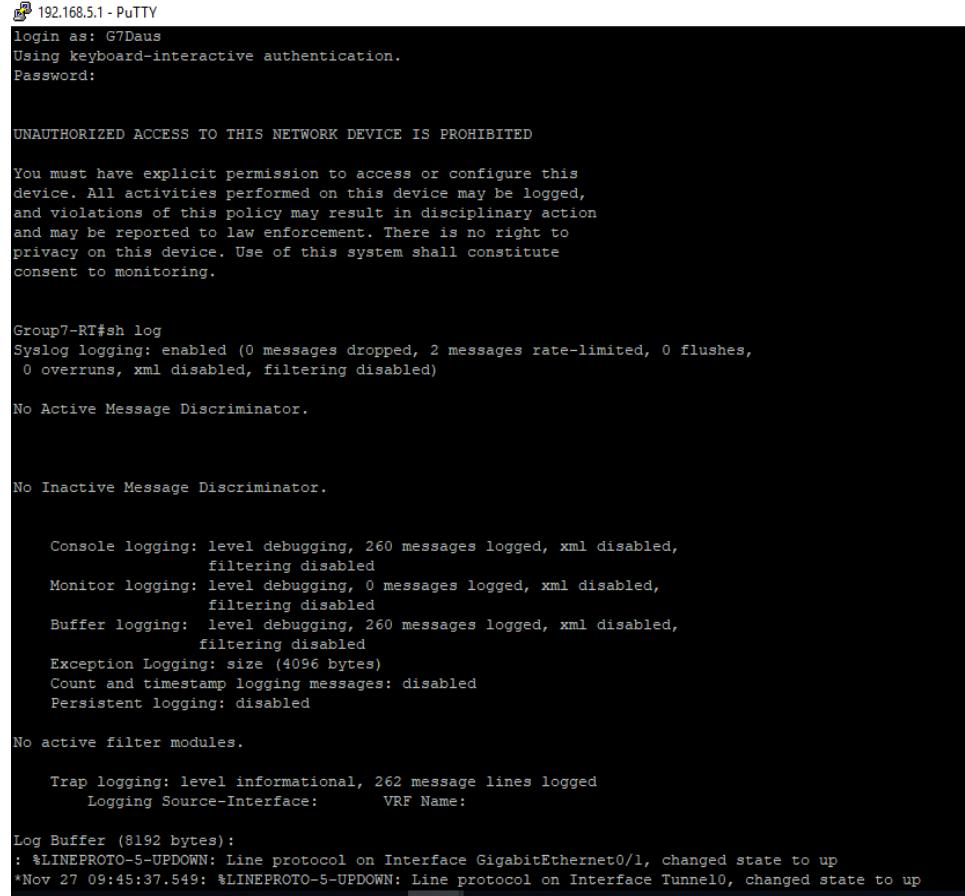
*
Group7-RT(config)#

```

Figure 5. 351 : Putty

Disable log to console or monitor sessions

Step 1: Login and use command **sh log** to show the logging.



192.168.5.1 - Putty
login as: G7Daus
Using keyboard-interactive authentication.
Password:

UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED
You must have explicit permission to access or configure this
device. All activities performed on this device may be logged,
and violations of this policy may result in disciplinary action
and may be reported to law enforcement. There is no right to
privacy on this device. Use of this system shall constitute
consent to monitoring.

Group7-RT#sh log
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes,
0 overruns, xml disabled, filtering disabled)
No Active Message Discriminator.

No Inactive Message Discriminator.

Console logging: level debugging, 260 messages logged, xml disabled,
filtering disabled
Monitor logging: level debugging, 0 messages logged, xml disabled,
filtering disabled
Buffer logging: level debugging, 260 messages logged, xml disabled,
filtering disabled
Exception Logging: size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled

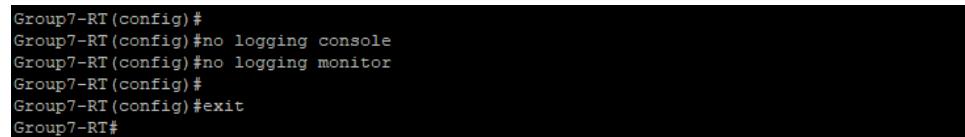
No active filter modules.

Trap logging: level informational, 262 message lines logged
Logging Source-Interface: VRF Name:

Log Buffer (8192 bytes):
: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
*Nov 27 09:45:37.549: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up

Figure 5. 352 : Putty

Step 2: Use command **no logging console** and **no logging monitor**.

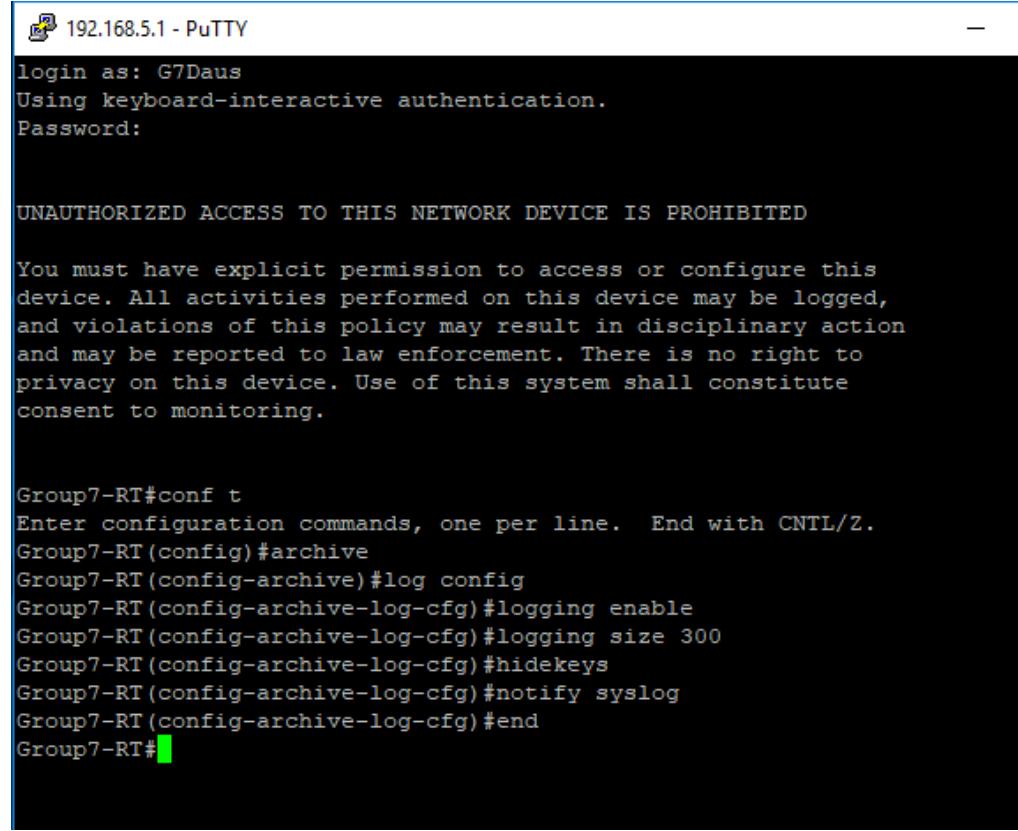


```
Group7-RT(config)#  
Group7-RT(config)#no logging console  
Group7-RT(config)#no logging monitor  
Group7-RT(config)#  
Group7-RT(config)#exit  
Group7-RT#
```

Figure 5. 353 : Putty

Enable configuration change notification and logging

```
#conf t  
#archive  
#log config  
#logging enable  
#logging size 300  
#hidekeys  
#notify syslog  
#end
```



The screenshot shows a PuTTY terminal window titled "192.168.5.1 - PuTTY". The session has been established with user "G7Daus" using keyboard-interactive authentication. The password prompt has been redacted. The terminal displays a warning message about unauthorized access being prohibited and a detailed statement of the device's monitoring policy. Below this, the configuration command sequence is shown, starting with "#conf t" and ending with "#end". The command "#log config" is present in the sequence.

```
192.168.5.1 - PuTTY  
login as: G7Daus  
Using keyboard-interactive authentication.  
Password:  
  
UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED  
  
You must have explicit permission to access or configure this  
device. All activities performed on this device may be logged,  
and violations of this policy may result in disciplinary action  
and may be reported to law enforcement. There is no right to  
privacy on this device. Use of this system shall constitute  
consent to monitoring.  
  
Group7-RT#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Group7-RT(config)#archive  
Group7-RT(config-archive)#log config  
Group7-RT(config-archive-log-cfg)#logging enable  
Group7-RT(config-archive-log-cfg)#logging size 300  
Group7-RT(config-archive-log-cfg)#hidekeys  
Group7-RT(config-archive-log-cfg)#notify syslog  
Group7-RT(config-archive-log-cfg)#end  
Group7-RT#
```

Figure 5. 354 : Putty

Log

Step 1: Open Putty Configuration. Select **Logging** and follow the figure below.

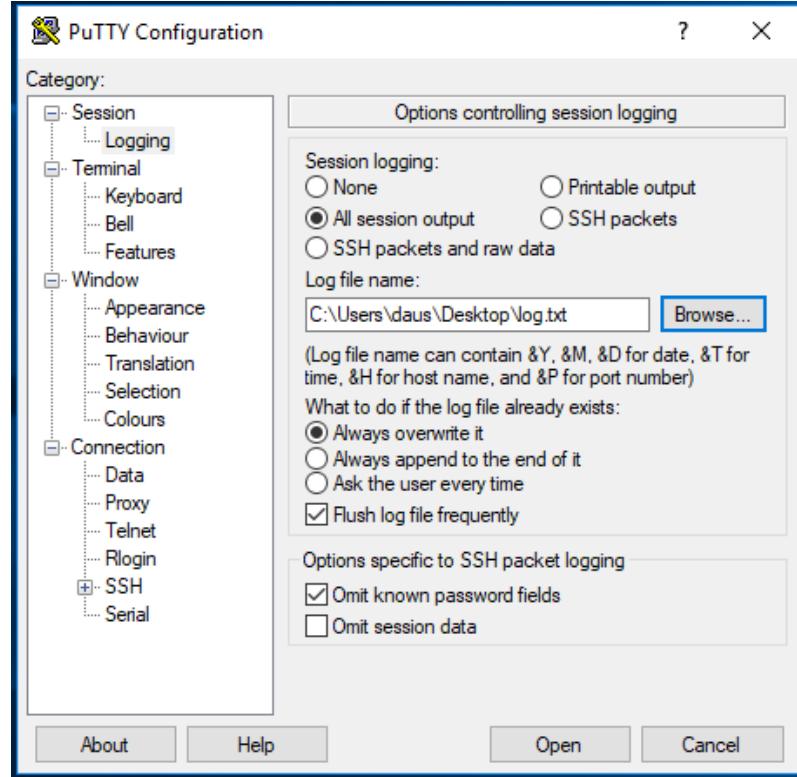


Figure 5. 355 : Putty Configuration

Step 2: Select the destination to save a file. Name it **log.txt**. Then, click **Save**.

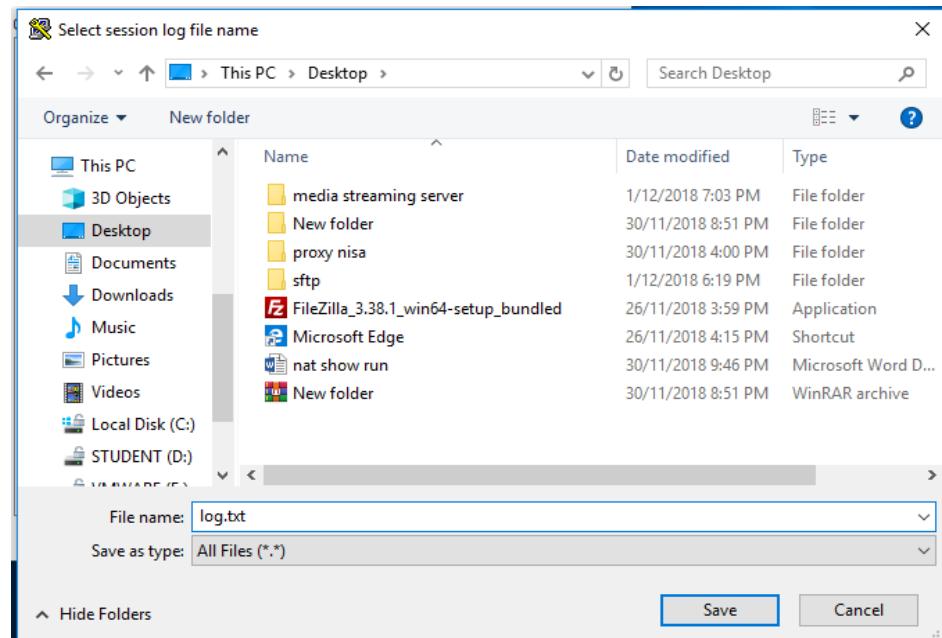


Figure 5. 356 : Select session log file name

Step 3: Select **Default Settings** and click **Open**.

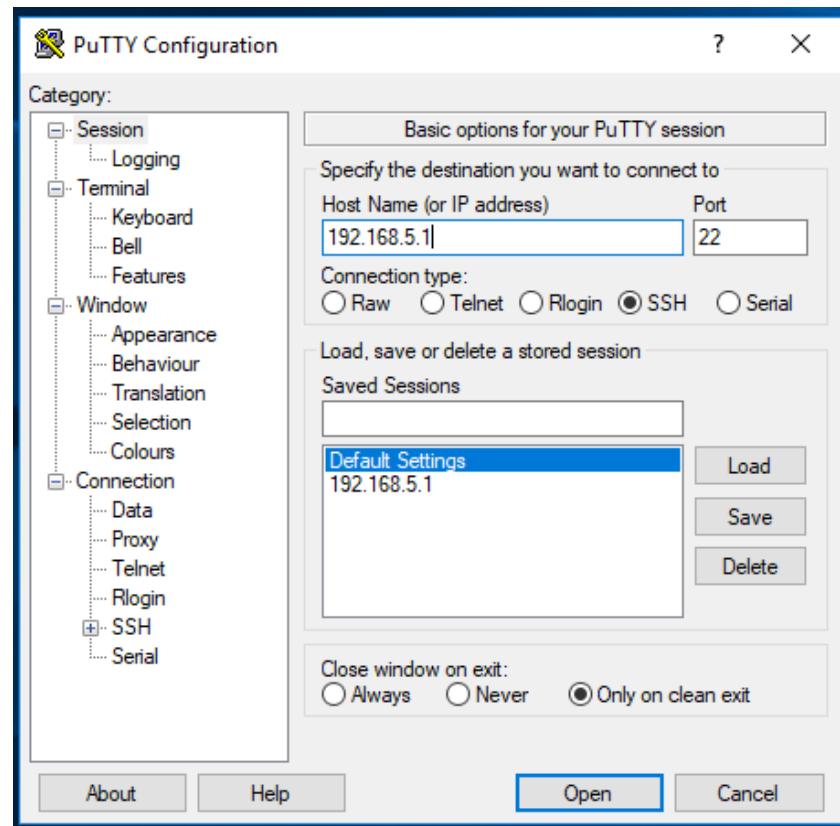
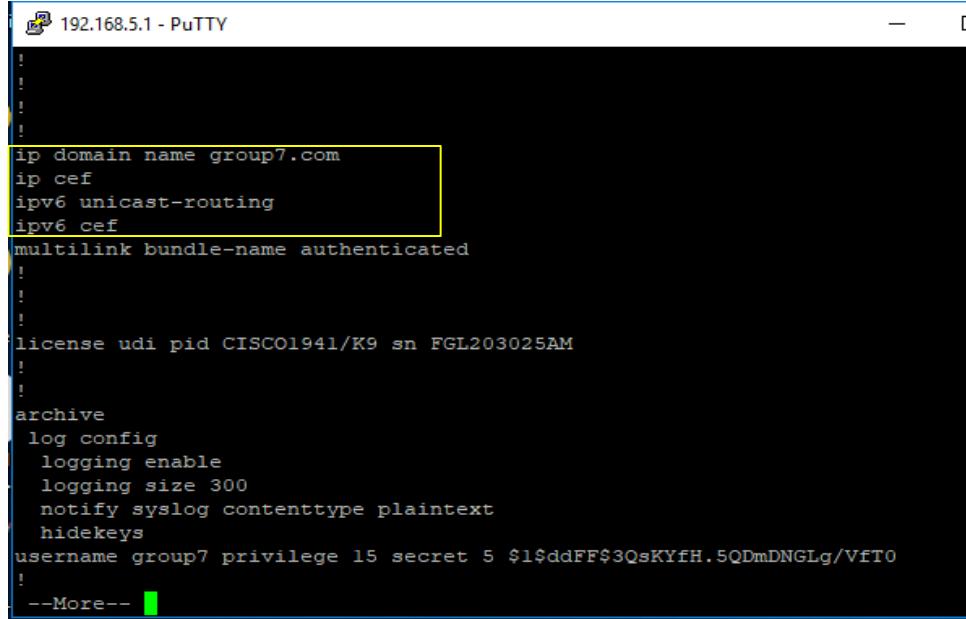


Figure 5. 357 : Putty Configuration

Disable DNS Lookup

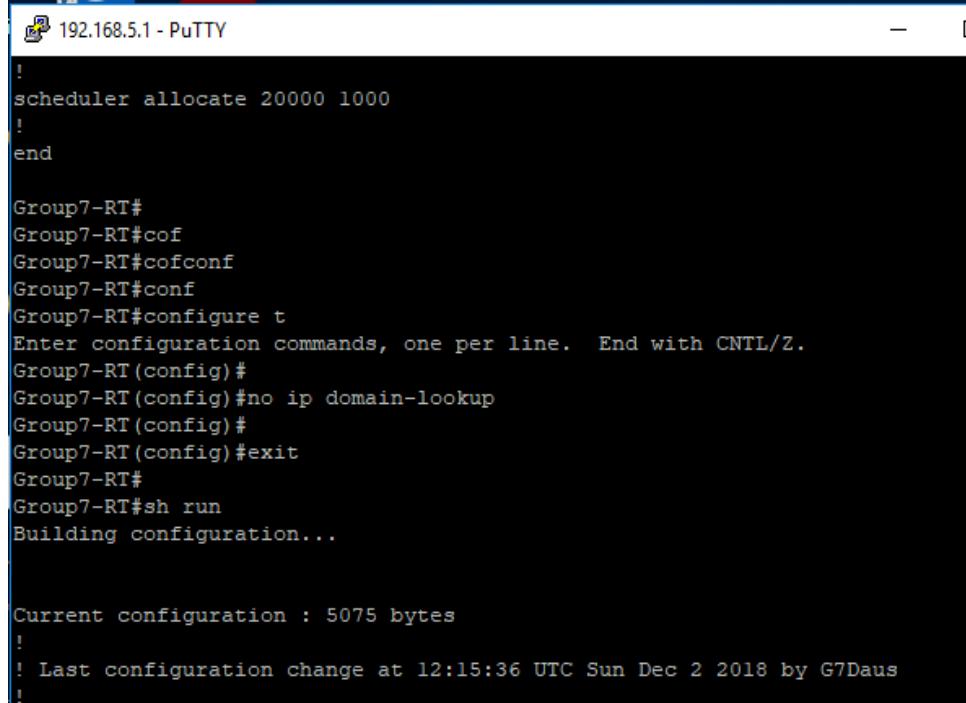
Step 1: Login as usual and use command show run to see the ip domain is enable.



```
!  
!  
!  
!  
ip domain name group7.com  
ip cef  
ipv6 unicast-routing  
ipv6 cef  
multilink bundle-name authenticated  
!  
!  
!  
license udi pid CISCO1941/K9 sn FGL203025AM  
!  
!  
archive  
log config  
logging enable  
logging size 300  
notify syslog contenttype plaintext  
hidekeys  
username group7 privilege 15 secret 5 $1$ddFF$3QsKYfH.5QDmDNGLg/VfT0  
!  
--More--
```

Figure 5. 358 : Putty

Step 2 : Use command **no ip domain-lookup**.



```
!  
scheduler allocate 20000 1000  
!  
end  
  
Group7-RT#  
Group7-RT#cof  
Group7-RT#cofconf  
Group7-RT#conf  
Group7-RT#configure t  
Enter configuration commands, one per line. End with CNTL/Z.  
Group7-RT(config)#  
Group7-RT(config)#no ip domain-lookup  
Group7-RT(config)#  
Group7-RT(config)#exit  
Group7-RT#  
Group7-RT#sh run  
Building configuration...  
  
Current configuration : 5075 bytes  
!  
! Last configuration change at 12:15:36 UTC Sun Dec 2 2018 by G7Daus  
!
```

Figure 5. 359 : Putty

5.2.21 Remote login using SSH

Step 1: SSH configuration for router:

```
# conf t
# ip domain-name group7.com
# crypto key generate rsa general-keys modulus 1024
# line vty 0 5
# transport input ssh
# login local
# username group7 privilege 15 secret group7123
# exit
# conf t
# ip ssh version 2
# exit
# copy running-config startup-config
```

```
Group7-RT>en
Group7-RT#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Group7-RT(config)#ip domain-name group7.com
Group7-RT(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: Group7-RT.group7.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)

Group7-RT(config)#
*Oct 18 09:06:58.748: %SSH-5-ENABLED: SSH 1.99 has been enabled
Group7-RT(config)#line vty 0 5
Group7-RT(config-line)#transport input ssh
```

Figure 5. 360 : Configuration for router

```
Group7-RT(config-line)#login local
Group7-RT(config-line)#username group7 privilege 15 secret group7123
Group7-RT(config)#exit
```

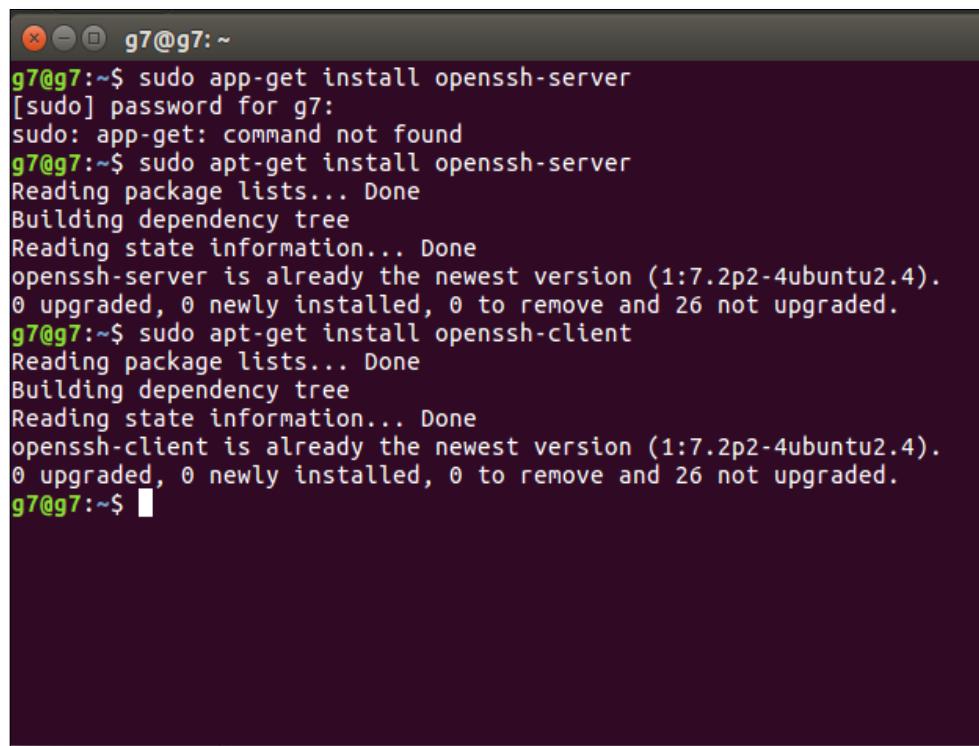
Figure 5. 361 : Login local

```
Group7-RT(config)#ip ssh version 2  
Group7-RT(config)#exit
```

Figure 5. 362 : IP SSH v2

Step 2: SSH configuration on Ubuntu

```
# sudo apt-get install openssh-server
```



The screenshot shows a terminal window titled 'g7@g7: ~'. The user runs several commands to manage the OpenSSH package. First, they attempt to use 'app-get' instead of 'apt-get', which fails because the command is not found. They then successfully run 'apt-get install openssh-server', which installs the package without upgrading it. Next, they run 'apt-get install openssh-client', which also installs the client without upgrading it. Finally, they run 'apt-get upgrade', which outputs that no packages are upgradeable.

```
g7@g7:~$ sudo app-get install openssh-server  
[sudo] password for g7:  
sudo: app-get: command not found  
g7@g7:~$ sudo apt-get install openssh-server  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
openssh-server is already the newest version (1:7.2p2-4ubuntu2.4).  
0 upgraded, 0 newly installed, 0 to remove and 26 not upgraded.  
g7@g7:~$ sudo apt-get install openssh-client  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
openssh-client is already the newest version (1:7.2p2-4ubuntu2.4).  
0 upgraded, 0 newly installed, 0 to remove and 26 not upgraded.  
g7@g7:~$
```

Figure 5. 363 : Configuration on Ubuntu

The screenshot shows a terminal window titled "g7@g7: ~" with the command "File: /etc/ssh/sshd_config". The file content is as follows:

```
# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::

#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600

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

Figure 5. 364 : Configuration file of sshd

The screenshot shows a terminal window titled "g7@g7: ~" with the command "File: /etc/ssh/sshd_config". The file content is as follows:

```
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 1024

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin prohibit-password
StrictModes yes

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

Figure 5. 365 : Configuration file of sshd

Step 3: SSH configuration on Fedora

```
# sudo yum install openssh-server
```

```
[g7@fedora-group7-com ~]$ sudo yum install openssh-server
Fedora 28 - x86_64 - Updates                               1.2 MB/s | 25 MB   00:19
Last metadata expiration check: 0:00:16 ago on Thu 04 Oct 2018 09:49:02 PM +08.
Package openssh-server-7.7p1-2.fc28.x86_64 is already installed, skipping.
Dependencies resolved.
Nothing to do.
Complete!
[g7@fedora-group7-com ~]$
```

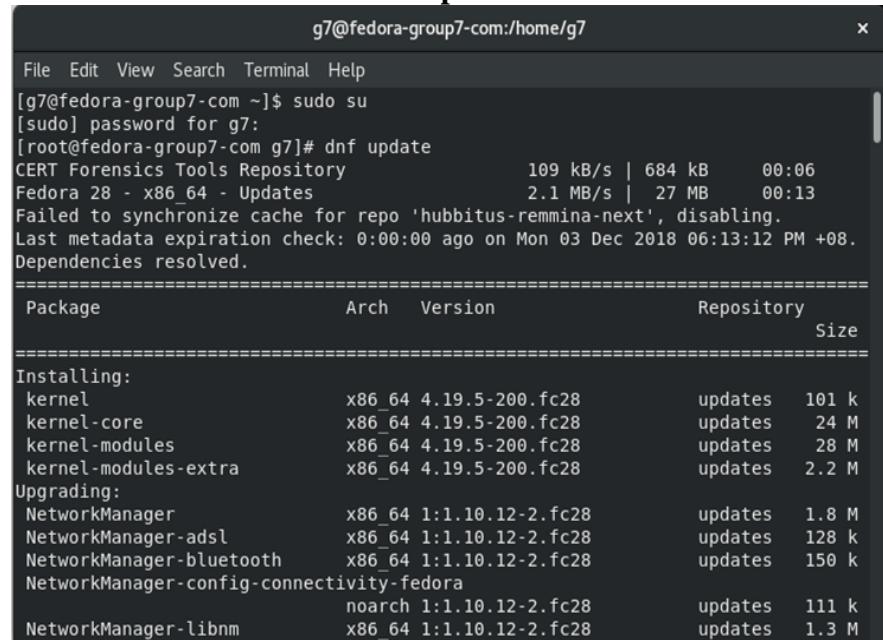
Figure 5. 366 : Install openssh-server

5.2.22 Linux server hardening

System Updates

Keeping the system up to date is necessary after installing any operation system. This initial step will reduce known vulnerabilities in the system.

Use command **sudo su** and **dnf update**.

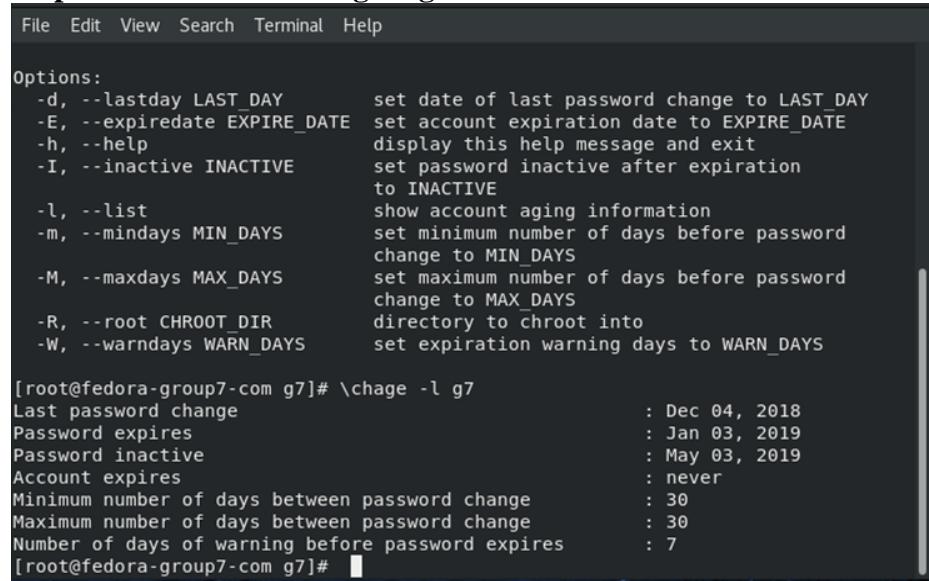


```
g7@fedora-group7-com:/home/g7
File Edit View Search Terminal Help
[g7@fedora-group7-com ~]$ sudo su
[sudo] password for g7:
[root@fedora-group7-com g7]# dnf update
CERT Forensics Tools Repository           109 kB/s | 684 kB     00:06
Fedora 28 - x86_64 - Updates             2.1 MB/s |  27 MB     00:13
Failed to synchronize cache for repo 'hubbitus-remmina-next', disabling.
Last metadata expiration check: 0:00:00 ago on Mon 03 Dec 2018 06:13:12 PM +08.
Dependencies resolved.
=====
Package          Arch    Version        Repository      Size
=====
Installing:
kernel          x86_64  4.19.5-200.fc28   updates       101 k
kernel-core      x86_64  4.19.5-200.fc28   updates       24 M
kernel-modules   x86_64  4.19.5-200.fc28   updates       28 M
kernel-modules-extra x86_64  4.19.5-200.fc28   updates       2.2 M
Upgrading:
NetworkManager   x86_64  1:1.10.12-2.fc28  updates       1.8 M
NetworkManager-adsl x86_64  1:1.10.12-2.fc28  updates       128 k
NetworkManager-bluetooth x86_64  1:1.10.12-2.fc28  updates       150 k
NetworkManager-config-connectivity-fedora noarch  1:1.10.12-2.fc28  updates       111 k
NetworkManager-libnm   x86_64  1:1.10.12-2.fc28  updates       1.3 M
```

Figure 5. 367: g7@fedora-group7-com:/home/g7

Password Expiry

Step 1: Use command **chage -l g7** to view the current status.



```
File Edit View Search Terminal Help
Options:
-d, --lastday LAST_DAY      set date of last password change to LAST_DAY
-E, --expiredate EXPIRE_DATE set account expiration date to EXPIRE_DATE
-h, --help                   display this help message and exit
-I, --inactive INACTIVE      set password inactive after expiration
                             to INACTIVE
-l, --list                   show account aging information
-m, --mindays MIN_DAYS      set minimum number of days before password
                             change to MIN_DAYS
-M, --maxdays MAX_DAYS      set maximum number of days before password
                             change to MAX_DAYS
-R, --root CHROOT_DIR       directory to chroot into
-W, --warndays WARN_DAYS    set expiration warning days to WARN_DAYS

[root@fedora-group7-com g7]# \chage -l g7
Last password change          : Dec 04, 2018
Password expires              : Jan 03, 2019
Password inactive              : May 03, 2019
Account expires                : never
Minimum number of days between password change : 30
Maximum number of days between password change : 30
Number of days of warning before password expires : 7
[root@fedora-group7-com g7]#
```

Figure 5. 368 : g7@fedora-group7-com:/home/g7

Step 2: Use command **chage -M 30 g7** to set **Maximum number of days between password change**. Note that option -M will update both “Password expires” and “Maximum number of days between password change”. Then, use command **chage -l g7** to see the current status.

```
[root@fedora-group7-com g7]# chage -M 30 g7
[root@fedora-group7-com g7]#
[root@fedora-group7-com g7]# \chage -l g7
Last password change : Dec 04, 2018
Password expires      : Jan 03, 2019
Password inactive     : May 03, 2019
Account expires        : never
Minimum number of days between password change : 30
Maximum number of days between password change : 30
Number of days of warning before password expires : 7
```

Figure 5. 369 : g7@fedora-group7-com:/home/g7

Step 3: Use command **chage -E “2019-03-01” g7** to set the date of **Account Expires**. Then, use command **chage -l g7** to see the current status.

```
[root@fedora-group7-com g7]# chage -E "2019-03-01" g7
[root@fedora-group7-com g7]#
[root@fedora-group7-com g7]# \chage -l g7
Last password change : Dec 04, 2018
Password expires      : Jan 03, 2019
Password inactive     : Feb 02, 2019
Account expires        : Mar 01, 2019
Minimum number of days between password change : 30
Maximum number of days between password change : 30
Number of days of warning before password expires : 7
```

Figure 5. 370 : g7@fedora-group7-com:/home/g7

Step 4: Use command **chage -I 30 g7** to set the **Password Inactives**. The “Password inactive” date is set to 30 days from the “Password expires” value. Then, use command **chage -l g7** to see the current status.

```
[root@fedora-group7-com g7]# chage -I 30 g7
[root@fedora-group7-com g7]#
[root@fedora-group7-com g7]# \chage -l g7
Last password change : Dec 04, 2018
Password expires      : Jan 03, 2019
Password inactive     : Feb 02, 2019
Account expires        : Jun 01, 2019
Minimum number of days between password change : 30
Maximum number of days between password change : 30
Number of days of warning before password expires : 7
```

Figure 5. 371 : g7@fedora-group7-com:/home/g7

Step 5: Use command **chage -m 30 g7** to set the **Minimum number of days between password change**. Then, use command **chage -l g7** to see the current status.

```
[root@fedora-group7-com g7]# chage -m 30 g7
[root@fedora-group7-com g7]# \chage -l g7
Last password change : Dec 04, 2018
Password expires      : Jan 03, 2019
Password inactive     : Feb 02, 2019
Account expires        : Mar 01, 2019
Minimum number of days between password change : 30
Maximum number of days between password change : 30
Number of days of warning before password expires : 7
[root@fedora-group7-com g7]#
```

Figure 5. 372 : g7@fedora-group7-com:/home/g7

Step 6: Use command **chage -W 7 g7** to set the **Number of days of warning before password expires**. Then, use command **chage -l g7** to see the current status.

```
[root@fedora-group7-com g7]# chage -W 7 g7
[root@fedora-group7-com g7]# \chage -l g7
Last password change : Dec 04, 2018
Password expires      : Jan 03, 2019
Password inactive     : Feb 02, 2019
Account expires        : Mar 01, 2019
Minimum number of days between password change : 30
Maximum number of days between password change : 30
Number of days of warning before password expires : 7
[root@fedora-group7-com g7]#
```

Figure 5. 373: g7@fedora-group7-com:/home/g7

Disable Unnecessary Port

Disable unused open port can prevent unauthorized access. To find out which port are currently opened, Nmap software is used to scan available ports.

Type command **nmap -v -sT localhost** to display list of scan ports.

```
[root@fedora-group7-com g7]# nmap -v -sT localhost
Starting Nmap 7.60 ( https://nmap.org ) at 2018-12-04 20:07 +08
Initiating Connect Scan at 20:07
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 21/tcp on 127.0.0.1
Discovered open port 139/tcp on 127.0.0.1
Discovered open port 111/tcp on 127.0.0.1
Discovered open port 445/tcp on 127.0.0.1
Discovered open port 22/tcp on 127.0.0.1
Discovered open port 464/tcp on 127.0.0.1
Discovered open port 5666/tcp on 127.0.0.1
Discovered open port 749/tcp on 127.0.0.1
Discovered open port 631/tcp on 127.0.0.1
Discovered open port 88/tcp on 127.0.0.1
Completed Connect Scan at 20:07, 0.03s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00018s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 990 closed ports
```

Figure 5. 374 : g7@fedora-group7-com:/home/g7

```

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
88/tcp    open  kerberos-sec
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
631/tcp   open  ipp
749/tcp   open  kerberos-adm
5666/tcp  open  nrpe

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
          Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
[root@fedora-group7-com g7]#

```

Figure 5. 375 : g7@fedora-group7-com:/home/g7

Disable CUPS service

Run command **service cups stop**.

Check CUPS status by using command **nmap -v -sT localhost**.

```

[root@fedora-group7-com g7]# service cups stop
Redirecting to /bin/systemctl stop cups.service
[root@fedora-group7-com g7]# nmap -v -sT localhost

Starting Nmap 7.60 ( https://nmap.org ) at 2018-12-04 20:13 +08
Initiating Connect Scan at 20:13
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 111/tcp on 127.0.0.1
Discovered open port 21/tcp on 127.0.0.1
Discovered open port 22/tcp on 127.0.0.1
Discovered open port 445/tcp on 127.0.0.1
Discovered open port 139/tcp on 127.0.0.1
Discovered open port 749/tcp on 127.0.0.1
Discovered open port 464/tcp on 127.0.0.1
Discovered open port 5666/tcp on 127.0.0.1
Discovered open port 88/tcp on 127.0.0.1
Completed Connect Scan at 20:13, 0.02s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00012s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 991 closed ports

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
88/tcp    open  kerberos-sec
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
749/tcp   open  kerberos-adm
5666/tcp  open  nrpe

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
          Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
[root@fedora-group7-com g7]#

```

Figure 5. 376 : g7@fedora-group7-com:/home/g7

5.2.23 Windows server hardening

Installation and Configure a Security Policy

Step 1: Search for Administrative Tools and click on Security Configuration Wizard.

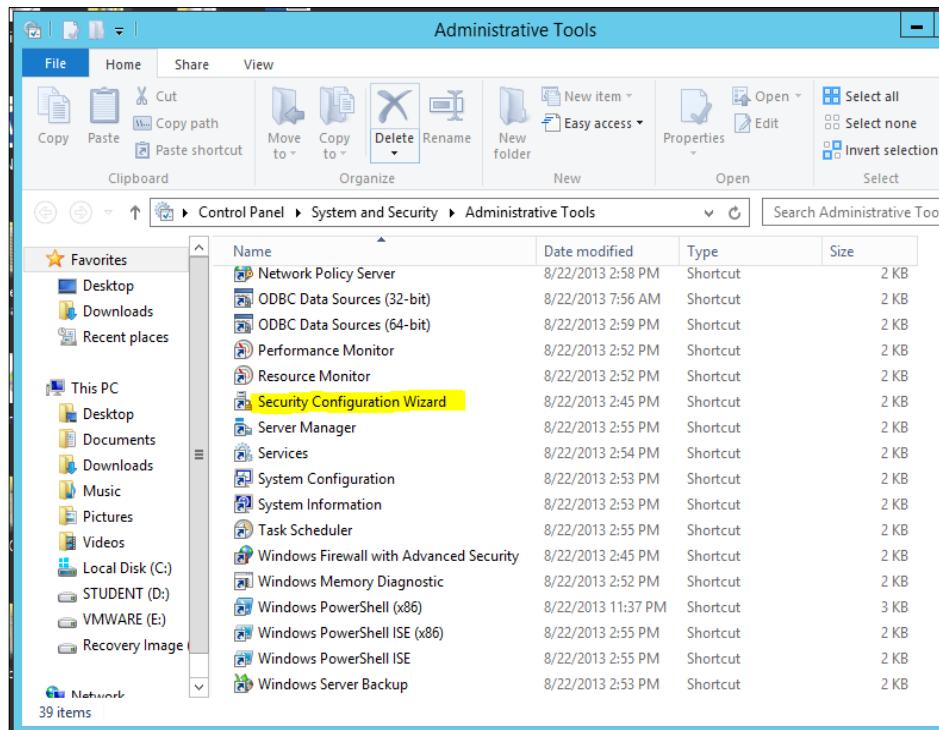


Figure 5. 377 : Administrative Tools

Step 2: Open page of the Security Configuration Wizard. Click Next to go to next page.



Figure 5. 378 : First Page of the Security Configuration Wizard

Step 3: Select “Create a new security policy” and click Next.



Figure 5. 379 : Configuration Action

Step 4: Insert Server name which is winsrv.group7.com and click Next.

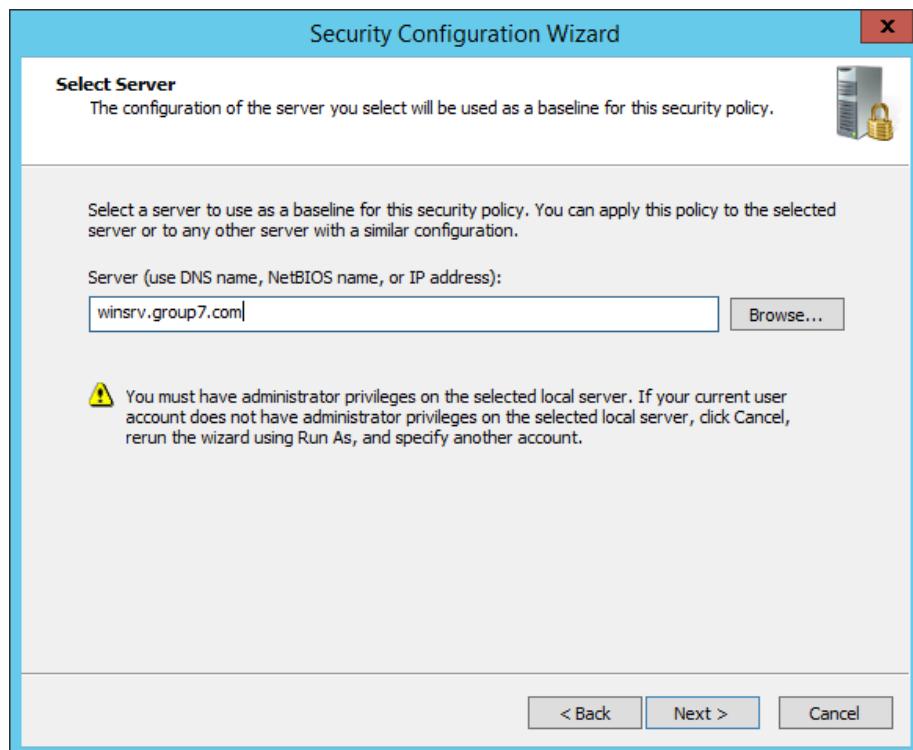


Figure 5. 380 : Select Server

Step 5: Processing Complete and click Next.

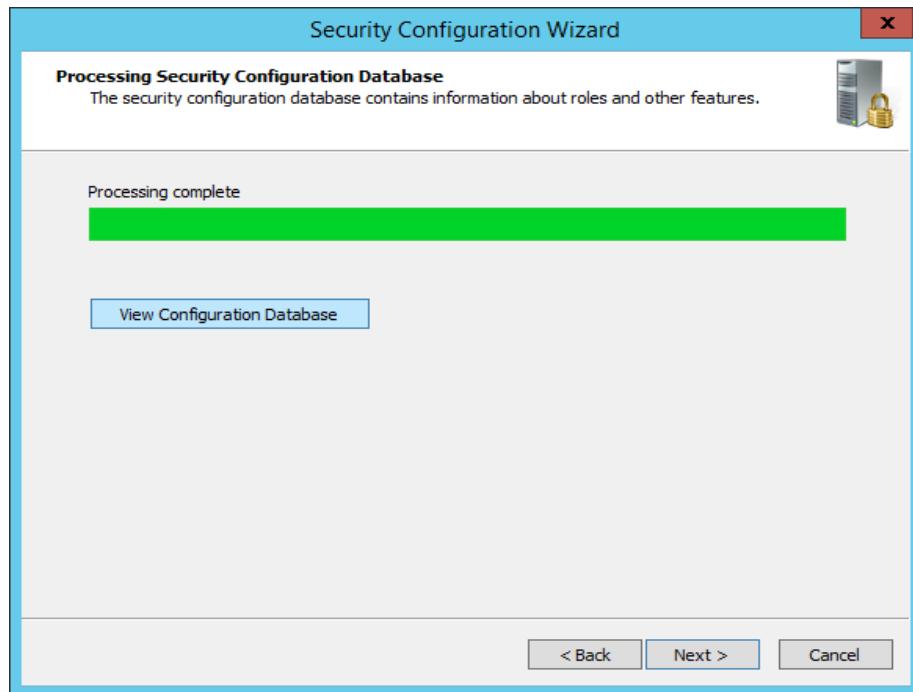


Figure 5. 381: Processing Security Configuration Database

Step 6: First page of Role-Based Service Configuration will show up when previous process is done. Click Next.

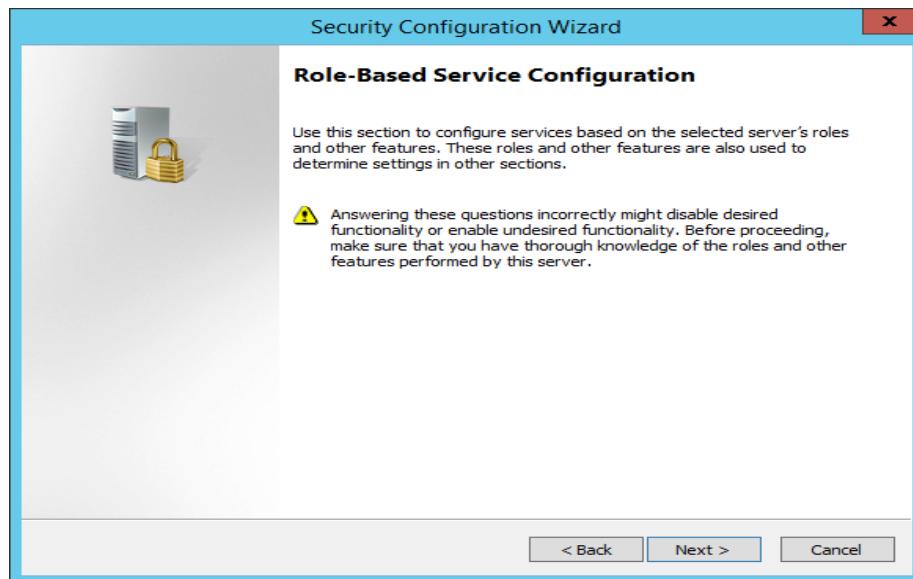


Figure 5. 382: Role-Based Service Configuration Page

Step 7: Select server roles that installed on the Server and Click Next.

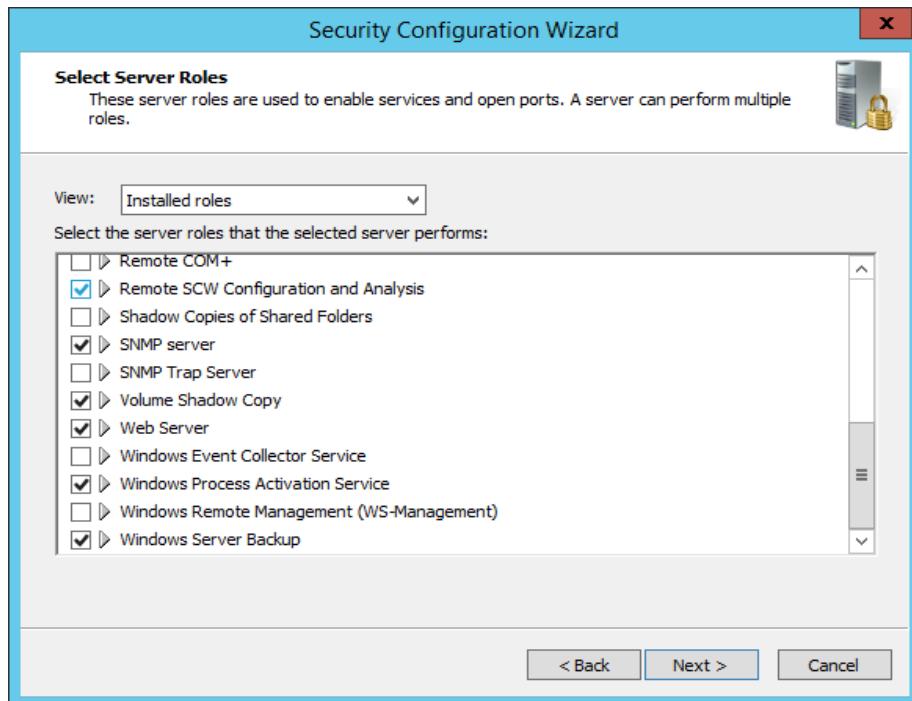


Figure 5. 383 : Select Server Roles

Step 8: Select client features that the server performs. Click Next.

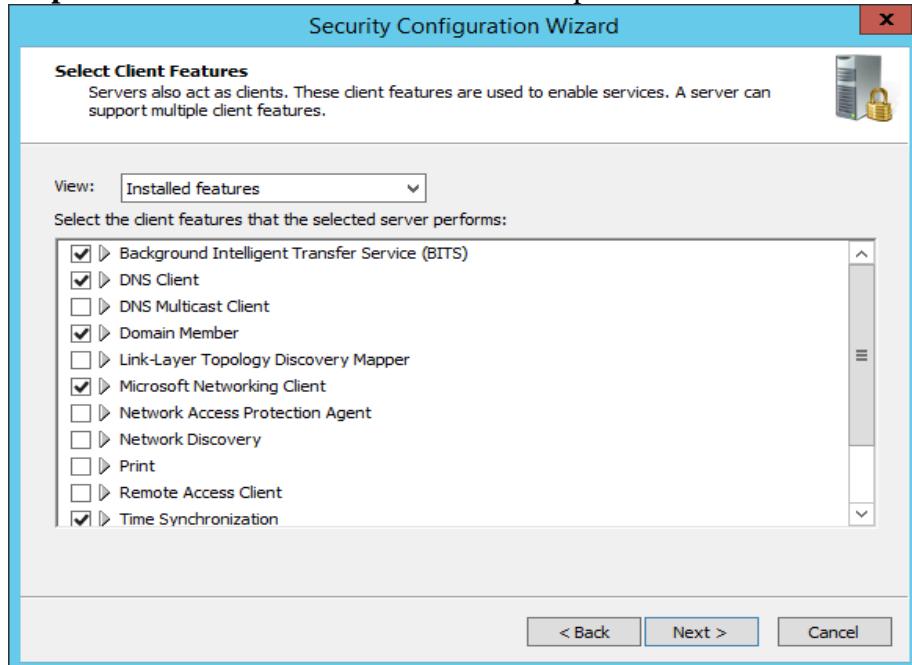


Figure 5. 384 : Client Features

Step 9: Select options used to administrate the server and click Next.

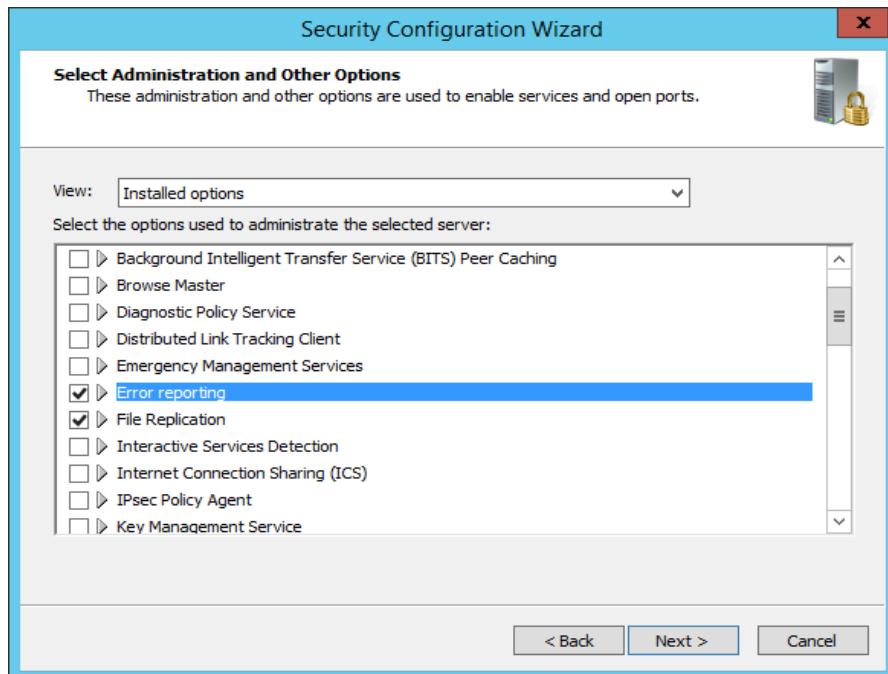


Figure 5. 385 : List of Administration and Other Options



Figure 5. 386 : List Administration and Other Options (cont)

Step 10: Select the additional services that the server requires and click Next.

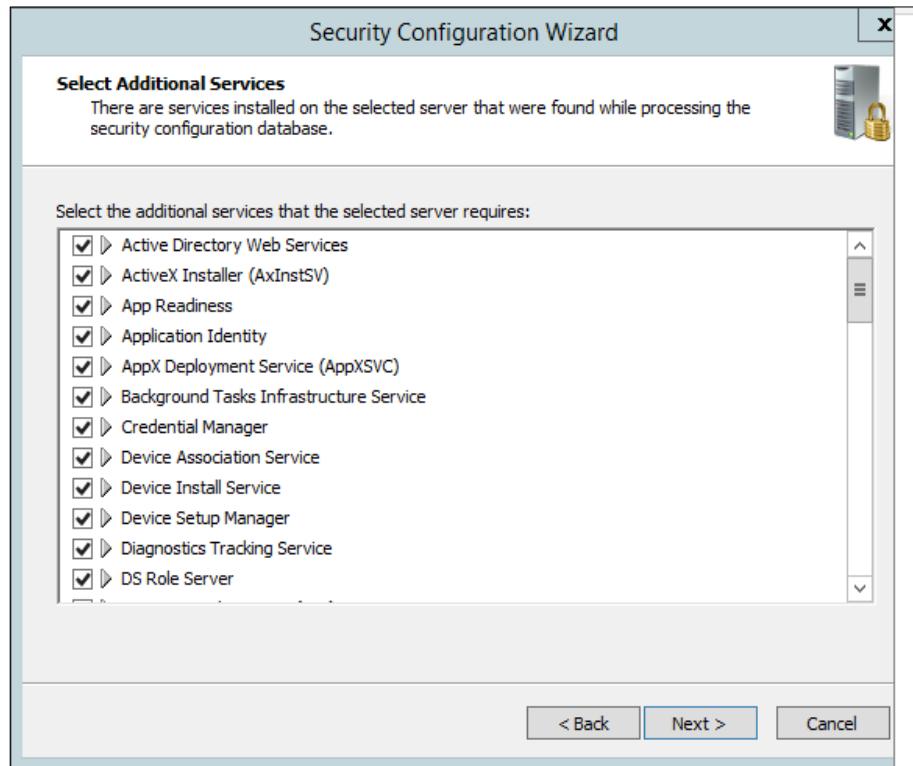


Figure 5. 387 : Additional Services

Step 11: Select “Do not change the startup mode and the service” and click Next.

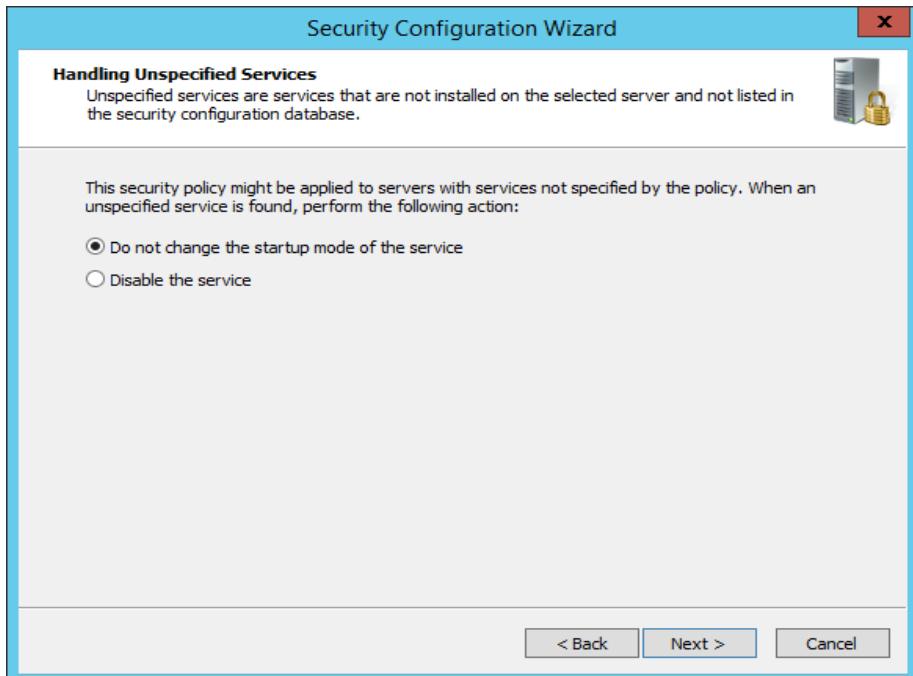


Figure 5. 388 : Handling Unspecified Services

Step 13: Confirm the service changes then click Next.

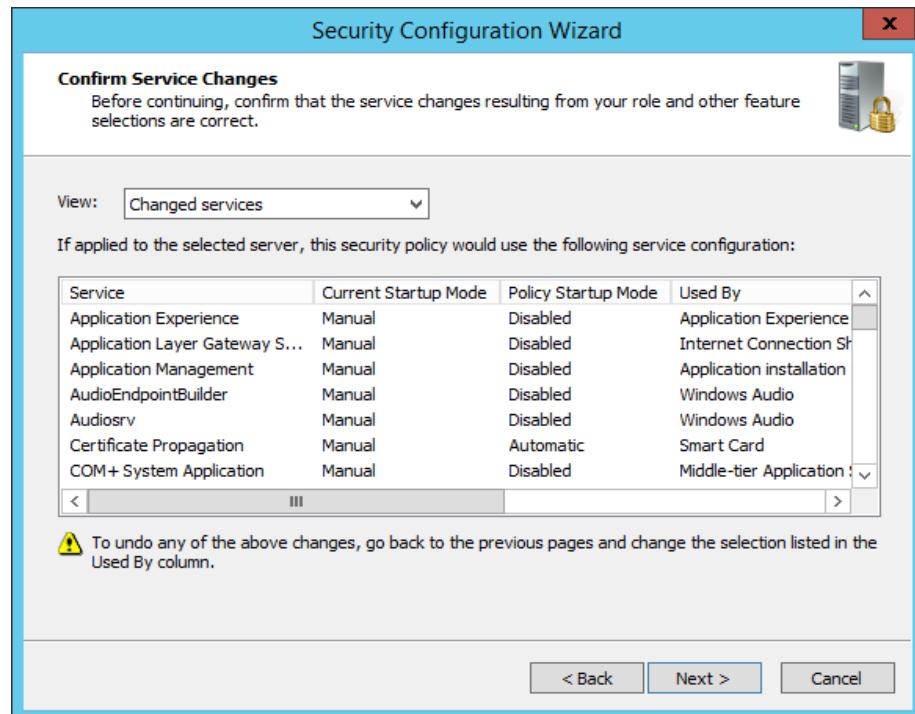


Figure 5. 389 : Confirm service changes

Step 14: Page for Network Security pop up and click Next.

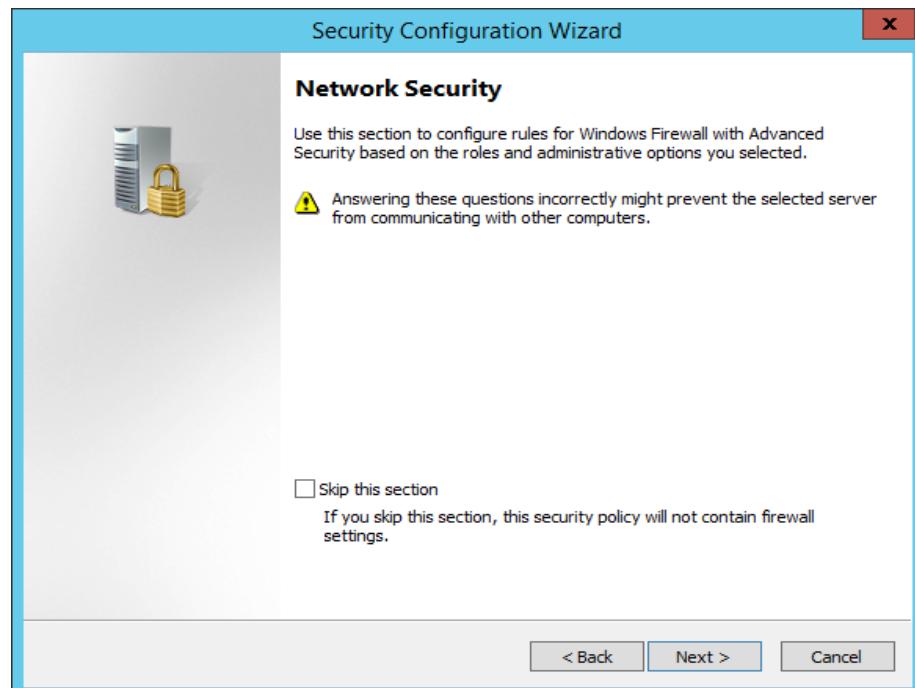


Figure 5. 390 : Network Security

Step 14: Select network security rules and click next.

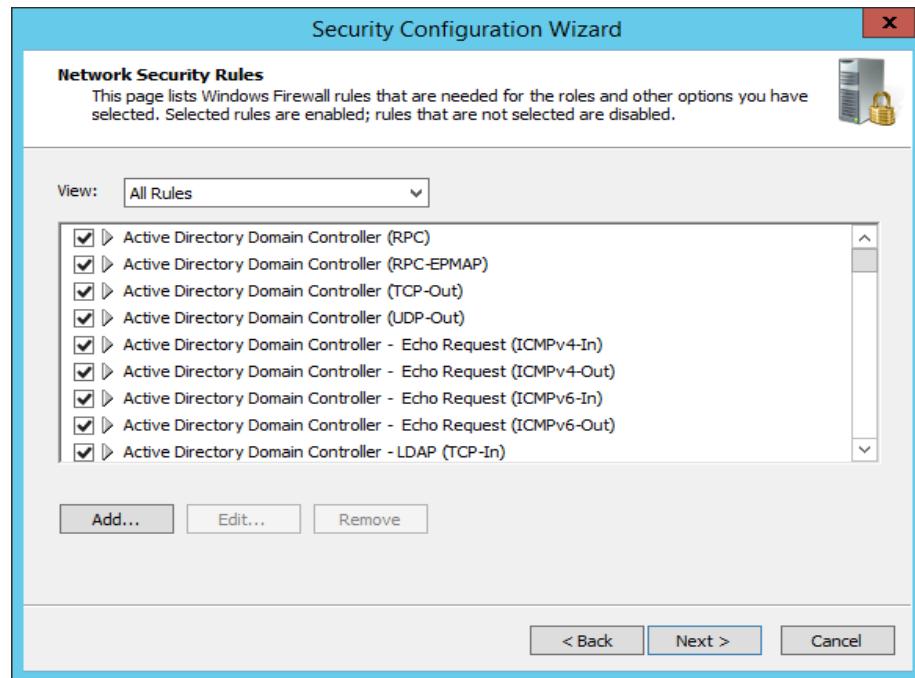


Figure 5. 391 : Network Security Rules

Step 15: Page for Registry Setting shows and click Next.



Figure 5. 392 : Registry Setting

Step 16: Select the attributes for Server Message Block (SMB) Security Signatures.

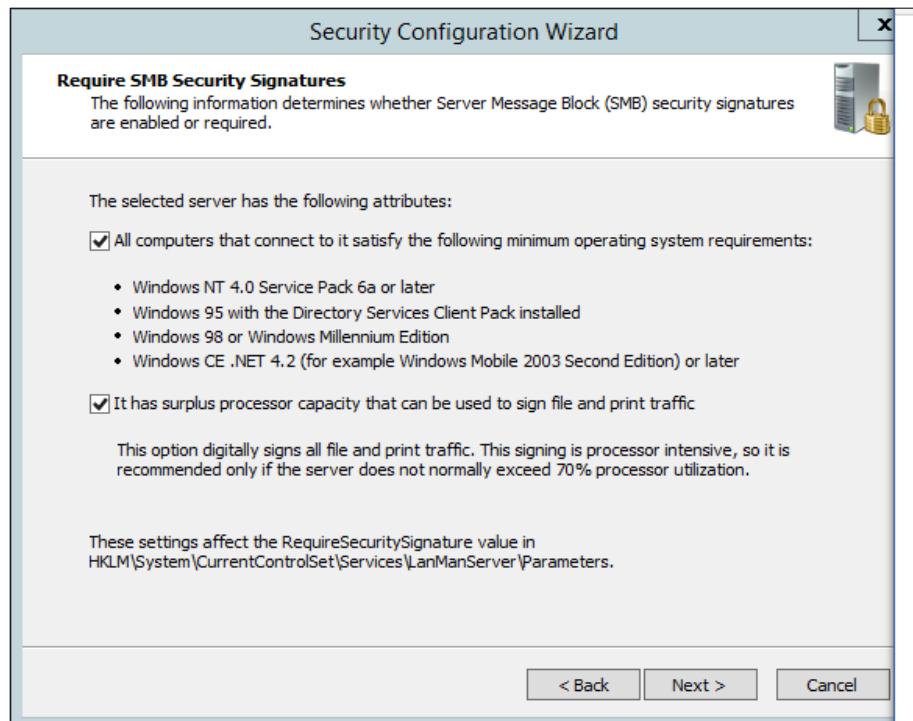


Figure 5. 393 : Require SMB Security Signatures

Step 17: Determine whether LDAP signing is required by security policy.

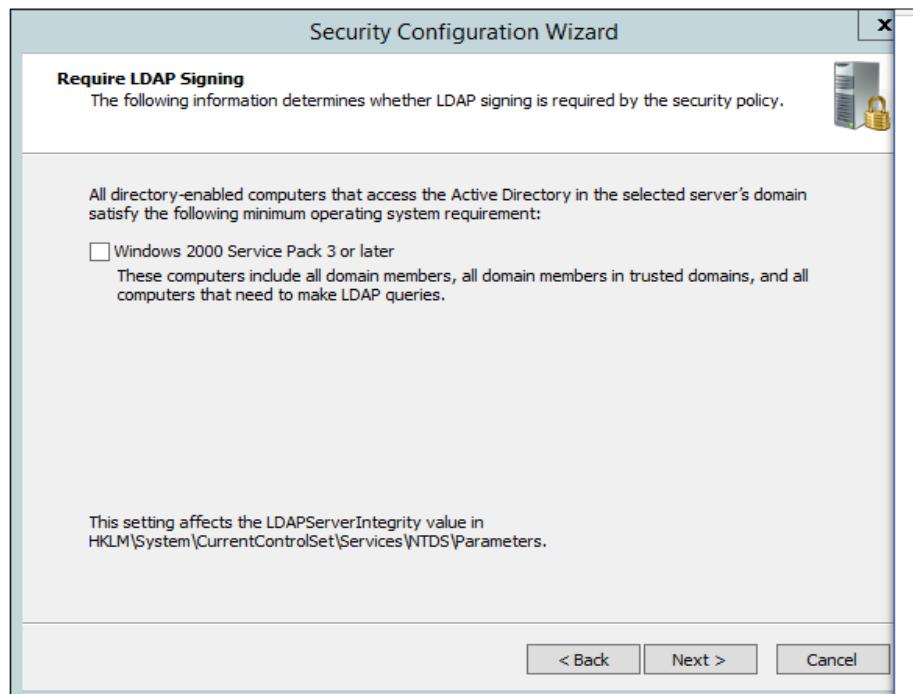


Figure 5. 394 : LDAP Signing

Step 18: Select Domain Accounts as methods uses to authenticate with remote computers and click Next.

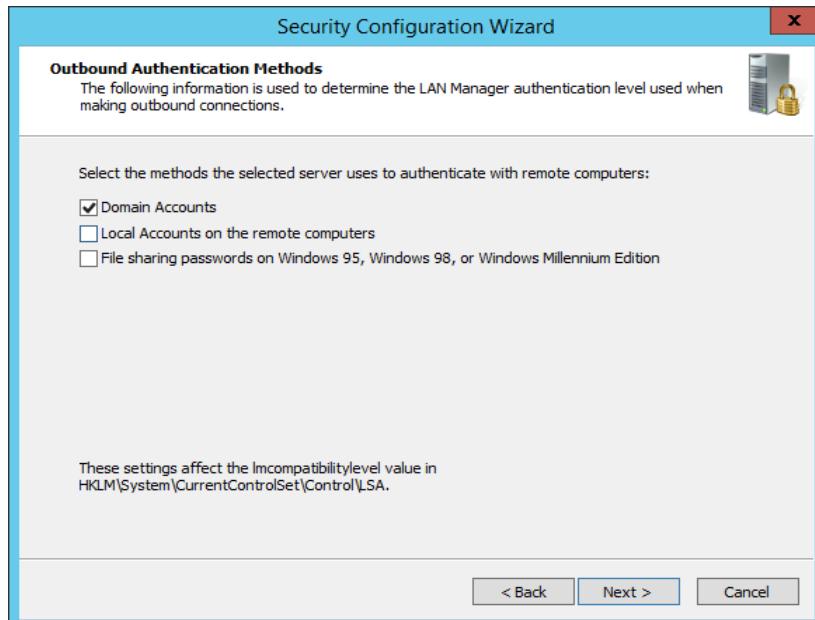


Figure 5. 395 : Outbound Authentication Methods

Step 19: Select Windows NT 4.0 Service Pack 6a or later operating systems and then click Next.

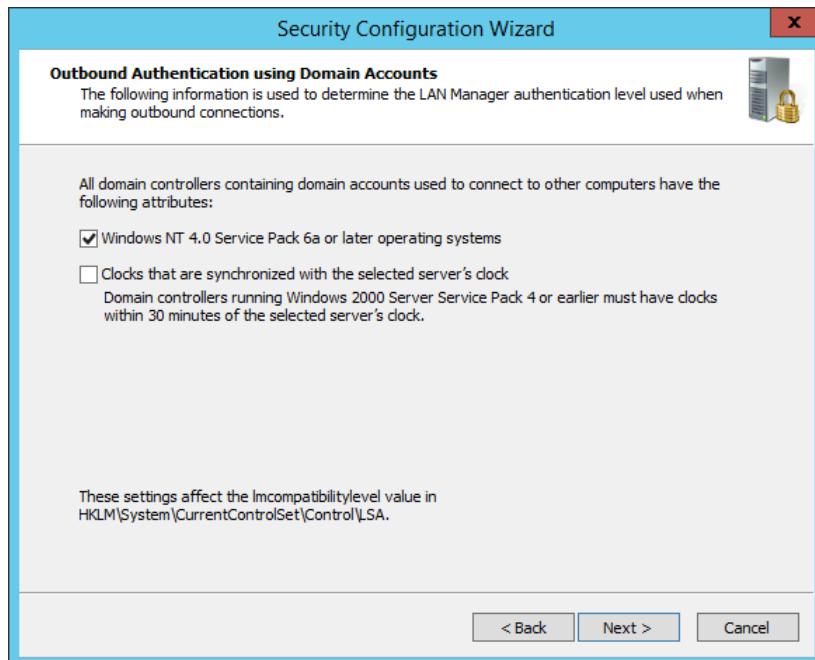


Figure 5. 396 : Outbound Authentication using Domain Accounts

Step 20: Shows the registry setting summary and click next.

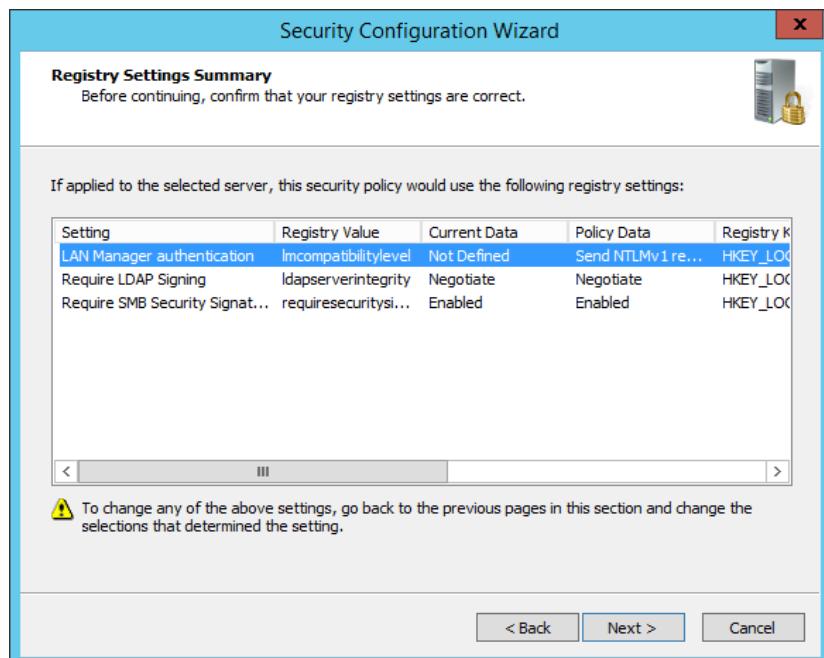


Figure 5. 397: Registry Setting Summary

Step 21: First page of the Audit Policy and click Next.

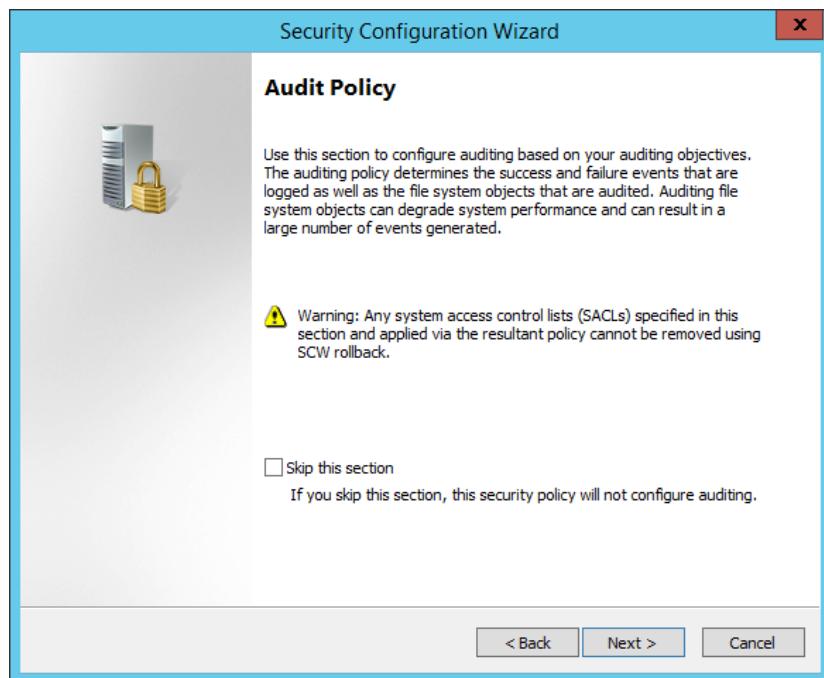


Figure 5. 398 : Audit Policy

Step 22: Select “Audit successful and unsuccessful activities” and click Next.



Figure 5. 399 : System Audit Policy

Step 23: Summary of the audit policy shows up and click Next.

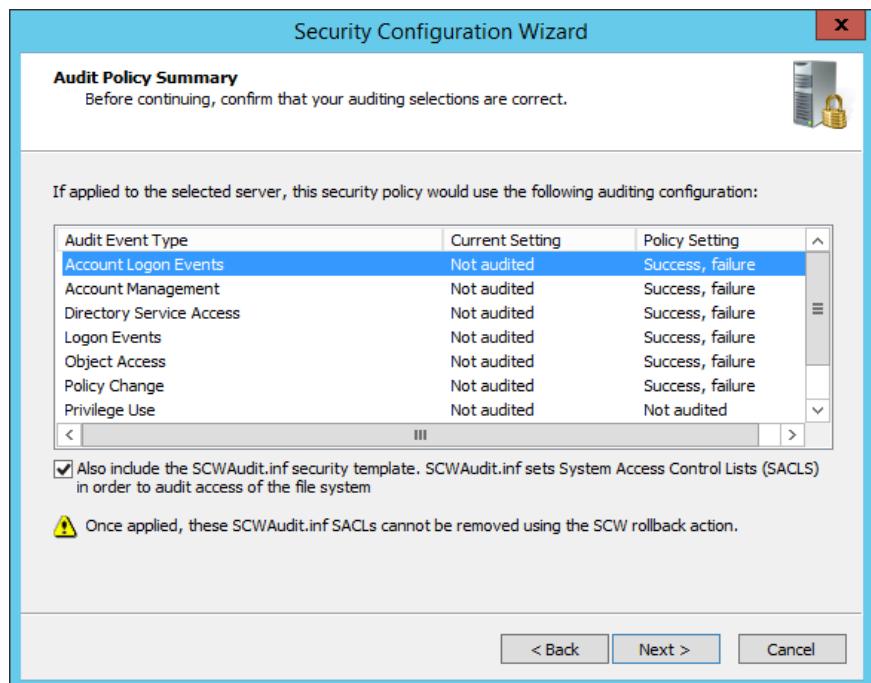


Figure 5. 400 : Audit Policy Summary

Step 24: Save the security policy and click Next.

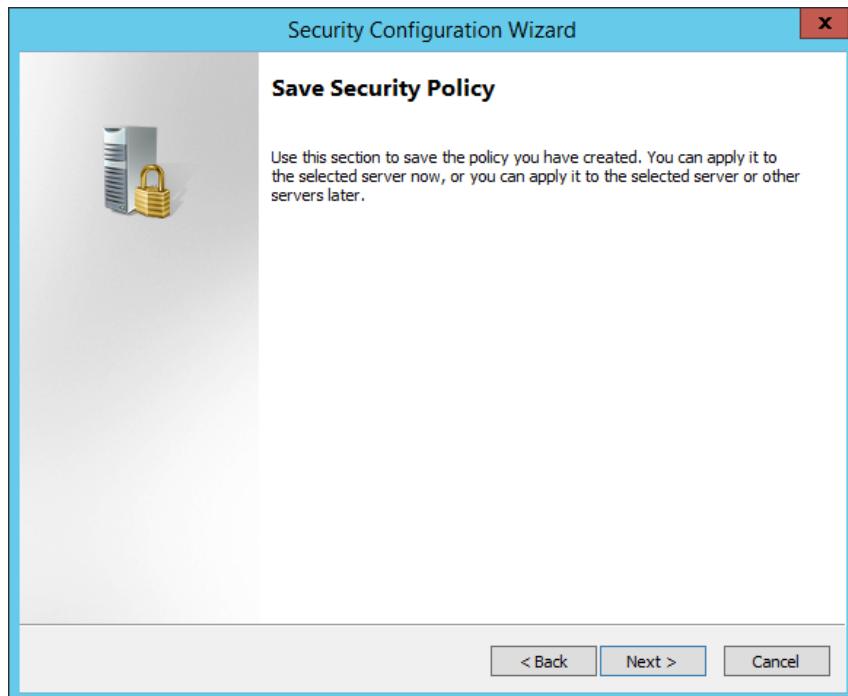


Figure 5. 401 : Save Security Policy

Step 25: Save name and location for the security policy file and click Next.

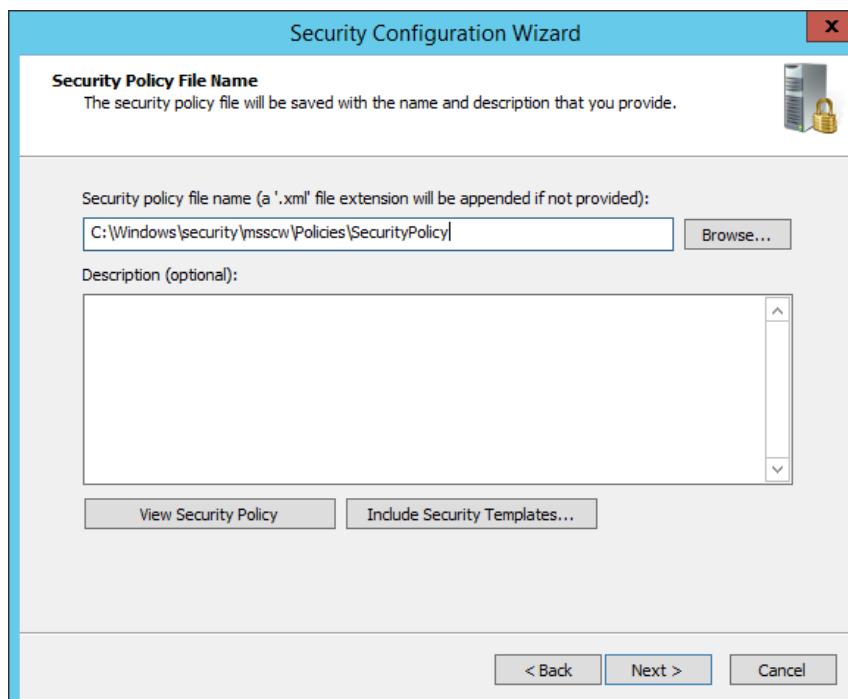


Figure 5. 402 : Security Policy File Name

Step 26: Select apply now to apply security policy and click Next.

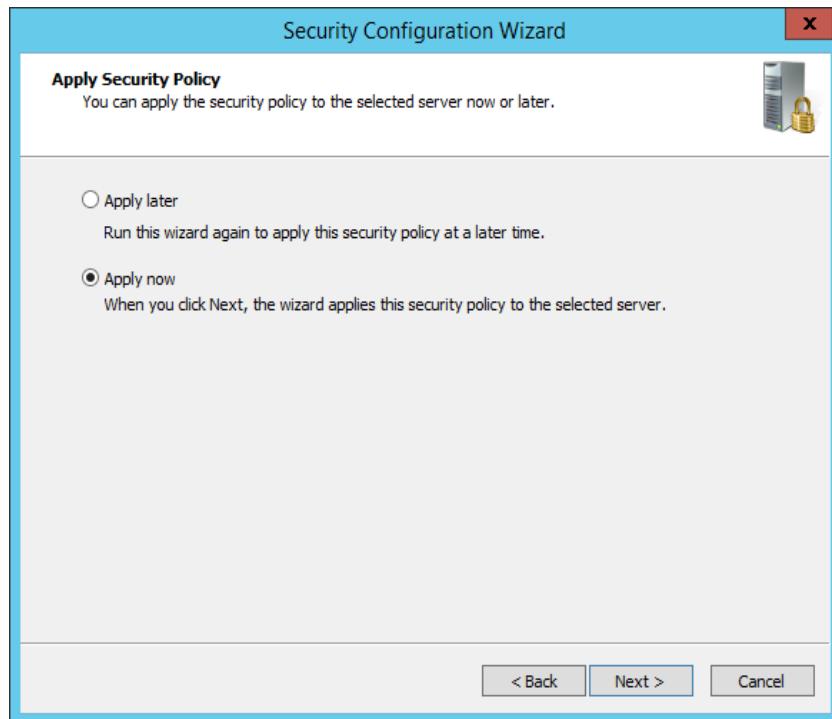


Figure 5. 403 : Apply Security Policy

Step 27: Wizard has completed configuring security policy. Click Finish.

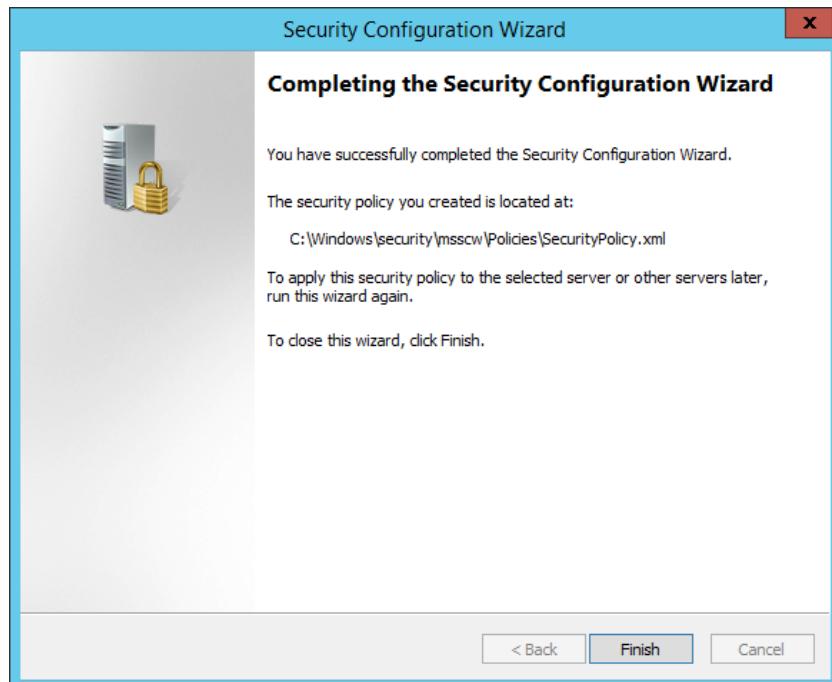


Figure 5. 404 : Security Configuration Wizard Complete

Disable or Delete Unnecessary Accounts

Step 1: Go the Active Domain Services and Computer in Server Manager.

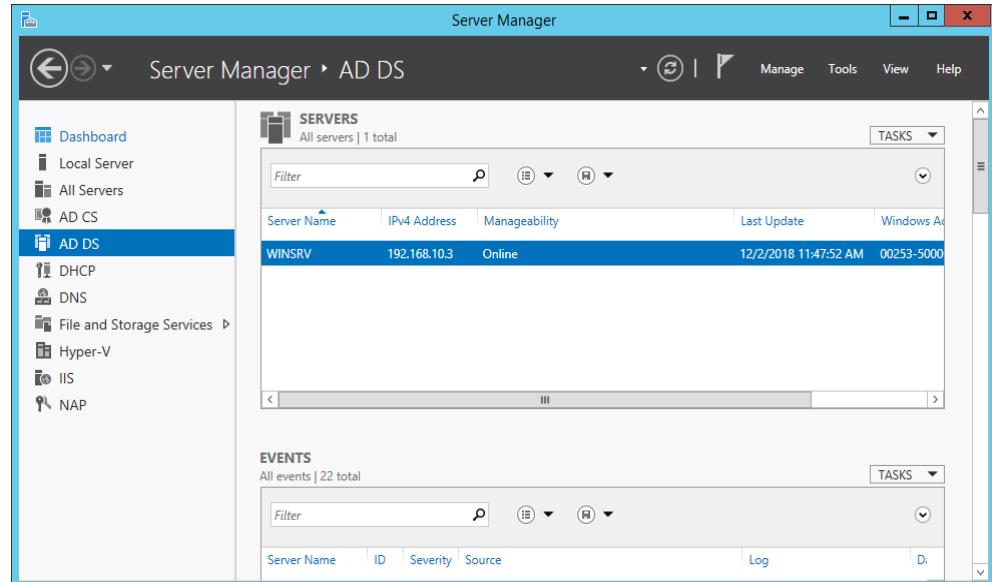


Figure 5. 405 : Server Manager

Step 2: Right click on the WINSRV and click on Active Directory Users and Computer and it will show a window.

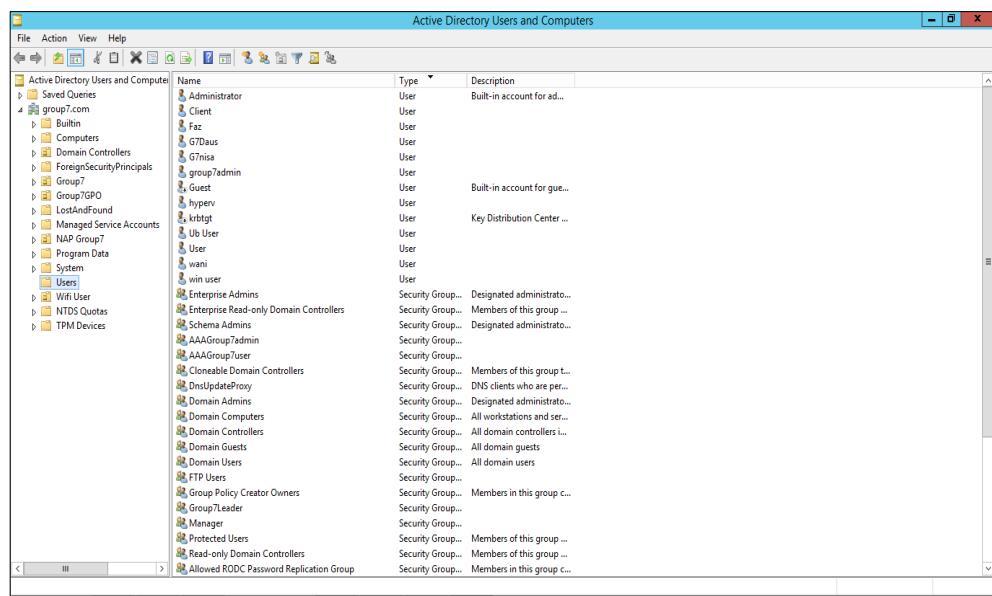


Figure 5. 406 : Active Directory Users and Computers

Step 3: Right click Guest account and choose Disable Account.

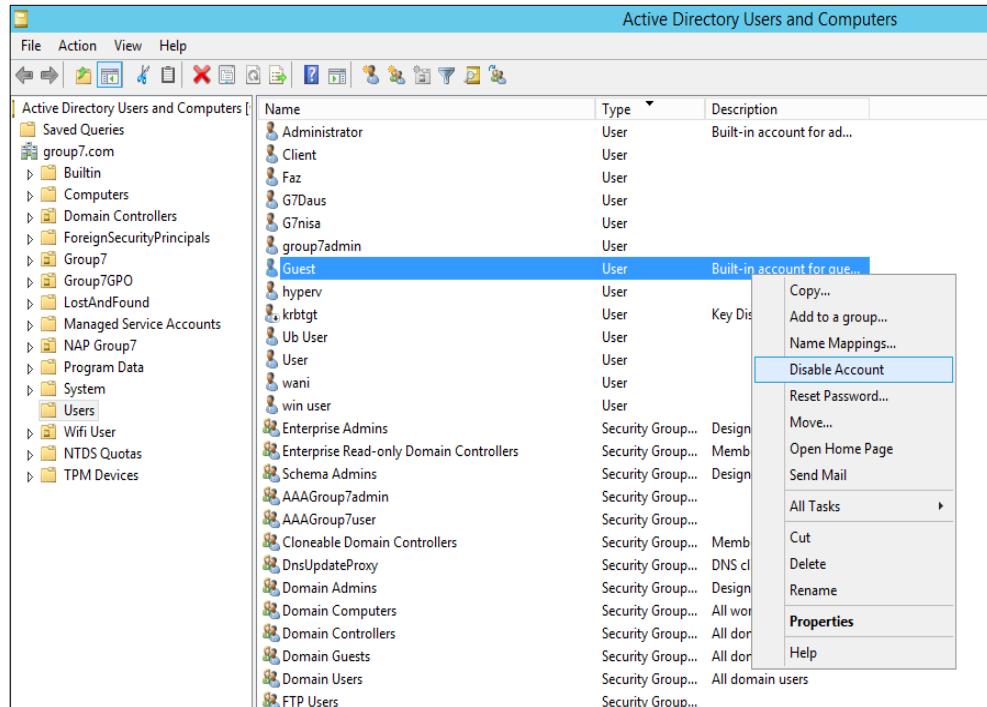


Figure 5. 407 : Disable Guest Account

Configure Auditing

Step 1: Open Server Manager and click Tools and choose Local Security Policy.

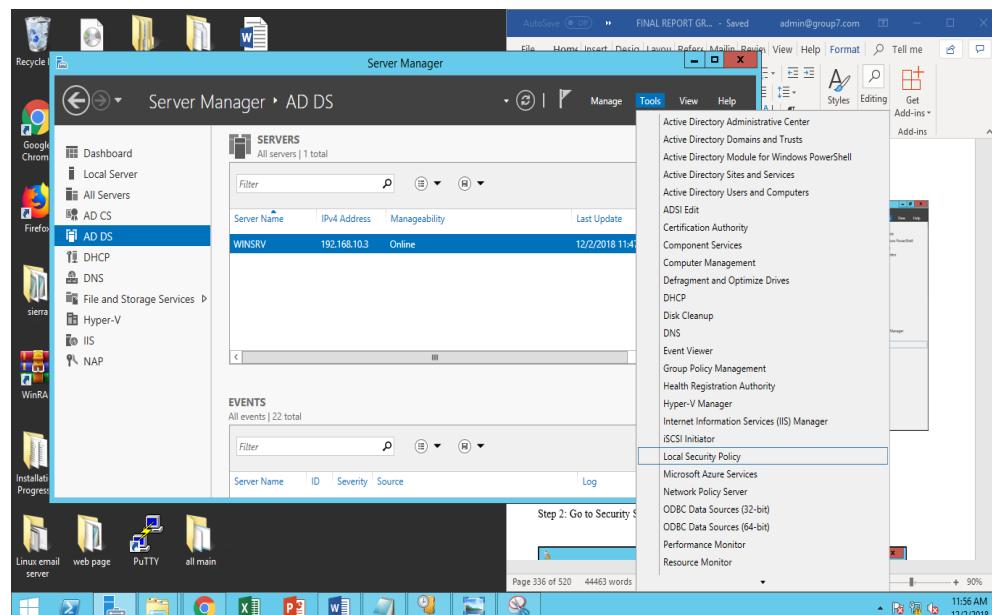
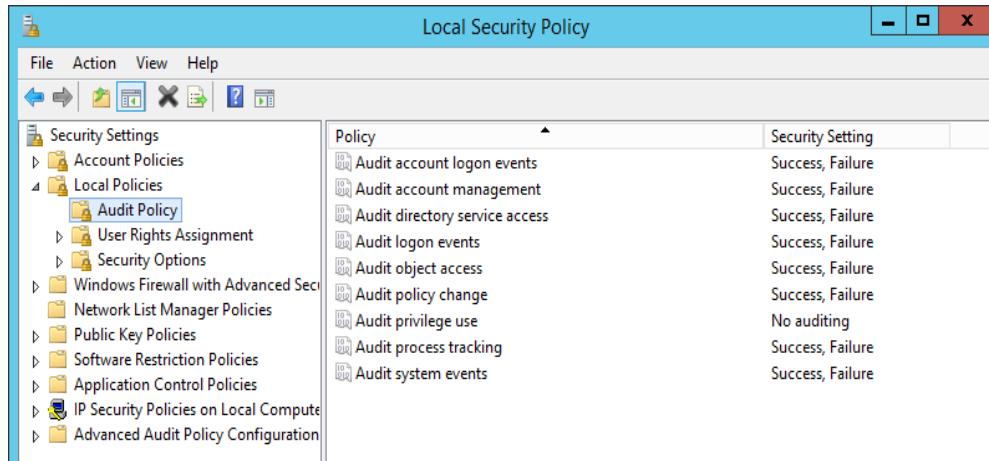


Figure 5. 408 : Server Manager

Step 2: Go to Security Setting, choose Local Policies and click on Audit Policy.



The screenshot shows the Windows Local Security Policy snap-in. The left pane displays a tree view of security settings, with 'Audit Policy' selected under 'Local Policies'. The right pane lists various audit policies with their corresponding security settings:

Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	No auditing
Audit process tracking	Success, Failure
Audit system events	Success, Failure

Figure 5. 409 : Local Security Policy

Step 3: In Windows Server 2012, Audit Policy default setting had already chosen for success and failure for each policy but for each policy but only Audit privilege are not. Double click on Audit privilege then select Success and Failure.

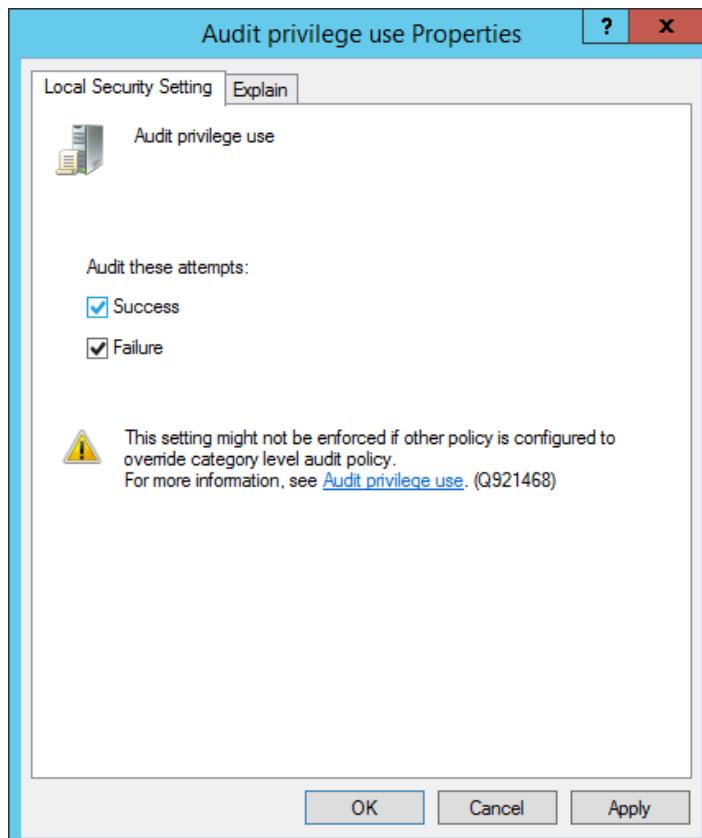


Figure 5. 410 : Audit Privilege use Properties

Updates and Patches.

Step 1: Search for Windows Update.

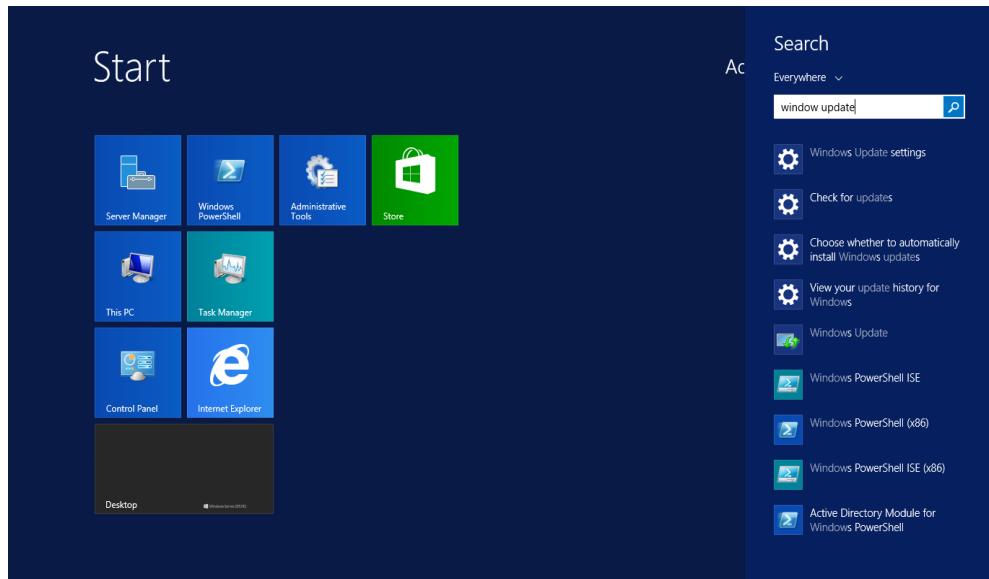


Figure 5. 411 : Search Windows Update

Step 2: Change settings to Install updates automatically and click OK.

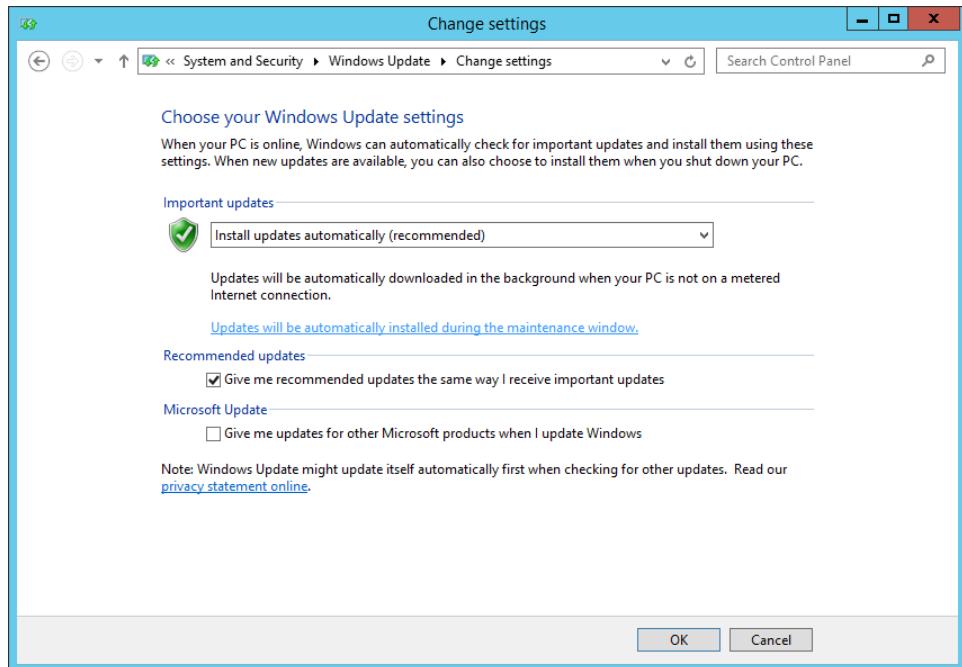


Figure 5. 412 : Windows Update Settings

Enable Windows Firewall

Step 1: Open Server Manager and click Windows Firewall with Advanced Security.

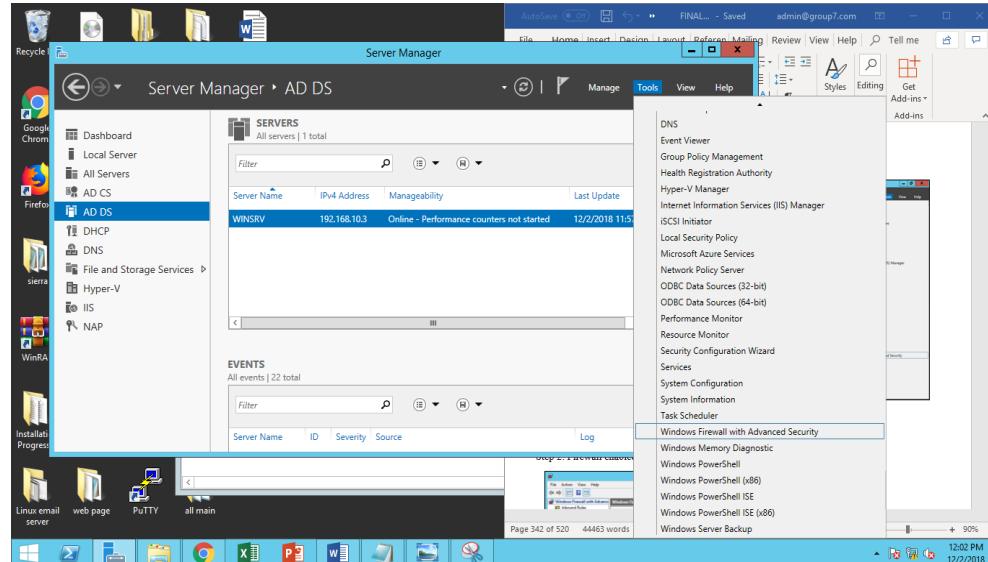


Figure 5.413 : Server Manager

Step 2: Check whether Firewall is enabled or not.

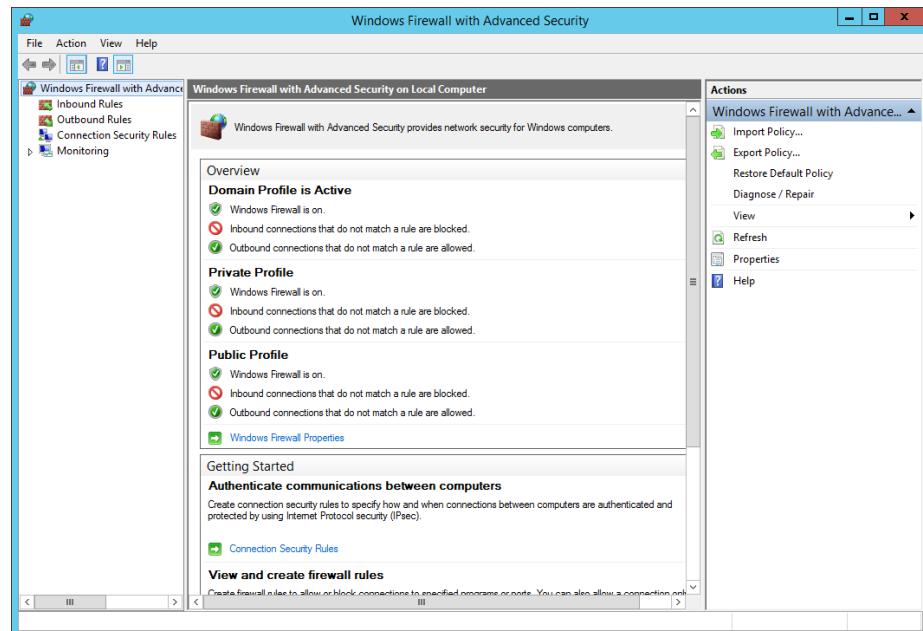


Figure 5.414 : Windows Firewall with Advanced Security.

Disable Automatic Services.

Step 1: Open Run dialog box and type in services.msc to open Services.

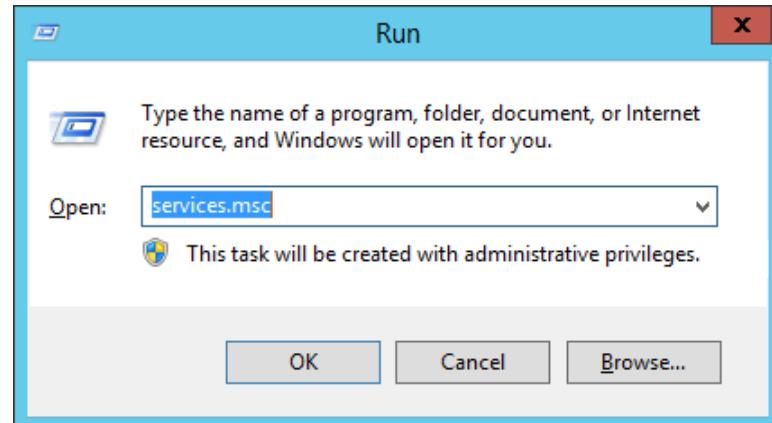


Figure 5. 415 : Run dialog Box

Step 2: Change the startup type of Distributed Transaction Coordinator Properties from Automatic to Disabled.

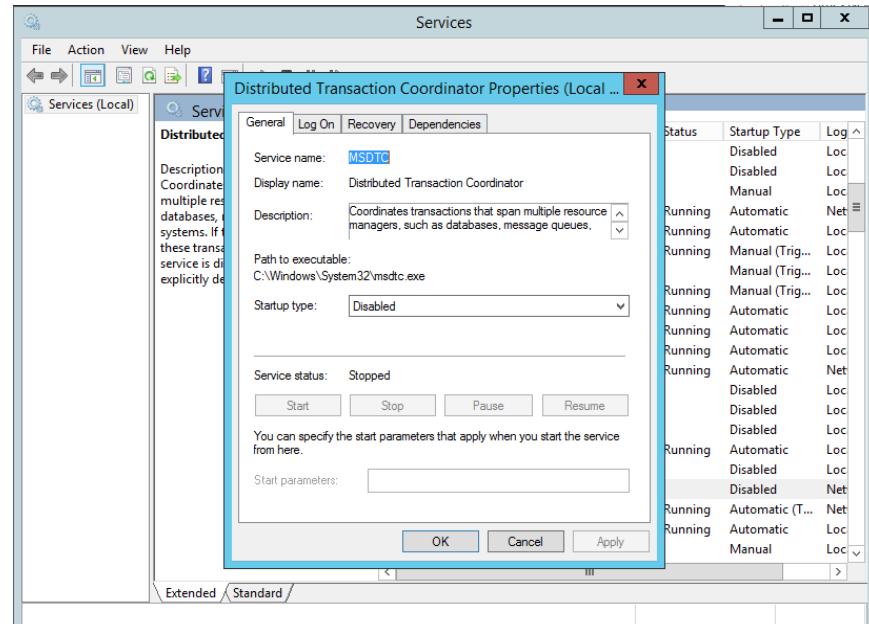
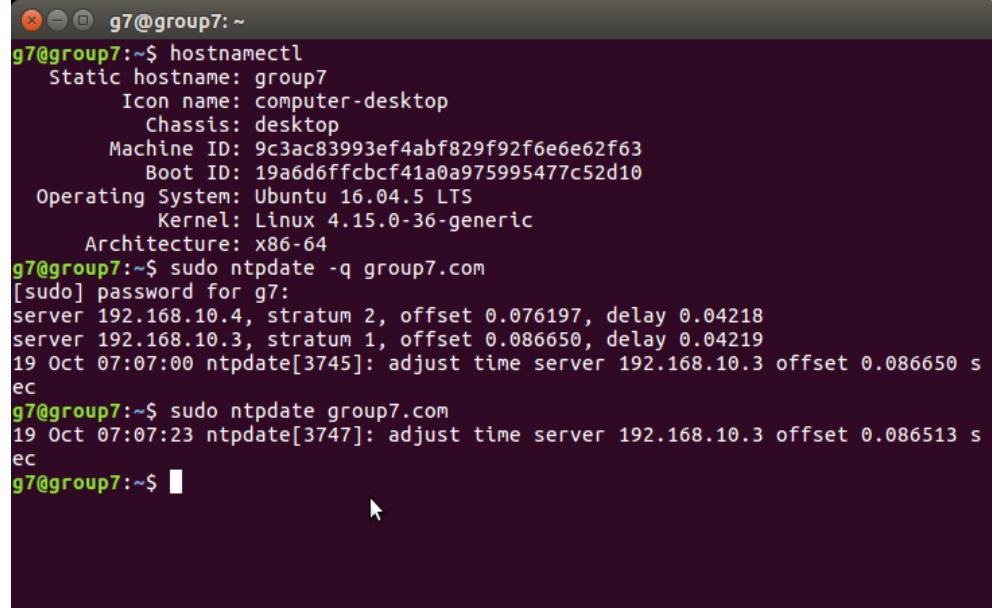


Figure 5. 416 : Disable Distributed Transaction Coordinator Properties

Reason: Coordinates transactions that are distributed across multiple computer systems and/or resource managers, such as databases, message queues, file systems, or other transaction-protected resource managers. We are not using this service, so we just disabled it.

5.2.24 Authentication user by integrating AD with Linux

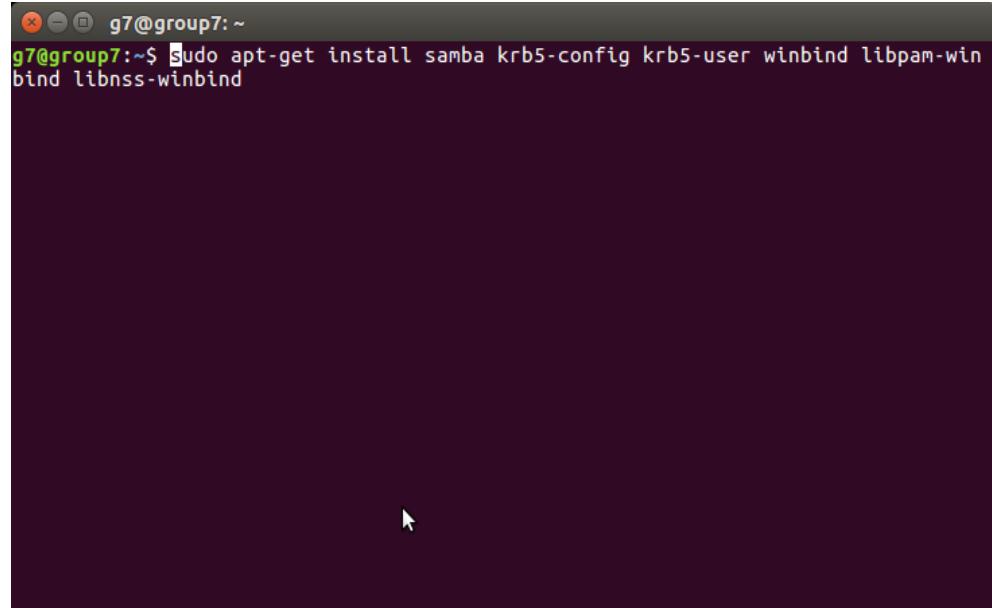
Step 1: Check hostname on Ubuntu by typing hostnamectl and adjust its time with Windows Server 2012 server time.



```
g7@group7:~$ hostnamectl
Static hostname: group7
  Icon name: computer-desktop
  Chassis: desktop
Machine ID: 9c3ac83993ef4abf829f92f6e6e62f63
  Boot ID: 19a6d6ffcbcfc41a0a975995477c52d10
Operating System: Ubuntu 16.04.5 LTS
  Kernel: Linux 4.15.0-36-generic
Architecture: x86-64
g7@group7:~$ sudo ntpdate -q group7.com
[sudo] password for g7:
server 192.168.10.4, stratum 2, offset 0.076197, delay 0.04218
server 192.168.10.3, stratum 1, offset 0.086650, delay 0.04219
19 Oct 07:07:00 ntpdate[3745]: adjust time server 192.168.10.3 offset 0.086650 sec
g7@group7:~$ sudo ntpdate group7.com
19 Oct 07:07:23 ntpdate[3747]: adjust time server 192.168.10.3 offset 0.086513 sec
g7@group7:~$
```

Figure 5. 417 : Check computer's hostname

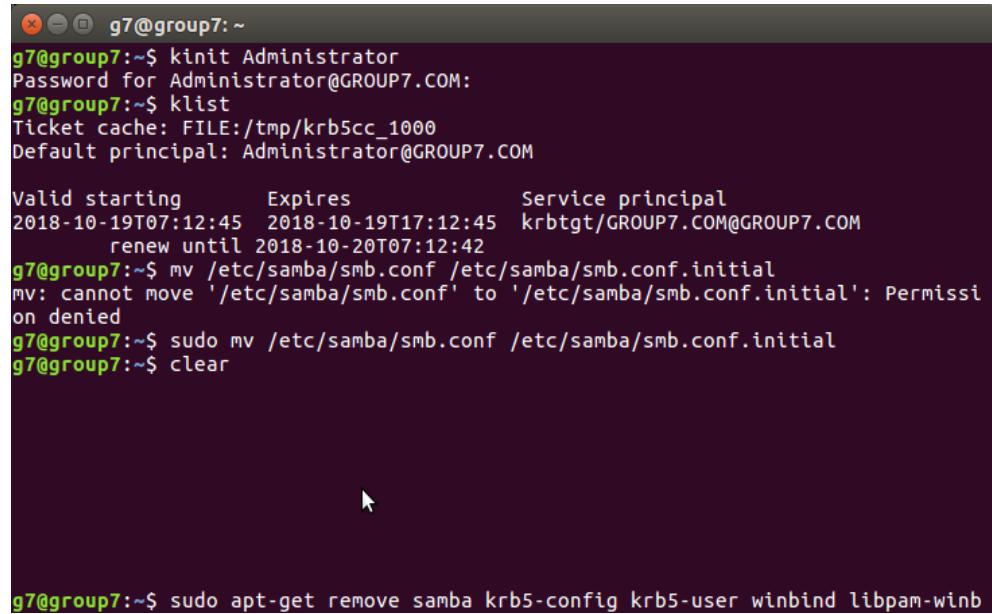
Step 2: Install required packages by issuing command below.



```
g7@group7:~$ sudo apt-get install samba krb5-config krb5-user winbind libpam-winbind libnss-winbind
```

Figure 5. 418 : Install required libraries and packages

Step 3: Issue command `kinit` as Administrator which the Administrator is the admin from Windows Server Active Directory. Next, issue command ‘`klist`’ to make sure that we had entered the domain. Rename the original Samba configuration file to avoid any mistake or error while we configure Samba with WinBind.



```

g7@group7:~$ kinit Administrator
Password for Administrator@GROUP7.COM:
g7@group7:~$ klist
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: Administrator@GROUP7.COM

Valid starting     Expires            Service principal
2018-10-19T07:12:45  2018-10-19T17:12:45  krbtgt/GROUP7.COM@GROUP7.COM
                  renew until 2018-10-20T07:12:42
g7@group7:~$ mv /etc/samba/smb.conf /etc/samba/smb.conf.initial
mv: cannot move '/etc/samba/smb.conf' to '/etc/samba/smb.conf.initial': Permission denied
g7@group7:~$ sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.initial
g7@group7:~$ clear

g7@group7:~$ sudo apt-get remove samba krb5-config krb5-user winbind libpam-winb

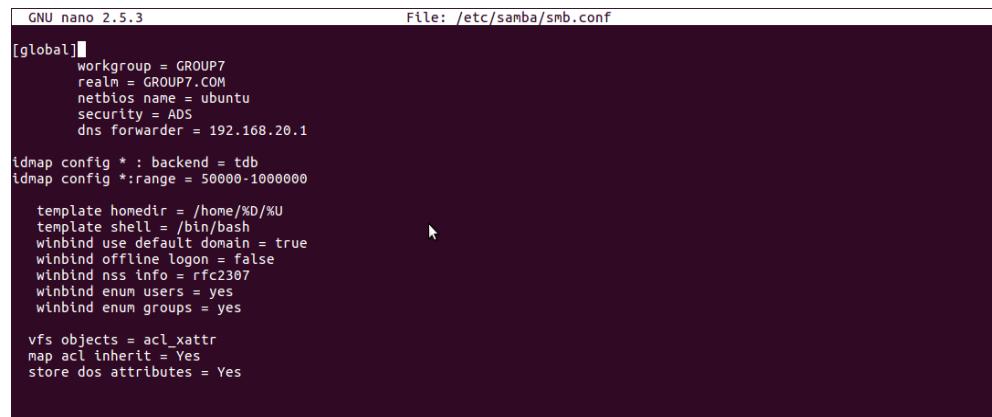
```

Figure 5. 419: *kinit and klist command*

Step 4: We need to create a new Samba configuration file by typing

`sudo nano /etc/samba/smb.conf`

Step 5: Create a new Samba configuration file that contain following



```

GNU nano 2.5.3                                     File: /etc/samba/smb.conf
[global]
workgroup = GROUP7
realm = GROUP7.COM
netbios name = ubuntu
security = ADS
dns forwarder = 192.168.20.1

idmap config * : backend = tdb
idmap config *:range = 50000-1000000

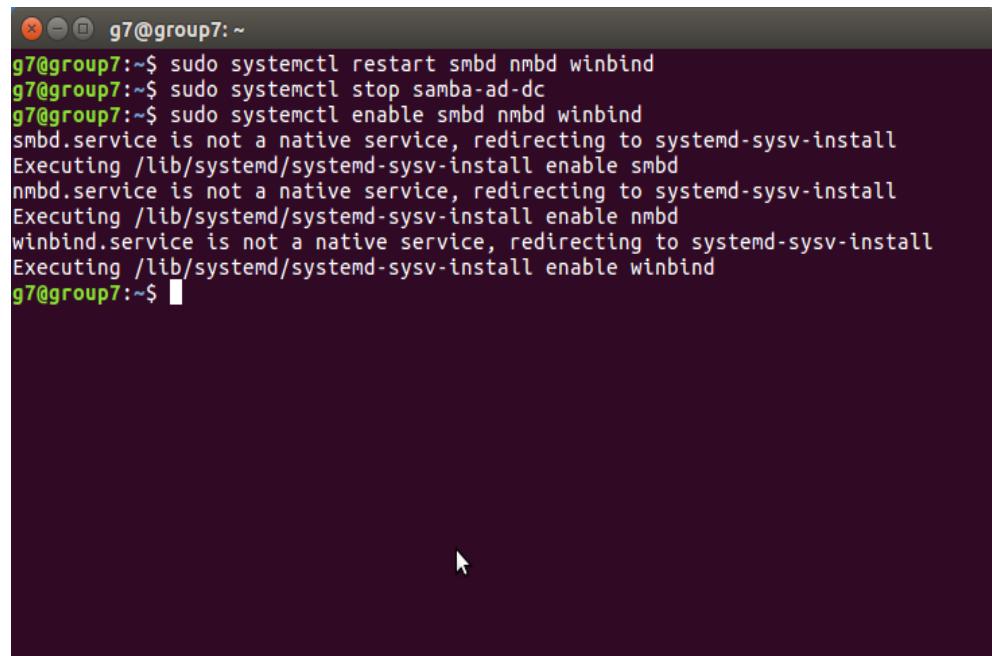
template homedir = /home/%D/%U
template shell = /bin/bash
winbind use default domain = true
winbind offline logon = false
winbind nss info = rfc2307
winbind enum users = yes
winbind enum groups = yes

vfs objects = acl_xattr
map acl inherit = Yes
store dos attributes = Yes

```

Figure 5. 420 : *Samba Configuration*

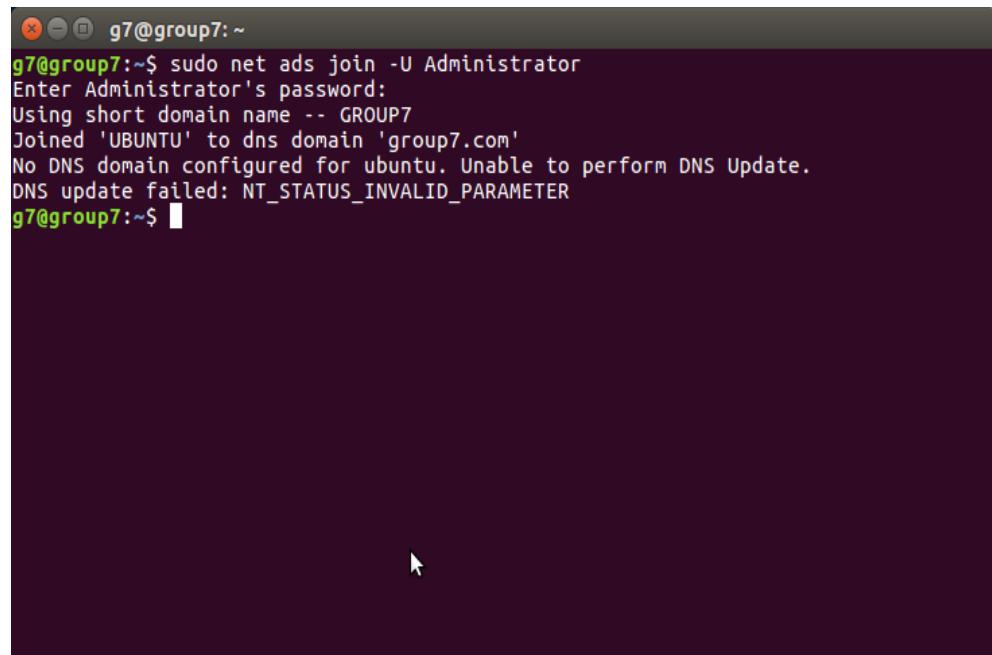
Step 6: Restart Samba and Winbind services.



```
g7@group7:~$ sudo systemctl restart smbd nmbd winbind
g7@group7:~$ sudo systemctl stop samba-ad-dc
g7@group7:~$ sudo systemctl enable smbd nmbd winbind
smbd.service is not a native service, redirecting to systemd-sysv-install
Executing /lib/systemd/systemd-sysv-install enable smbd
nmbd.service is not a native service, redirecting to systemd-sysv-install
Executing /lib/systemd/systemd-sysv-install enable nmbd
winbind.service is not a native service, redirecting to systemd-sysv-install
Executing /lib/systemd/systemd-sysv-install enable winbind
g7@group7:~$
```

Figure 5. 421 : Restart SMBD, NMBD and WinBind Service

Step 7: Join the Active Directory as Administrator and enter Administrator password. Ignore the error output on the last line.



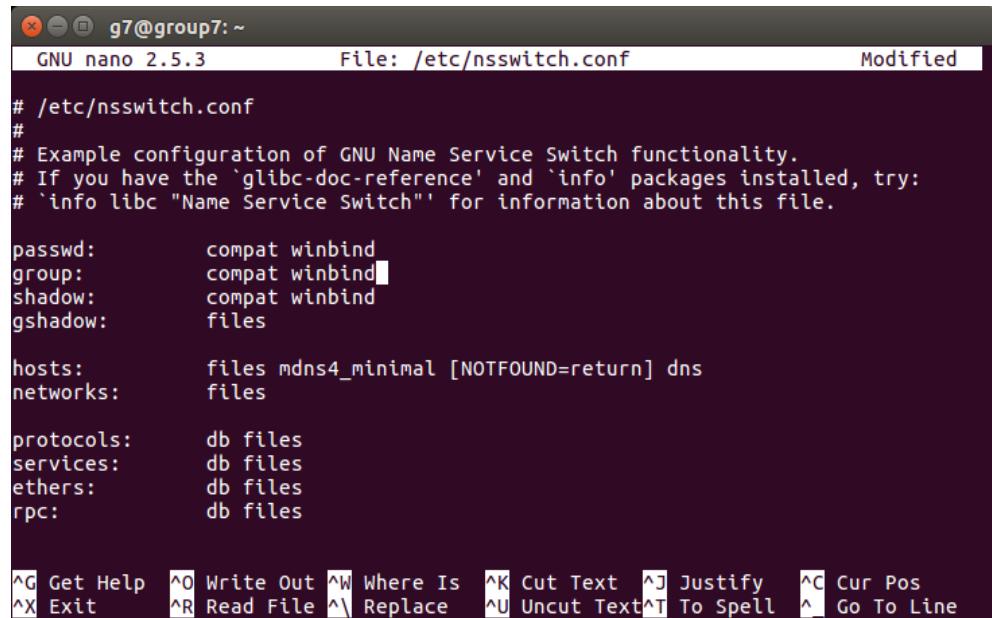
```
g7@group7:~$ sudo net ads join -U Administrator
Enter Administrator's password:
Using short domain name -- GROUP7
Joined 'UBUNTU' to dns domain 'group7.com'
No DNS domain configured for ubuntu. Unable to perform DNS Update.
DNS update failed: NT_STATUS_INVALID_PARAMETER
g7@group7:~$
```

Figure 5. 422 : Join Group7 Domain

Step 8: Edit the nsswitch.conf by typing

```
sudo nano /etc/nsswitch.conf
```

Step 9: Modify *nsswitch.conf* and add *winbind* after *compat* in the first three lines.



```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the 'glibc-doc-reference' and 'info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

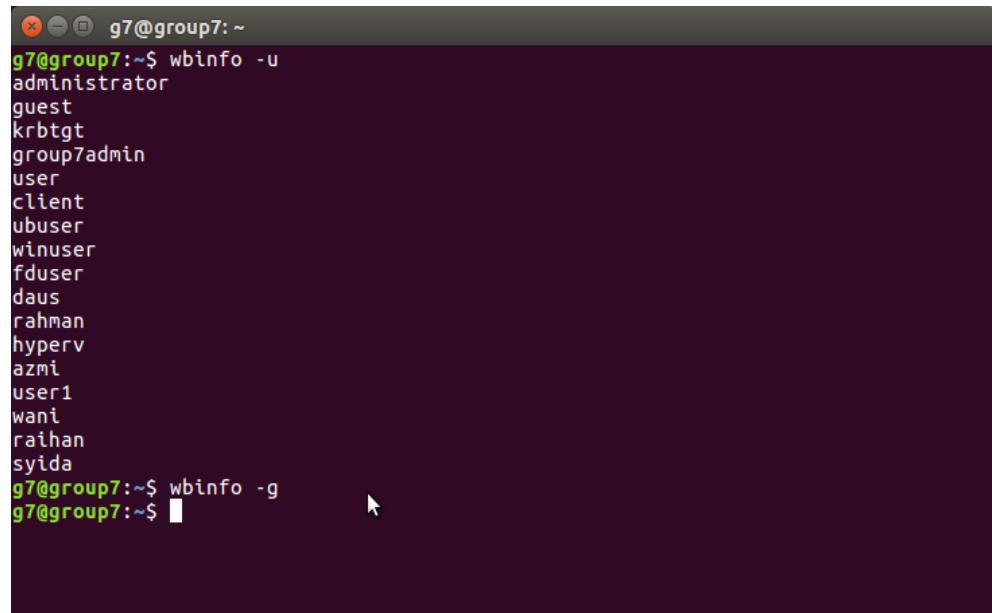
passwd:      compat winbind
group:       compat winbind
shadow:      compat winbind
gshadow:     files

hosts:        files mdns4_minimal [NOTFOUND=return] dns
networks:    files

protocols:   db files
services:    db files
ethers:      db files
rpc:         db files
```

Figure 5. 423 : NSSwitch Configuration

Step 10: Check for registered users in AD.



```
g7@group7:~$ wbinfo -u
administrator
guest
krbtgt
group7admin
user
client
ubuser
winuser
fduser
daus
rahman
hyperv
azmi
user1
wani
raihan
syida
g7@group7:~$ wbinfo -g
g7@group7:~$
```

Figure 5. 424 : AD Users

Step 11: Update the PAM authentication module by issuing *sudo pam-auth-update* and click the third option.

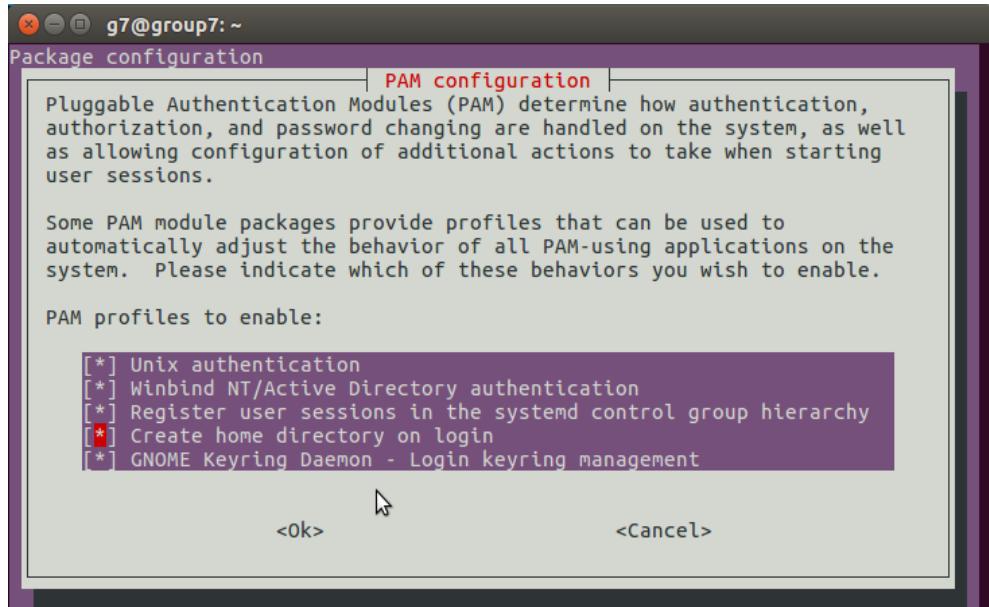


Figure 5. 425 : PAM Configuration

Step 12: Get entry username and password for Active Directory in Windows Server 2012.

A screenshot of a terminal window titled "g7@group7: ~". The window displays command-line output from several "sudo getent" commands. The first command, "sudo getent passwd | grep 'domain users'", shows the entry for the "domain users" group. The second command, "sudo getent group | grep 'domain users'", shows the same group entry again. The third command, "sudo getent group | grep daus", shows the entry for the "daus" user. The terminal prompt "g7@group7:~\$" is visible at the end of the output.

Figure 5. 426 : Get AD User's Password

5.2.25 Wireless user authentication using Radius server

Step 1: Create group **group7** and user in group7.com

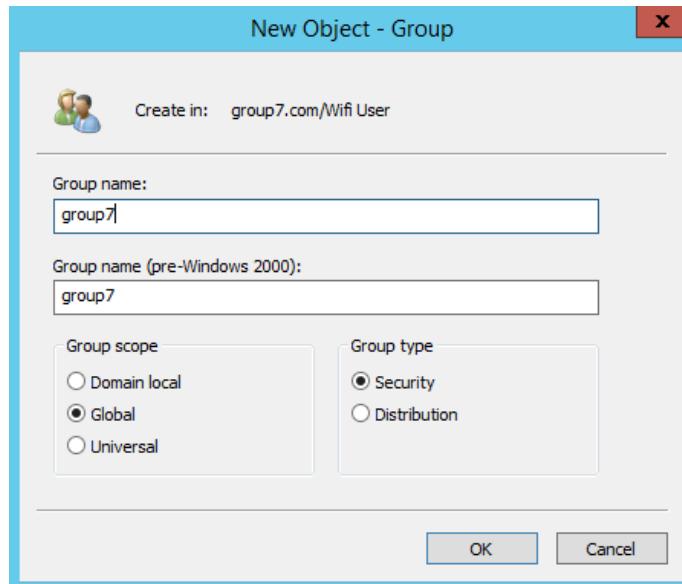


Figure 5. 427 : Create **group7** in group7.com

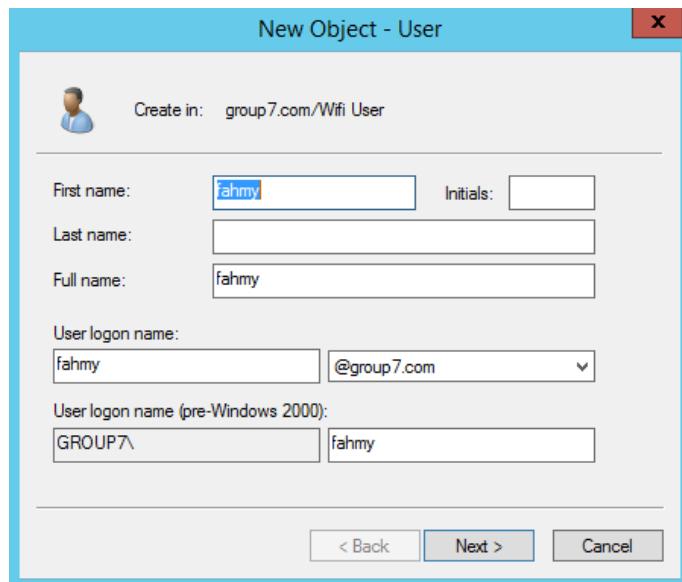


Figure 5. 428: Create user **fahmy** in group7.com

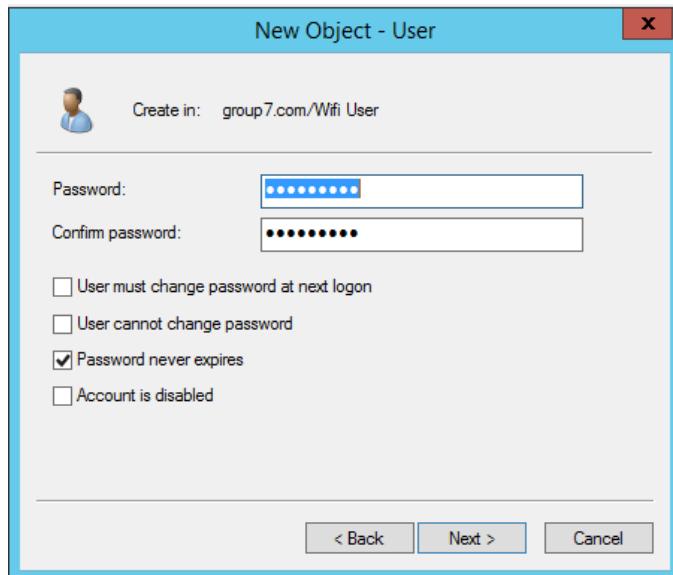


Figure 5. 429 : Assign password for the user

Name	Type	Description
fahmy	User	
group7	Security Group...	
yugen	User	

Figure 5. 430 : List of users that has been created

Step 2: Click on *Add Roles and Feature Wizard* for installation and click next.

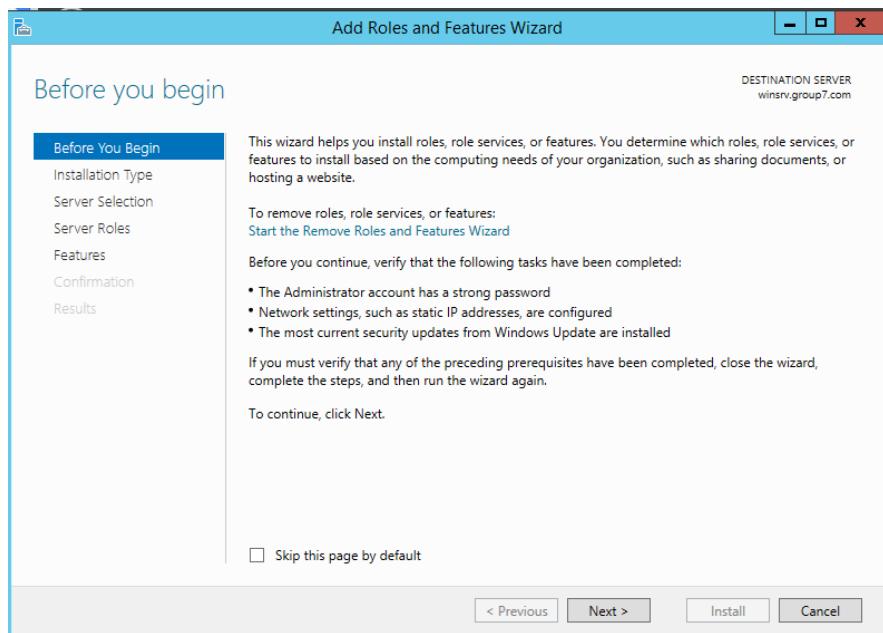


Figure 5. 431 : The confirmation before installation

Step 3: Click on ***Role-based or feature-based installation*** and click next.

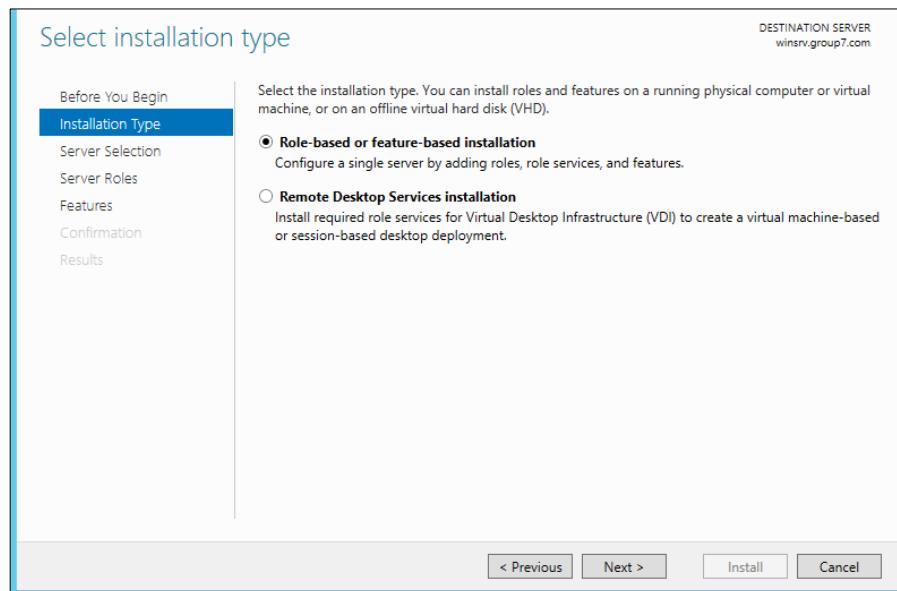


Figure 5. 432 : Select installation type

Step 4: Click on ***select a server from the server pool*** and click next.

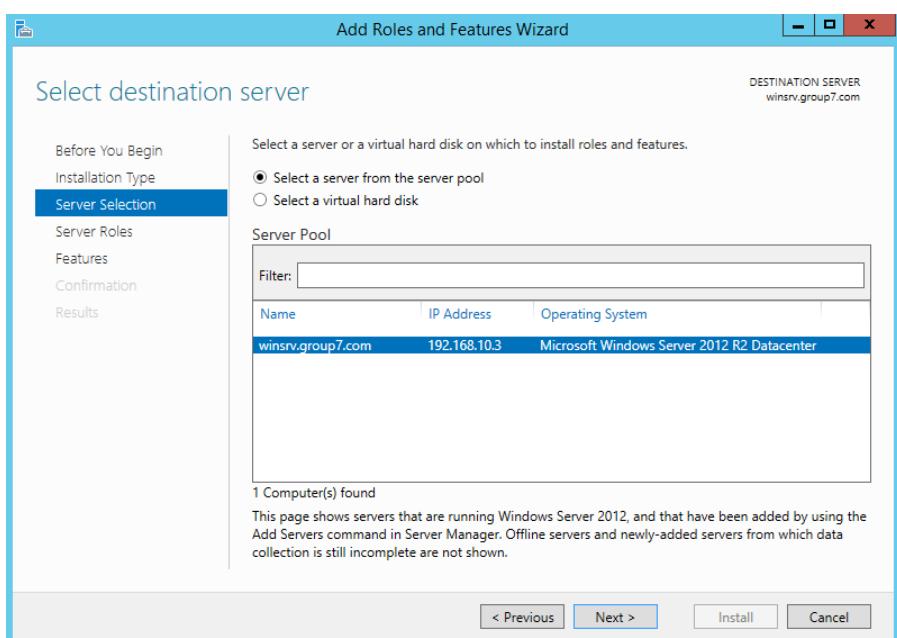


Figure 5. 433 : Server selection

Step 5: Select *Active Directory Certificate Services* and click Next

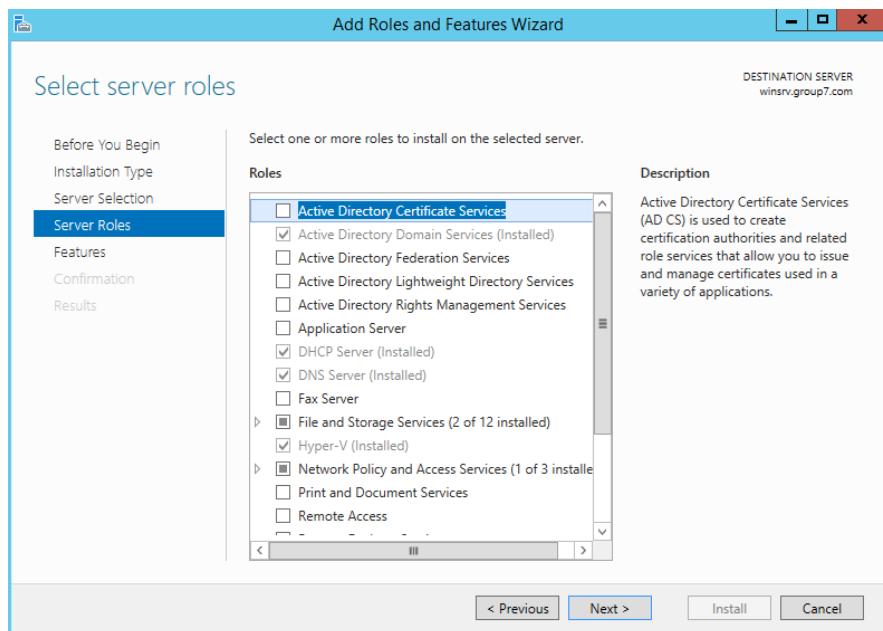


Figure 5. 434 : Selecting Server Roles for installing AD CS

Step 6: Select add features and choose *.Net Framework 3.5 Features* and click next.

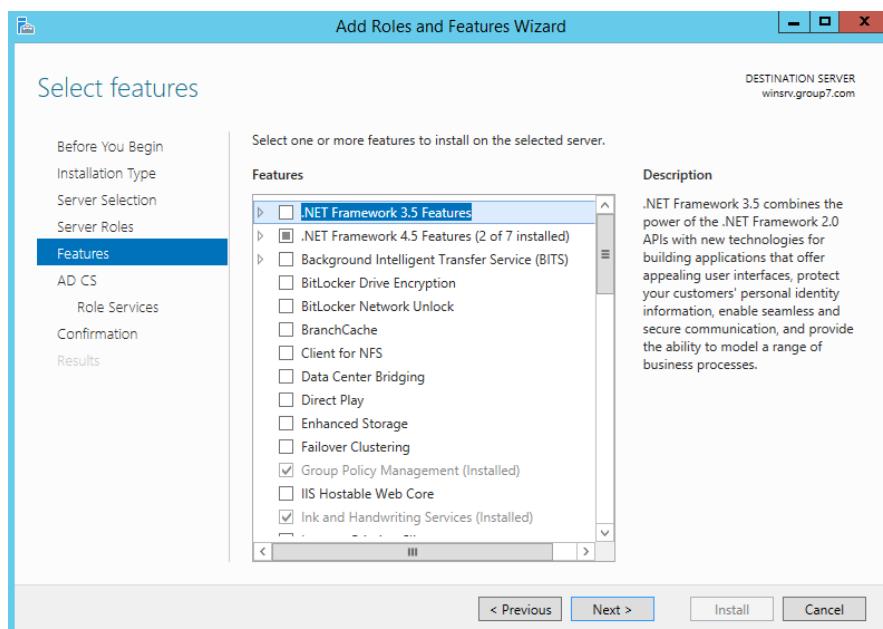


Figure 5. 435 : Select feature for installation

Step 7: Tick Certification Authority and click Next

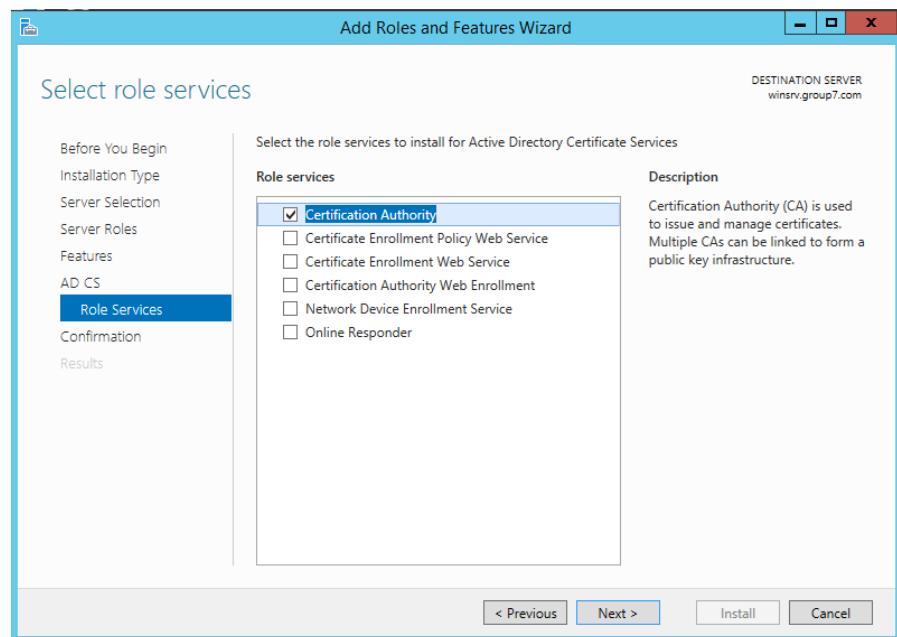


Figure 5. 436 : Selecting Role Services for Certification Authority

Step 8: Check whether the choice to install is correct or not and then click Install

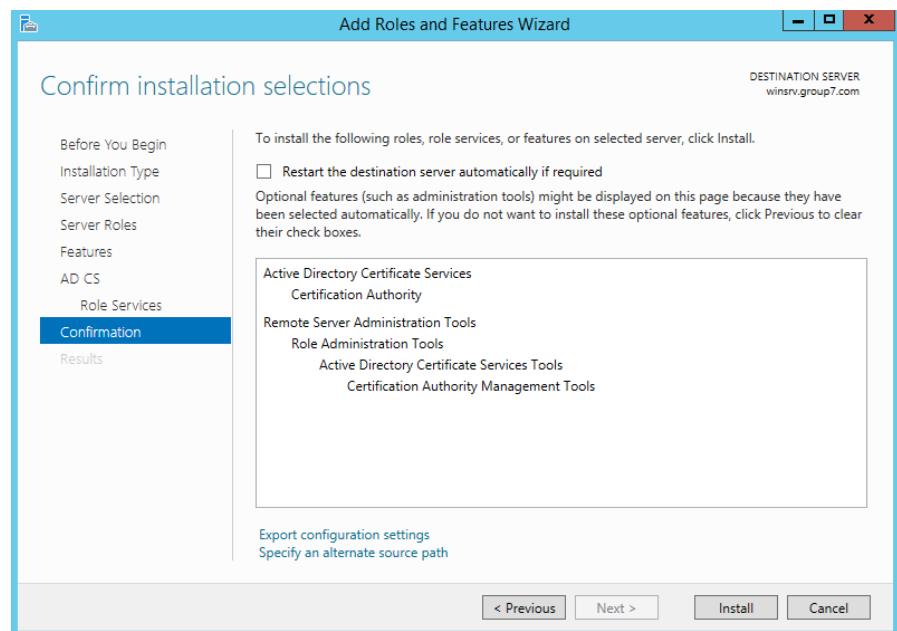


Figure 5. 437 : Confirmation for installation selection

Step 9: Open *AD CS Configuration* and click next

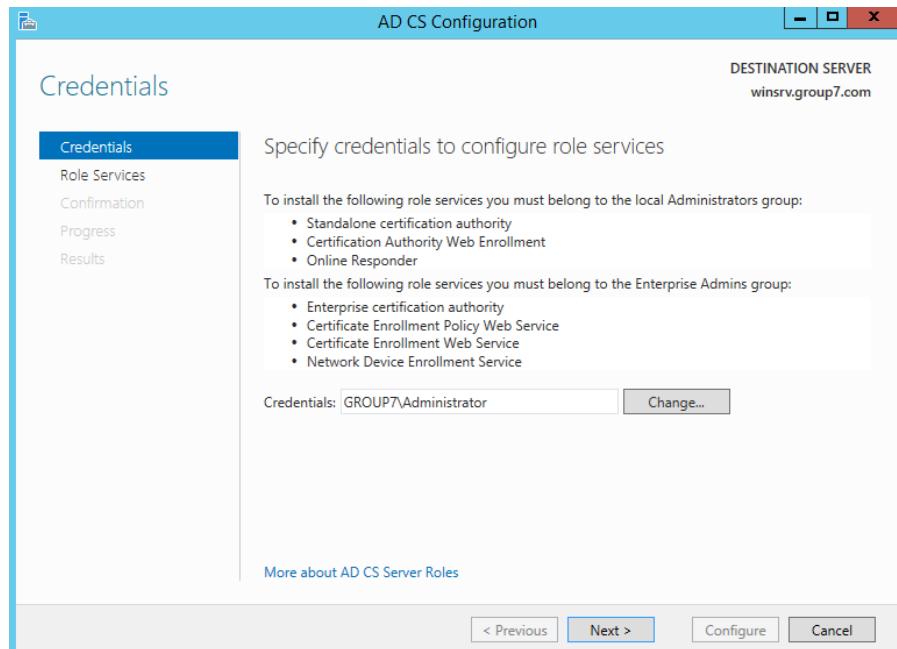


Figure 5. 438 : Specify credentials to configure role services

Step 9: Tick Certification Authority and click Next

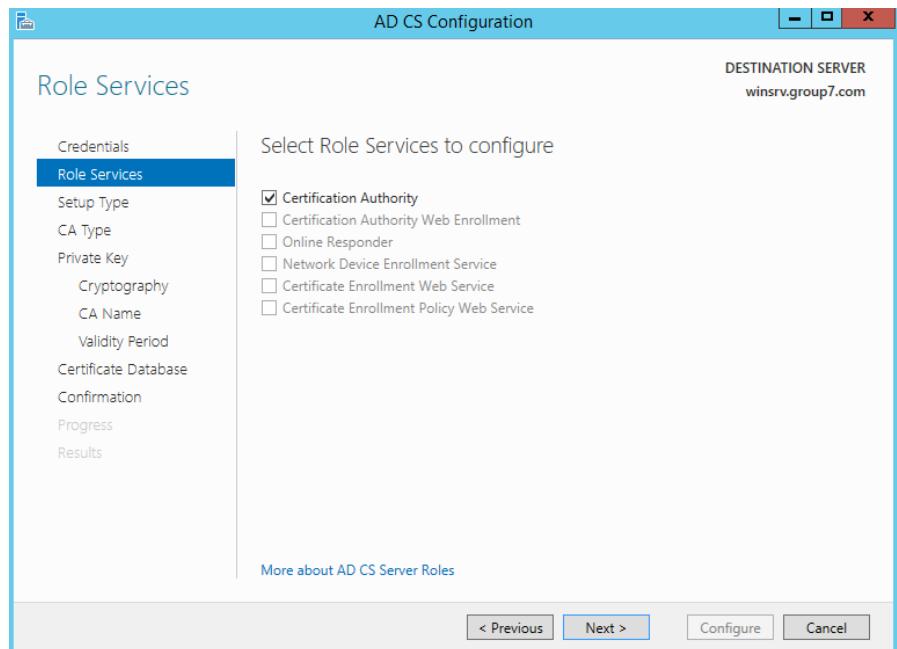


Figure 5. 439 : Selecting Role Services for Certification Authority

Step 10: Specify Setup Type: Enterprise and click Next

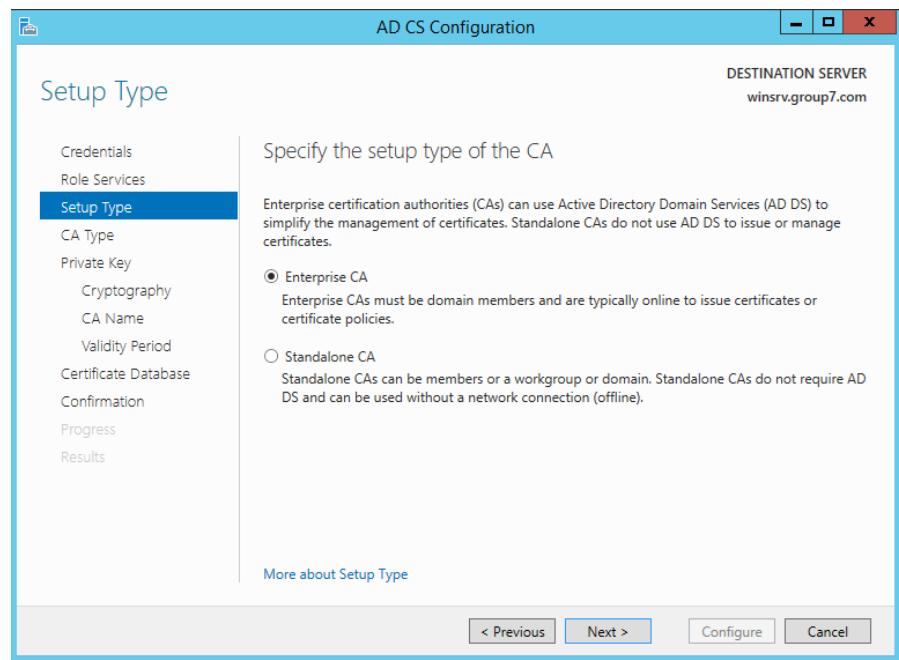


Figure 5. 440 : Selecting Specify Setup Type

Step 11: On Specify CA Type and then select **Root CA** and click Next

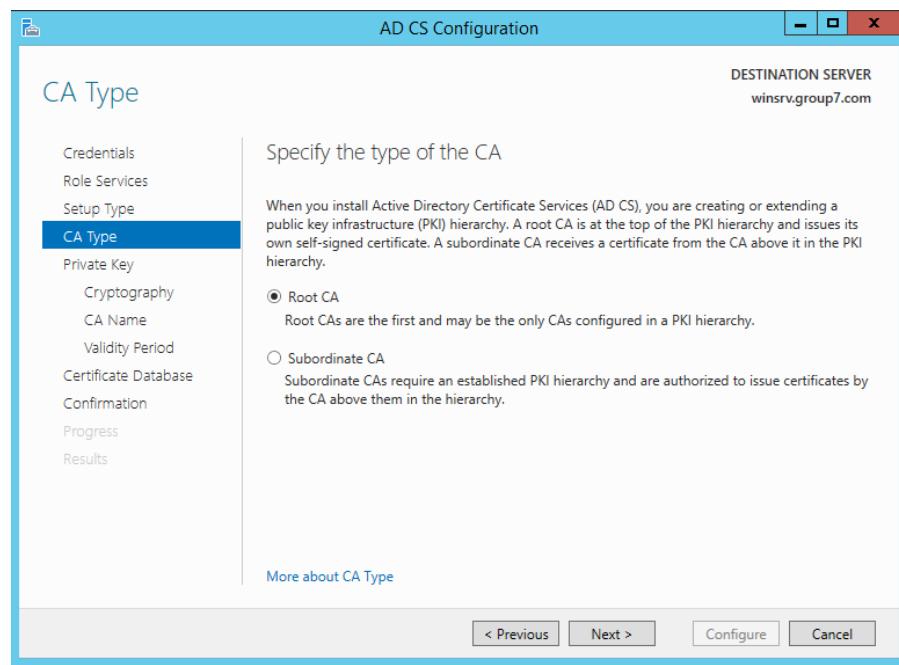


Figure 5. 441 : Selecting Specify CA Type

Step 12: On Set Up Private Key and then select *Create a new private key* and click Next

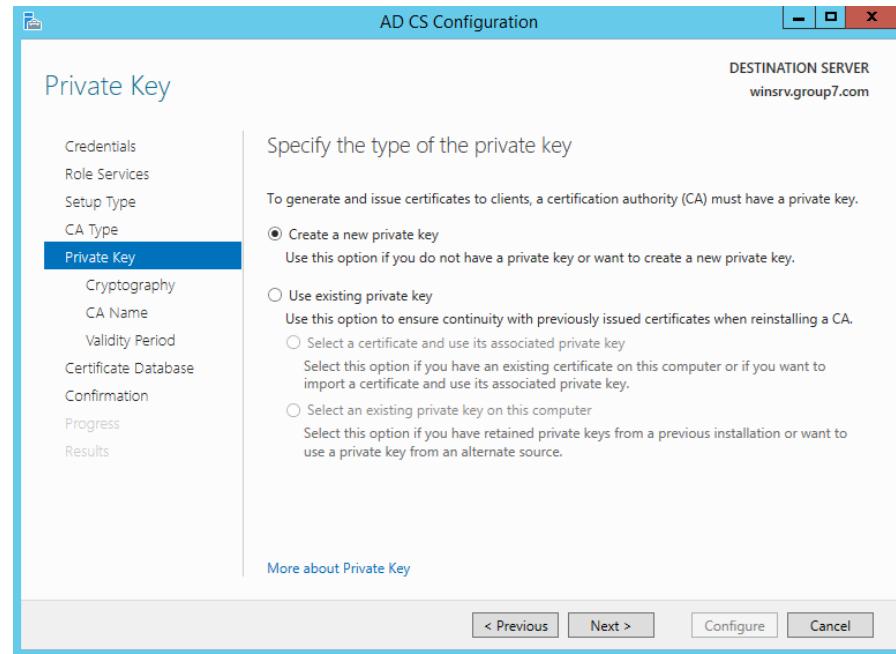


Figure 5. 442 : Setting up the Private Key

Step 13: Configure Cryptography for C A and *select SHA1* and click Next

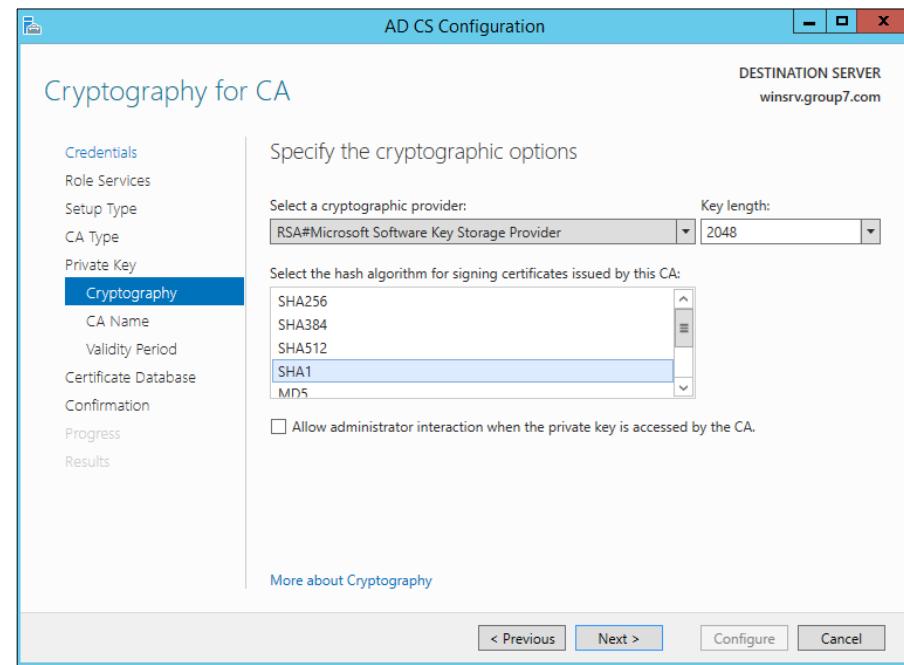


Figure 5. 443 : Configuring Cryptography for CA

Step 14: Configure CA Name and click Next

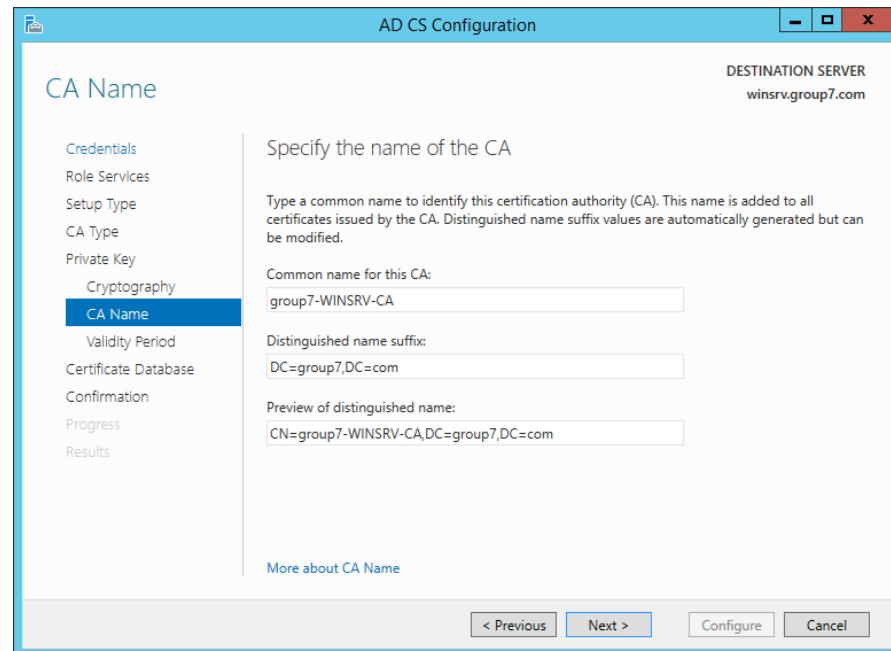


Figure 5. 444 : Configuring CA Naming

Step 15: Select validity period for the certificate generated for this CA and click Next

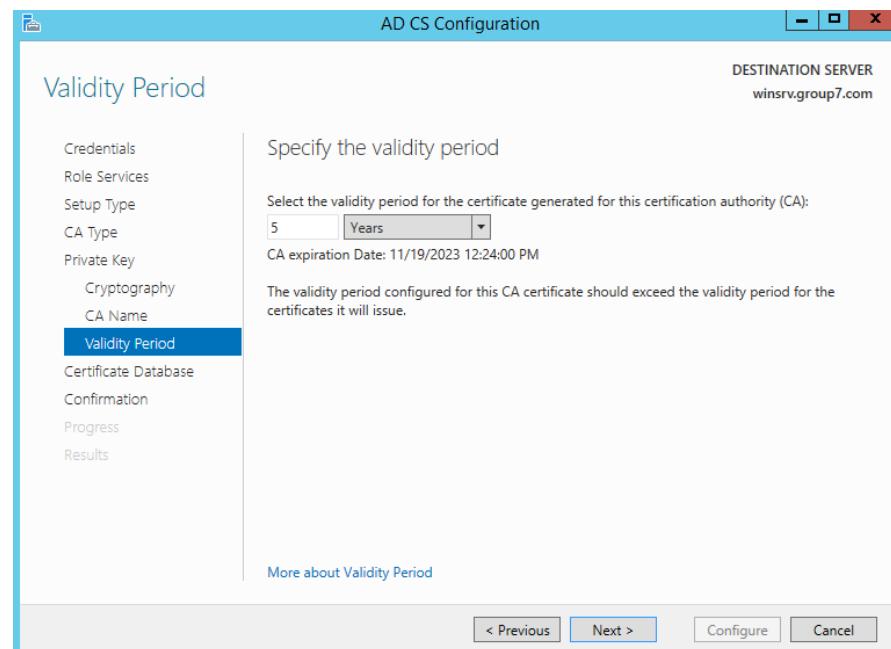


Figure 5. 445 : Setting the validity Period

Step 16: Configure Certificate Database and click Next.

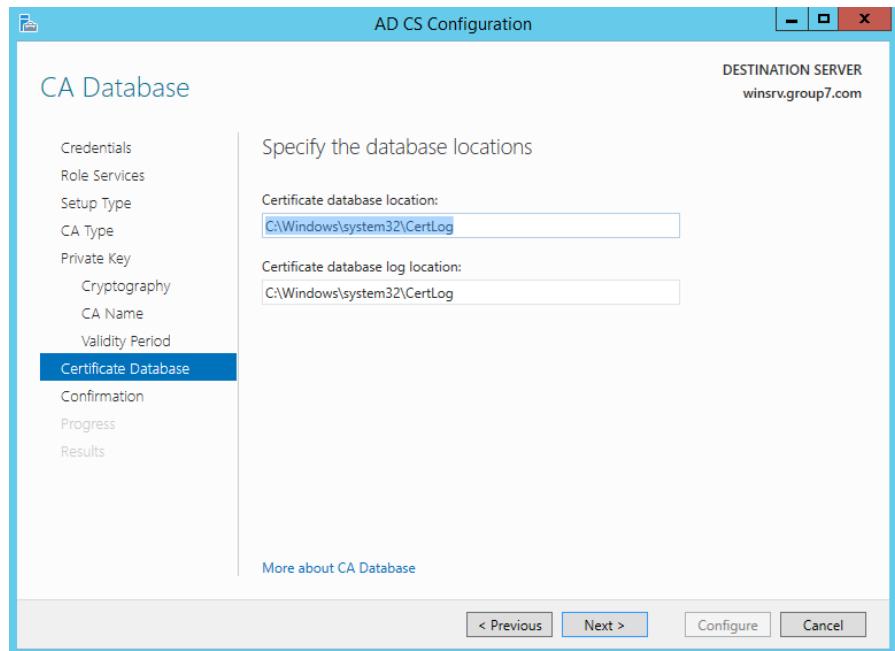


Figure 5. 446 : Configuring Certificate Database

Step 17: Confirm Installation Selections and click Configure

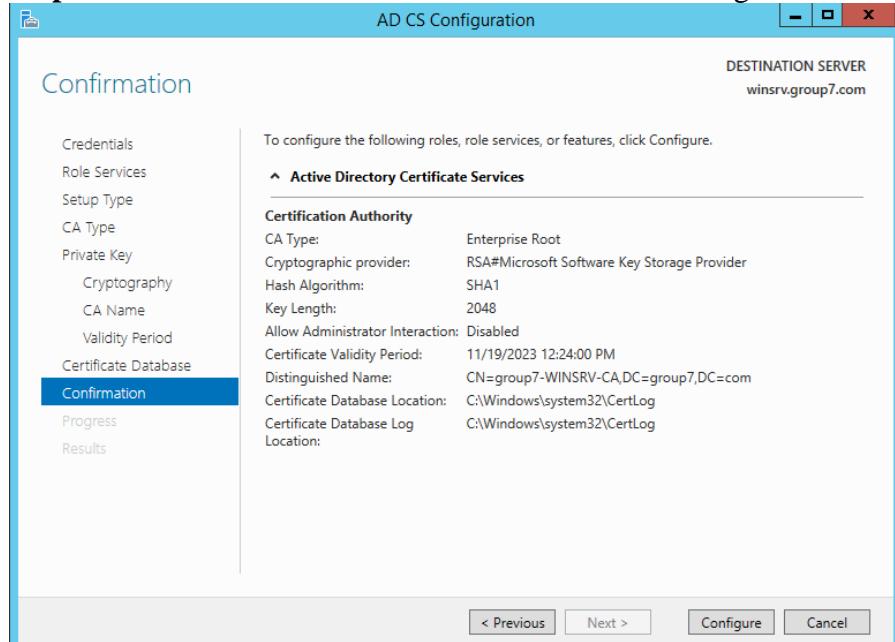


Figure 5. 447 : Confirmation the Installation Selections

Step 18: On Certificate Enrollment and click Close

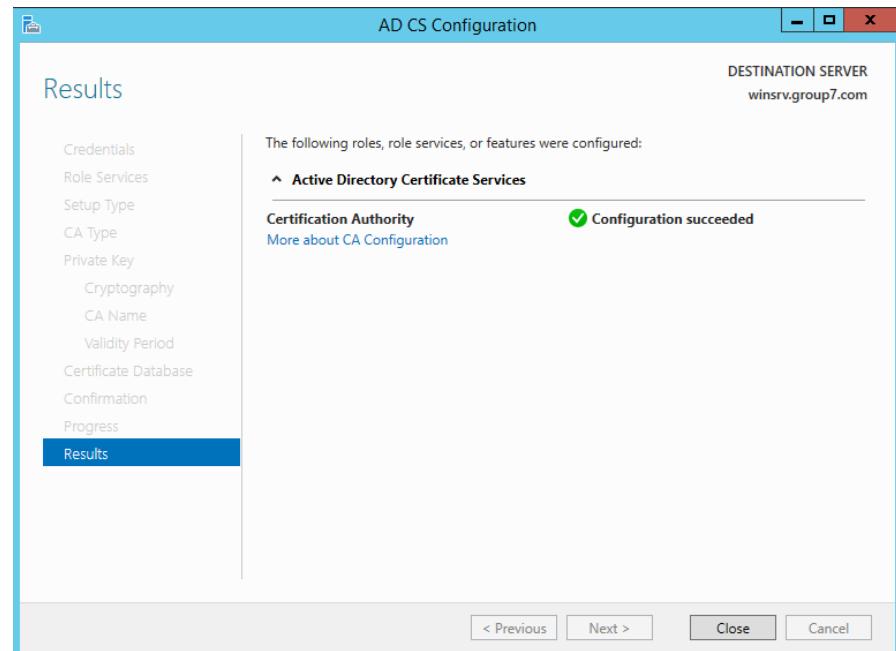


Figure 5. 448 : Showing Certificate Installation Results

Step 19: Open the Microsoft Management Console then Right click and *Select All Tasks and Request New Certificate*

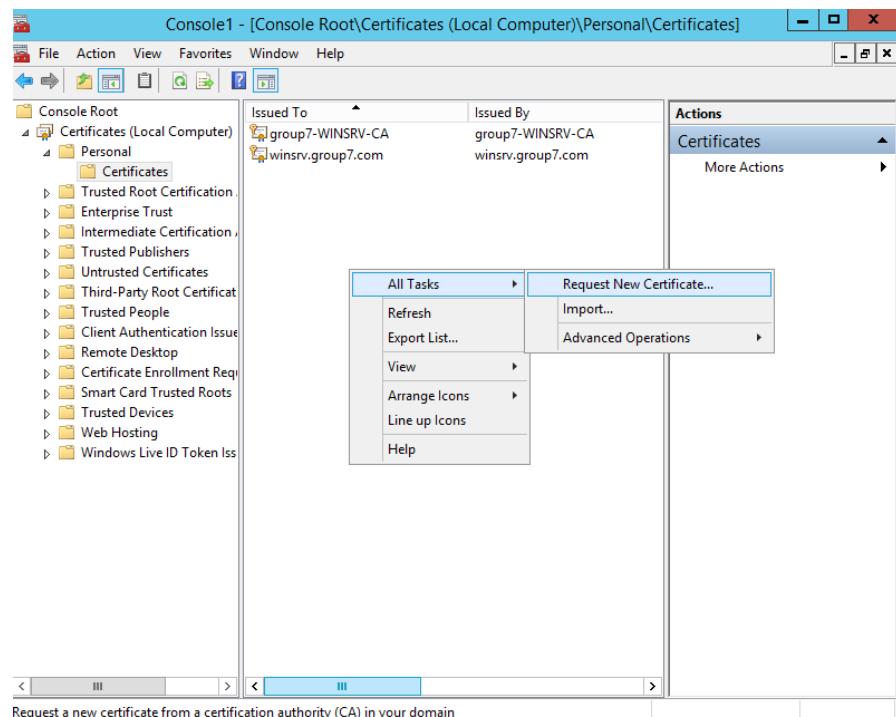


Figure 5. 449 : Showing Microsoft Management Console to add Certificate

Step 20: On Certificate Enrolment and click Next

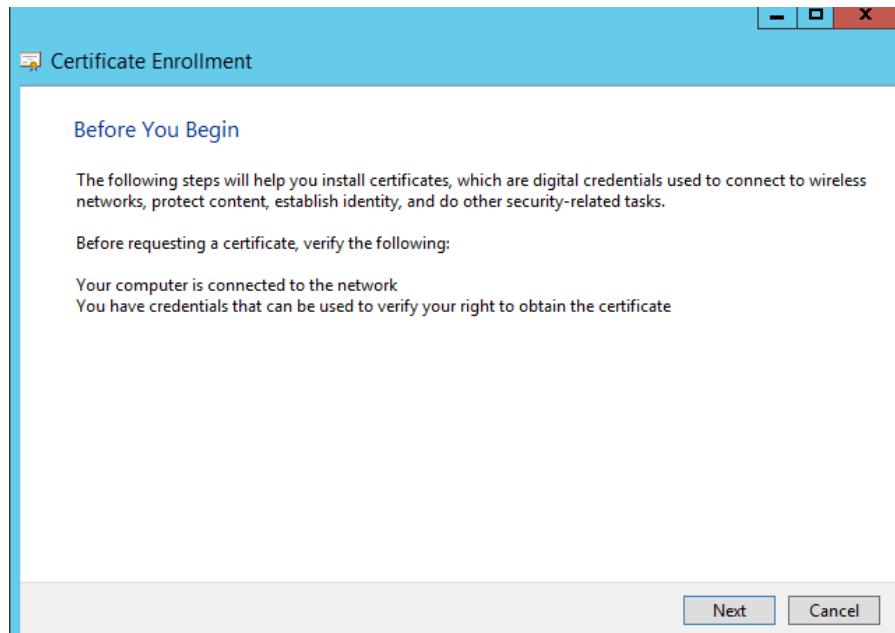


Figure 5. 450 : Starting Certificate Enrolment

Step 21: Active Directory Enrolment Policy and click Next

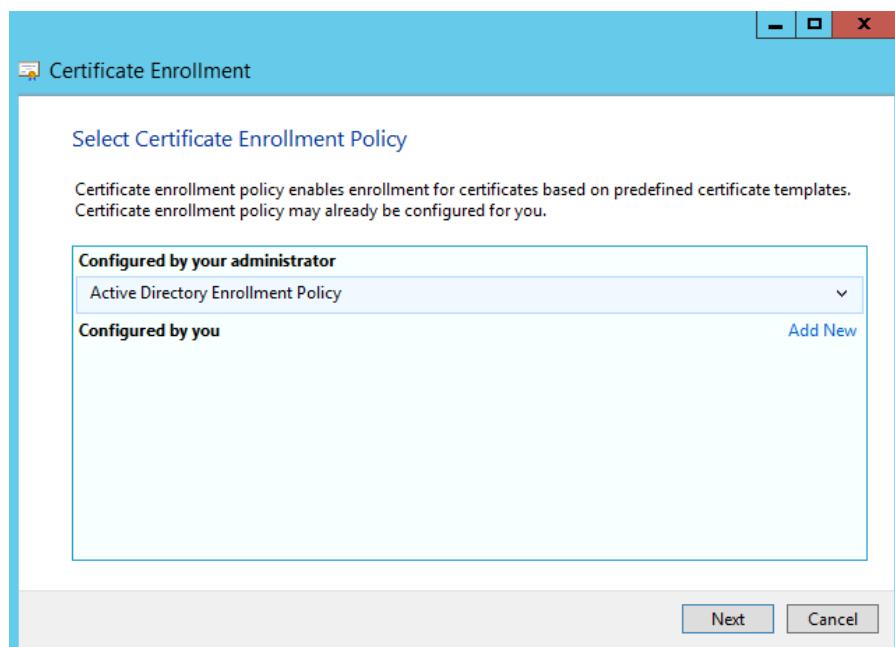


Figure 5. 451 : Selecting Certificate Enrolment Policy

Step 22: Select Domain Controller and click enrol

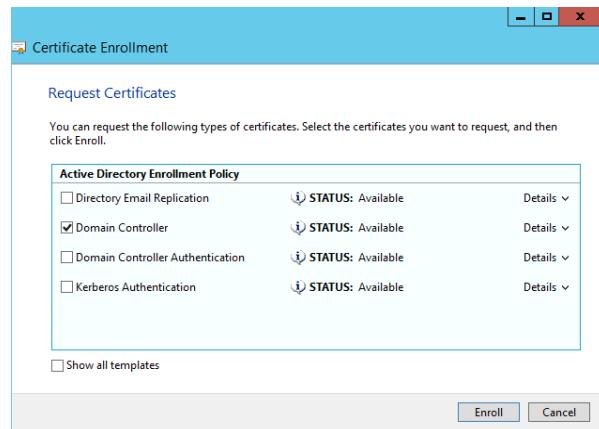


Figure 5. 452 : Showing Certificate Enrolment

Step 23: Open Network Policy Server and Select *server for 802.1X Wireless or Wired Connections*

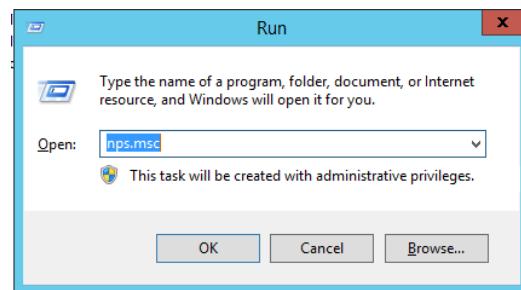


Figure 5. 453 : Command run for NPS

Step 24: Configure 802.1X and *Select Secure Wireless Connection* and click Next

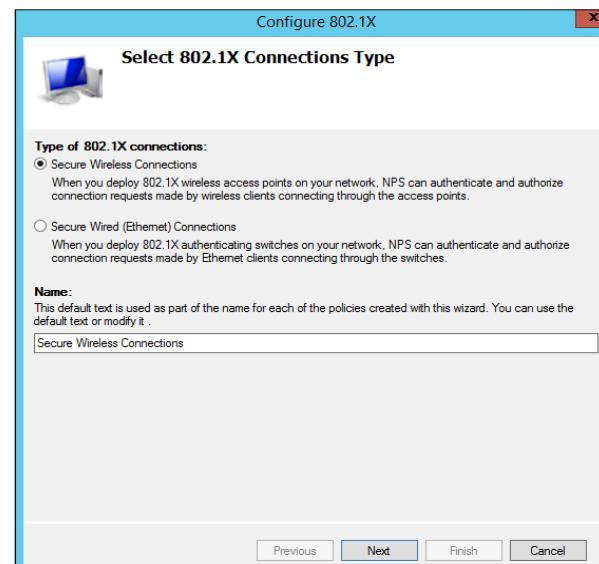


Figure 5. 454 Selecting 802.1X Connections Type

Step 25: Specify a RADIUS client and click Add “Group7” and click next



Figure 5. 455 : Selecting specify a RADeUS client

Step 26: Add New RADeUS Client and Add Friendly name, IP and shared secret and Click Ok

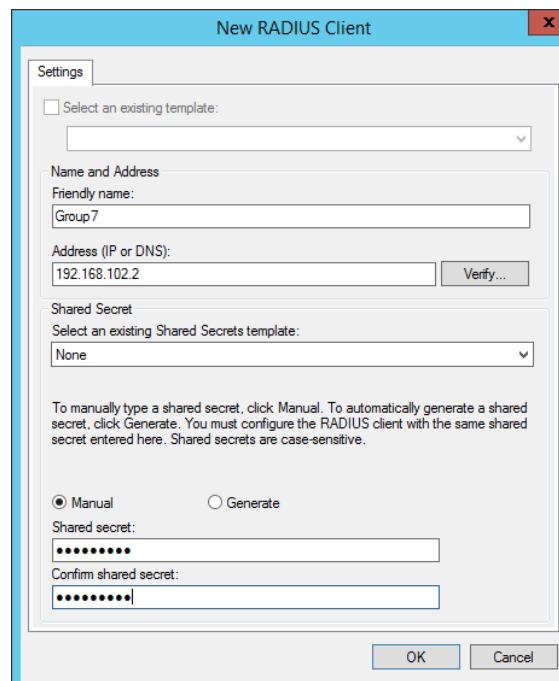


Figure 5. 456 : Adding new RADeUS Client for wireless

Step 27: Select the EAP type then choose Microsoft: Protected EAP (PEAP) and Click Next



Figure 5. 457 : Configuring an Authentication Method

Step 28: Select User Groups and Click Add “GROUP7\group7”

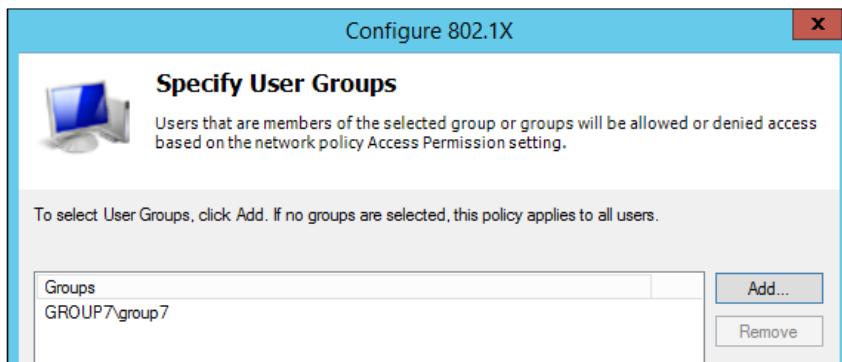


Figure 5. 458 : Specifying User Group

Step 29: On Configure Traffic Controls and Click Next

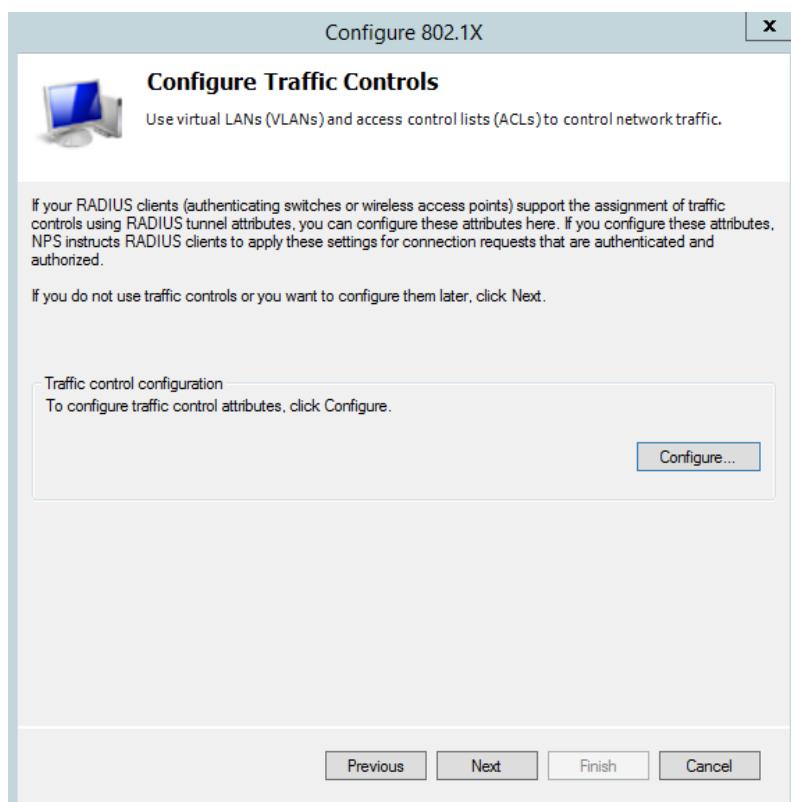


Figure 5. 459 : Showing Configure Traffic Controls

Step 30: Successfully and configured the RADIUS clients and Click Finish

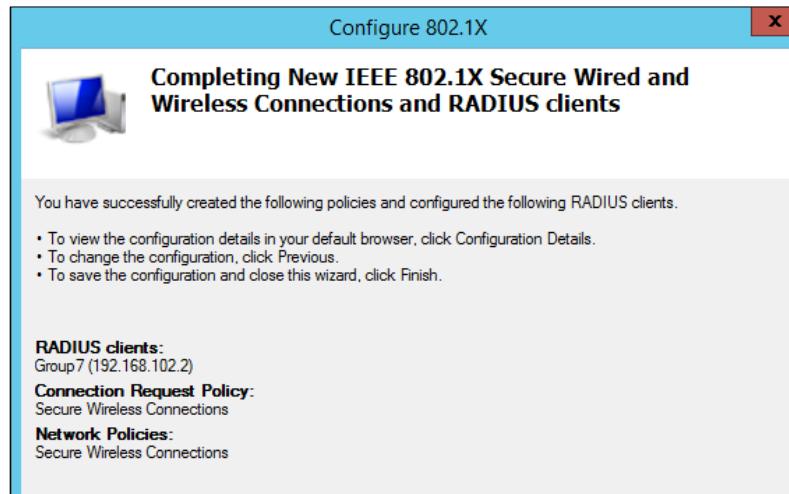


Figure 5. 460 : Successfully Completing Wireless Connections and RADIUS clients

Step 30: Select the “group7-WINSRV-CA” then right click. Choose All Task and the Export

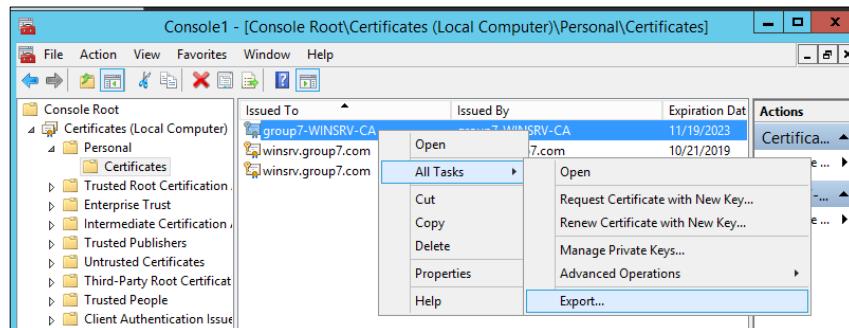


Figure 5. 461 : Showing Microsoft Management Console

Step 31: On Certificate Export Wizard and Click Next



Figure 5. 462 : Showing Certificate Export Wizard

Step 32: Fill the File name “radi_cert” and click save

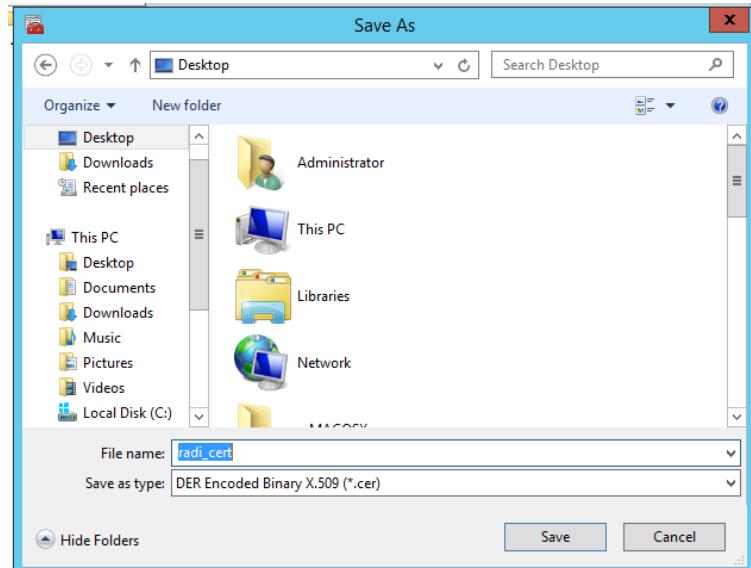


Figure 5. 463 : Specifying the name of the file

Step 32: On Desktop will show the successfully file being export



Figure 5. 464 : Showing successfully file being export

5.2.26 IDS with port mirror

A. Installation of Snort as IDS

Step 1: Install required package for Snort.

```
root@group7:/home/g7/Downloads/snort-2.9.12
root@group7:/home/g7/Downloads/snort-2.9.12# sudo apt-get install -y libnghhttp2-
dev
```

Figure 5. 465 : Required Libraries

```
root@g7:~
root@g7:~# apt-get install openssh-server ethtool build-essential libpcap-dev libpcap3-dev libdumbnet-dev bison flex zlib1g-dev liblzma-dev openssl libssl-dev
```

Figure 5. 466 : Required Packages

Step 2: Download DAQ (Data Acquisition)

```
root@g7:~# wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
--2018-10-15 22:42:24-- https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
Resolving www.snort.org (www.snort.org)... 2400:cb00:2048:1::6810:404b, 2400:cb0
0:2048:1::6810:414b, 2400:cb00:2048:1::6810:3f4b, ...
Connecting to www.snort.org (www.snort.org)|2400:cb00:2048:1::6810:404b|:443...
failed: Network is unreachable.
Connecting to www.snort.org (www.snort.org)|2400:cb00:2048:1::6810:414b|:443...
failed: Network is unreachable.
Connecting to www.snort.org (www.snort.org)|2400:cb00:2048:1::6810:3f4b|:443...
failed: Network is unreachable.
Connecting to www.snort.org (www.snort.org)|2400:cb00:2048:1::6810:424b|:443...
failed: Network is unreachable.
```

Figure 5. 467 : DAQ

Step 3: Copy downloaded file to download directory.

Step 4: Unzip daq-2.0.6.tar.gz

```
root@g7:/home/g7/Downloads
root@g7:/home/g7/Downloads# tar -zvxf daq-2.0.6.tar.gz
daq-2.0.6/
daq-2.0.6/ChangeLog
daq-2.0.6/missing
daq-2.0.6/daq.dsp
daq-2.0.6/configure
daq-2.0.6/sfbpf/
daq-2.0.6/sfbpf/sf_bpf_printer.c
daq-2.0.6/sfbpf/IP6_misc.h
daq-2.0.6/sfbpf/sf_gencode.c
daq-2.0.6/sfbpf/llc.h
daq-2.0.6/sfbpf/ppp.h
daq-2.0.6/sfbpf/grammar.y
daq-2.0.6/sfbpf/sf_nameaddr.c
daq-2.0.6/sfbpf/sf_bpf_filter.c
daq-2.0.6/sfbpf/sfbpf_dlt.h
daq-2.0.6/sfbpf/etheritype.h
daq-2.0.6/sfbpf/arcnet.h
daq-2.0.6/sfbpf/ieee80211.h
daq-2.0.6/sfbpf/sfbpf_int.h
daq-2.0.6/sfbpf/namedb.h
daq-2.0.6/sfbpf/Makefile.am
daq-2.0.6/sfbpf/runlex.sh
daq-2.0.6/sfbpf/atmuni31.h
```

Figure 5. 468 : Decompress DAQ

Step 5: Change directory to daq-2.0.6 and run. /configure, make and make install.

```
root@g7:/home/g7/Downloads# cd daq-2.0.6/
```

Figure 5. 469 : Change Directory to DAQ

```
./configure && make && make install
```

Figure 5. 470 : Install DAQ

Step 6: Download Snort from its website and decompress it.

Step 7: Change current directory to snort folder.

Step 8: Type ./configure --enable-sourcefire,&& make && make install.

```
root@g7:/home/g7/Downloads/snort-2.9.12# ./configure --enable-sourcefire && make && make install
```

Figure 5. 471 : Install Snort with Source Fire enable

```
root@g7:/home/g7/Downloads/snort-2.9.12# ldconfig
```

Figure 5. 472 : Create a systemd link

```
root@g7:/home/g7/Downloads/snort-2.9.12# ln -s /usr/local/bin/snort /usr/sbin/snort
```

Figure 5. 473 : Create a link to sbin folder

Step 9: Check whether snort is successfully installed by typing snort -v.

```
g7@g7:~$ snort -V
      _--> Snort! <--_
   o" ,'-)~ Version 2.9.12 GRE (Build 325)
    '``` By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
     ved. Copyright (C) 2014-2018 Cisco and/or its affiliates. All rights reserved.
          Copyright (C) 1998-2013 Sourcefire, Inc., et al.
          Using libpcap version 1.7.4
          Using PCRE version: 8.38 2015-11-23
          Using ZLIB version: 1.2.8
```

Figure 5. 474 : Snort Version

Step 10: Add group and user for snort.

```
g7@g7:~$ sudo groupadd snort
[sudo] password for g7:
g7@g7:~$ sudo useradd snort -r -s /sbin/nologin -c SNORT_IDS -g snort
g7@g7:~$
```

Figure 5. 475 : Add Snort Group and User

Step 11: Create directory for Snort's rule, log and dynamic rules.

```
g7@g7:~$ sudo mkdir -p /etc/snort/rules
g7@g7:~$ sudo mkdir
mkdir mkdosfs
g7@g7:~$ sudo mkdir /var/lo
local/ lock/ log/
g7@g7:~$ sudo mkdir /var/lo
local/ lock/ log/
g7@g7:~$ sudo mkdir /var/log/snort
g7@g7:~$ sudo mkdir /usr/local/lib/snort_dynamicrules
```

Figure 5. 476 : Create Snort's folder in etc

Step 12: Create white list, black list and local rules files.

```
g7@g7:~$ sudo touch /etc/snort/rules/white_list.rules
g7@g7:~$ sudo touch /etc/snort/rules/black_list.rules
g7@g7:~$ sudo touch /etc/snort/rules/local.rules
```

Figure 5. 477 : Create black list, white list and local rules

Step 13: Copy Snort's rules in folder snort-2.9.12 and Snort community rules to Snort rules directory in /etc/snort/rules.

```
g7@g7:~$ sudo cp /home/g7/Downloads/snort-2.9.12/etc/*.conf* /etc/snort
g7@g7:~$ sudo cp /home/g7/Downloads/snort-2.9.12/etc/*.map /etc/snort
```

Figure 5. 478 : Copy configuration and map to /etc/snort

```
g7@g7:~$ sudo cp /home/g7/Downloads/community-rules/community.rules /etc/snort/r
ules/
```

Figure 5. 479 : Copy community rules to rules directory

Step 14: Type sudo nano /etc/snort/snort.conf and edit Snort configuration file for

- IP address that Snort monitor
- Path of RULE_PATH, SO_RULE_PATH,
PREPROC_RULE_PATH, WHITE_LIST_PATH,
BLACK_LIST_PATH.
- Output to log file with name snort.log

Uncomment include \$RULE_PATH for both local and community rules.

```
# 3) Configure the base detection engine
# 4) Configure dynamic loaded libraries
# 5) Configure preprocessors
# 6) Configure output plugins
# 7) Customize your rule set
# 8) Customize preprocessor and decoder rule set
# 9) Customize shared object rule set
#####
#
# Step #1: Set the network variables. For more information, see README.variabl$#####
#
# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.10.3,192.168.10.4,192.168.20.3,192.168.30.3
#
# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET !$HOME_NET

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

Figure 5. 480 : Protected IP

```
# 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 rules
var SO_RULE_PATH so_rules
var PREPROC_RULE_PATH preproc_rules

# If you are using reputation preprocessor set these
# Currently there is a bug with relative paths, they are relative to where snor$#
# 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
var BLACK_LIST_PATH /etc/snort/rules

#####
#
# Step #2: Configure the decoder. For more information, see README.decode#####
#
^C Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell ^_ Go To Line
```

Figure 5. 481 : Path to rules

```

g7@g7:~          GNU nano 2.5.3      File: /etc/snort/snort.conf

# 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 rules
var SO_RULE_PATH so_rules
var PREPROC_RULE_PATH preproc_rules
#
# If you are using reputation preprocessor set these
# Currently there is a bug with relative paths, they are relative to where snor$ 
# 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
var BLACK_LIST_PATH /etc/snort/rules

#####
# Step #2: Configure the decoder. For more information, see README.decode
#####

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

```

Figure 5. 482 : Path to black list and white list IPs

```

g7@g7:~          GNU nano 2.5.3      File: /etc/snort/snort.conf      Modified

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 snort.log, limit 128, nostamp, mpls event types, vlan event types

# 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
# output alert_syslog: LOG_AUTH LOG_ALERT

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

```

Figure 5. 483 : Output Snort to log file

```

g7@g7:~          GNU nano 2.5.3      File: /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
#####

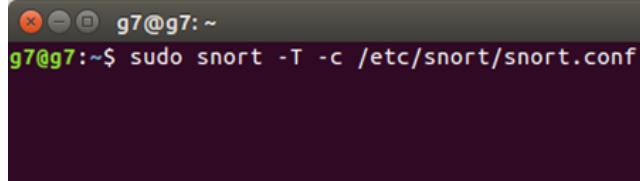
# site specific rules
include $RULE_PATH/local.rules
include $RULE_PATH/community.rules
#
include $RULE_PATH/app-detect.rules
include $RULE_PATH/attack-responses.rules
include $RULE_PATH/backdoor.rules
include $RULE_PATH/bad-traffic.rules
include $RULE_PATH/blacklist.rules
include $RULE_PATH/botnet-cnc.rules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

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

```

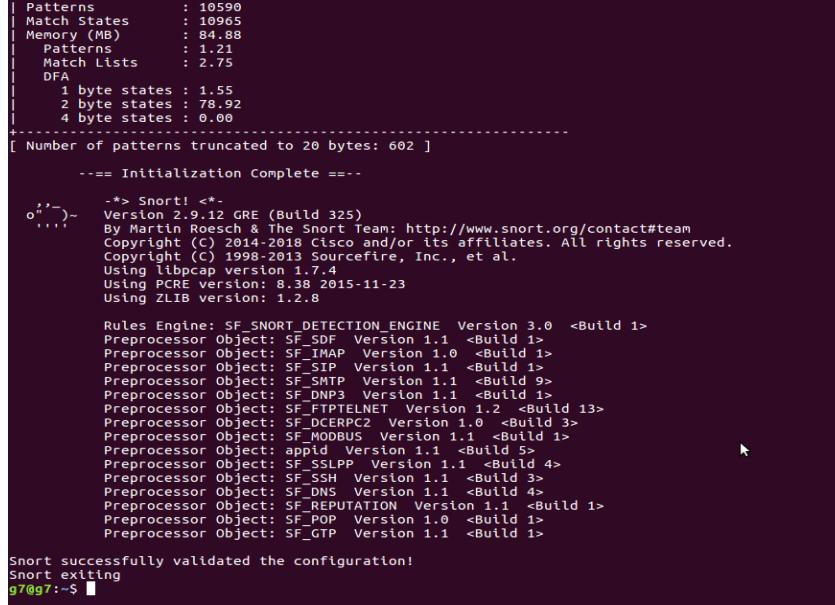
Figure 5. 484 : Uncomment any rules available

Step 15: Type sudo snort -T -c /etc/snort/snort.conf to validate Snort Rules



```
g7@g7:~$ sudo snort -T -c /etc/snort/snort.conf
```

Figure 5. 485 : Verify Snort's Configuration

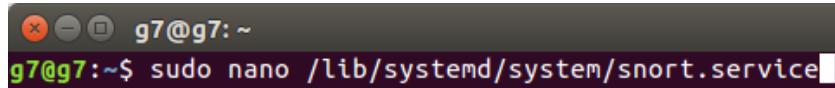


```
Patterns          : 10590
Match States     : 10965
Memory (MB)      : 84.88
Patterns          : 1.21
Match Lists       : 2.75
DFA
  1 byte states : 1.55
  2 byte states : 78.92
  4 byte states : 0.00
[ Number of patterns truncated to 20 bytes: 602 ]
--- Initialization Complete ---
-> Snort! <-
Version 2.9.12 GRE (Build 325)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2018 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.7.4
Using PCRE version: 8.38 2015-11-23
Using ZLIB version: 1.2.8
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.0 <Build 1>
Preprocessor Object: SF_SDP Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SQL Version 1.1 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: apf_id Version 1.1 <Build 5>
Preprocessor Object: SF_SSLP Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>

Snort successfully validated the configuration!
Snort exiting
g7@g7:~$
```

Figure 5. 486 : Snort Successfully Verify Configuration

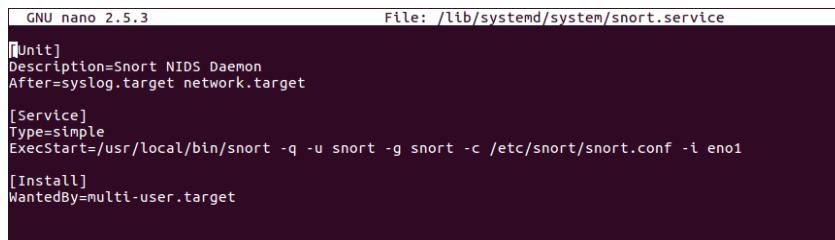
Step 16: We need to make Snort runs on background and be able to catch any incoming traffic by make a Snort Daemon.



```
g7@g7:~$ sudo nano /lib/systemd/system/snort.service
```

Figure 5. 487 : Create a startup script

Step 17: Modify the snort.service file as shown as below.



```
GNU nano 2.5.3                                     File: /lib/systemd/system/snort.service

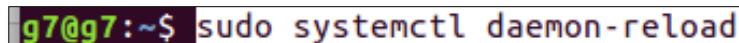
[Unit]
Description=Snort NIDS Daemon
After=syslog.target network.target

[Service]
Type=simple
ExecStart=/usr/local/bin/snort -q -u snort -g snort -c /etc/snort/snort.conf -i eno1

[Install]
WantedBy=multi-user.target
```

Figure 5. 488 : Snort.Service

Step 18: Reload daemon and check the status of Snort.



```
g7@g7:~$ sudo systemctl daemon-reload
```

Figure 5. 489 : Reload Daemon

```
g7@g7:~$ sudo systemctl status snort
● snort.service - Snort NIDS Daemon
  Loaded: loaded (/lib/systemd/system/snort.service; disabled; vendor preset: e
  Active: inactive (dead)

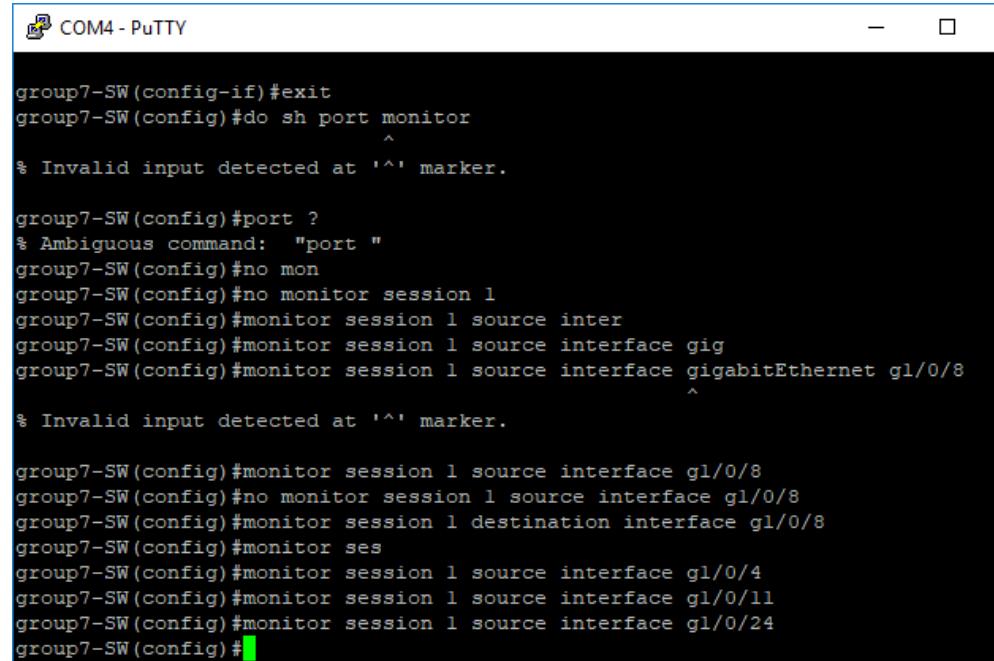
g7@g7:~$ sudo systemctl restart snort
g7@g7:~$ sudo systemctl status snort
● snort.service - Snort NIDS Daemon
  Loaded: loaded (/lib/systemd/system/snort.service; disabled; vendor preset: e
  Active: active (running) since Rab 2018-10-17 00:56:48 +08; 1s ago
    Main PID: 9878 (snort)
   CGroup: /system.slice/snort.service
           └─9878 /usr/local/bin/snort -q -u snort -g snort -c /etc/snort/snort.

Okt 17 00:56:48 g7 systemd[1]: Started Snort NIDS Daemon.
```

Figure 5. 490 : Snort Status

B. Configure Port Mirror.

Step 1: Configure monitor session 1



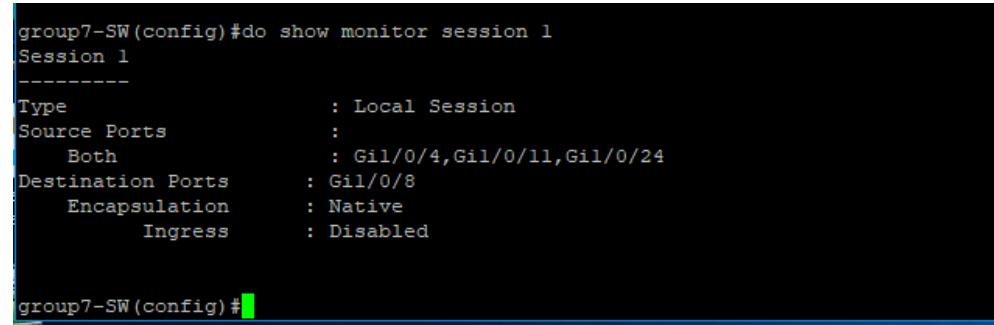
```
group7-SW(config-if)#exit
group7-SW(config)#do sh port monitor
^
% Invalid input detected at '^' marker.

group7-SW(config)#port ?
% Ambiguous command: "port"
group7-SW(config)#no mon
group7-SW(config)#no monitor session 1
group7-SW(config)#monitor session 1 source inter
group7-SW(config)#monitor session 1 source interface gig
group7-SW(config)#monitor session 1 source interface gigabitEthernet g1/0/8
^
% Invalid input detected at '^' marker.

group7-SW(config)#monitor session 1 source interface g1/0/8
group7-SW(config)#no monitor session 1 source interface g1/0/8
group7-SW(config)#monitor session 1 destination interface g1/0/8
group7-SW(config)#monitor ses
group7-SW(config)#monitor session 1 source interface g1/0/4
group7-SW(config)#monitor session 1 source interface g1/0/11
group7-SW(config)#monitor session 1 source interface g1/0/24
group7-SW(config)#[
```

Figure 5. 491 : Create monitor session

Step 2: Verify the monitor session has created.



```
group7-SW(config)#do show monitor session 1
Session 1
-----
Type          : Local Session
Source Ports   :
    Both      : G1/0/4,G1/0/11,G1/0/24
Destination Ports : G1/0/8
    Encapsulation : Native
    Ingress       : Disabled

group7-SW(config)#[
```

Figure 5. 492 : Monitor Session 1

5.2.27 IPsec VPN for remote employees

Installation of VPN Server

Step 1: Installing VPN Sever



Figure 5. 493 : SoftEther VPN Setup Wizard

Step 2: Select SoftEther VPN Server.

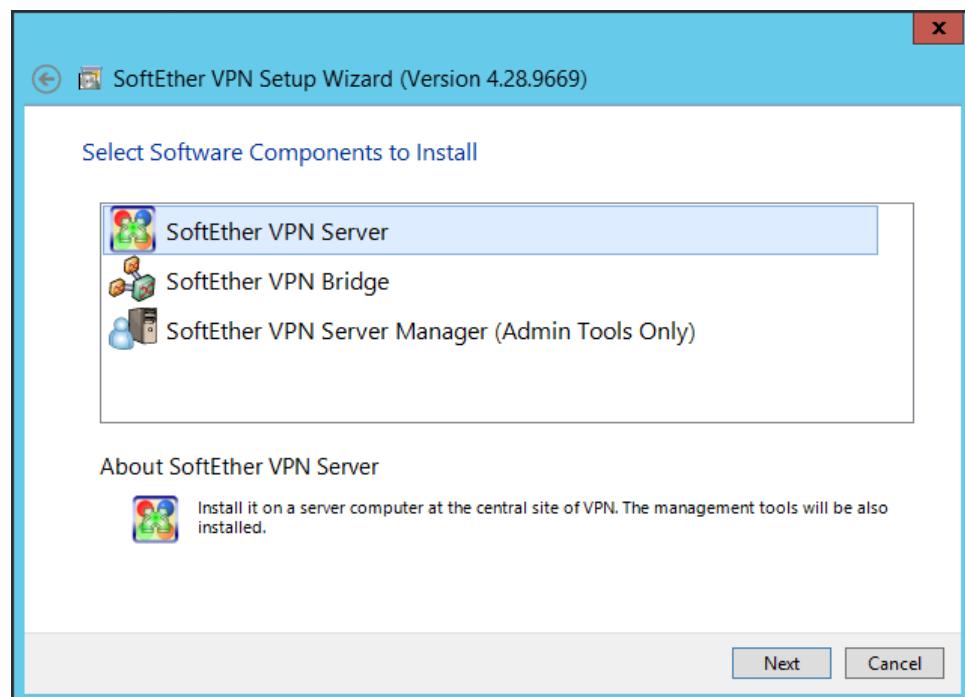


Figure 5. 494 : Software Components to Install

Step 3: Tick on agree and click **Next**

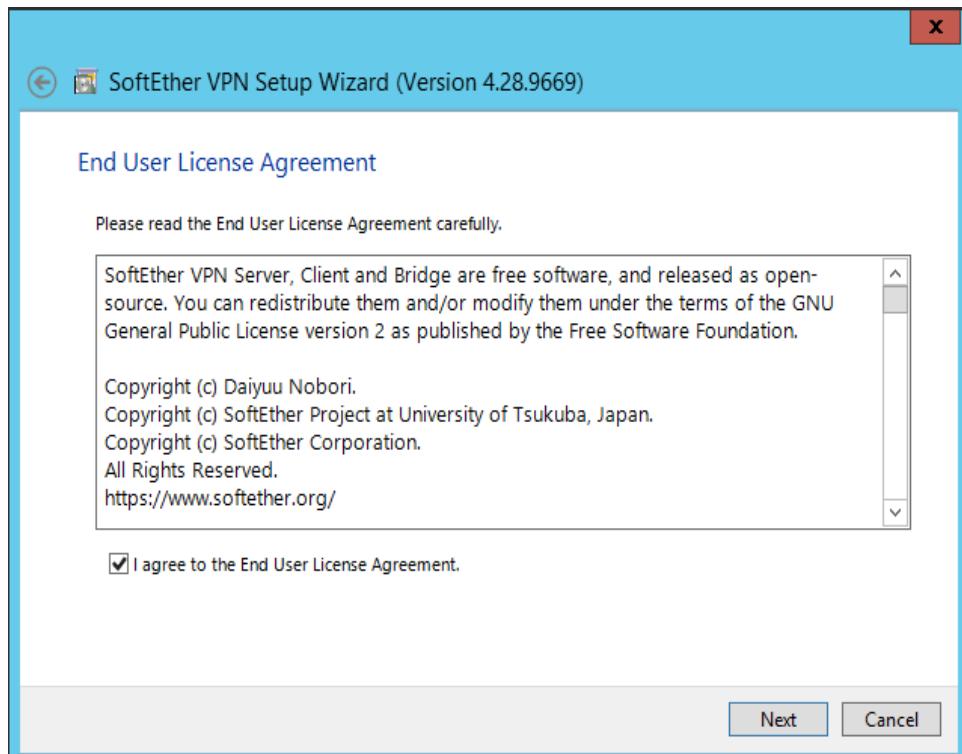


Figure 5. 495 : End User License Agreement

Step 4: Click **Next**.

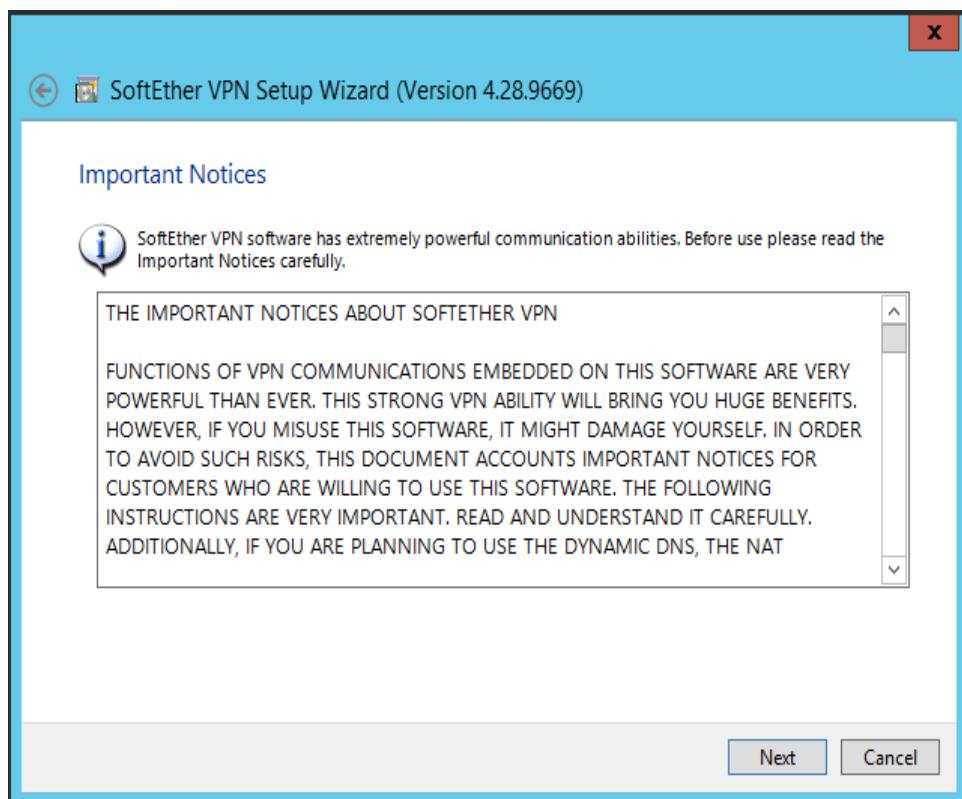


Figure 5. 496 : Important Notices

Step 5: Click **Next**.

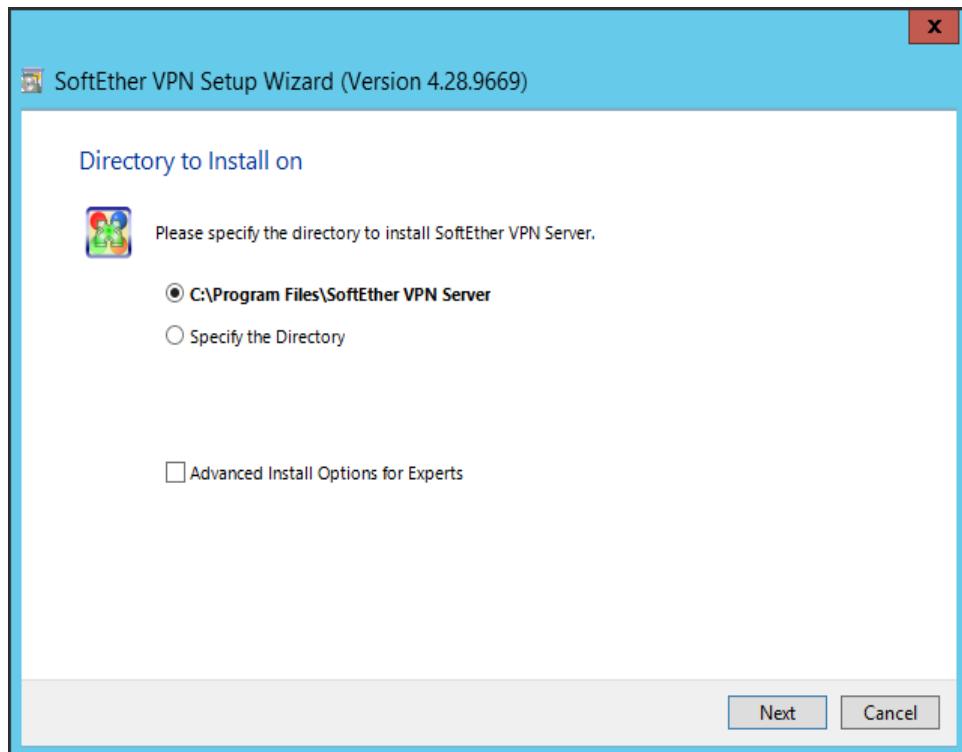


Figure 5. 497 : Directory to Install

Step 6: SoftEther VPN Server is ready to install and click **Next**.

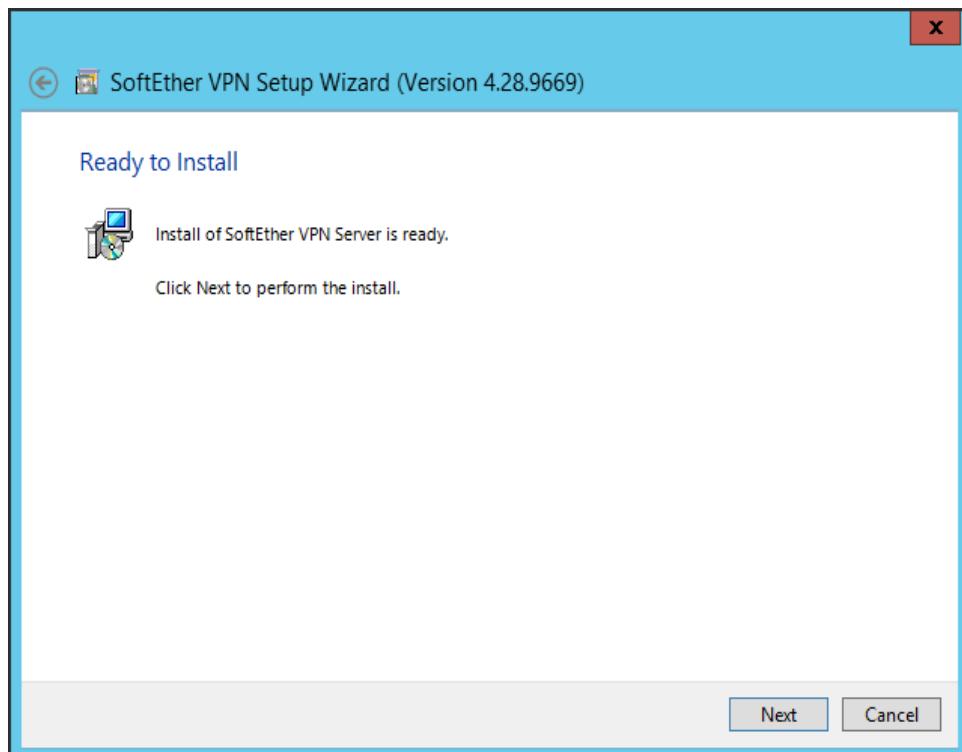


Figure 5. 498 : Ready to Install

Step 7: The installation was in progress.

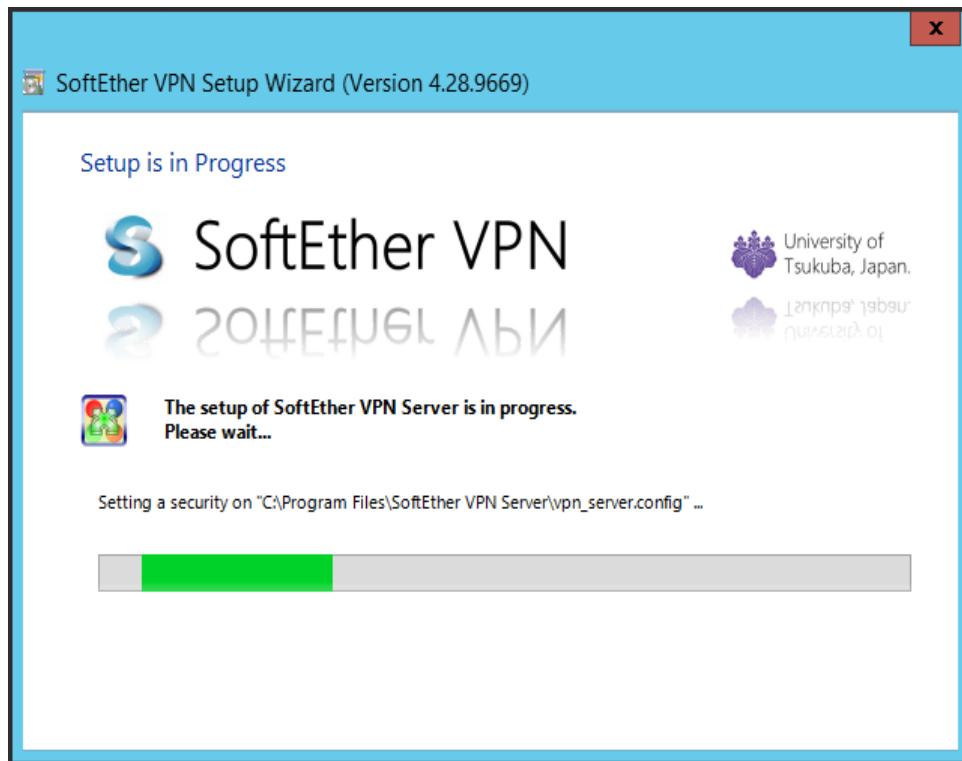


Figure 5. 499 : Setup is in Progress

Step 8: The installation was done and click **Finish**.

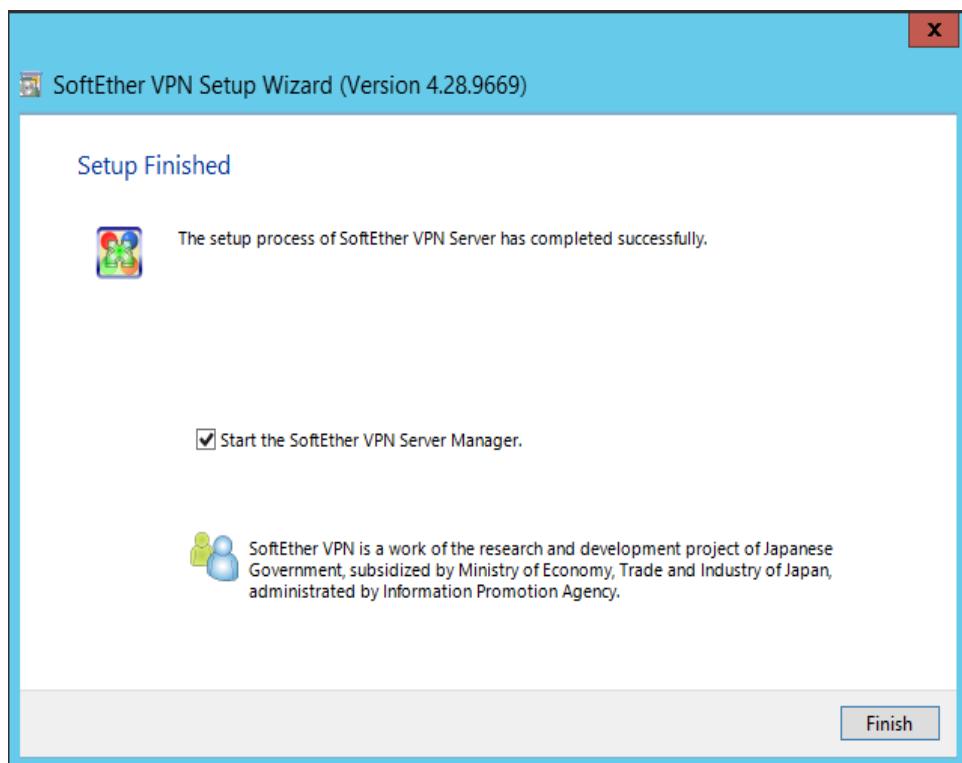


Figure 5. 500 : Setup Finished

Step 9: Click icon SoftEther VPN Server Manager on desktop and it will be appeared as below. Then, double click on **localhost**.



Figure 5. 501 : SoftEther VPN Server Manager

Step 10: Set the **Setting Name** as **VPN**. Named the Host Name with IP address of the server and select **Port Number 5555**. Set the password to connect administration mode. Then, click **OK**.

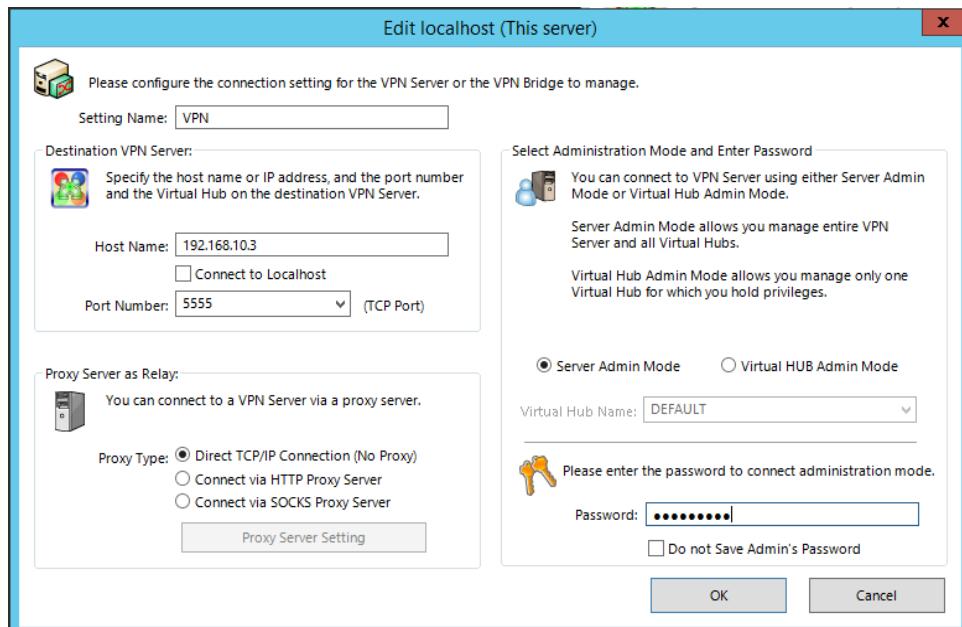


Figure 5. 502 : Edit localhost (This server)

Step 11: Set the **New Password** and **Confirm Password** then click **OK**.



Figure 5. 503 : Change Administrator Password

Step 12: The setting will change as the figure below.



Figure 5. 504 : SoftEther VPN Server Manager

Step 13: Tick at **Remote Access VPN Server** and click **Next**.

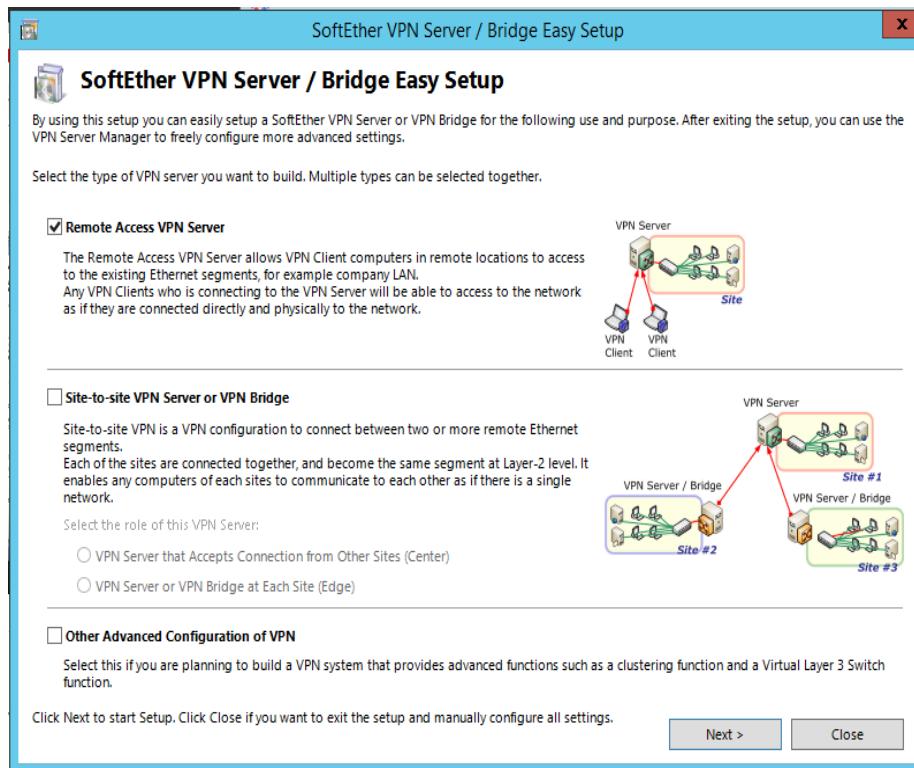


Figure 5. 505 : SoftEther VPN Server / Bridge Easy Setup

Step 14: Popup **Easy Setup** shows the default Virtual Hub Name is **VPN**.

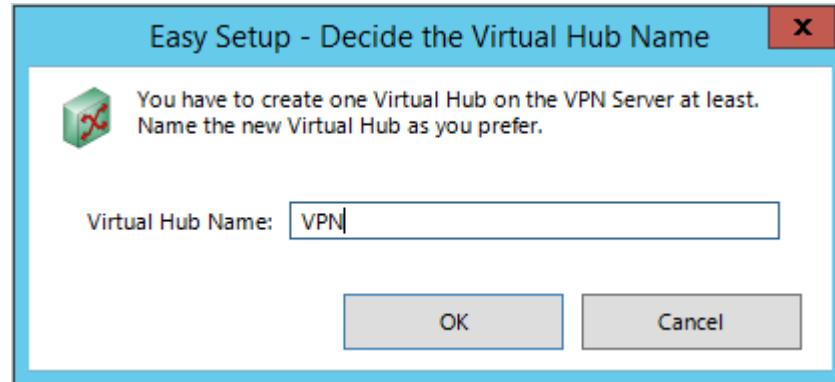


Figure 5. 506 : Easy Setup – Decide the Virtual Hub Name

Step 15: The Dynamic DNS Hostname was given and click **Exit**.

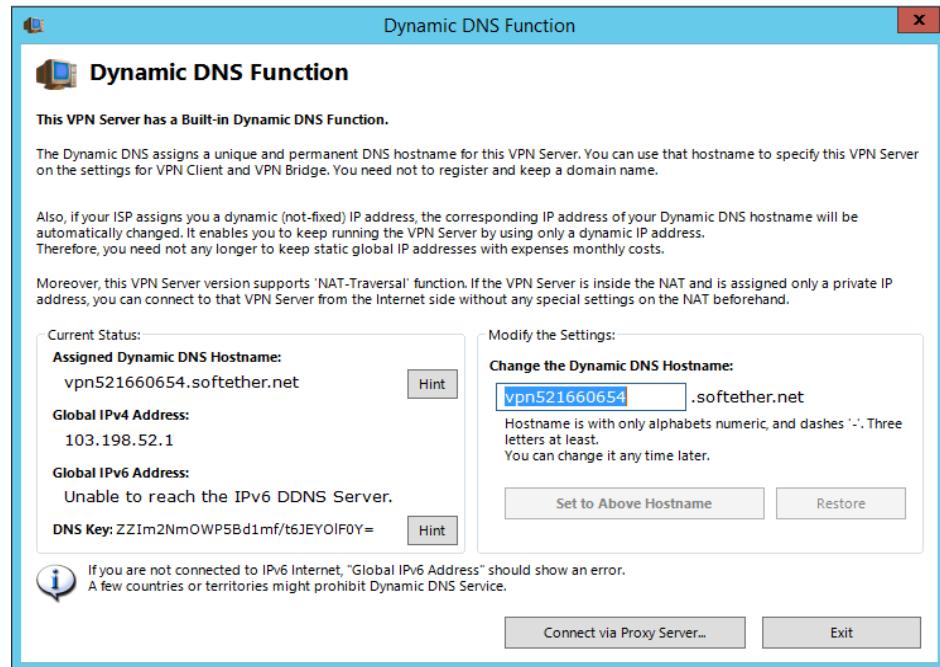


Figure 5. 507 : Dynamic DNS Function

Step 16: Tick right for **Enable L2TP Server Function (L2TP over IPsec)** and **Enable L2TP Server Function (Raw L2TP with No Encryption)**. Then, click **OK**.

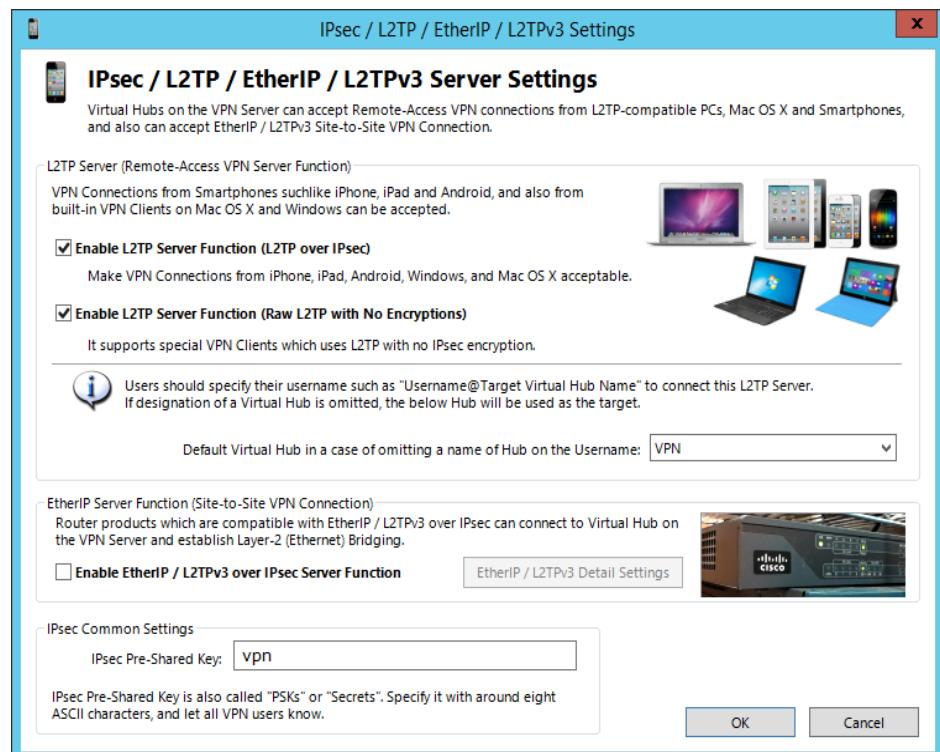


Figure 5. 508 : IPsec / L2TP / EtherIP / L2TPv3

Step 17: Tick at **Enable VPN Azure** and click **OK**.

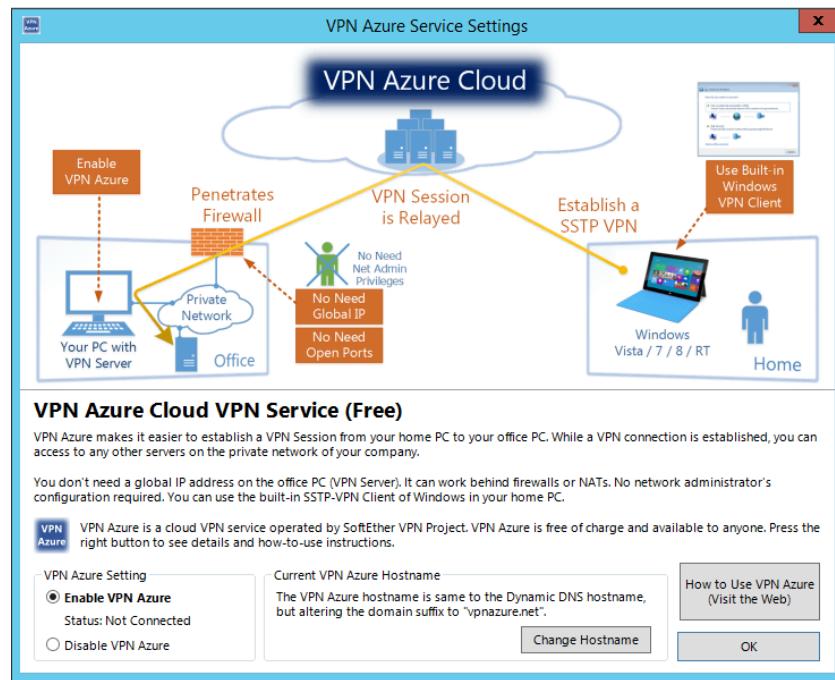


Figure 5. 509 : VPN Azure Service Settings

Step 18: Click on **Create Users**.

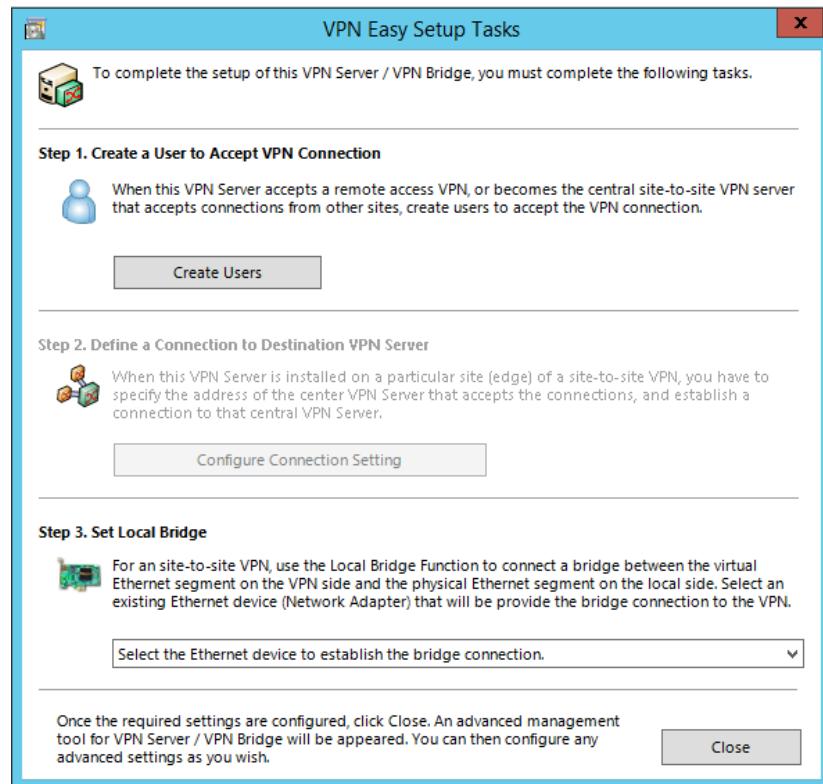


Figure 5. 510 : VPN Easy setup Tasks

Step 19: Create a User Name, Full Name and the Password for New User.

Then, click **OK**.

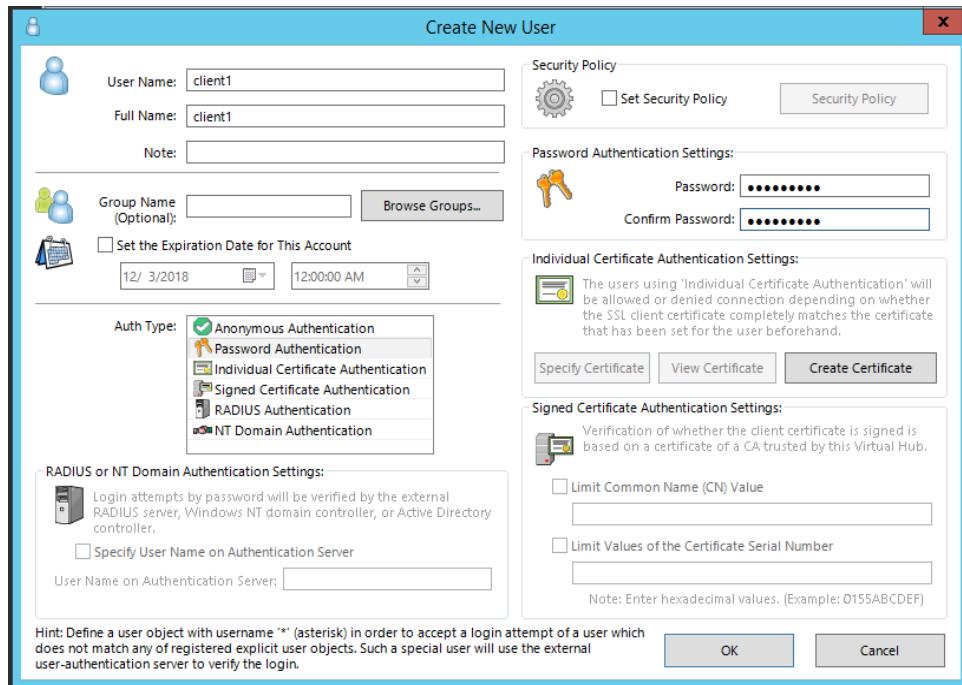


Figure 5. 511 : Create User

Step 20: User client1 has been created the click **Exit**.

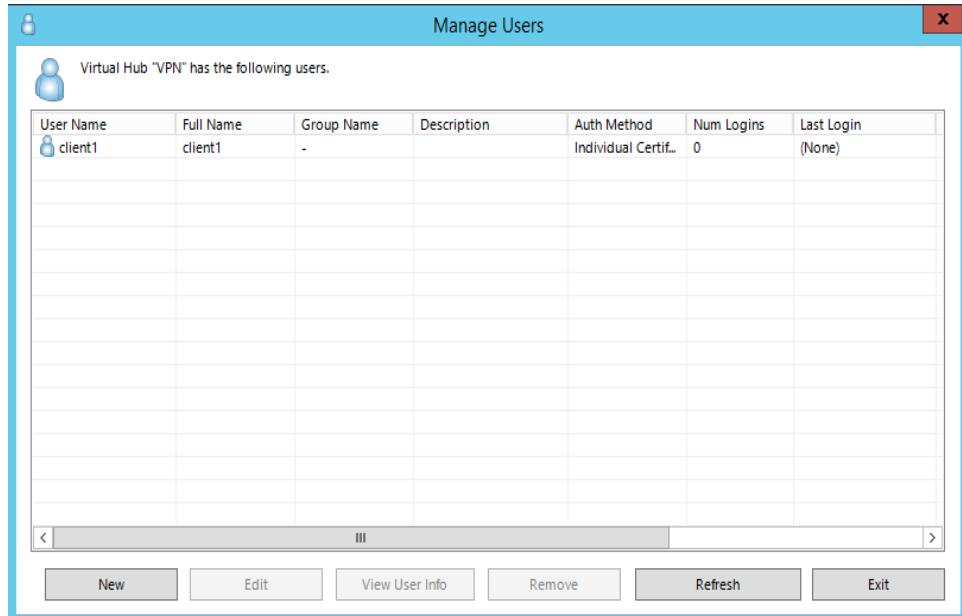


Figure 5. 512 : Manage Users

Step 21: Create certificate by filling the blank. Then, click **OK**.

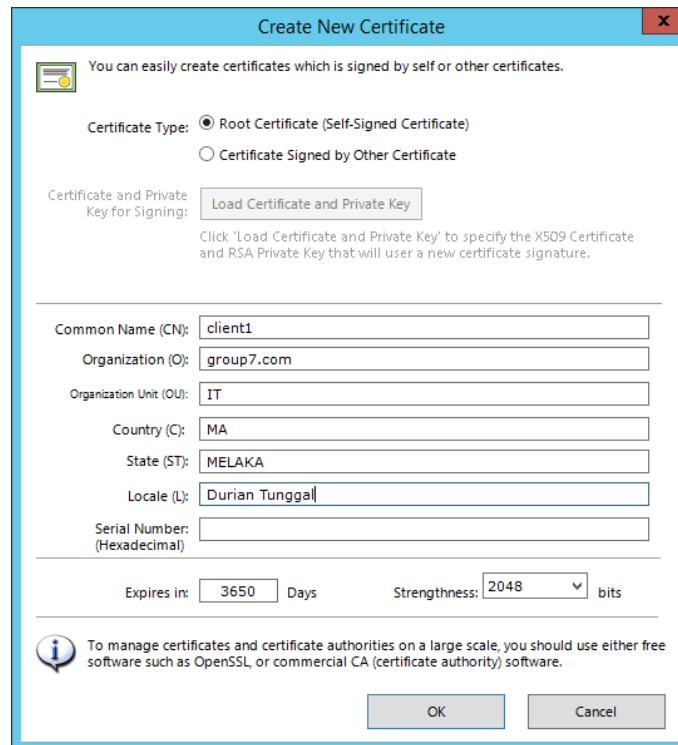


Figure 5. 513 : Create New Certificate

Step 22: Save the certificate as **X509 Certificate (.CER)** and **Private Key file (.KEY)**. Set the passphrase of the certificate to encrypt.

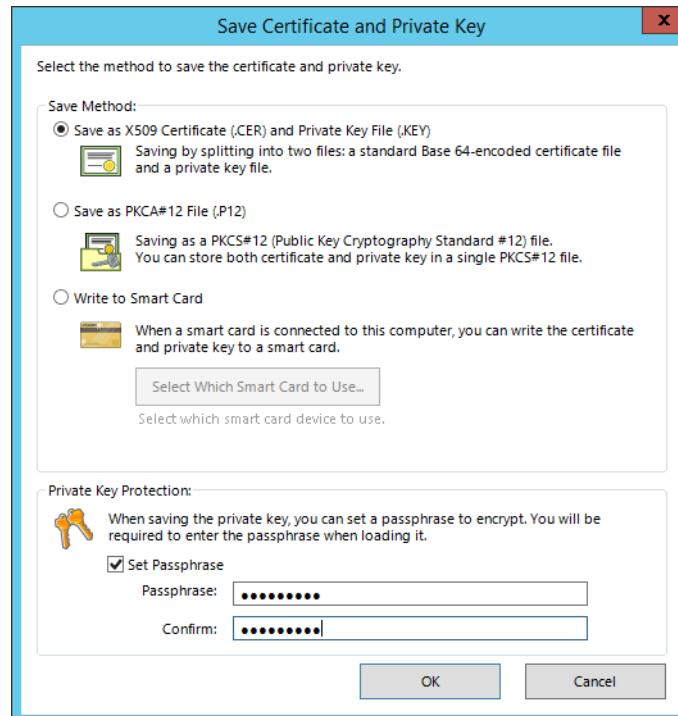


Figure 5. 514 : Save Certificate and Private Key

Step 23: Save the certificate as **client1**.

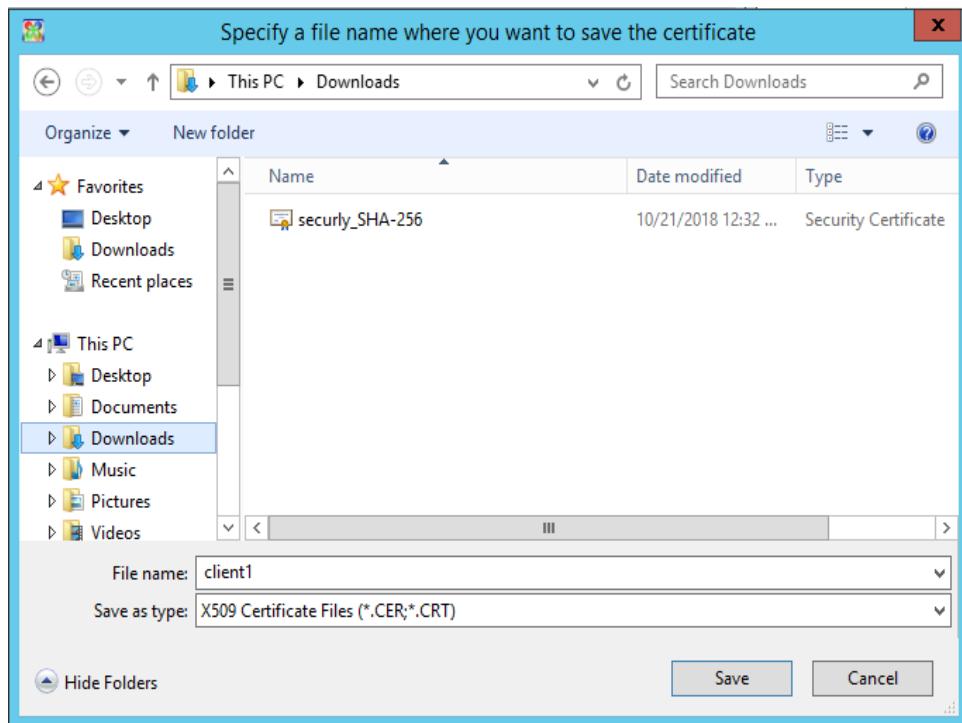


Figure 5. 515 : Specify a file name where you want to save the certificate

Step 24: The certificate of client1 was saved in the folder **IPSec VPN** at the desktop.

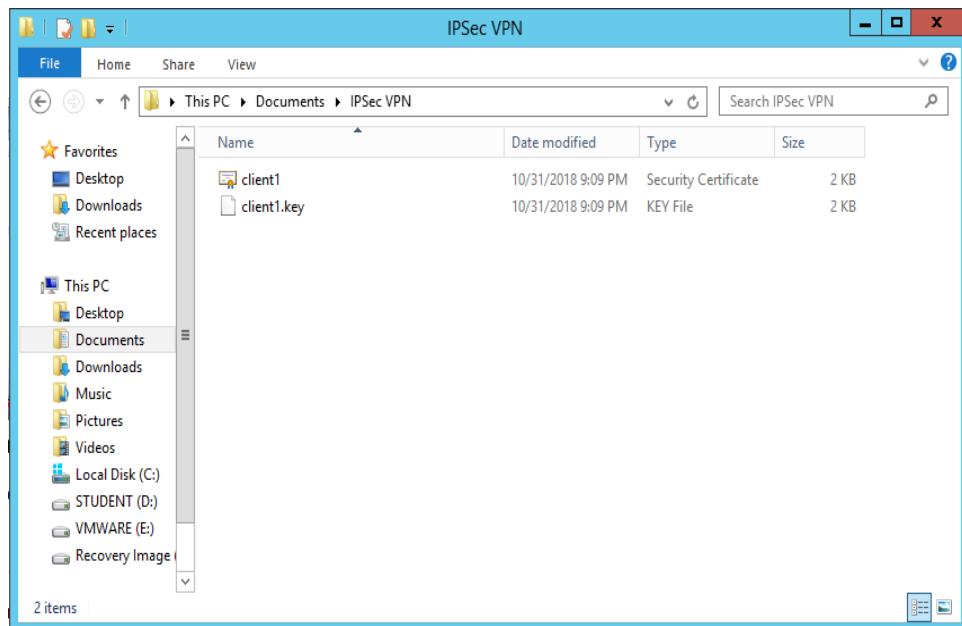


Figure 5. 516 : IPSec VPN folder

Installation of SoftEther VPN Client

Step 1: Installing VPN Client

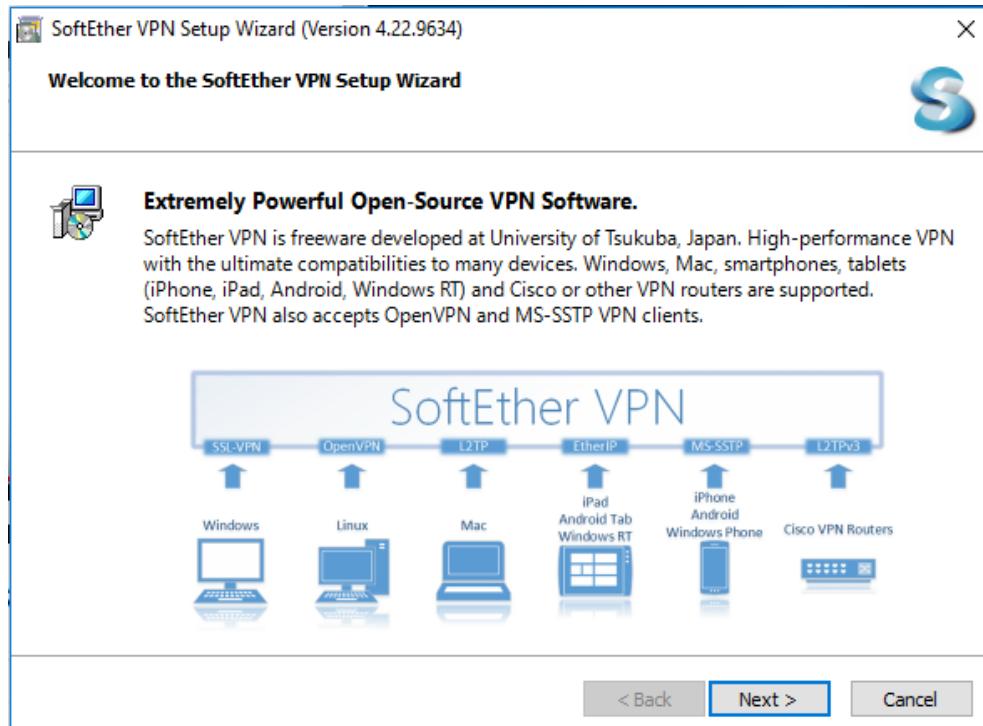


Figure 5. 517 : SoftEther VPN Setup Wizard

Step 2: Select SoftEther VPN Client.

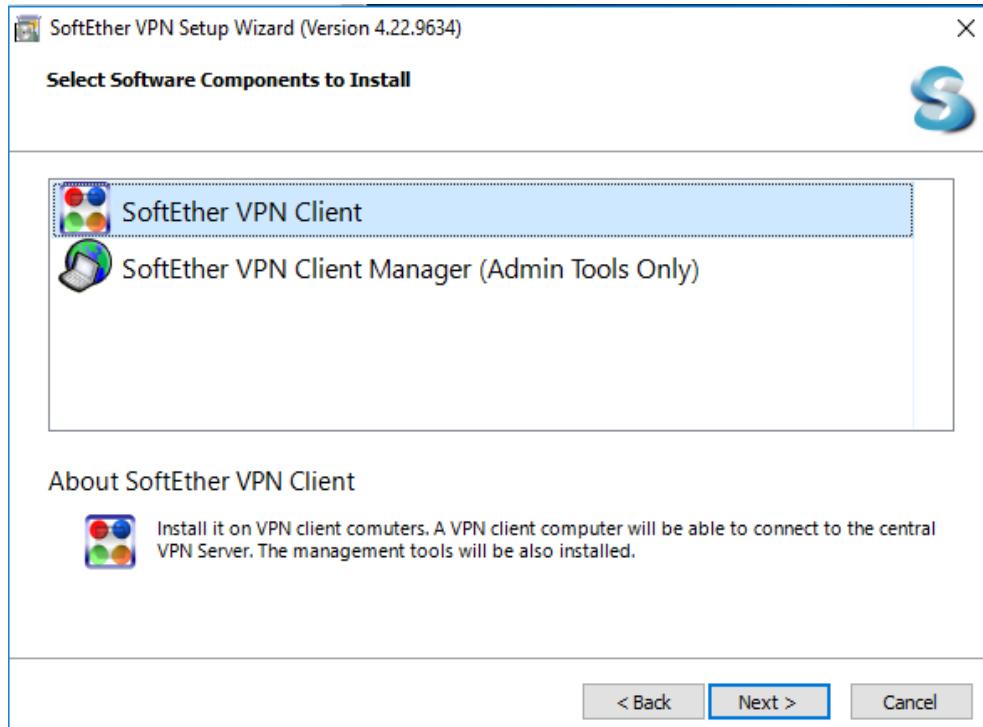


Figure 5. 518 : Software Components to Install

Step 3: Tick agree and click Next.

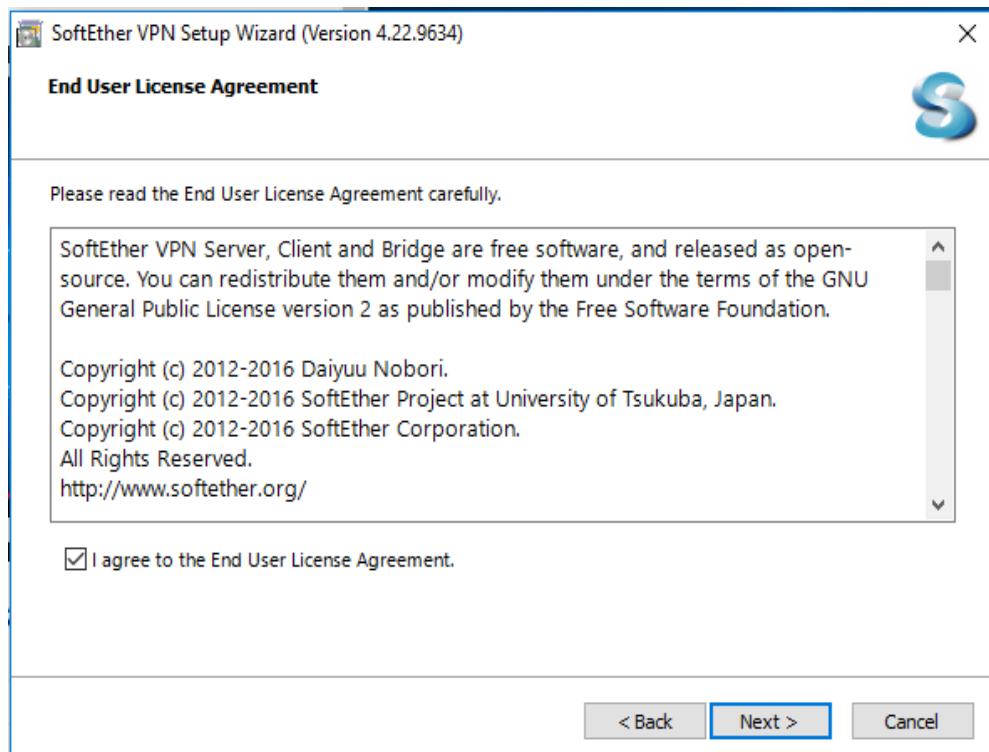


Figure 5. 519 : End User License Agreement

Step 4: Click Next.

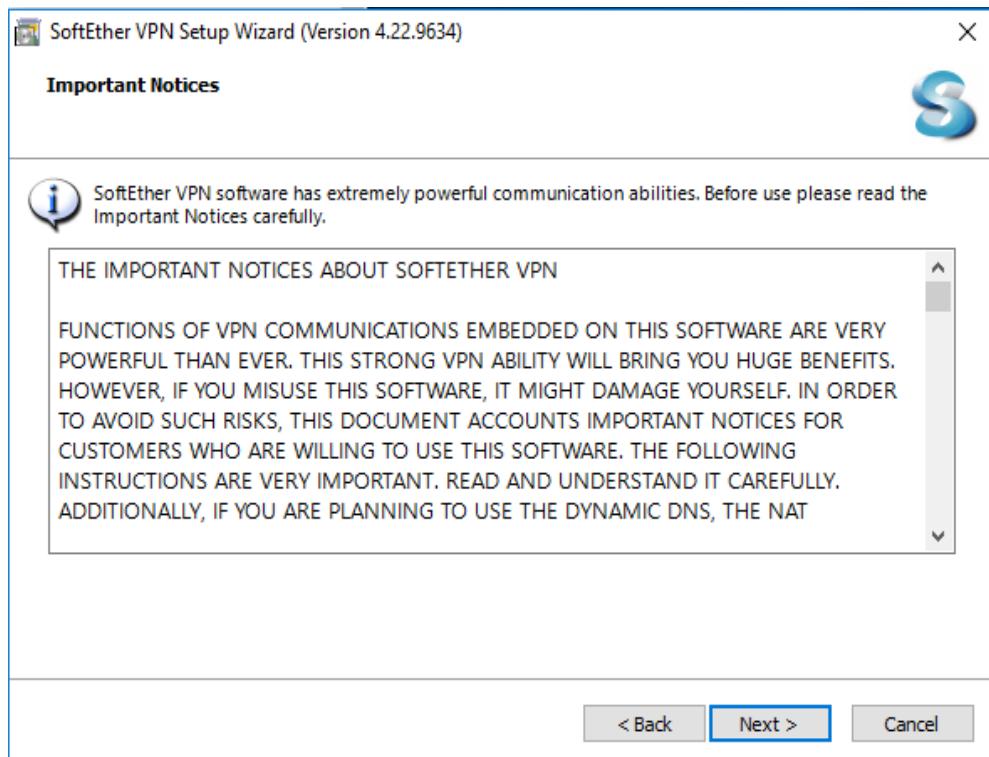


Figure 5. 520 : Important Notices

Step 5: Click Next.

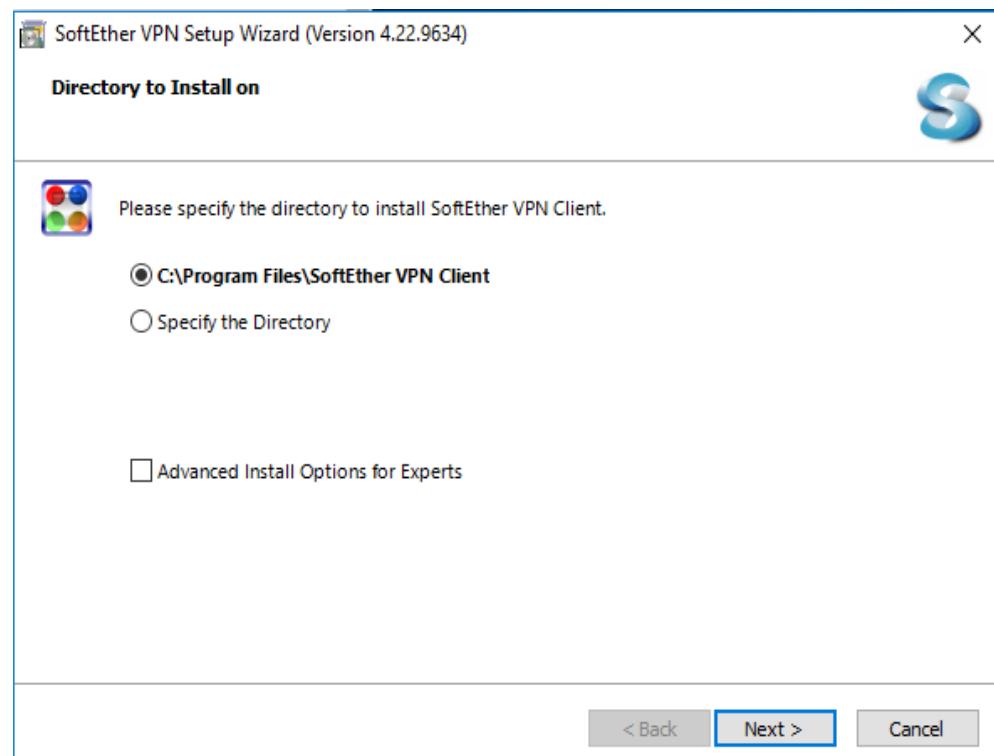


Figure 5. 521 : Directory to Install

Step 6: The SoftEther VPN is ready to install. Click Next.

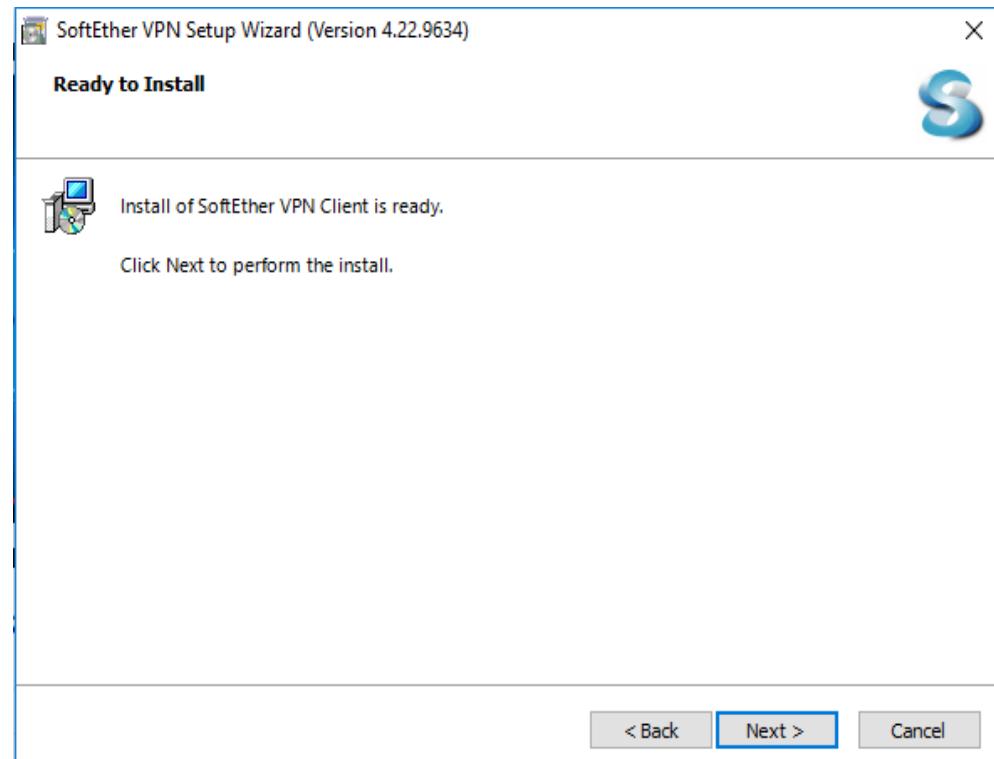


Figure 5. 522 : Ready to Install

Step 7: Installation in progress.

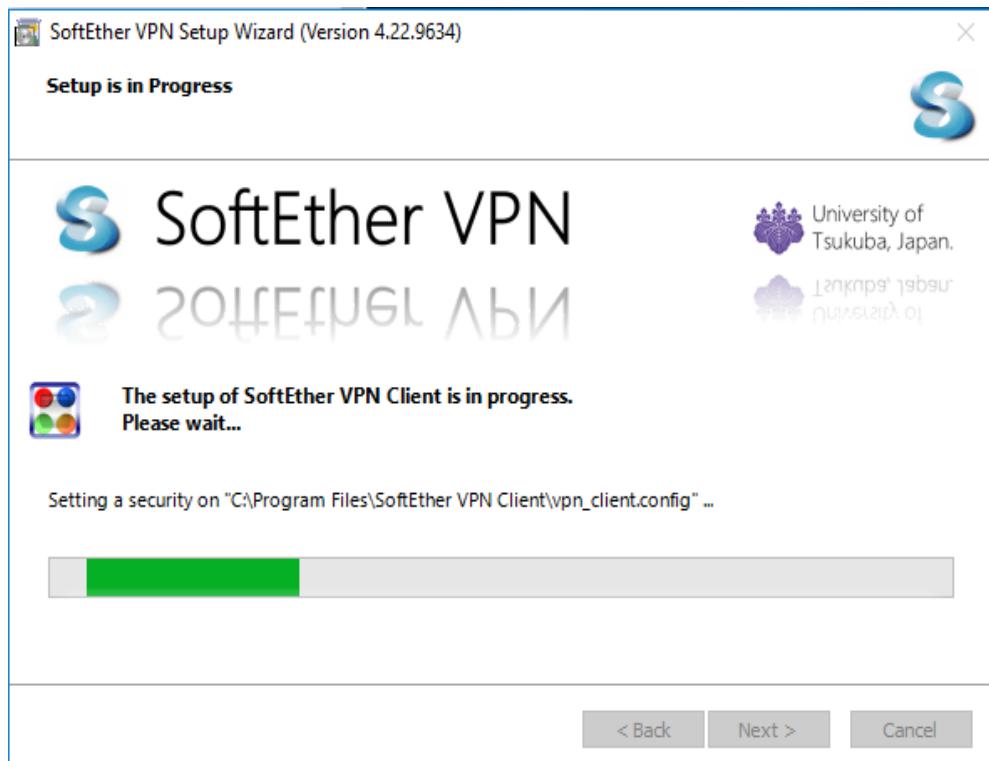


Figure 5. 523 : Setup is in Progress

Step 8: The Setup was finished. Then, click **Finish**.

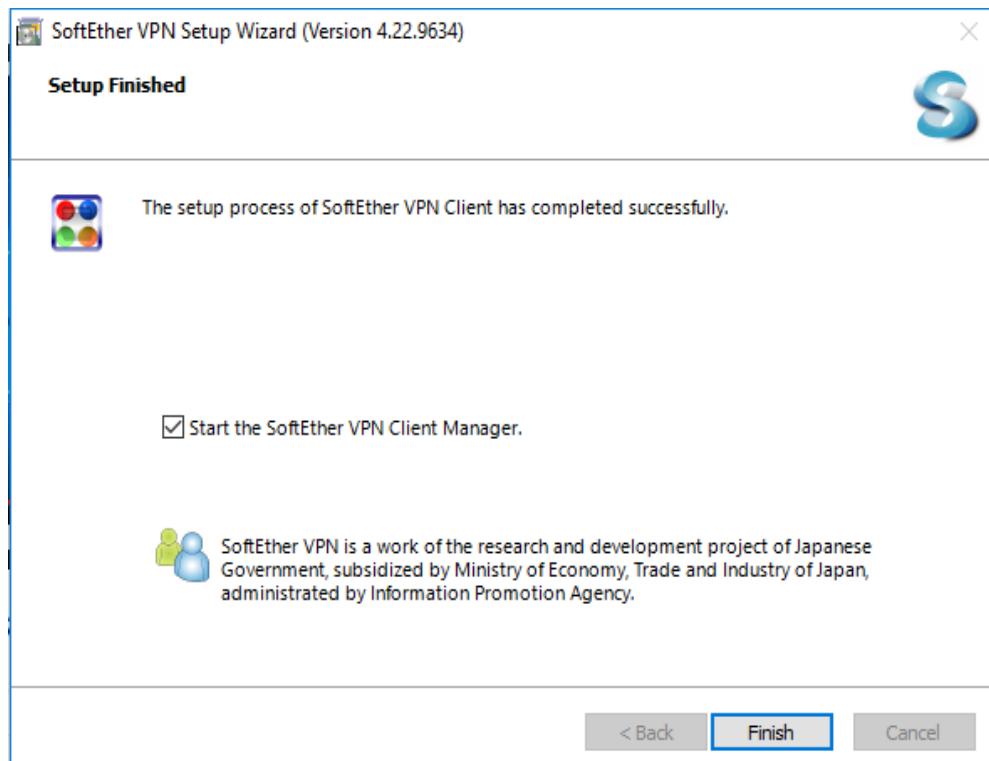


Figure 5. 524 : Setup Finished

Step 9: Click on New VPN Connection.

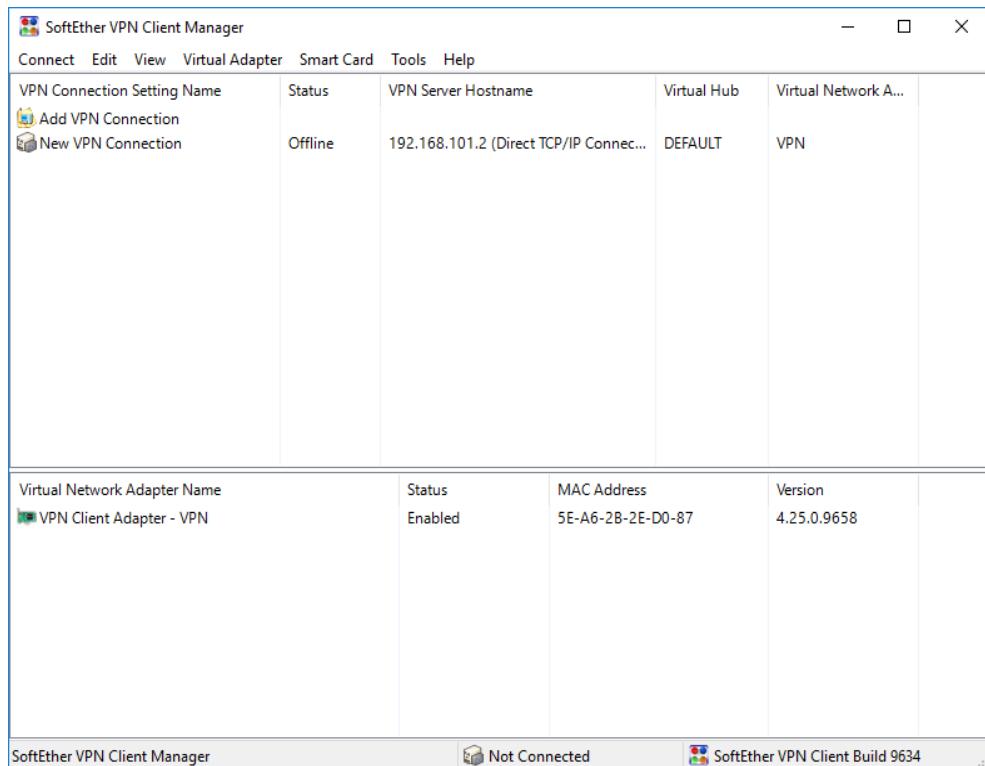


Figure 5. 525 Add VPN Connection

Step 10: Setting the Client connection.

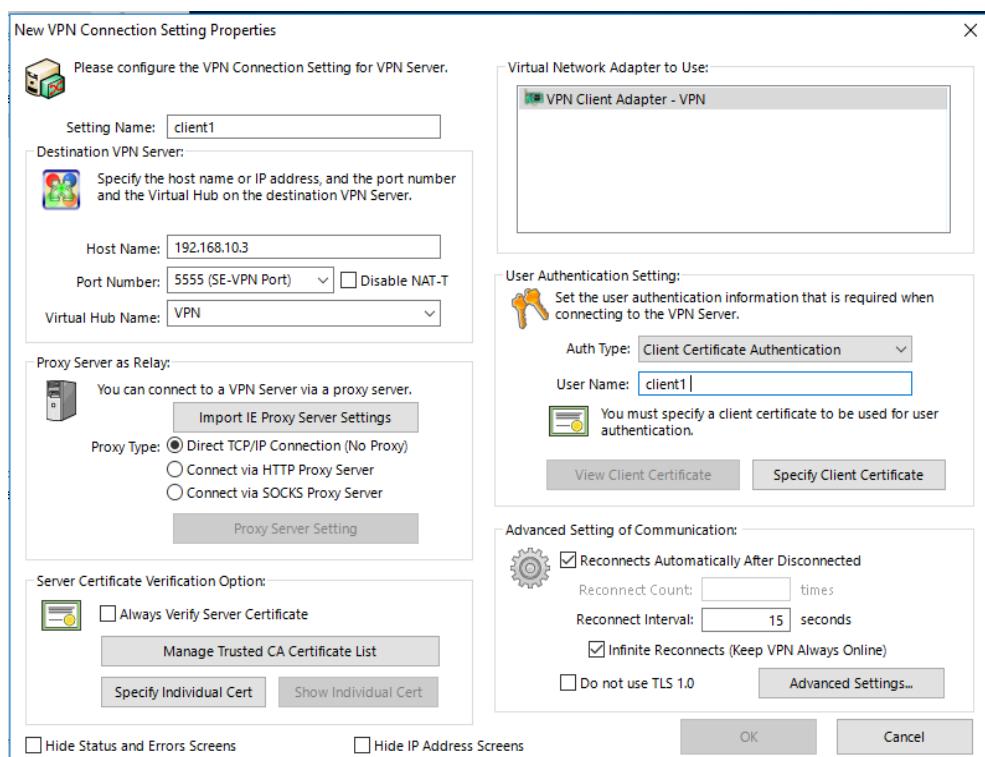


Figure 5. 526 VPN Connection Setting Properties

Step 11: client1 has been created.

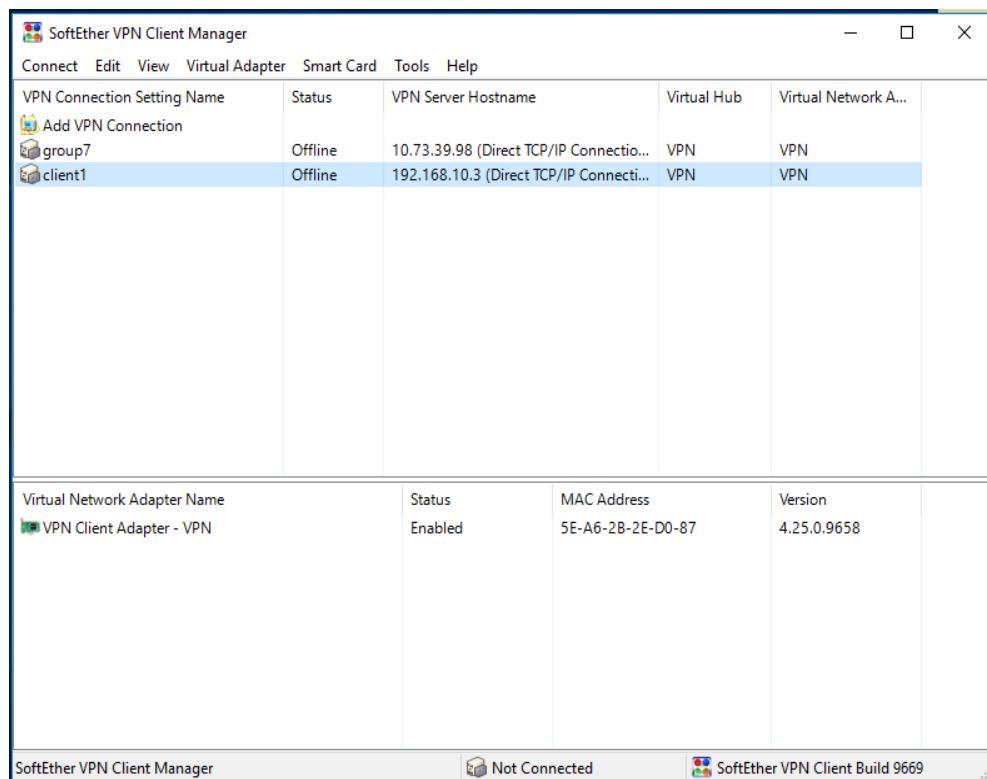
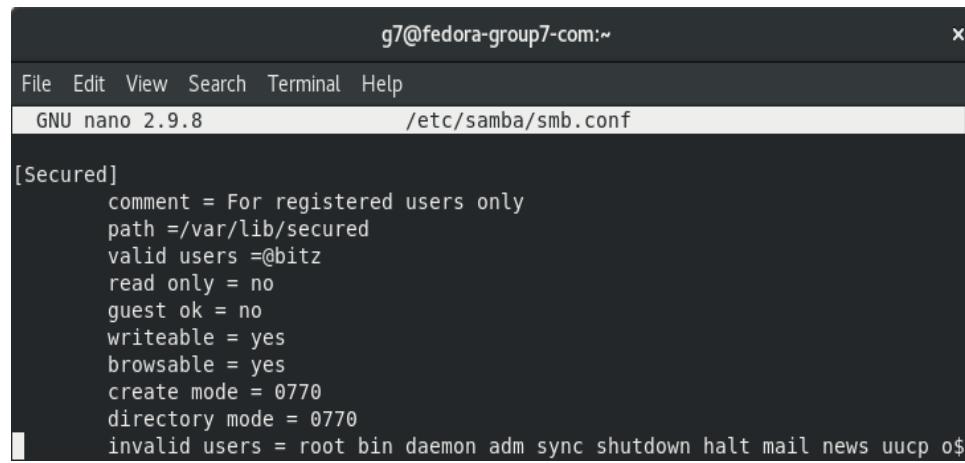


Figure 5. 527 : SoftEther VPN Client Manager

5.2.28 Samba security services

Samba Group Based Directory



```
g7@fedora-group7-com:~
```

```
File Edit View Search Terminal Help
```

```
GNU nano 2.9.8 /etc/samba/smb.conf
```

```
[Secured]
comment = For registered users only
path =/var/lib/secured
valid users =@bitz
read only = no
guest ok = no
writeable = yes
browsable = yes
create mode = 0770
directory mode = 0770
invalid users = root bin daemon adm sync shutdown halt mail news uucp o$
```

Figure 5. 528 : Samba Group Configuration

Step 1: In Secured configuration, create another folder for secured share.

```
# sudo mkdir /var/lib/secured.
```

Step 2: Change the folder permission and owner to allow only permitted group can access which is bitz group.

```
# sudo chmod -R root:bitz /var/lib/secured
# sudo chown -R 0775 /var/lib/secured
```

Step 3: Create another user called ‘yap’ and assigned to bitz group.

Step 4: Add user ‘yap’ into samba and change its password using

```
# smbpasswd -a yap
```

Step 5: Add valid users = @bitz.

Step 6: Add invalid users to prevent invalid users to login to directory.

Samba User's Directory

```
[mi]
path = /var/lib/mi
valid users = mi
force user = mi
guest ok = no
writeable = yes
browsable = yes
read only = no

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

Figure 5. 529 : Samba User's Directory

Step 1: Create user named *mi*.

Step 2: Create a folder called as *mi*.

```
# sudo mkdir /var/lib/mi
```

Step 3: Modify the folder permission to user *mi*.

```
# sudo chown -R mi:mi /var/lib/mi
# sudo chmod -R 0775 /var/lib/mi
```

5.2.29 Port Security

Step 1: Run command ***show port-security*** to check if there are any port have been configured

Step 2: Type a command for ***errdisable*** which is to avoid having to manually intervene every time a port-security violation forces an interface into the error-disabled state, one can enable auto-recovery for port security violations.

```
Switch(config)# errdisable recovery cause psecure-violation
```

```
Switch(config)# errdisable recovery interval 600
```

Step 3: Set the port which one port will remember only one mac address by using static mac address

```
group7-SW(config)#int g1/0/8
group7-SW(config-if)#switchport port-security
group7-SW(config-if)#switchport port-security maximum 1
group7-SW(config-if)#switchport port-security mac-address 18:60:24:8e:45:e3
Found duplicate mac-address 1860.248e.45e3.
group7-SW(config-if)#switchport port-security violation shutdown
group7-SW(config-if)#end
```

Figure 5. 530 : Command on Ubuntu

```
group7-SW(config)#int g1/0/11
group7-SW(config-if)#switchport port-security
group7-SW(config-if)#switchport port-security maximum 1
group7-SW(config-if)#switchport port-security mac-address 18:60:24:8e:45:e8
Found duplicate mac-address 1860.248e.45e8.
group7-SW(config-if)#switchport port-security violation shutdown
group7-SW(config-if)#end
```

Figure 5. 531 : Command on Fedora

```
group7-SW(config)#int g1/0/4
group7-SW(config-if)#sw
group7-SW(config-if)#switchport port-sec
group7-SW(config-if)#switchport port-security maximum 2
group7-SW(config-if)#switchport port-security mac-address 18-60-24-8E-44-E8
group7-SW(config-if)#switchport port-security violation shutdown
group7-SW(config-if)#end
```

Figure 5. 532 : Command on Windows

Step 4: Set the other port which had been assign to the server with mac address sticky

```
group7-SW(config)#int g1/0/9
group7-SW(config-if)#switchport port-security
group7-SW(config-if)#switchport port-security maximum 1
group7-SW(config-if)#switchport port-security mac-address sticky
group7-SW(config-if)#switchport port-security violation shutdown
group7-SW(config-if)#end
group7-SW(config)#int g1/0/7
group7-SW(config-if)#switchport port-security
group7-SW(config-if)#switchport port-security maximum 1
group7-SW(config-if)#switchport port-security mac-address sticky
group7-SW(config-if)#switchport port-security violation shutdown
group7-SW(config-if)#end
```

Figure 5. 533 : Command for Ubuntu

```
group7-SW(config)#int g1/0/10
group7-SW(config-if)#switchport port-security
group7-SW(config-if)#switchport port-security maximum 1
group7-SW(config-if)#switchport port-security mac-address sticky
group7-SW(config-if)#switchport port-security violation shutdown
group7-SW(config-if)#end

group7-SW(config)#int g1/0/12
group7-SW(config-if)#switchport port-security
group7-SW(config-if)#switchport port-security maximum 1
group7-SW(config-if)#switchport port-security mac-address sticky
group7-SW(config-if)#switchport port-security violation shutdown
group7-SW(config-if)#end
```

Figure 5. 534 : Command for Fedora

```
group7-SW(config)#int range g1/0/5-6
group7-SW(config-if-range)#switchport port-security
group7-SW(config-if-range)#switchport port-security maximum 1
group7-SW(config-if-range)#$port-security mac-address sticky
group7-SW(config-if-range)#switchport port-security violation shutdown
group7-SW(config-if-range)#end
```

Figure 5. 535 : Command for Windows

CHAPTER 6 - TESTING

6.1 INTRODUCTION

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

6.2 SERVICES TESTING

6.2.1 DNS (IPv4 & IPv6)

We test the DNS by right click on server name and choose launch nslookup. We enter the IP address and the FQDN to check whether it is successfully or not. nslookup is a useful suite of tools for looking at DNS records. The nslookup command allows you to question your domains name servers, and find out much more information regarding your domains DNS. We will ping by domain name and IP address.

- Domain Name: group7.com.
- IPv4 Address: 192.168.10.3
- IPv6 Address: 2001:db8:7777:10::3

```
C:\Users\Administrator>nslookup
Default Server: group7.com
Address: 2001:db8:7777:10::3

> group7.com
Server: group7.com
Address: 2001:db8:7777:10::3

Name:   group7.com
Addresses: 2001:db8:7777:10:9878:3c40:fa9b:80b4
           2001:db8:7777:10::3
           2001:db8:7777:20::3
           192.168.10.3
           192.168.20.3

> 2001:db8:7777:20::3
Server: group7.com
Address: 2001:db8:7777:10::3

Name:   ns2.group7.com
Address: 2001:db8:7777:20::3

> 2001:db8:7777:10::3
Server: group7.com
Address: 2001:db8:7777:10::3

Name:   group7.com
Address: 2001:db8:7777:10::3

> 192.168.10.3
Server: group7.com
Address: 2001:db8:7777:10::3

Name:   winsrv.group7.com
Address: 192.168.10.3

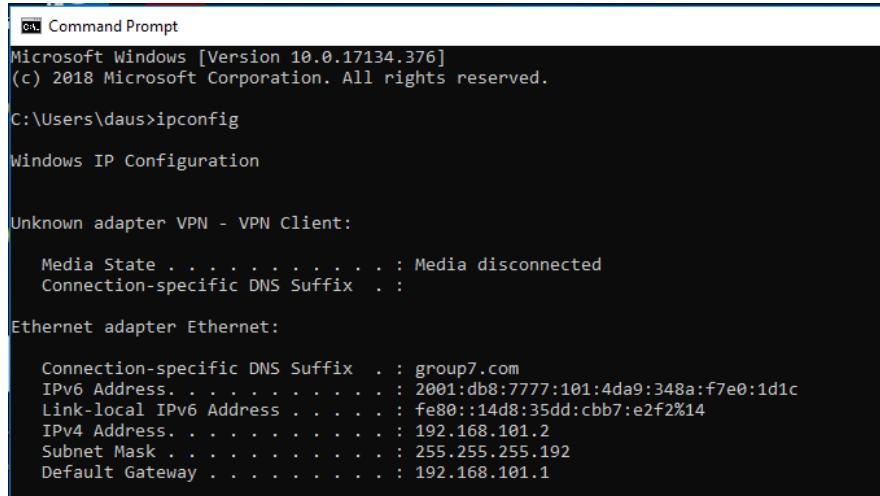
> 192.168.20.3
Server: group7.com
Address: 2001:db8:7777:10::3

Name:   ns2.group7.com
Address: 192.168.20.3
```

Figure 6. 1 : nslookup IPv4 and IPv6

6.2.2 DHCP (IPv4)

Testing for DHCP is done by using the command prompt from the client by entering “ipconfig”. The function of this command is to displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. From all the information displayed, focus on the IPv6 address and DHCP enabled. The IP should correspond to what has been set for client IP address and the DHCP Enabled should be yes.



```
Windows Command Prompt
Microsoft Windows [Version 10.0.17134.376]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\daus>ipconfig

Windows IP Configuration

Unknown adapter VPN - VPN Client:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Ethernet adapter Ethernet:
  Connection-specific DNS Suffix . : group7.com
  IPv6 Address . . . . . : 2001:db8:7777:101:4da9:348a:f7e0:1d1c
  Link-local IPv6 Address . . . . : fe80::14d8:35dd:cbb7:e2f2%14
  IPv4 Address . . . . . : 192.168.101.2
  Subnet Mask . . . . . : 255.255.255.192
  Default Gateway . . . . . : 192.168.101.1
```

Figure 6. 2 : Ipconfig

6.2.3 DHCP (IPv6)

Testing for DHCP is done by using the command prompt from the client by entering “ipconfig”. The function of this command is to displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. From all the information displayed, focus on the IPv6 address and DHCP enabled. The IP should correspond to what has been set for client IP address and the DHCP Enabled should be yes.

```
Connection-specific DNS Suffix . : group7.com
IPv6 Address . . . . . : 2001:db8:7777:101:4da9:348a:f7e0:1d1c
Link-local IPv6 Address . . . . . : fe80::14d8:35dd:cbb7:e2f2%14
IPv4 Address . . . . . : 192.168.101.2
Subnet Mask . . . . . : 255.255.255.192
Default Gateway . . . . . : 192.168.101.1
```

Figure 6. 3 : Show ipconfig

6.2.4 Inter VLAN and VLSM addressing

Step 1: Testing connection by ping Router using command “**ping 192.168.5.1**”.

```
[g7@fedora-group7-com ~]$ ping 192.168.5.1
PING 192.168.5.1 (192.168.5.1) 56(84) bytes of data.
64 bytes from 192.168.5.1: icmp_seq=1 ttl=255 time=0.513 ms
64 bytes from 192.168.5.1: icmp_seq=2 ttl=255 time=0.660 ms
64 bytes from 192.168.5.1: icmp_seq=3 ttl=255 time=0.680 ms
64 bytes from 192.168.5.1: icmp_seq=4 ttl=255 time=0.650 ms
64 bytes from 192.168.5.1: icmp_seq=5 ttl=255 time=0.651 ms
^C
```

Figure 6. 4 : Command prompt fedora

Step 2: Testing connection by ping Windows Server using command “**ping 192.168.10.3**”.

```
[g7@fedora-group7-com ~]$ ping 192.168.10.3
PING 192.168.10.3 (192.168.10.3) 56(84) bytes of data.
64 bytes from 192.168.10.3: icmp_seq=1 ttl=127 time=0.996 ms
64 bytes from 192.168.10.3: icmp_seq=2 ttl=127 time=1.13 ms
64 bytes from 192.168.10.3: icmp_seq=3 ttl=127 time=1.08 ms
64 bytes from 192.168.10.3: icmp_seq=4 ttl=127 time=0.936 ms
64 bytes from 192.168.10.3: icmp_seq=5 ttl=127 time=1.05 ms
^C
--- 192.168.10.3 ping statistics ---
```

Figure 6. 5 : Command prompt fedora

Step 3: Testing connection by ping Client using command “**ping 192.168.101.2**”.

```
[g7@fedora-group7-com ~]$ ping 192.168.101.2
PING 192.168.101.2 (192.168.101.2) 56(84) bytes of data.
64 bytes from 192.168.101.2: icmp_seq=1 ttl=127 time=0.636 ms
64 bytes from 192.168.101.2: icmp_seq=2 ttl=127 time=0.731 ms
64 bytes from 192.168.101.2: icmp_seq=3 ttl=127 time=0.700 ms
64 bytes from 192.168.101.2: icmp_seq=4 ttl=127 time=0.789 ms
64 bytes from 192.168.101.2: icmp_seq=5 ttl=127 time=0.677 ms
64 bytes from 192.168.101.2: icmp_seq=6 ttl=127 time=0.818 ms
64 bytes from 192.168.101.2: icmp_seq=7 ttl=127 time=0.705 ms
64 bytes from 192.168.101.2: icmp_seq=8 ttl=127 time=0.671 ms
64 bytes from 192.168.101.2: icmp_seq=9 ttl=127 time=0.782 ms
64 bytes from 192.168.101.2: icmp_seq=10 ttl=127 time=0.820 ms
64 bytes from 192.168.101.2: icmp_seq=11 ttl=127 time=0.722 ms
^C
--- 192.168.101.2 ping statistics ---
```

Figure 6. 6 : Command prompt fedora

6.2.5 Routing & NAT

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

```
Group7-RT#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
tcp 200.200.201.4:50550 192.168.10.3:50550 200.200.201.8:22  200.200.201.8:22
--- 200.200.201.4      192.168.10.3      ---              ---
--- 200.200.201.5      192.168.20.3      ---              ---
--- 200.200.201.6      192.168.30.3      ---              ---
icmp 200.200.201.1:1   192.168.101.2:1    200.200.201.10:1  200.200.201.10:1
```

Figure 6. 7 : NAT mapping.

Step 2: Testing connection by ping public ip neighbour using command “*ping <ip address>*”.

```
Group7-RT#ping 200.200.201.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.200.201.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
Group7-RT#ping 200.200.201.9
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.200.201.9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Group7-RT#
```

Figure 6. 8 : Ping public ip address neighbour from Router.

6.2.6 Active Directory

Active Directory (AD)

Active Directory is not specifically tested as it is not a service required but was created to be a baseline for supporting several services such as user authentication by using radius server, user authentication and authorization window authentication for server hardening and integrate AS with Linux Server. Since these services were tested successfully, AD was running smoothly.

GPO

Testing for public user that we have created two-group policy for public users which include the following users (Ali and Saleh). So, to do the testing

Step 1: log on from **Saleh** user.

Step 2: Open **command prompt**

```
C:\WINDOWS\system32>gpresult /r
Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© 2018 Microsoft Corporation. All rights reserved.

Created on 7/12/2018 at 11:31:07 AM

RSOP data for GROUP7\saleh on DESKTOP-B27D93U : Logging Mode
-----
OS Configuration: Member Workstation
OS Version: 10.0.17134
Site Name: N/A
Roaming Profile: N/A
Local Profile: C:\Users\saleh
Connected over a slow link?: No

USER SETTINGS
-----
CN=Saleh,OU=public,DC=group7,DC=com
Last time Group Policy was applied: 7/12/2018 at 11:29:56 AM
Group Policy was applied from: winsrv.group7.com
Group Policy slow link threshold: 500 kbps
Domain Name: GROUP7
Domain Type: Windows 2008 or later

Applied Group Policy Objects
-----
public
The following GPOs were not applied because they were filtered out
-----
Local Group Policy
Filtering: Not Applied (Empty)

The user is a part of the following security groups
-----
Domain Users
Everyone
BUILTIN\Users
NT AUTHORITY\INTERACTIVE
CONSOLE\LOGON
```

Step 3: Enter this command to check the group policy of Saleh **gpresult /r**

Figure 6. 9 : Show that our group policy is applied on Saleh user

Step 4: Run snipping tool

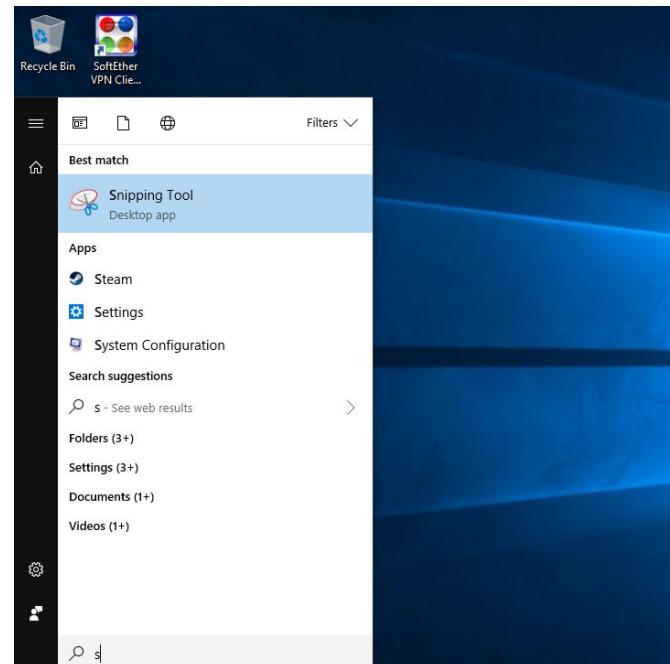


Figure 6. 10 : Run Snipping Tool

Step 5: then an error window will show that cannot use this tool **software restriction policy**.

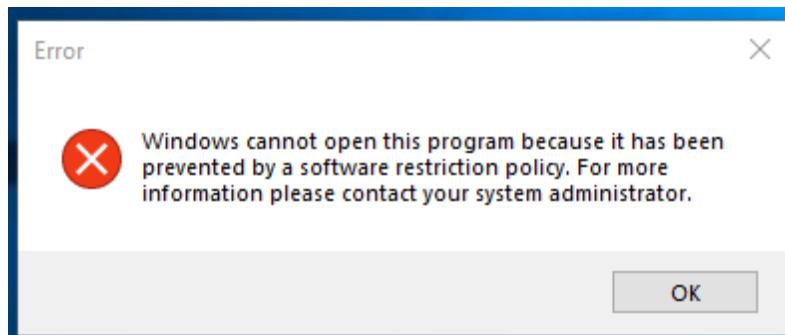


Figure 6. 11 : Error window for disable sniping tool to the user.

6.2.7 Proxy Server

Step 1: At client PC, open **Browser** and click **Setting**, then click **Open proxy setting**.

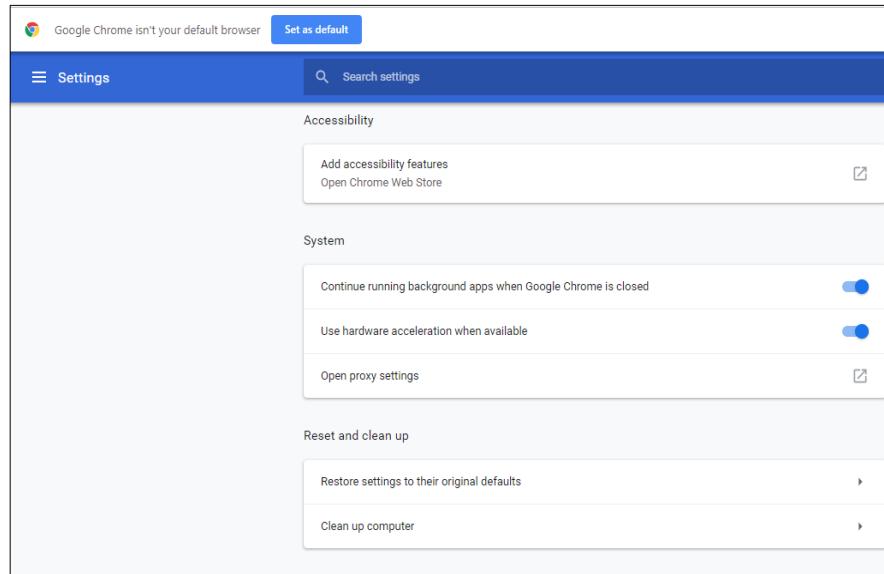


Figure 6. 12 : Browser's setting

Step 2: After that, go to **Connections** and click **LAN settings**.

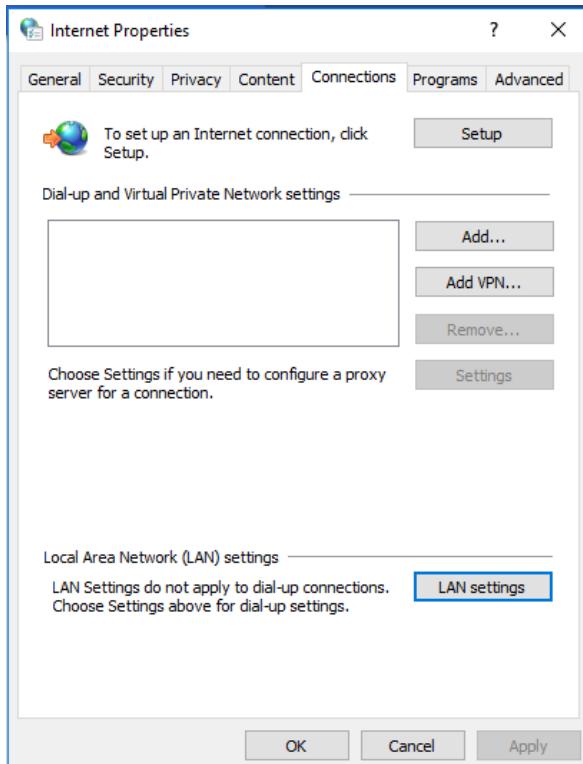


Figure 6. 13 : LAN settings

Step 3: In the **Connection Settings**, click on the “**Manual proxy configuration**”. On the **HTTP Proxy**, enter the IP address of the Proxy Server and assign the port that Proxy will be listen. Then, tick on “**Use this proxy server for all protocols**” and click button **OK**.

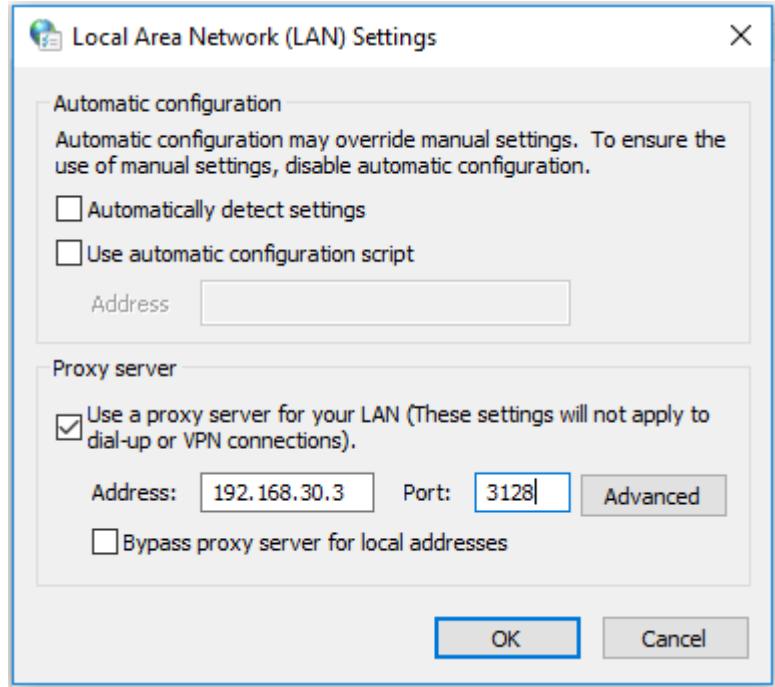


Figure 6. 14 : Insert IP Address

Step 4: Open web browser and access the domain of **www.facebook.com** and **www.instagram.com**. Both sites have been blocked in Proxy Server and the output is client cannot access the sites.

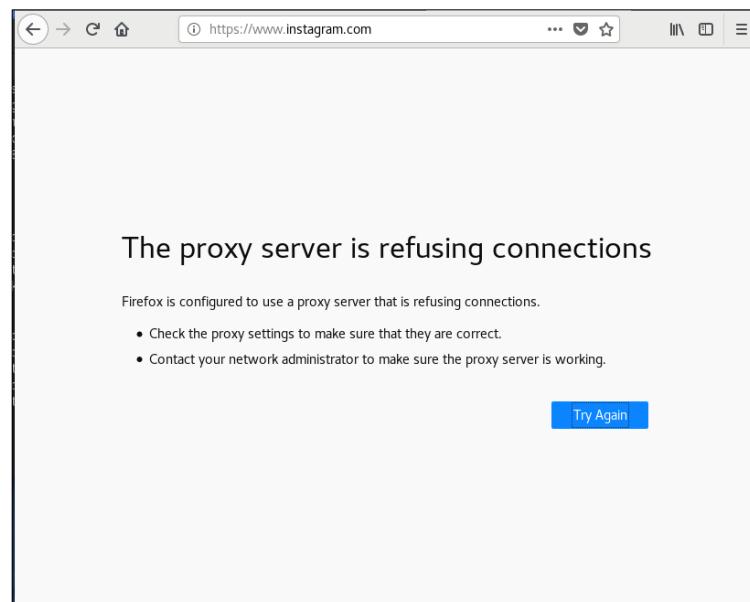
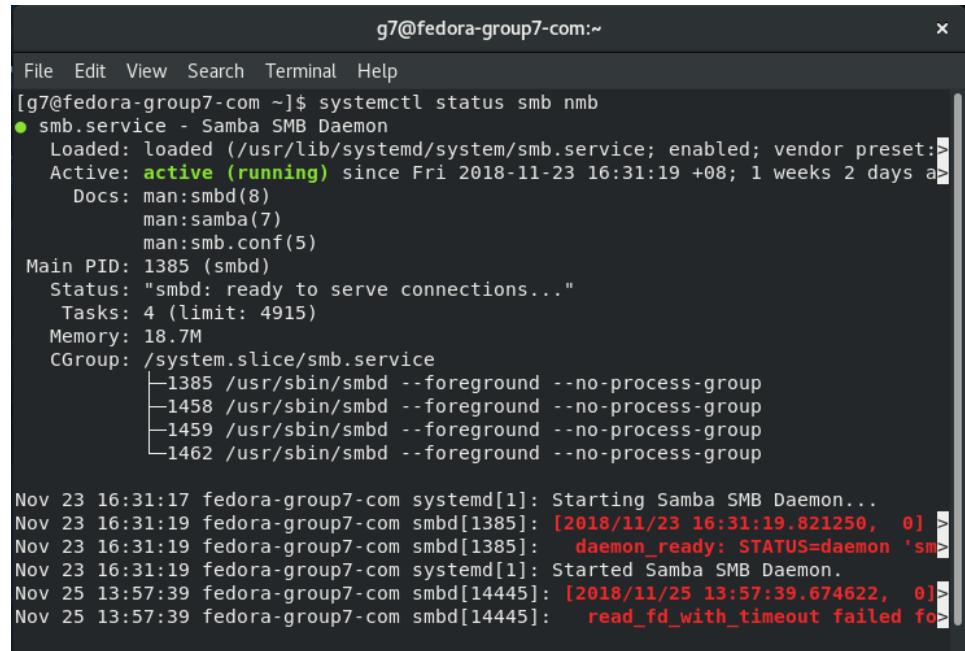


Figure 6. 15 : Connection refuse

6.2.8 Samba

Step 1: Check status smb nmb whether it's running or not



```
g7@fedora-group7-com:~
```

```
File Edit View Search Terminal Help
[g7@fedora-group7-com ~]$ systemctl status smb nmb
● smb.service - Samba SMB Daemon
  Loaded: loaded (/usr/lib/systemd/system/smb.service; enabled; vendor preset:disabled)
  Active: active (running) since Fri 2018-11-23 16:31:19 +08; 1 weeks 2 days ago
    Docs: man:smbd(8)
          man:samba(7)
          man:smb.conf(5)
  Main PID: 1385 (smbd)
    Status: "smbd: ready to serve connections..."
      Tasks: 4 (limit: 4915)
     Memory: 18.7M
    CGroup: /system.slice/smb.service
            ├─1385 /usr/sbin/smbd --foreground --no-process-group
            ├─1458 /usr/sbin/smbd --foreground --no-process-group
            ├─1459 /usr/sbin/smbd --foreground --no-process-group
            └─1462 /usr/sbin/smbd --foreground --no-process-group

Nov 23 16:31:17 fedora-group7-com systemd[1]: Starting Samba SMB Daemon...
Nov 23 16:31:19 fedora-group7-com smbd[1385]: [2018/11/23 16:31:19.821250,  0] >
Nov 23 16:31:19 fedora-group7-com smbd[1385]:   daemon_ready: STATUS=daemon 'sm...
Nov 23 16:31:19 fedora-group7-com systemd[1]: Started Samba SMB Daemon.
Nov 25 13:57:39 fedora-group7-com smbd[14445]: [2018/11/25 13:57:39.674622,  0]>
Nov 25 13:57:39 fedora-group7-com smbd[14445]:   read_fd_with_timeout failed fo...
```

Figure 6. 16 : Check status smb nmb

Step 2: Testing samba by sharing file in var/lib/share

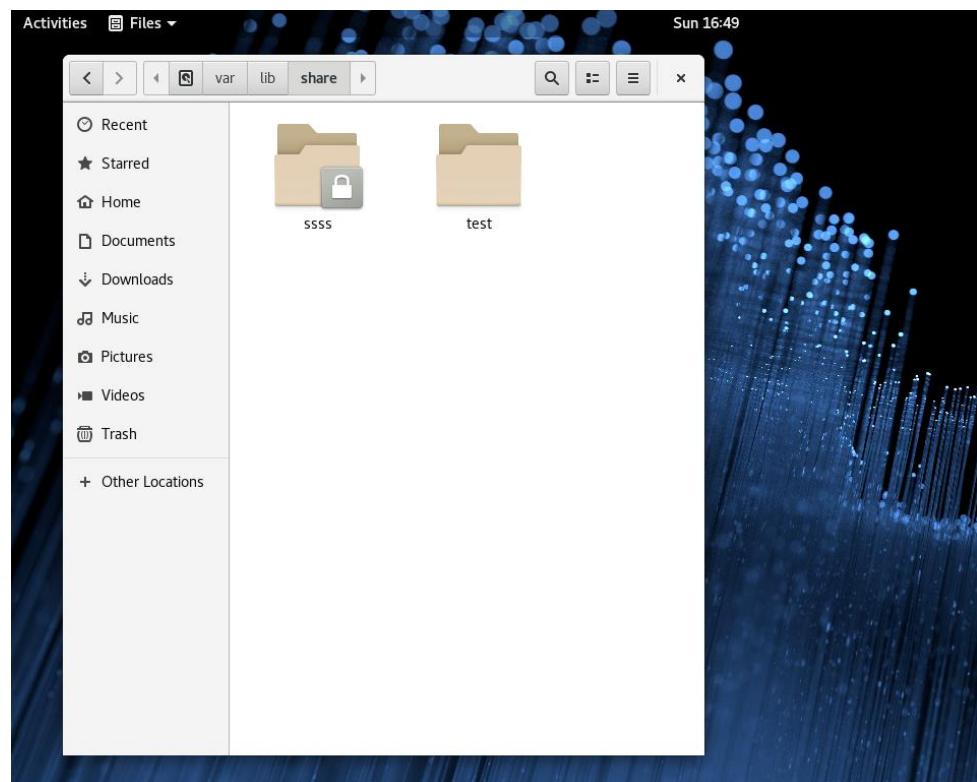


Figure 6. 17 : Testing samba by sharing file

Step 3: Enter IP address 192.168.30.3 in client pc and see the shared folder

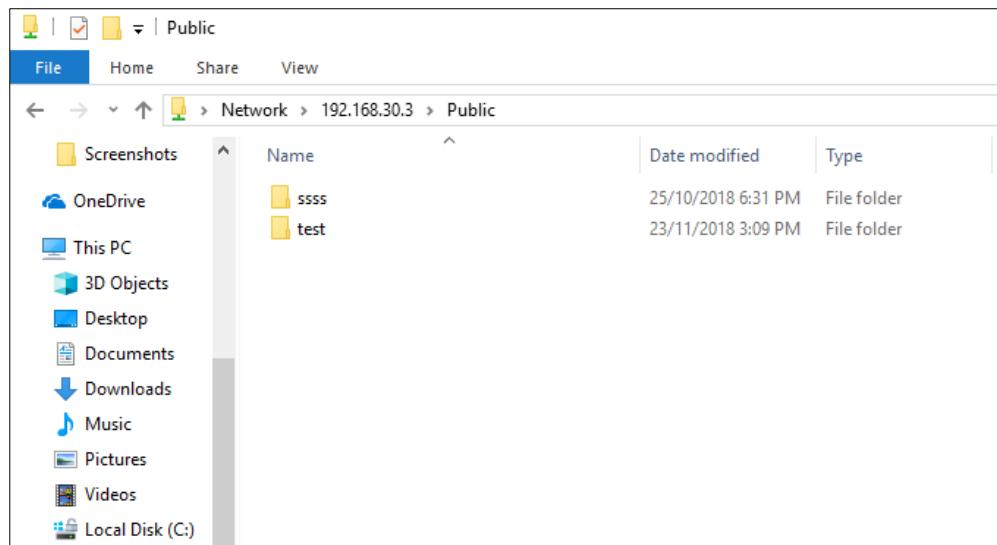


Figure 6. 18 : Shared file in client pc

6.2.9 Network Management System

Step 1: Open `localhost/nagios/` at browser to open homepage nagios.

The screenshot shows the Nagios Core homepage. The left sidebar contains a navigation menu with sections like General, Current Status, Reports, and System. The main content area features the Nagios logo and version information (Version 4.4.2, August 16, 2018). It includes sections for 'Get Started' (with bullet points about monitoring infrastructure), 'Quick Links' (with links to Nagios Library, Nagios Lab, Nagios Exchange, Nagios Support, Nagios.com, and Nagios.org), 'Latest News' (empty), and 'Don't Miss...' (empty). A copyright notice at the bottom states: 'Copyright © 2010-2018 Nagios Core Development Team and Community Contributors. Copyright © 1999-2009 Ethan Galstad. See the THANKS file for more information on contributors.' and 'Nagios Core is licensed under the GNU General Public License and is provided AS IS with NO WARRANTY OF ANY KIND, INCLUDING THE WARRANTY OF MERCHANTABILITY.'

Figure 6. 19 : Nagios core homepage.

Step 2: Click on ‘hosts’ on the left panel and newly added client will be visible.

The screenshot shows the Nagios host page. The left sidebar has the same navigation menu as the homepage. The main content area displays 'Host Status Details For All Host Groups'. It shows a table with columns: Host, Status, Last Check, Duration, and Status Information. There are five hosts listed: fedora, localhost, router, switch, and windows. All hosts are marked as UP. The status information for each host includes PING OK - Packet loss = 0%, RTA values ranging from 0.07 ms to 1.05 ms. Above the table, there are two summary boxes: 'Host Status Totals' (Up: 5, Down: 0, Unreachable: 0, Pending: 0) and 'Service Status Totals' (Ok: 30, Warning: 0, Unknown: 0, Critical: 3, Pending: 0).

Figure 6. 20 : Nagios host page.

Step 3: Click on ‘service’ on the left panel and will display all service status in each server.

The screenshot shows the Nagios web interface at localhost/nagios/. The left sidebar includes sections for General, Home, Documentation, Current Status (with links to Tactical Overview Map, Hosts, Services, Host Groups, Service Groups, Problems, and System), Reports (Availability, Trends, Alerts, History, Summary, Histogram, Notifications, Event Log), and System (Comments, Downtime, Process Info, Performance Info). The main content area displays 'Service Status Details For All Hosts' with a limit of 100 results. It shows a table with columns: Host, Service, Status, Last Check, Duration, Attempt, and Status Information. The table lists services for fedora, localhost, router, switch, and windows hosts, including PING, SSH, and Swap Usage services. Most services are in the 'OK' state, while some like PING and SSH on the windows host are in 'CRITICAL' state.

Figure 6. 21 : Services on Nagios has been installed to monitor.

This screenshot is identical to Figure 6.21 but focuses on the windows host. The table in the main content area shows detailed service status information for the windows host, including Current Load, Current Users, HTTP, PING, Root Partition, SSH, Swap Usage, and Total Processes. The SSH service is listed as 'CRITICAL' due to a socket timeout error.

Figure 6. 22 : Extend for nagios service page.

Step 4: Click on ‘histogram’ on the left panel and select host or service.

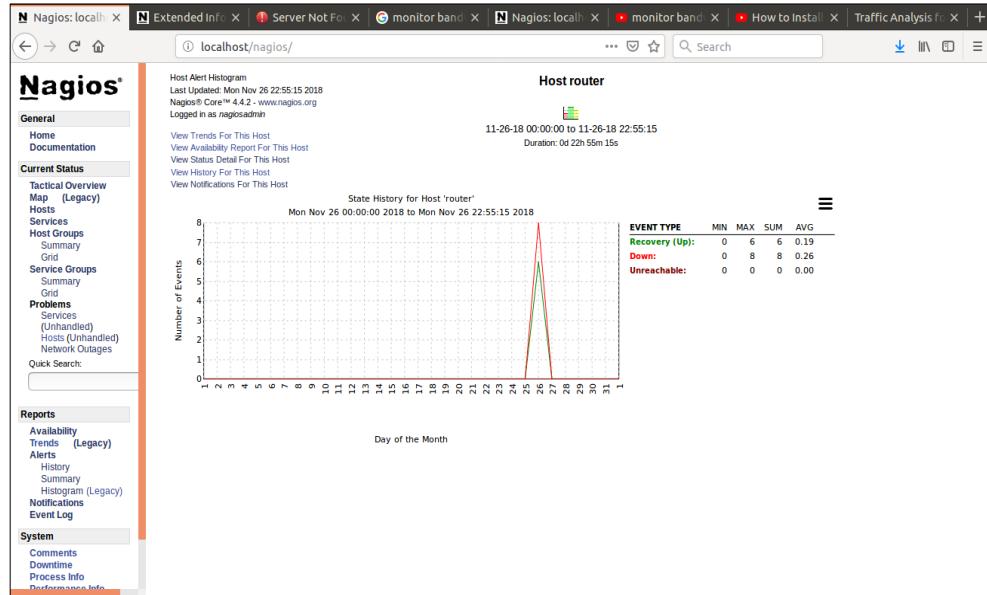


Figure 6. 23 : Router histogram

Step 5: Click on ‘map’ on the left panel to show logical monitoring map on Nagios.

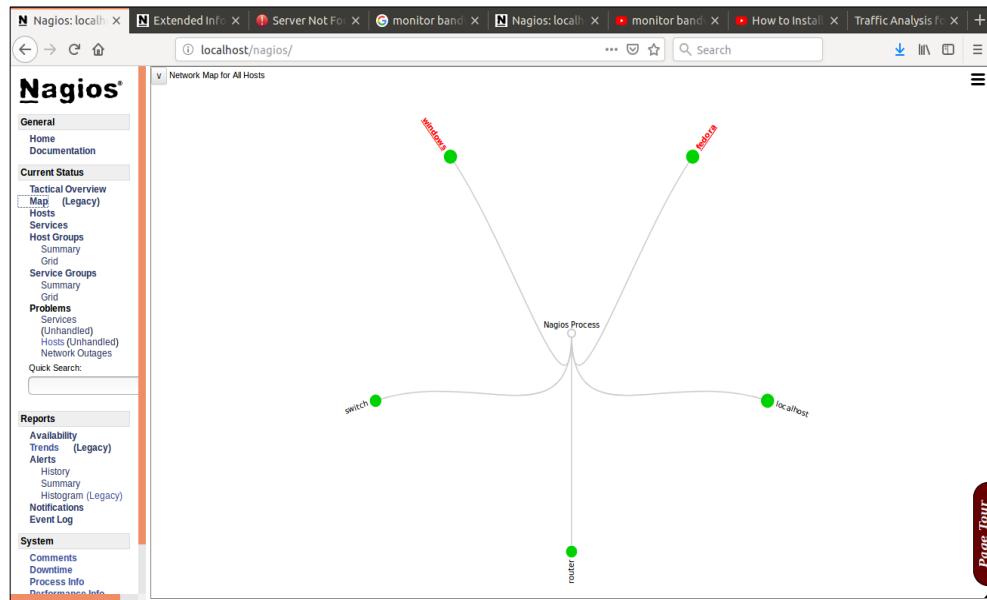
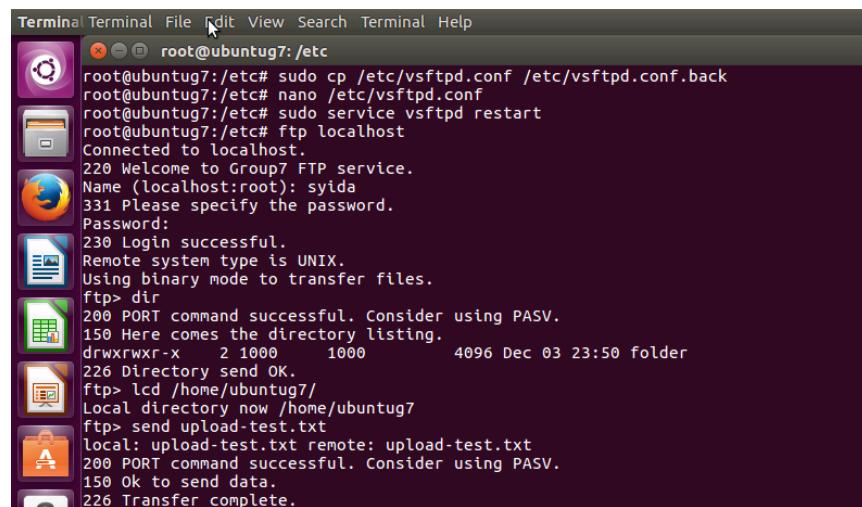


Figure 6. 24 : Nagios map.

6.2.10 Server Virtualization

Testing FTP

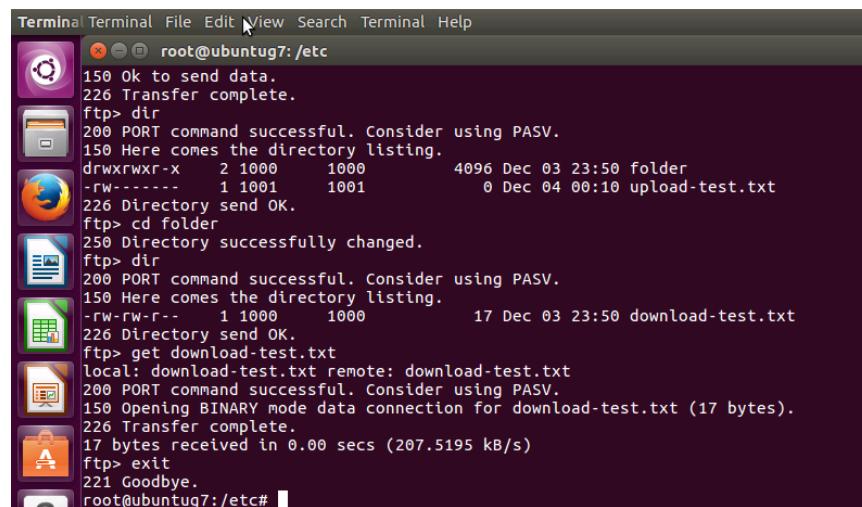
Step 1: After ftp user successfully login, enter home directory by using command “lcd /home/ubuntu7” and then send the document text file.



```
Terminal Terminal File Edit View Search Terminal Help
root@ubuntug7:/etc
root@ubuntug7:/etc# sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.back
root@ubuntug7:/etc# nano /etc/vsftpd.conf
root@ubuntug7:/etc# sudo service vsftpd restart
root@ubuntug7:/etc# ftp localhost
Connected to localhost.
220 Welcome to Group7 FTP service.
Name (localhost:root): syida
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxr-x 2 1000 1000 4096 Dec 03 23:50 folder
226 Directory send OK.
ftp> lcd /home/ubuntu7/
Local directory now /home/ubuntu7
ftp> send upload-test.txt
local: upload-test.txt remote: upload-test.txt
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
```

Figure 6. 25 : Send document text file

Step 2: Next, enter home directory and then get the document text file.



```
Terminal Terminal File Edit View Search Terminal Help
root@ubuntug7:/etc
150 Ok to send data.
226 Transfer complete.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxr-x 2 1000 1000 4096 Dec 03 23:50 folder
-rw----- 1 1001 1001 0 Dec 04 00:10 upload-test.txt
226 Directory send OK.
ftp> cd folder
250 Directory successfully changed.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r-- 1 1000 1000 17 Dec 03 23:50 download-test.txt
226 Directory send OK.
ftp> get download-test.txt
local: download-test.txt remote: download-test.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for download-test.txt (17 bytes).
17 bytes received in 0.00 secs (207.5195 kB/s)
226 Transfer complete.
221 Goodbye.
root@ubuntug7:/etc#
```

Figure 6. 26 : Get document text file

Step 3: In home directory, you will see the document text file inside ftp-files folder transfer to home directory which means the send file transfer was successful.

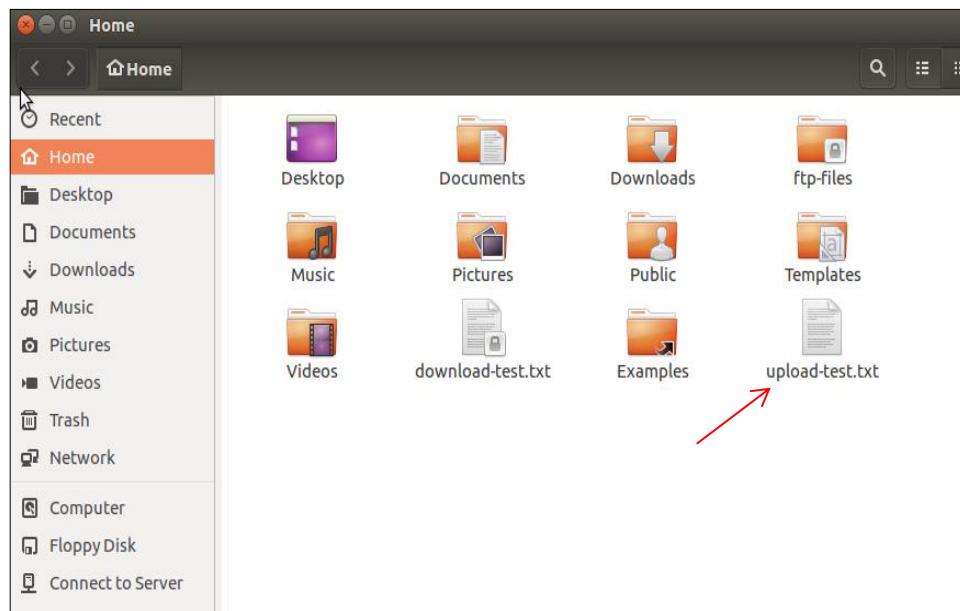


Figure 6. 27 : Files in home directory

Step 4: In ftp files that you have created at the beginning, you will see the document text file inside the folder in ftp-files folder in home directory which means the get file transfer was successful.

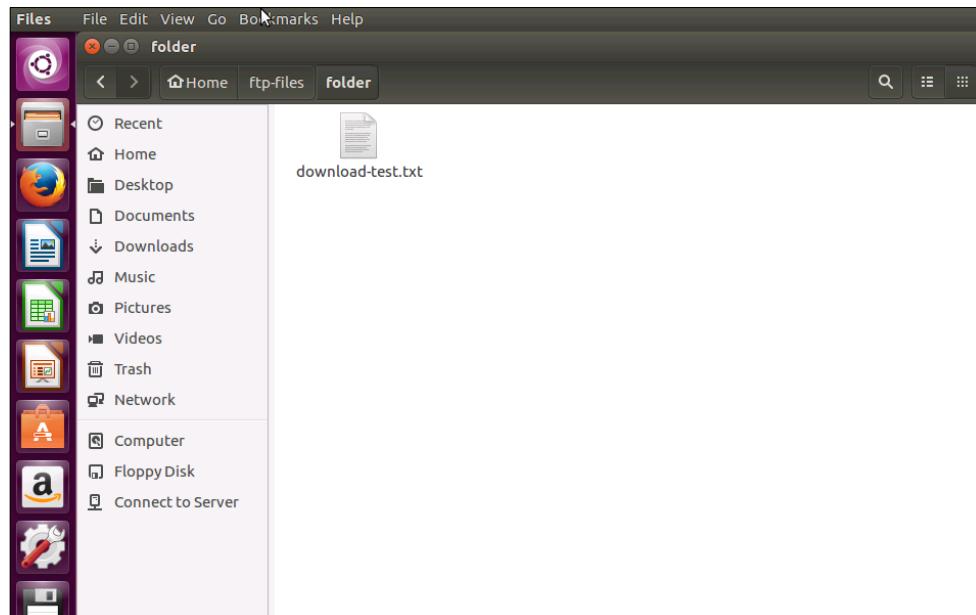
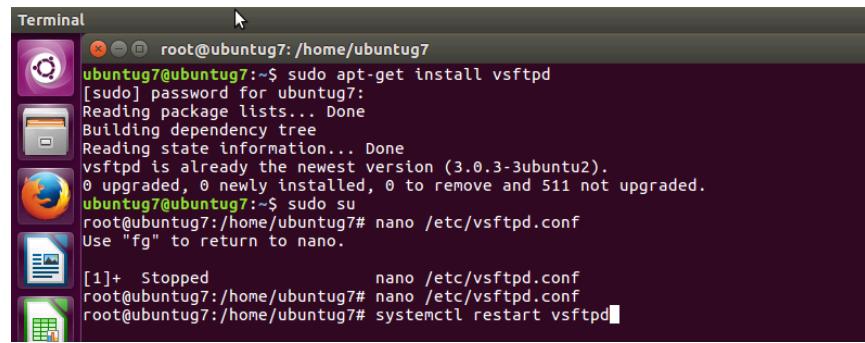


Figure 6. 28 : File text in folder in ftp file

Step 5: Restart vsftpd using command “systemctl restart vsftpd”



```
root@ubuntug7:~$ sudo apt-get install vsftpd
[sudo] password for ubuntug7:
Reading package lists... Done
Building dependency tree
Reading state information... Done
vsftpd is already the newest version (3.0.3-3ubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 511 not upgraded.
root@ubuntug7:~$ sudo su
root@ubuntug7:/home/ubuntug7# nano /etc/vsftpd.conf
Use "fg" to return to nano.

[1]+  Stopped                  nano /etc/vsftpd.conf
root@ubuntug7:/home/ubuntug7# nano /etc/vsftpd.conf
root@ubuntug7:/home/ubuntug7# systemctl restart vsftpd
```

Figure 6. 29 : Restart vsftpd

Step 6: Lastly, testing ftp by enter “ftp://192.168.10.4” in Mozilla Firefox.

The output as below:

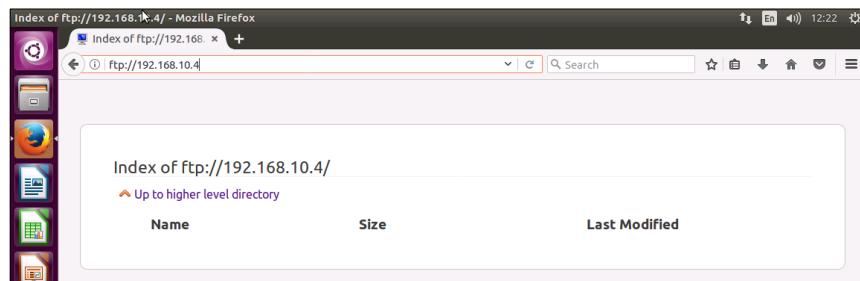


Figure 6. 30 : Testing ftp

Testing SFTP

Step 1: Testing sftp by using FileZilla by enter ip address 192.168.10.4

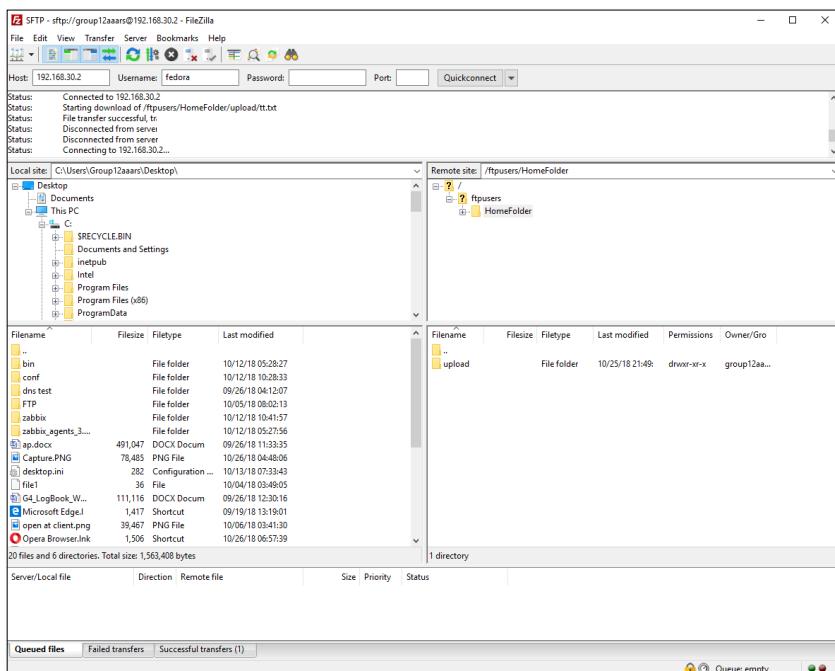


Figure 6. 31 : Test sftp in FileZilla

6.2.11 AAA (Authentication, Authorization, and Accounting) using Radius

Step 1: Open your putty to test your authentication.

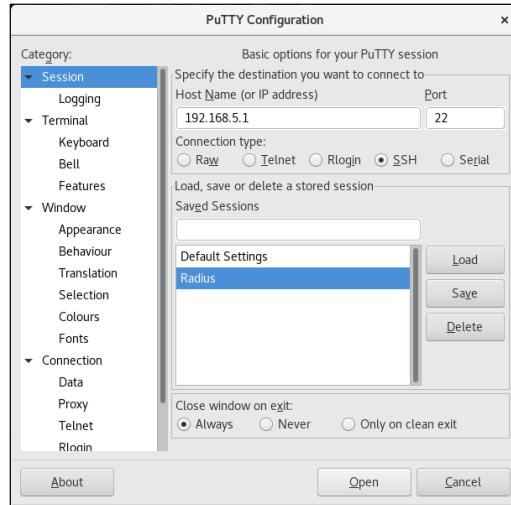


Figure 6. 32 : Putty configuration

Step 2: Then, enter router configuration by using AD user information (password and usernames). If the authentication passed, you have success configure your radius server. Then, insert command to show the privileges that you have insert.

```
192.168.5.1 - PuTTY
login as: G7daus
Using keyboard-interactive authentication.
Password:
Group7-RT#show priv
Current privilege level is 15
Group7-RT#
```

Figure 6. 33 : G7daus in groupadmin for AAA

```
192.168.5.1 - PuTTY
login as: G7nisa
Using keyboard-interactive authentication.
Password:
Group7-RT#show priv
Current privilege level is 10
Group7-RT#
```

Figure 6. 34 : G7nisa in groupuser for AAA

Step 3: Go to Server Manager, click Network Policy Server and then click on Properties to view the log files.

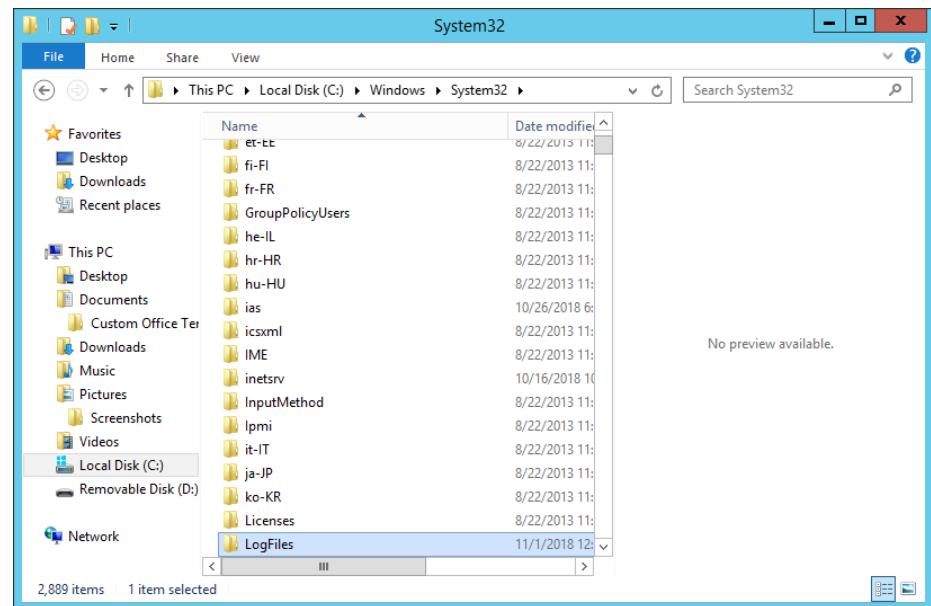


Figure 6. 35 : In the system32

6.2.12 Access Control List (ACL)

Step 1: ACL testing is done using the command show ip access-list in the router. This will show the output of how many matches found through the denied and permitted port. This then confirms that the ACL is successfully configured.

Step 2: Number of the matches shows there are packets was passing through the permitted services via interface G0/1.

```
access-list 1 permit 192.168.100.0 0.0.0.15
access-list 122 deny  tcp any host 200.200.200.4 eq 443
access-list 122 deny  tcp any host 200.200.200.6. eq ftp-data
access-list 122 deny  tcp any host 200.200.200.6. eq ftp
access-list 122 permit ip any any
```

Figure 6. 36 : ACL Configuration

Step 3: Before ACL been configured in Group 4 public ip address (200.200.200.6), Group 8 public ip address can access Group 7 folder using file sharing. (File Transfer Protocol).

```
group8@group8:~$ sftp sftp7@200.200.201.6
sftp7@200.200.201.6's password:

Permission denied, please try again.
sftp7@200.200.201.6's password:
Permission denied, please try again.
sftp7@200.200.201.6's password:
Connected to 200.200.201.6.
sftp> █
```

Figure 6. 37 : Before ACL Configuration

Step 4: After ACL has been configured on router, Group 8 public ip address cannot access Group 7 folder using file sharing (File Transfer Protocol).

```
group8@group8: ~
group8@group8:~$ sftp sftp7@200.200.201.6
ssh: connect to host 200.200.201.6 port 22: No route to host
Couldn't read packet: Connection reset by peer
group8@group8:~$ █
```

Figure 6. 38 After ACL Configuration

Step 5: Before ACL been configuredin Group 7 public ip address (200.200.200.6), Group 8 public ip address can access Group 7 secured web page. (HTTPS).



Figure 6. 39 : Before ACL Configuration

Step 6: After ACL been configured in Group 7 public ip address (200.200.200.6), Group 8 public ip address cannot access Group 7 secured web page. (HTTPS).

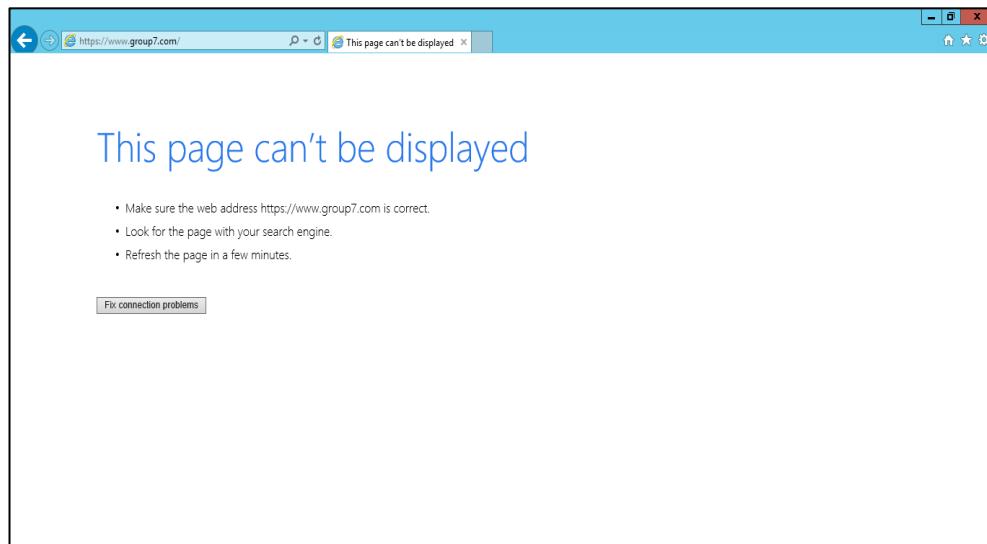


Figure 6. 40 : After ACL Configuration

6.2.13 Secured FTP

SSH File Transfer Protocol

Command Line

Step 1: Open the terminal in any server, type the command line ‘`sftp sftp7@192.168.30.3`’ to login. After insert the password, connection to SFTP server will be establish.

```
C:\Users\daus>sftp sftp7@192.168.30.3
sftp7@192.168.30.3's password:
Permission denied, please try again.
sftp7@192.168.30.3's password:
Connected to sftp7@192.168.30.3.
```

Figure 6. 41 : Establishing SFTP connection.

Step 2: Type the ‘`lpwd`’ to check local directory currently on. Using ‘`lcd`’ command to change the path.

```
sftp> lpwd
Local working directory: C:\Users\daus
sftp> pwd
Remote working directory: /
sftp> cd /files
Couldn't canonicalize: No such file or directory
sftp> cd /file
sftp> ls
Firefox Installer.exe    Microsoft Edge.lnk      jabba.txt
```

Figure 6. 42 : Checking local directory and inside the directory.

Step 3: Operation download from SFTP server to local machine by using ‘`get`’ and follow by files name.

```
sftp> get jabba.txt
Fetching /file/jabba.txt to jabba.txt
```

Figure 6. 43 : Downloading ‘jabba.txt’ file from SFTP server

Step 4: Operation upload from local machine to SFTP server by using ‘`put`’ and follow by files name.

```
sftp> put Sftp7Cuba.txt
Uploading Sftp7Cuba.txt to /file/Sftp7Cuba.txt
Sftp7Cuba.txt
```

Figure 6. 44 : Uploading ‘Sftp7Cuba.txt’ to SFTP server.

Step 5: Enter ‘exit’ to close SFTP connection.

```
sftp> exit
```

Figure 6. 45 : End the SFTP connection.

Filezilla

Step 1: Open filezilla at any terminal, enter host address, hostname, password and port. Click ‘Quicksearch’ to proceed.

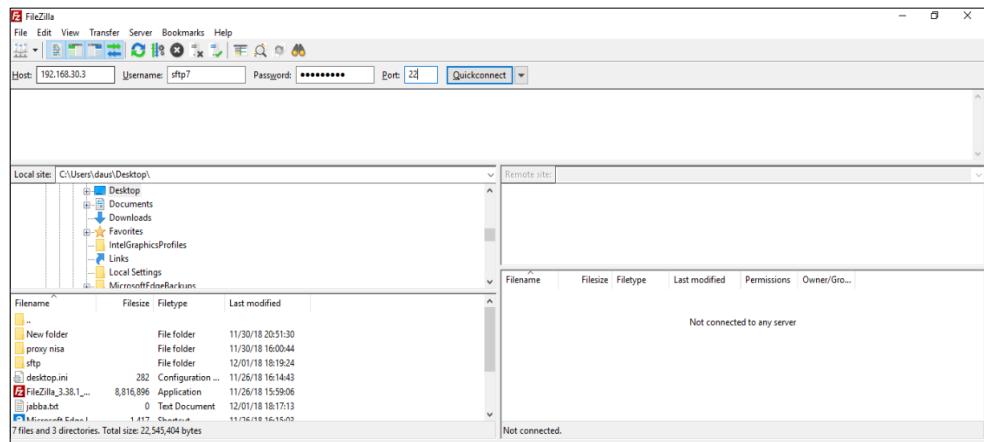


Figure 6. 46 : Establish connection using Filezilla.

Step 2: Select the local directory for the operation.

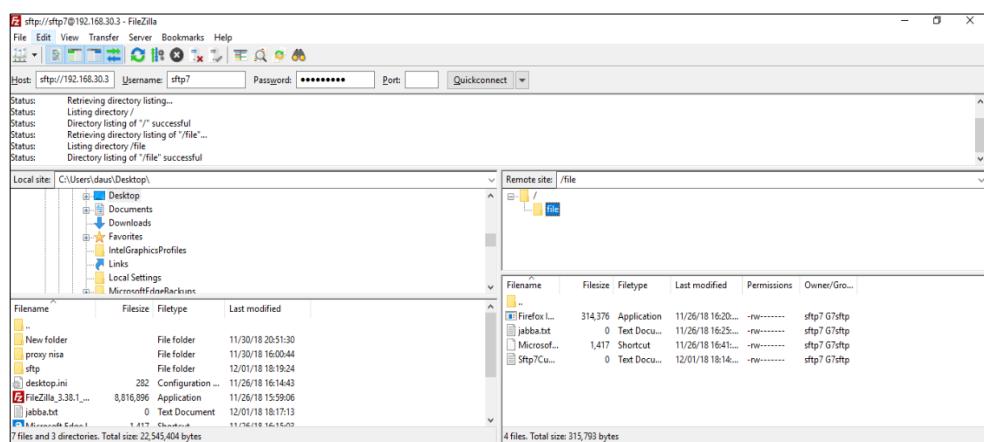


Figure 6. 47 : Local directory selected.

Step 3: Select files to download or upload, drag the files to opposite section.

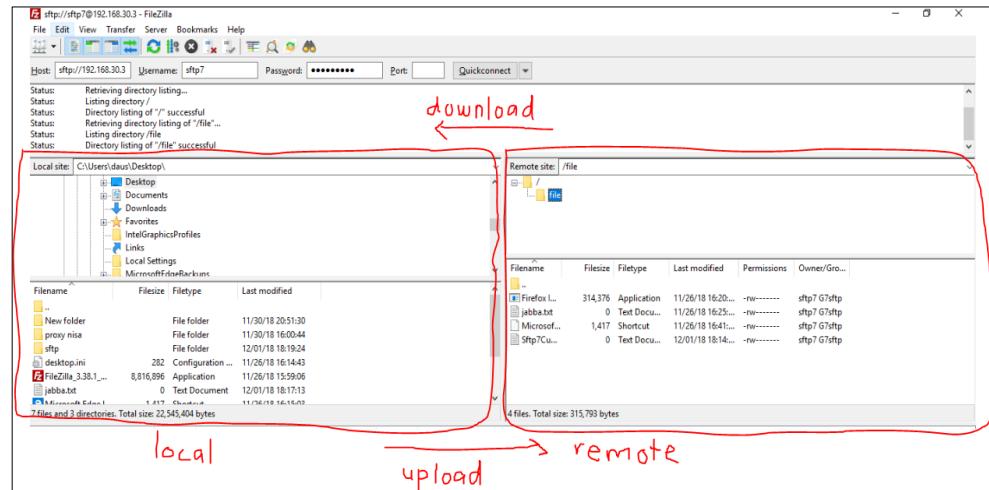


Figure 6. 48 : Upload and download operation using Filezilla.

6.2.14 Web, SSL & Virtual Hosting Linux Email Server

The web testing <http://www.group7.com>, <http://192.168.10.3>, <http://www.vhgroup7.com> and <http://www.group7.com> was successfully on three servers and client.



Figure 6. 49 : Web testing using domain name.

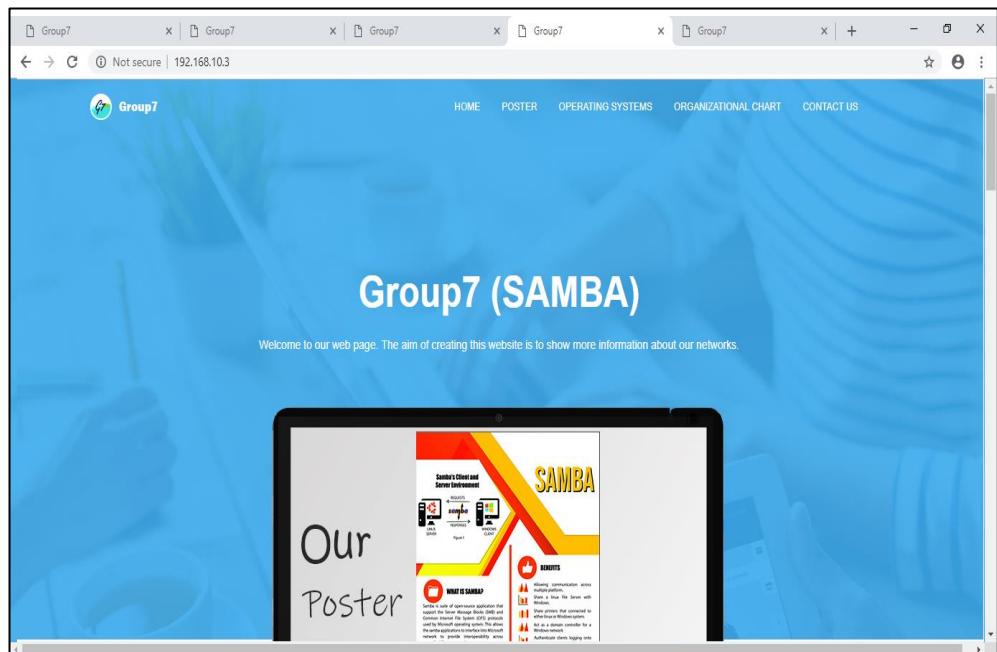


Figure 6. 50 : Web testing using IP Address.

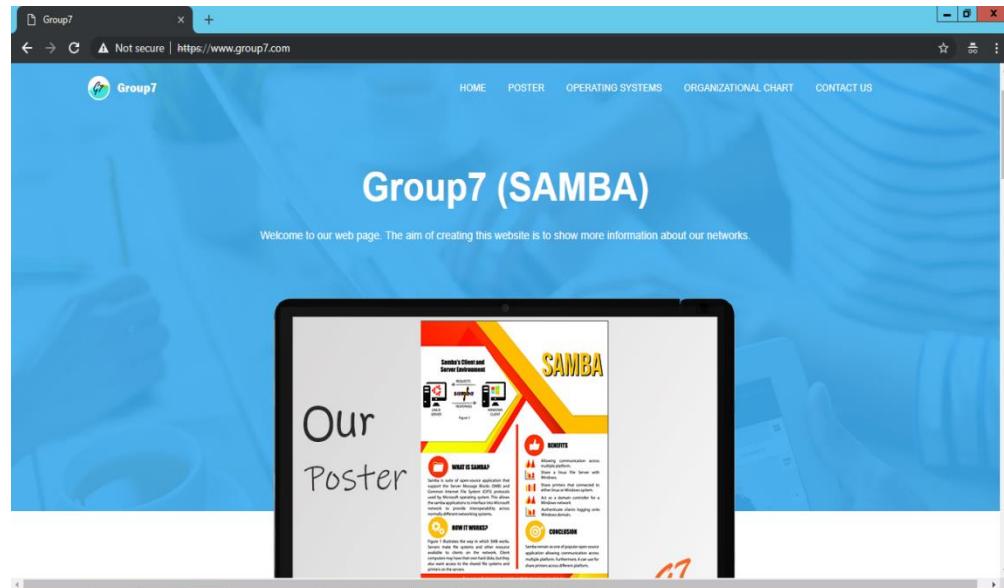


Figure 6. 51 : Testing Secure browser.

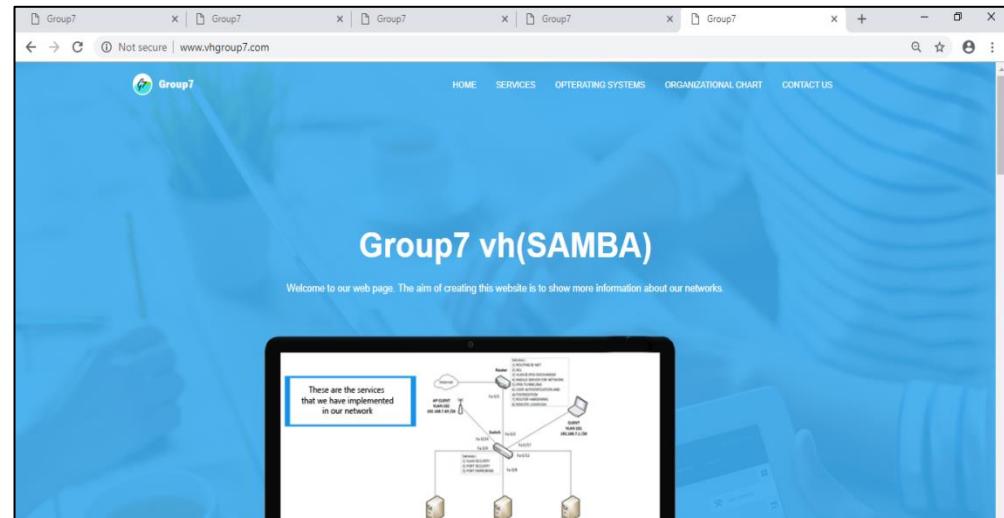


Figure 6. 52 : Testing virtual hosting web.

6.2.15 Linux Email Server

Step 1: Go to mail.group7.com to login insert name and password that already create

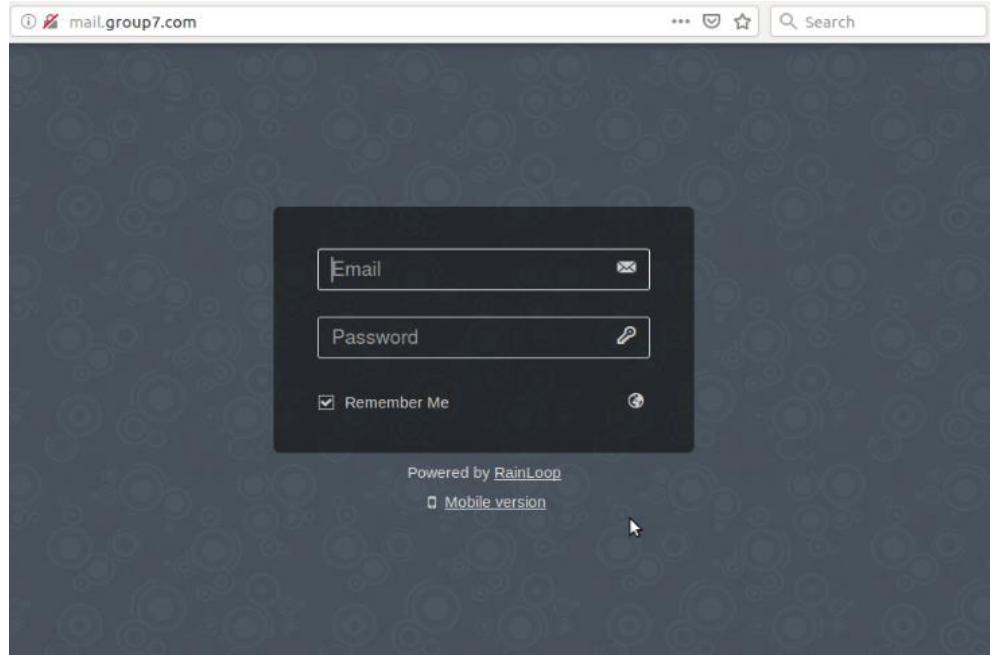


Figure 6. 53 : Login to RainLoop Email server

Step 2: Compose Email

To: fahmy@group7.com

From: daus@group7.com

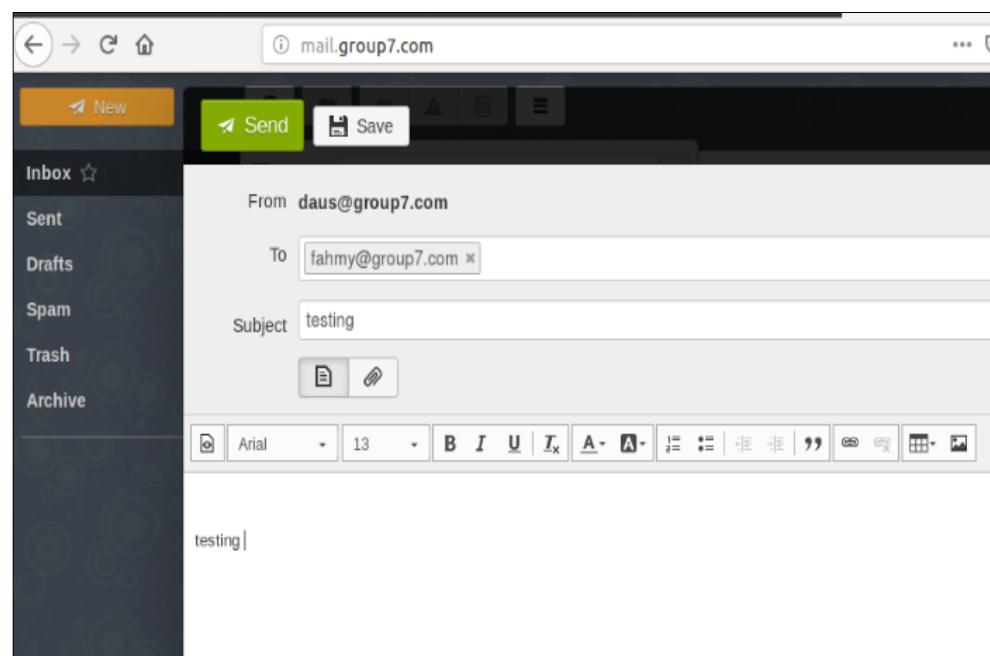


Figure 6. 54 : Compose email from RainLoop Email server

Step 3: Receive email to fahmy@group.com from daus@group7.com

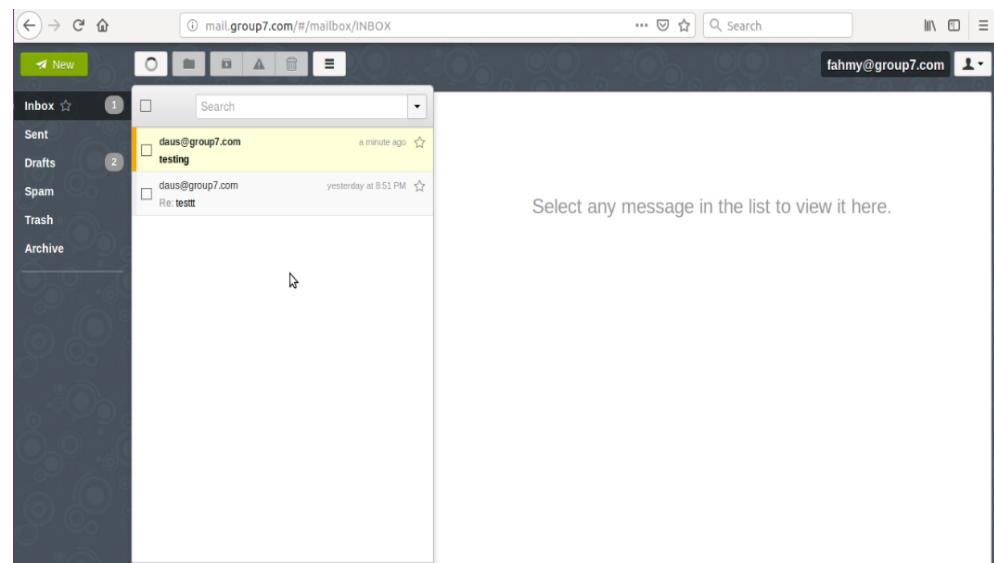


Figure 6. 55 : Receive email

6.2.16 IPv6 Web with IPv6 Tunneling

Step 1: Testing website using hostname www.ipv6webgroup7.com



Figure 6. 56 : Testing website using hostname

Step 2: Testing website using ip address

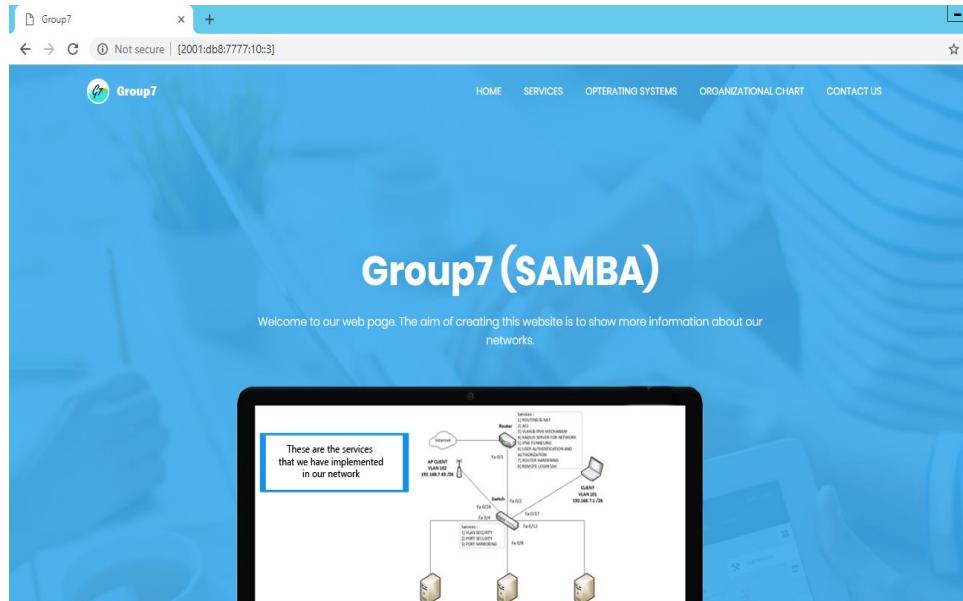


Figure 6. 57 : Testing website using Ipv6 address

Step 3: Open the browser at neighbour's pc and type

<http://ipv6webgroup7.com>



Figure 6. 58 : Website group7 in neighbour's group

6.2.17 Media streaming server

Step 1: Go to media streaming server website using localhost/32400 via browser, then login using the username.

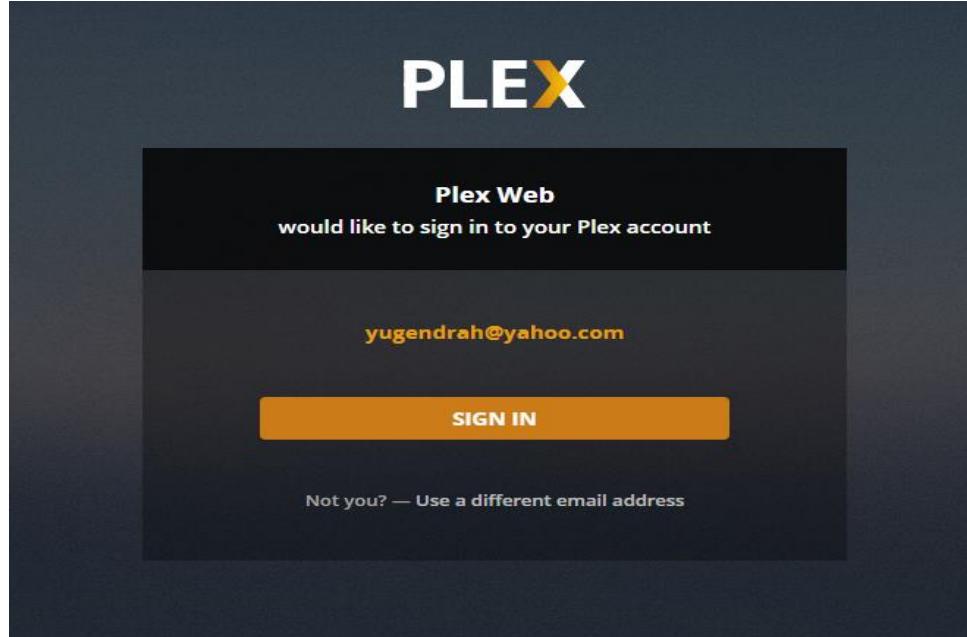


Figure 6. 59 : Login using the username

Step 2: Once login you can see the media file on the dashboard.

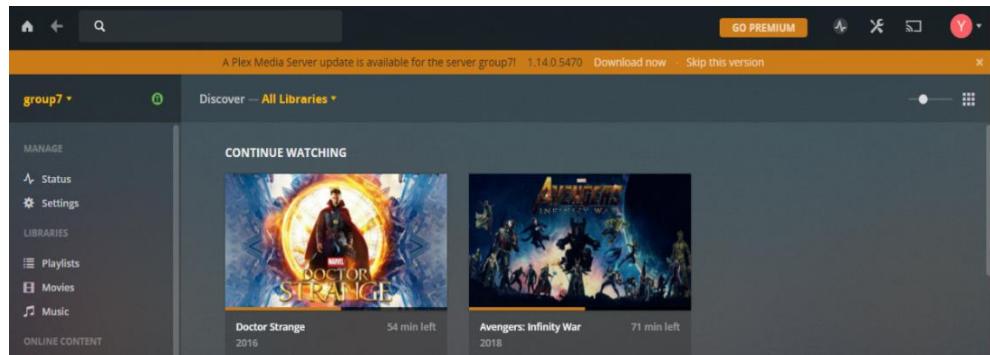


Figure 6. 60 : Plex dashboard

Step 3: Click the media file from library then it will play.

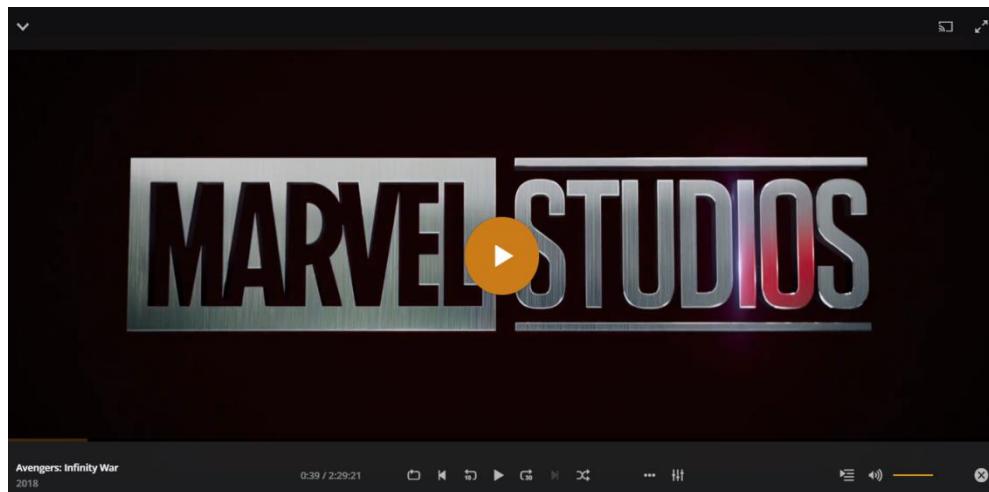


Figure 6. 61 : Media file is playing from client site

6.2.18 Cloud server

Step 1: Login to admin account and create several accounts for the cloud server.

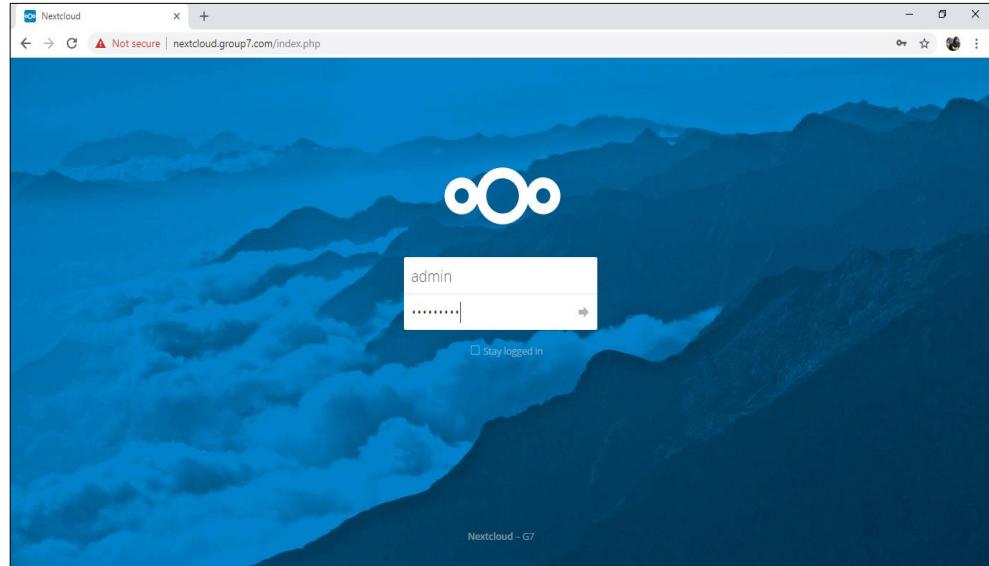


Figure 6. 62 : Nextcloud login page

Step 2: Create several accounts for the cloud server and create group to specify the department.

Users - Nextcloud						
		Username	Password	Groups	Create	
Everyone	5	A admin	admin	*****	admin	no group
Admins	1	F firdaus	firdaus	*****	Account Department	Account Department
Account Department	2	N nisa	nisa	*****	no group	IT Department
IT Department	1	R raihan	raihan	*****	IT Department	Account Department, IT De...
		S syazwani	syazwani	*****	Account Department	Unlimited

Figure 6. 63 : Nextcloud admin page

Step 3: Test login the nexcloud using account that has been created. Insert *firdaus* as the username and password.

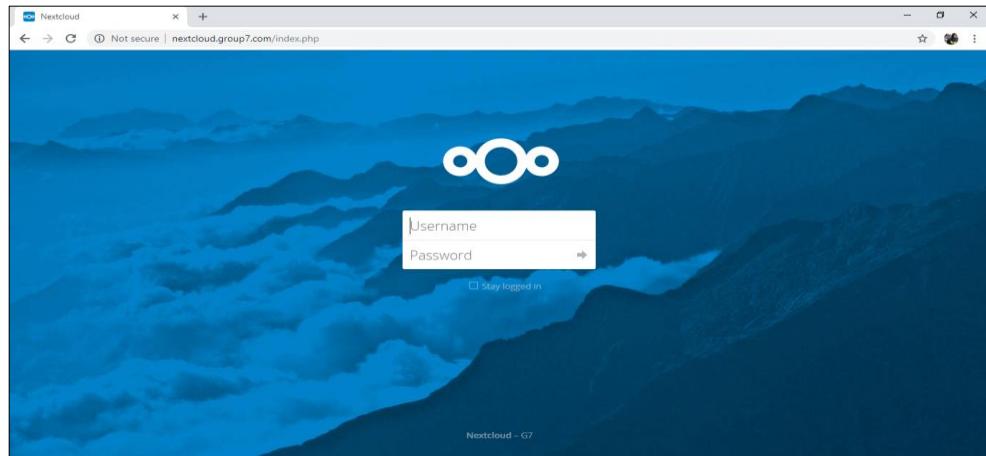


Figure 6. 64 : Nextcloud login page

Step 4: Insert the file and test download the file.

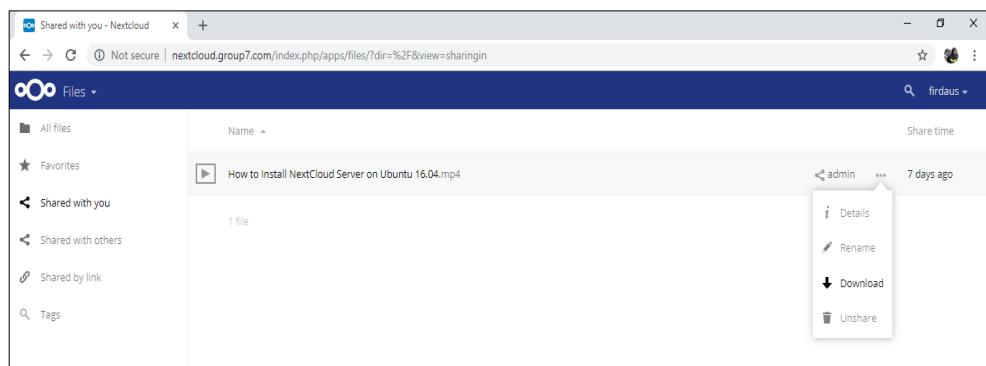


Figure 6. 65 : Upload and Download the file

Step 5: Play the video that has been uploaded.

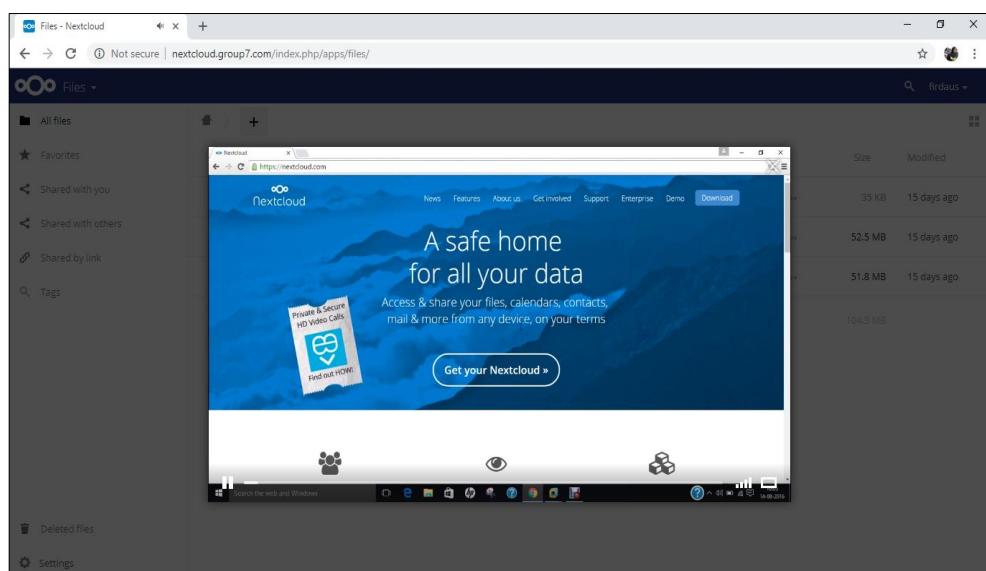


Figure 6. 66 : Play the video

6.2.19 VLAN Security

VLAN Security

Step 1: By using command ***show vlan brief*** on switch, we can know that Gi1/0/1-3, Gi1/0/13-15 are in **VLAN unusedPort** which is suspended.

group7-SW#show vlan brief			
VLAN	Name	Status	Ports
1	default	active	Gi1/0/22, Gi1/0/23, Gi1/1/1 Gi1/1/2, Gi1/1/3, Gi1/1/4
5	Trunk	active	
10	WinServer	active	Gi1/0/4, Gi1/0/5, Gi1/0/6
20	UbuServer	active	Gi1/0/7, Gi1/0/8
30	vlan FedoServer	active	Gi1/0/10, Gi1/0/11, Gi1/0/12
60	unusedPorts	suspended	Gi1/0/1, Gi1/0/2, Gi1/0/3 Gi1/0/13, Gi1/0/14, Gi1/0/15
101	Client	active	Gi1/0/16, Gi1/0/17, Gi1/0/18
102	AP	active	Gi1/0/19, Gi1/0/20, Gi1/0/21
1002	fdci-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdinnet-default	act/unsup	
1005	trnet-default	act/unsup	

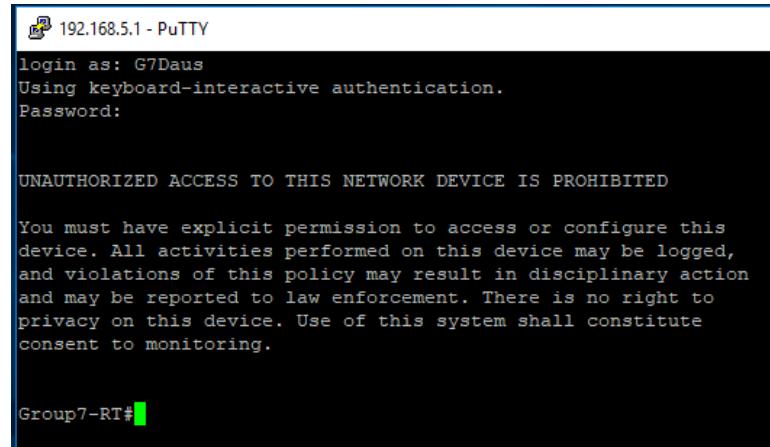
Figure 6. 67 : VLAN brief

Step 2: Try to connect a PC into Gi1/0/3, the connection cannot be made because the port signal didn't light up.

6.2.20 Router hardening

Enable Login Banner

The banner will be appeared after login.

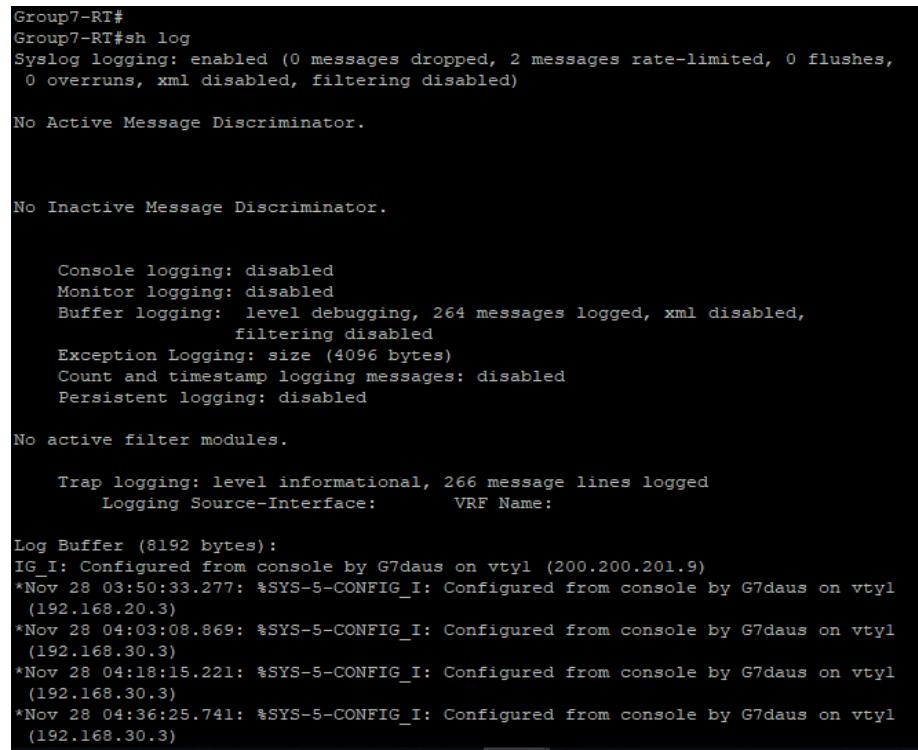


A screenshot of a Putty terminal window titled "192.168.5.1 - PuTTY". The window shows a login prompt: "login as: G7Daus", "Using keyboard-interactive authentication.", and "Password:". Below the password field, a large white banner with black text reads: "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED" and "You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring.". At the bottom of the window, the prompt "Group7-RT#" is visible.

Figure 6. 68 : Putty

Disable log to console or monitor sessions

Use command **sh log** to show logging after disable log console and log monitor.

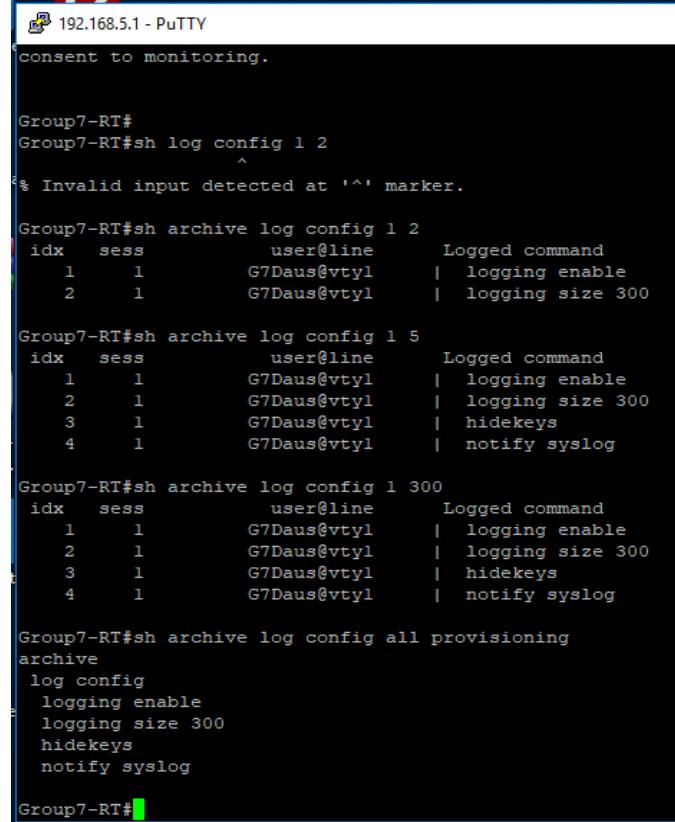


A screenshot of a Putty terminal window titled "Group7-RT#". The window displays the output of the "sh log" command. It shows various logging configurations: Syslog, No Active Message Discriminator, No Inactive Message Discriminator, Console, Monitor, Buffer, Exception Logging, Count and timestamp logging messages, Persistent logging, Trap logging, Log Buffer, and several configuration logs from the "IG I" interface. The output indicates that most logging levels are disabled or set to informational.

Figure 6. 69 : Putty

Enable configuration change notification and logging

Use command **sh archive log config 1 2**, **sh archive log config 1 5** and **sh archive log config all provisioning**.



192.168.5.1 - PuTTY

```
consent to monitoring.

Group7-RT#sh log config 1 2
^
% Invalid input detected at '^' marker.

Group7-RT#sh archive log config 1 2
  idx  sess      user@line      Logged command
    1    1        G7Daus@vtty1  |  logging enable
    2    1        G7Daus@vtty1  |  logging size 300

Group7-RT#sh archive log config 1 5
  idx  sess      user@line      Logged command
    1    1        G7Daus@vtty1  |  logging enable
    2    1        G7Daus@vtty1  |  logging size 300
    3    1        G7Daus@vtty1  |  hidekeys
    4    1        G7Daus@vtty1  |  notify syslog

Group7-RT#sh archive log config 1 300
  idx  sess      user@line      Logged command
    1    1        G7Daus@vtty1  |  logging enable
    2    1        G7Daus@vtty1  |  logging size 300
    3    1        G7Daus@vtty1  |  hidekeys
    4    1        G7Daus@vtty1  |  notify syslog

Group7-RT#sh archive log config all provisioning
archive
log config
  logging enable
  logging size 300
  hidekeys
  notify syslog

Group7-RT#
```

Figure 6. 70 : Putty

Log

Step 1: Login and enter command **conf t** and **exit**.



```
192.168.5.1 - PuTTY
login as: G7Daus
Using keyboard-interactive authentication.
Password:

UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED

You must have explicit permission to access or configure this
device. All activities performed on this device may be logged,
and violations of this policy may result in disciplinary action
and may be reported to law enforcement. There is no right to
privacy on this device. Use of this system shall constitute
consent to monitoring.

Group7-RT#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Group7-RT(config)#exit
Group7-RT#
```

Figure 6. 71 : Putty

Step 2: Click on the folder **log**.

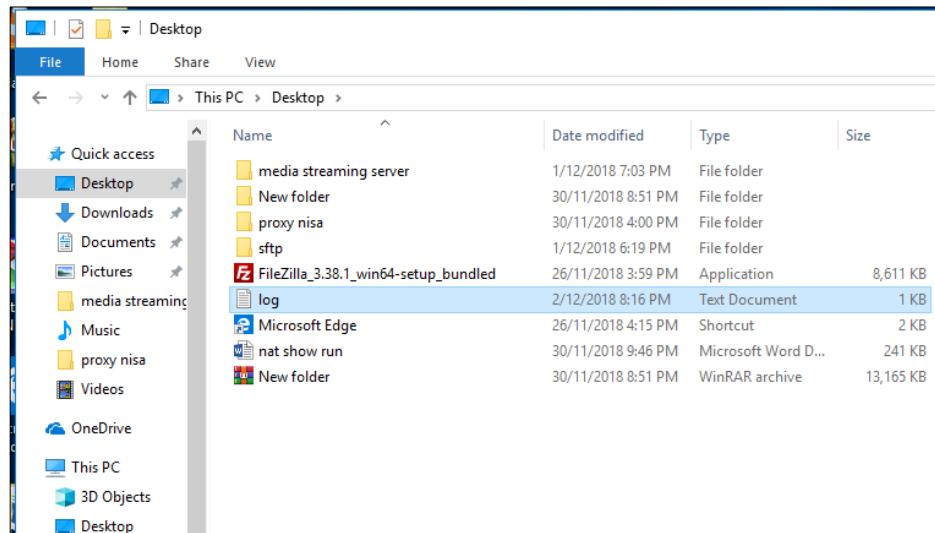


Figure 6. 72 : Desktop

Step 3: The text document will show the configuration in the Putty.

A screenshot of a Notepad window titled 'log - Notepad'. The window contains a PuTTY log from 2018.12.02 20:16:03. The log shows a password prompt and a configuration command. The text is as follows:

```
PuTTY log 2018.12.02 20:16:03
login as: G7Daus
Using keyboard-interactive authentication.
Password:

UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED

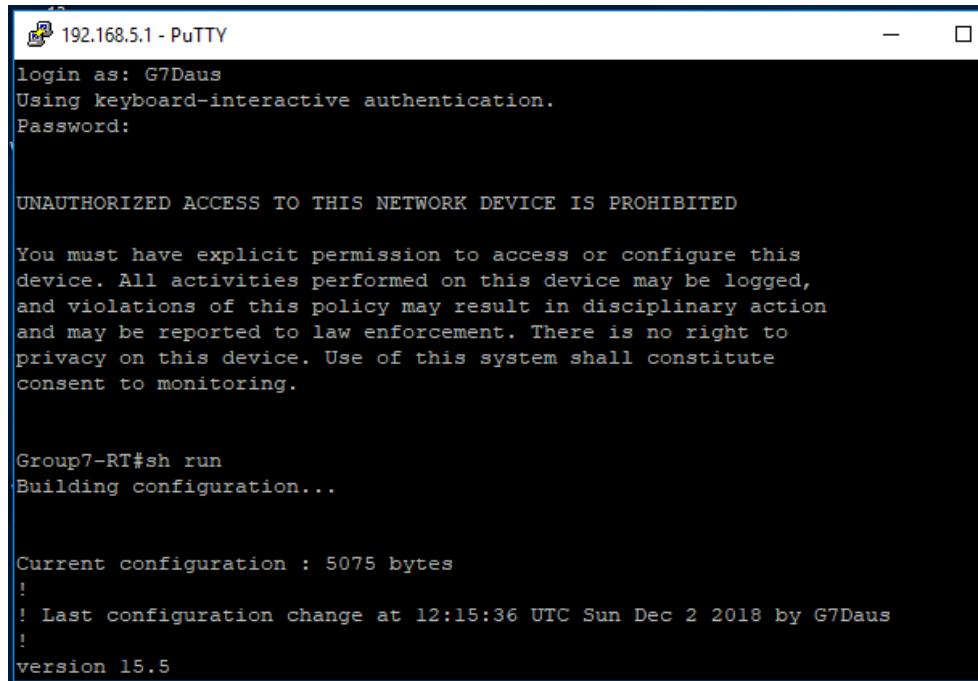
You must have explicit permission to access or configure this
device. All activities performed on this device may be logged,
and violations of this policy may result in disciplinary action
and may be reported to law enforcement. There is no right to
privacy on this device. Use of this system shall constitute
consent to monitoring.

Group7-RT#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Group7-RT(config)#exit
Group7-RT#
```

Figure 6. 73 : Log - Notepad

Disable DNS Lookup

Step 1: Enter command **sh run**.



```
192.168.5.1 - PuTTY
login as: G7Daus
Using keyboard-interactive authentication.
Password:

UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED

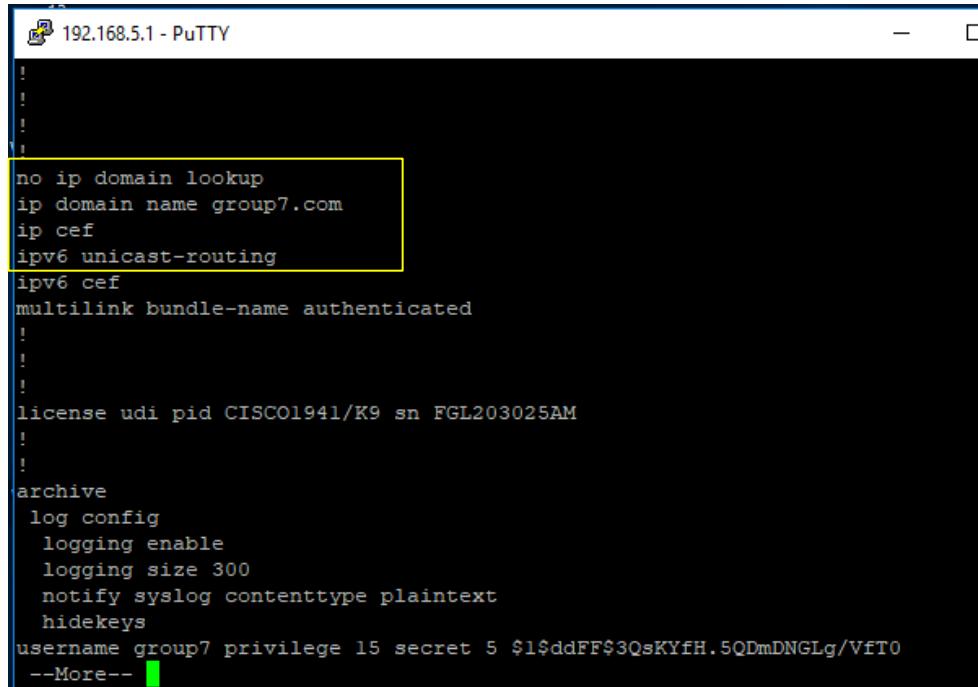
You must have explicit permission to access or configure this
device. All activities performed on this device may be logged,
and violations of this policy may result in disciplinary action
and may be reported to law enforcement. There is no right to
privacy on this device. Use of this system shall constitute
consent to monitoring.

Group7-RT#sh run
Building configuration...

Current configuration : 5075 bytes
!
! Last configuration change at 12:15:36 UTC Sun Dec 2 2018 by G7Daus
!
version 15.5
```

Figure 6. 74 : Putty

Step 2: It will show **no ip domain lookup** which it is disable.



```
192.168.5.1 - PuTTY
!
!
!
!
no ip domain lookup
ip domain name group7.com
ip cef
ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
!
!
!
license udi pid CISCO1941/K9 sn FGL203025AM
!
!
archive
log config
logging enable
logging size 300
notify syslog contenttype plaintext
hidekeys
username group7 privilege 15 secret 5 $1$ddFF$3QsKYfH.5QDmDNGLg/VfT0
--More--
```

Figure 6. 75 : Putty

6.2.21 Remote login using SSH

- SSH login to Ubuntu

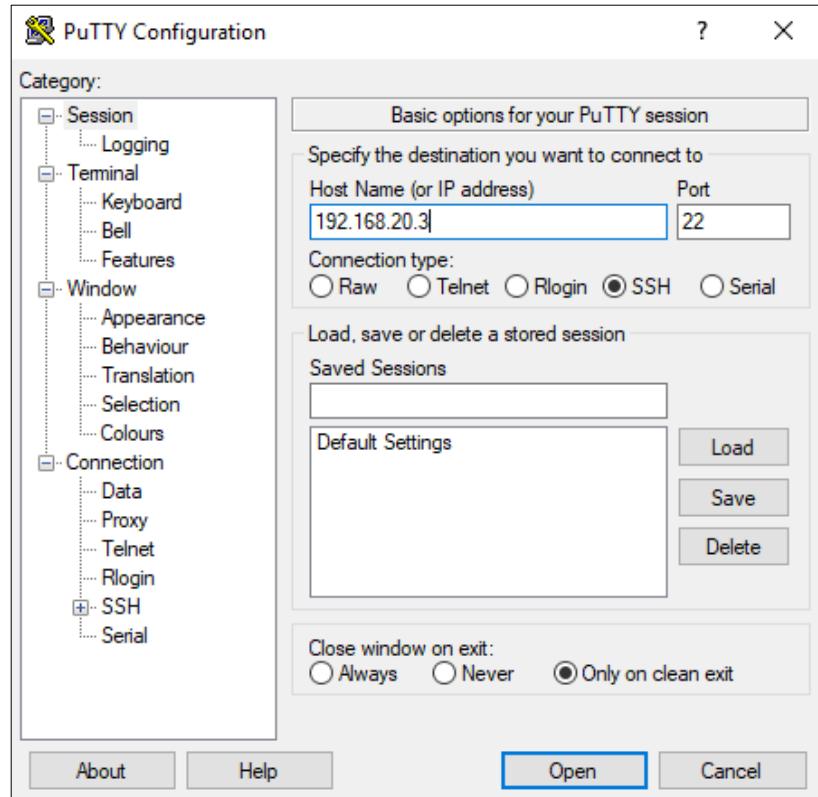


Figure 6. 76 : Putty configuration

```
g7@group7: ~
login as: g7
Using keyboard-interactive authentication.
Password:
Access denied
Using keyboard-interactive authentication.
Password:
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.15.0-36-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

g7@group7:~$
```

Figure 6. 77 : Login Ubuntu

- SSH login to Fedora

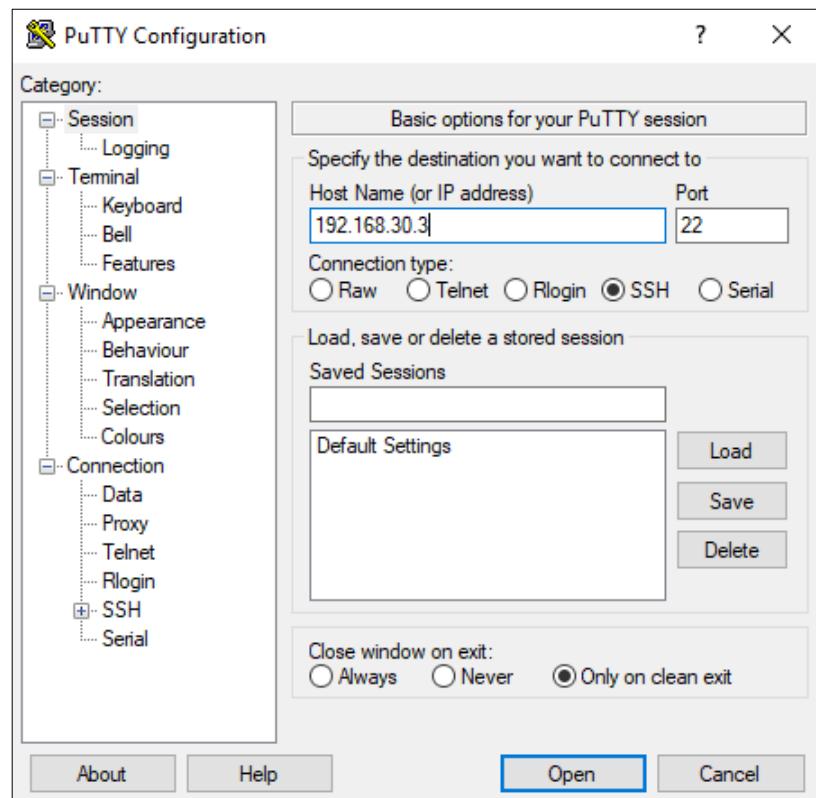


Figure 6. 78 : Putty configuration

```

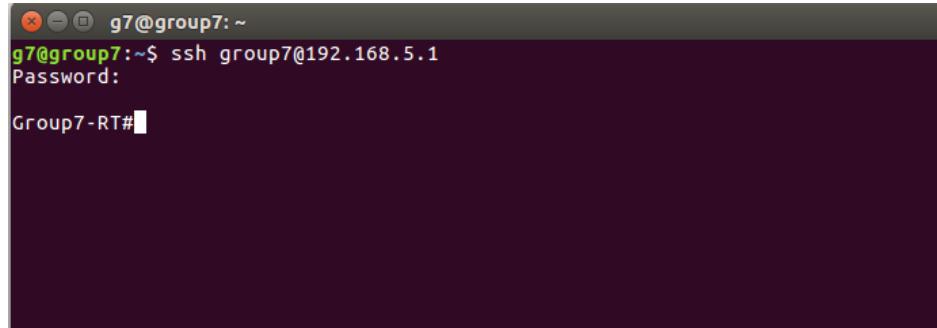
g7@fedora-group7-com:~ 
login as: g7
g7@192.168.30.3's password:
Last login: Fri Oct 19 20:35:15 2018 from 192.168.20.3
[g7@fedora-group7-com ~]$ 

```

Figure 6. 79 : Login Fedora

1. Testing SSH Login from Ubuntu

- SSH login to Router

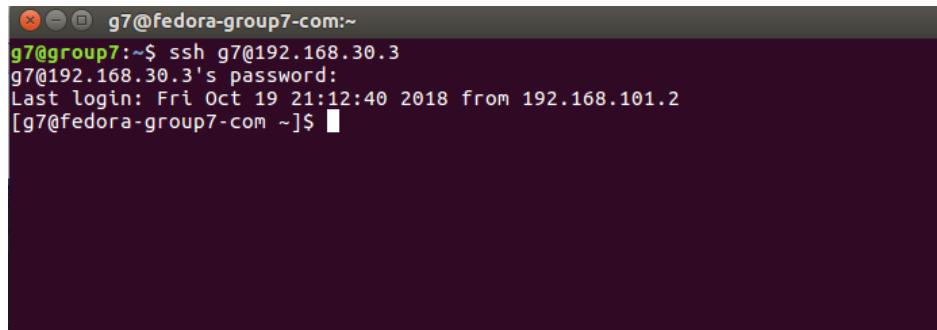


A terminal window titled "g7@group7: ~". The command "ssh group7@192.168.5.1" is entered, followed by a password prompt. The password "Group7-RT#■" is typed and submitted.

```
g7@group7: ~
g7@group7:~$ ssh group7@192.168.5.1
Password:
Group7-RT#■
```

Figure 6. 80 : Router

- SSH login to Fedora



A terminal window titled "g7@fedora-group7-com:~". The command "ssh g7@192.168.30.3" is entered, followed by a password prompt. The password "g7@192.168.30.3's password:" is typed and submitted. The response includes the last login information and the prompt "[g7@fedora-group7-com ~]\$ ■".

```
g7@fedora-group7-com:~
g7@group7:~$ ssh g7@192.168.30.3
g7@192.168.30.3's password:
Last login: Fri Oct 19 21:12:40 2018 from 192.168.101.2
[g7@fedora-group7-com ~]$ ■
```

Figure 6. 81 : Fedora

2. Testing SSH Login from Fedora

- SSH login to Router

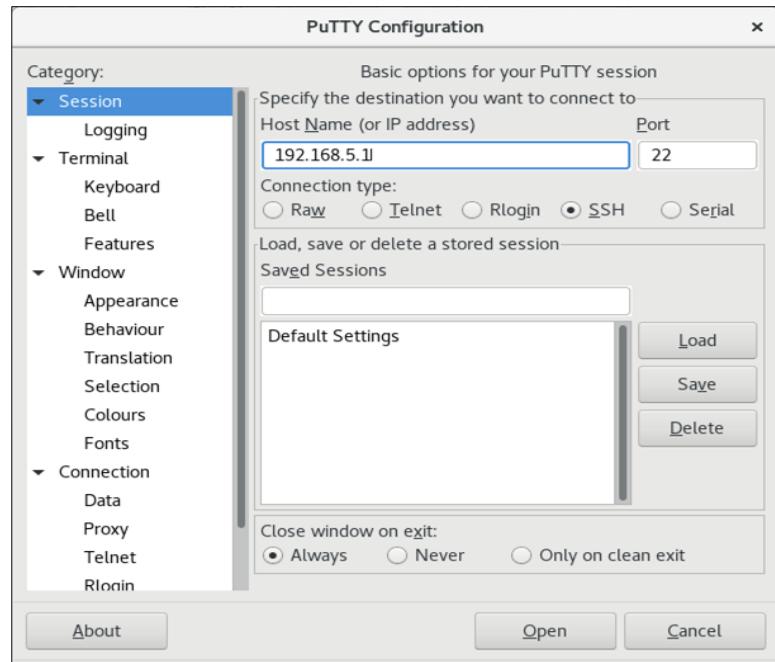


Figure 6. 82 : Putty Configuration

A terminal window titled '192.168.5.1 - PuTTY' is shown. The screen displays the following text:
login as: group7
Using keyboard-interactive authentication.
Password:
Group7-RT#

Figure 6. 83 : Router

- SSH login to Ubuntu

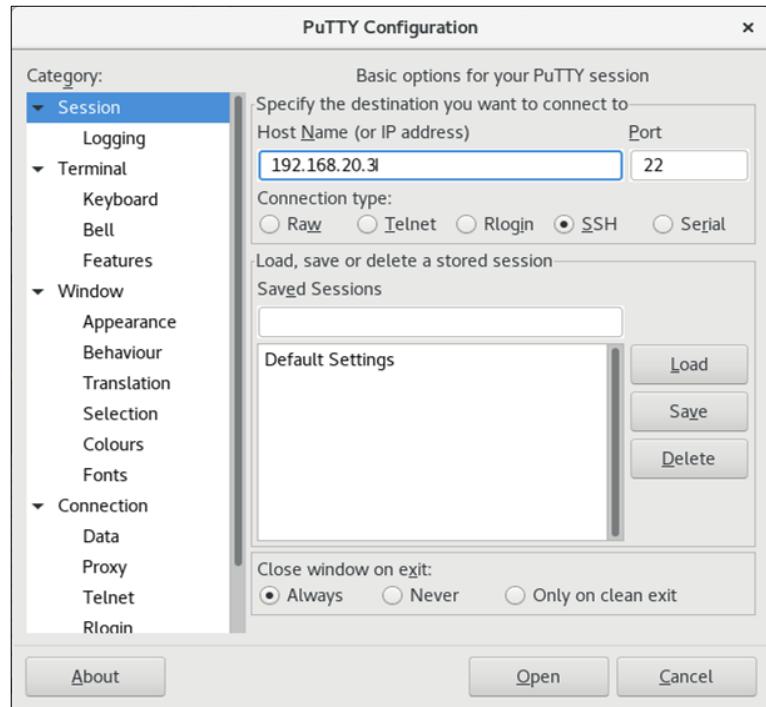


Figure 6. 84 : Putty Configuration

The screenshot shows a terminal window titled 'g7@group7: ~'. The session starts with a login prompt: 'login as: g7'. It then asks for a password. After logging in, it displays the welcome message for Ubuntu 16.04.5 LTS. It then lists available documentation links. Following that, it shows package update information: '11 packages can be updated.' and '1 update is a security update.' Finally, it shows the last login details: 'Last login: Fri Oct 19 14:26:31 2018 from 192.168.30.3'. The prompt 'g7@group7:~\$' is visible at the bottom.

Figure 6. 85 : Ubuntu

6.2.22 Linux server hardening

Password Expiry

Check for password status by running command **chage -l g7**.

```
[root@fedora-group7-com g7]# \chage -l g7
Last password change : Dec 04, 2018
Password expires      : Jan 03, 2019
Password inactive     : Feb 02, 2019
Account expires       : Mar 01, 2019
Minimum number of days between password change : 30
Maximum number of days between password change : 30
Number of days of warning before password expires : 7
[root@fedora-group7-com g7]#
```

Figure 6. 86 : g7@fedora-group7-com:/home/g7

Disable Unnecessary Port

Type command **nmap -v -sT localhost** to display list of scan ports after disable unnecessary service. CUPS service.

```
[root@fedora-group7-com g7]# nmap -v -sT localhost
Starting Nmap 7.60 ( https://nmap.org ) at 2018-12-04 20:07 +08
Initiating Connect Scan at 20:07
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 21/tcp on 127.0.0.1
Discovered open port 139/tcp on 127.0.0.1
Discovered open port 111/tcp on 127.0.0.1
Discovered open port 445/tcp on 127.0.0.1
Discovered open port 22/tcp on 127.0.0.1
Discovered open port 464/tcp on 127.0.0.1
Discovered open port 5666/tcp on 127.0.0.1
Discovered open port 749/tcp on 127.0.0.1
Discovered open port 631/tcp on 127.0.0.1
Discovered open port 88/tcp on 127.0.0.1
Completed Connect Scan at 20:07, 0.03s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00018s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 990 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
88/tcp    open  kerberos-sec
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
631/tcp   open  ipp
749/tcp   open  kerberos-adm
5666/tcp  open  nrpe

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
[root@fedora-group7-com g7]#
```

Figure 6. 87 : g7@fedora-group7-com:/home/g7

6.2.23 Windows server hardening

Step 1: Check all necessary security setting

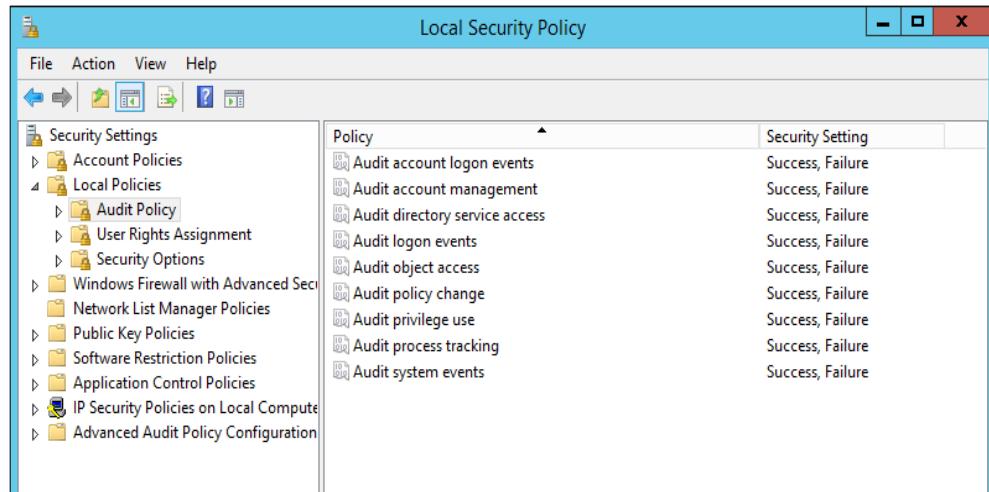


Figure 6. 88 : Local Security Policy

Step 2: Check firewall overview after enabling

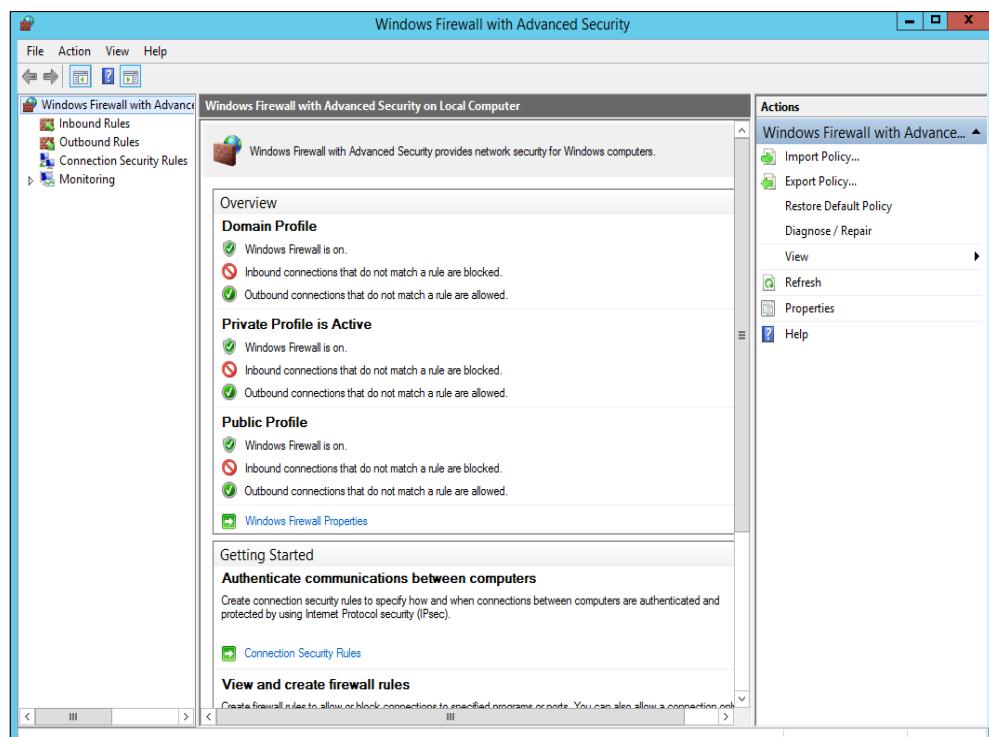


Figure 6. 89 : Windows Firewall with Advanced Security

Step 3: Checking password policy after enabling the password requirements.

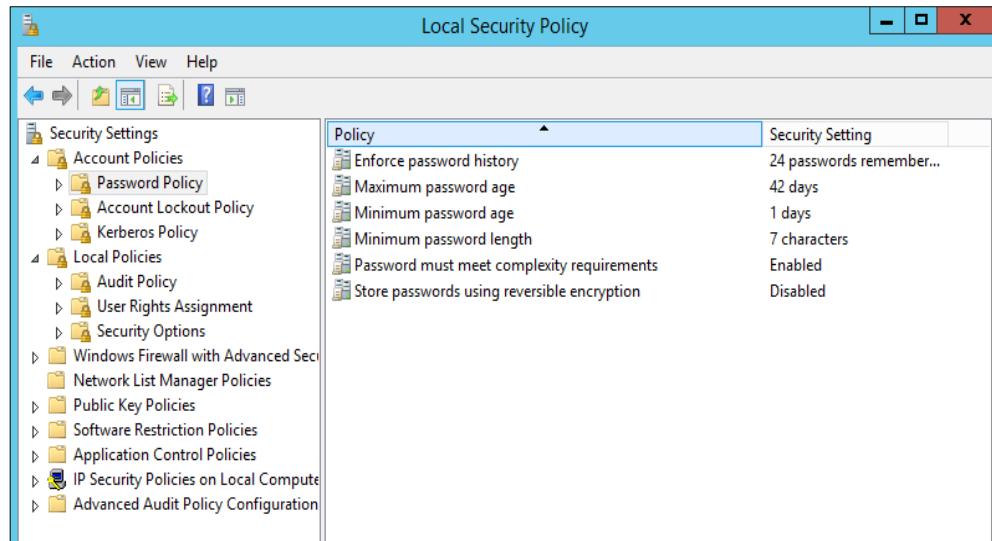


Figure 6. 90 : Password Policy

Step 4: Preview the Account Lockout Policy

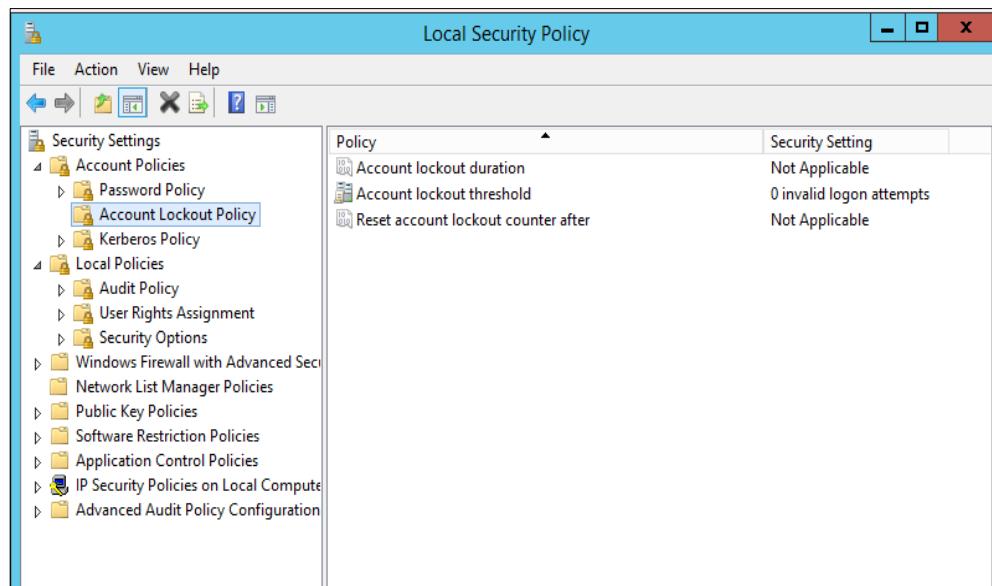


Figure 6. 91 : Account Lockout Policy

Step 5: Preview the Kerberos Policy

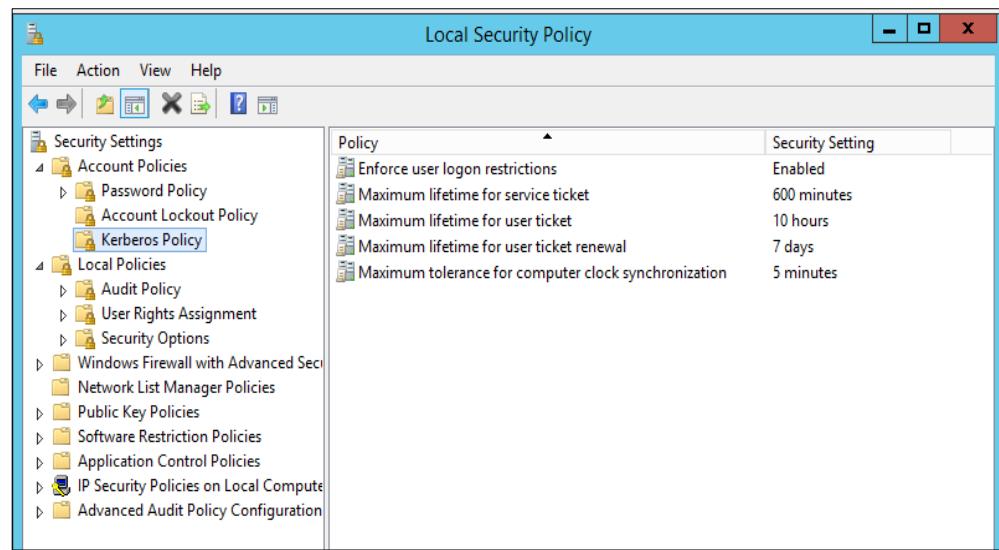


Figure 6. 92 : Kerberos Policy

6.2.24 Authentication user by integrating AD with Linux

Step 1: Create another user by using enterprise login.

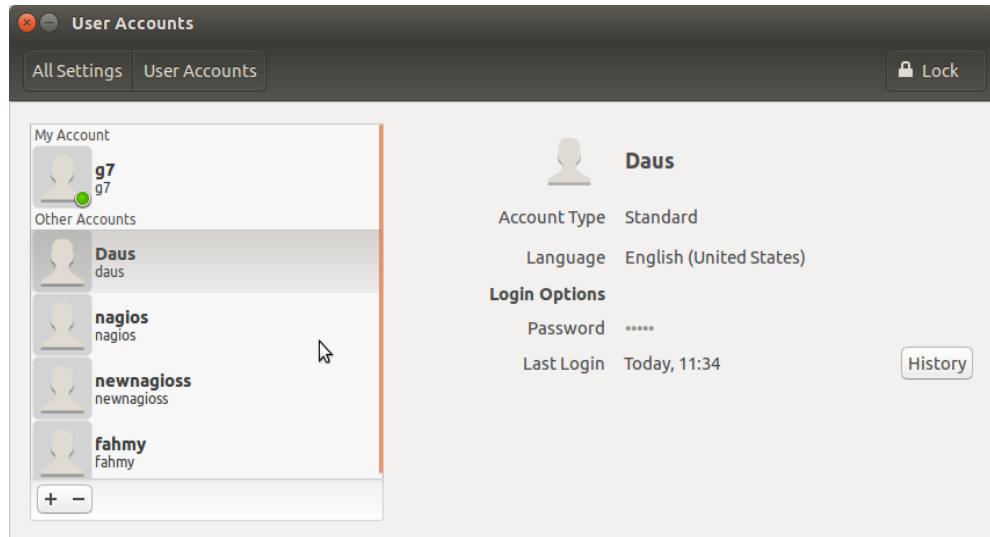


Figure 6. 93 : Login GUI

Step 2: Log in as root and change user to daus.

```
root@group7:~# su - daus
Creating directory '/home/GROUP7/daus'.
daus@group7:~$
```

Figure 6. 94 : Change User

6.2.25 Wireless user authentication using Radius server

Step 1: Open the network connection of laptop and connect to **group7** network.

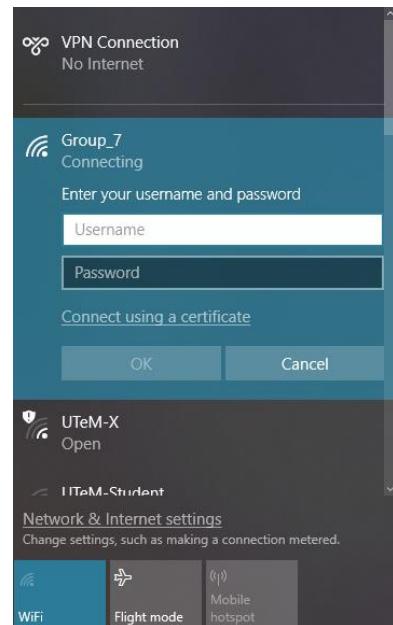


Figure 6. 95: Connect to group6 network

Step 2: Enter the username and password of AD and click OK

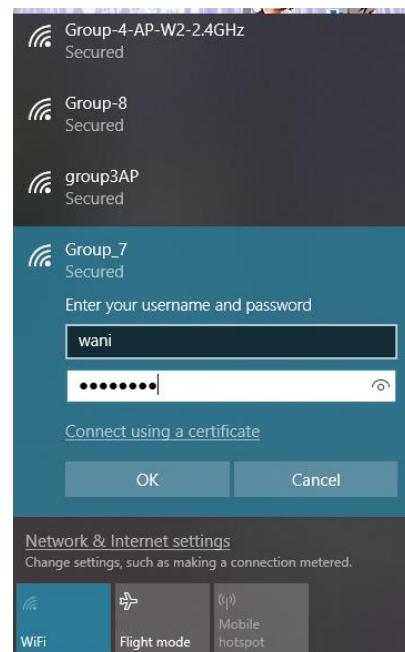


Figure 6. 96 : Enter the username and password to connect group7 network

Step 3: Click on the Connect button to connect the group7 network

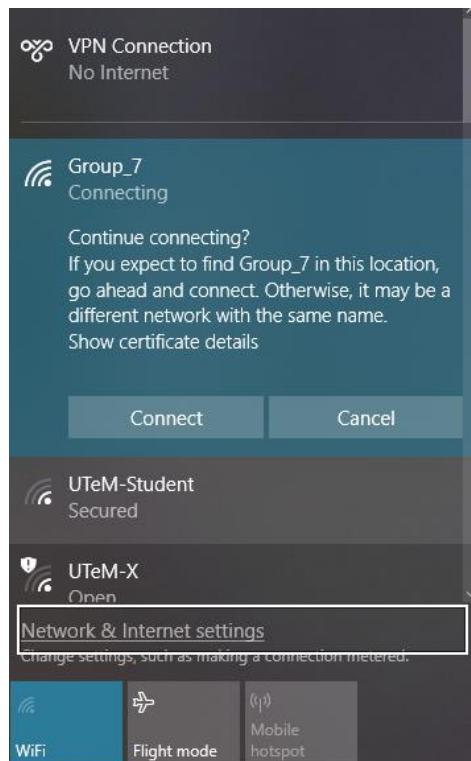


Figure 6. 97 Confirmation to connect to group7 network

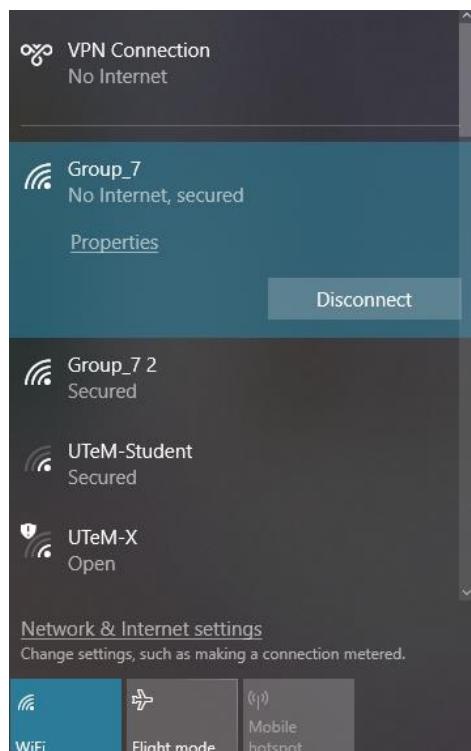


Figure 6. 98 : Connected to group7 network

6.2.26 IDS with port mirror

Step 1: Run Snort on console and on interface eno1 and ping to Fedora's IP which is 192.168.30.3 and monitor the result.

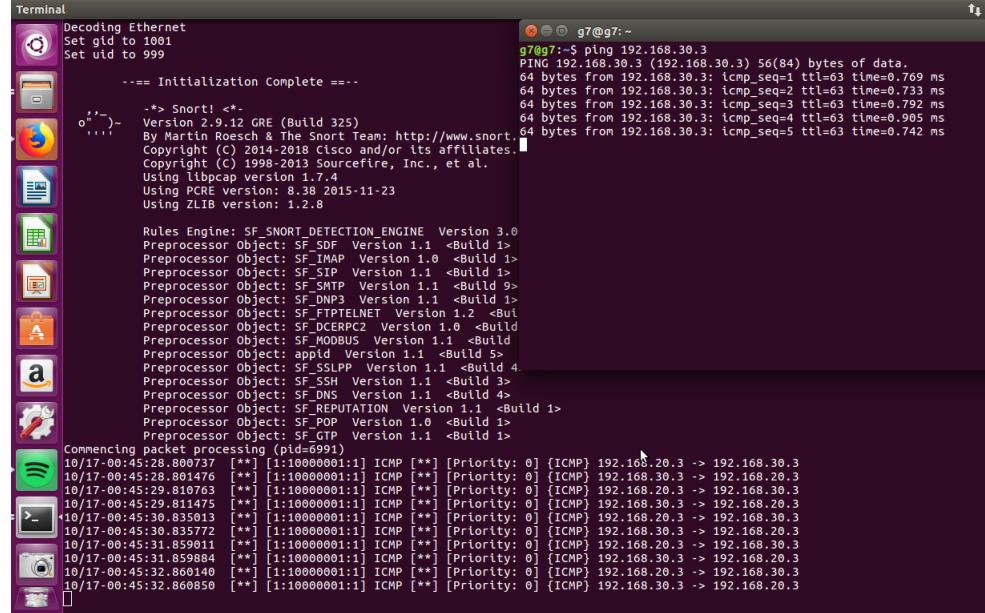


Figure 6. 99 : Snort Running

Step 2: Run sudo snort -r in Snort's log file and we can see the output is same as the console.

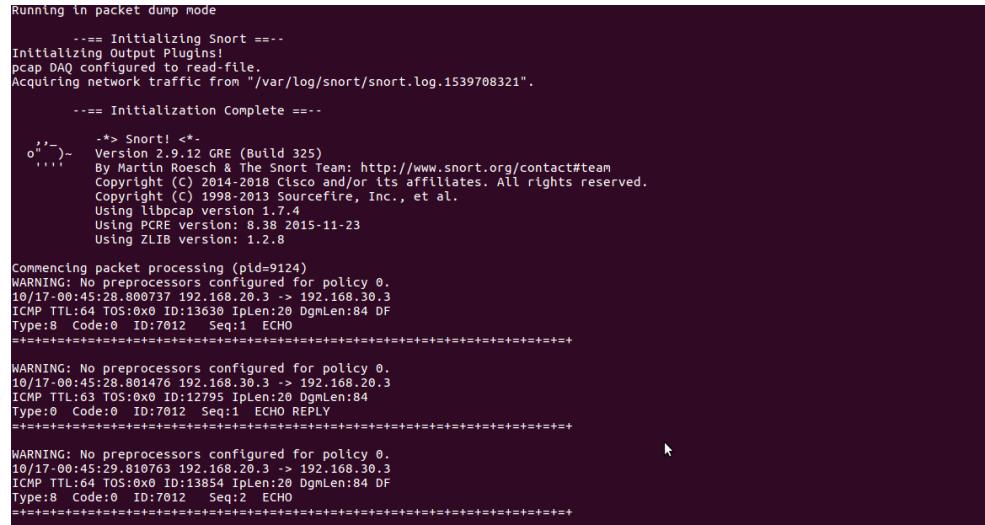


Figure 6. 100 : Snort's Log file

6.2.27 IPsec VPN for remote employees

Testing VPN connection on Laptop

Step 1: Click on **Open Network & Internet settings.**

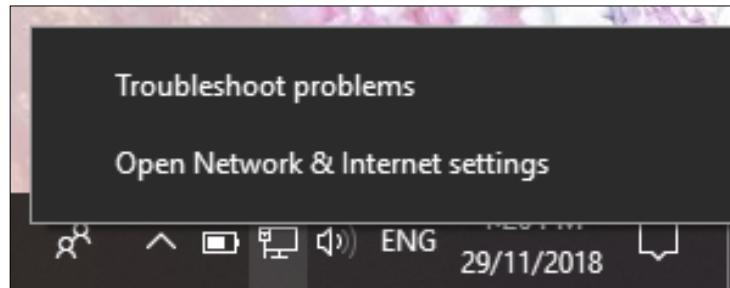


Figure 6. 101 : Internet Connection

Step 2: Click on **Network and Internet.**

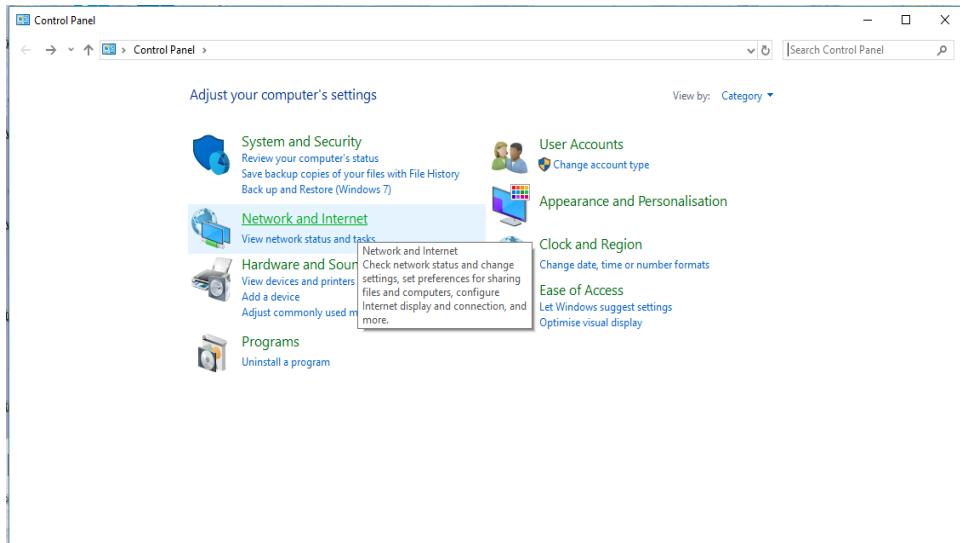


Figure 6. 102 : Control Panel

Step 3: Click on Network and Sharing Centre.

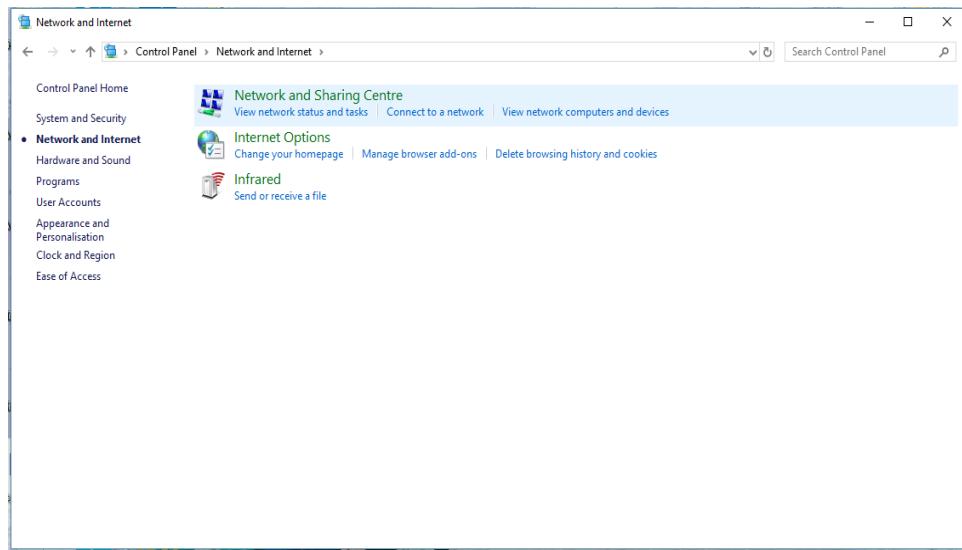


Figure 6. 103 : Network and Internet

Step 4: Click on Set up a new connection or network.

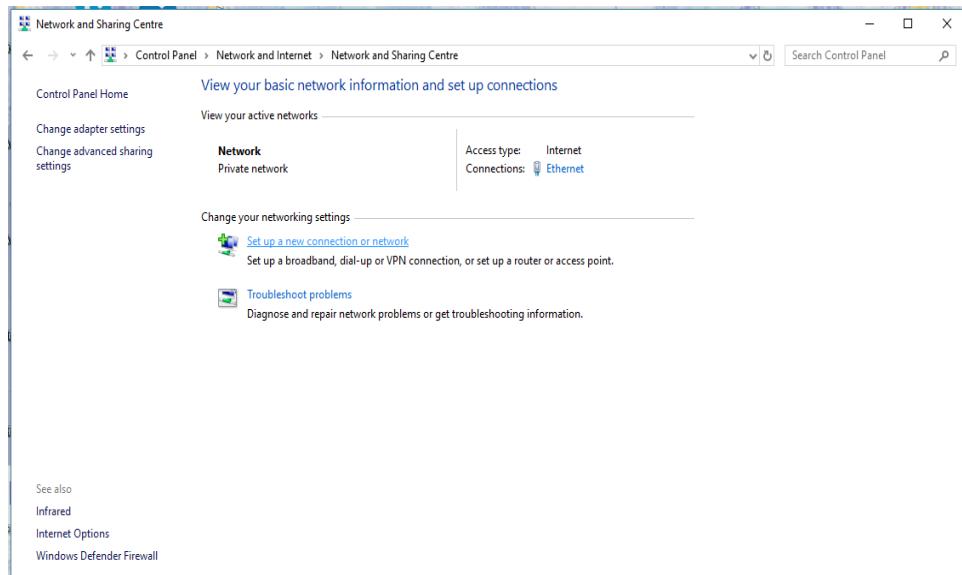


Figure 6. 104 : Network and Sharing Centre

Step 5: Select **Connect to a workplace**. Then, click **Next**.

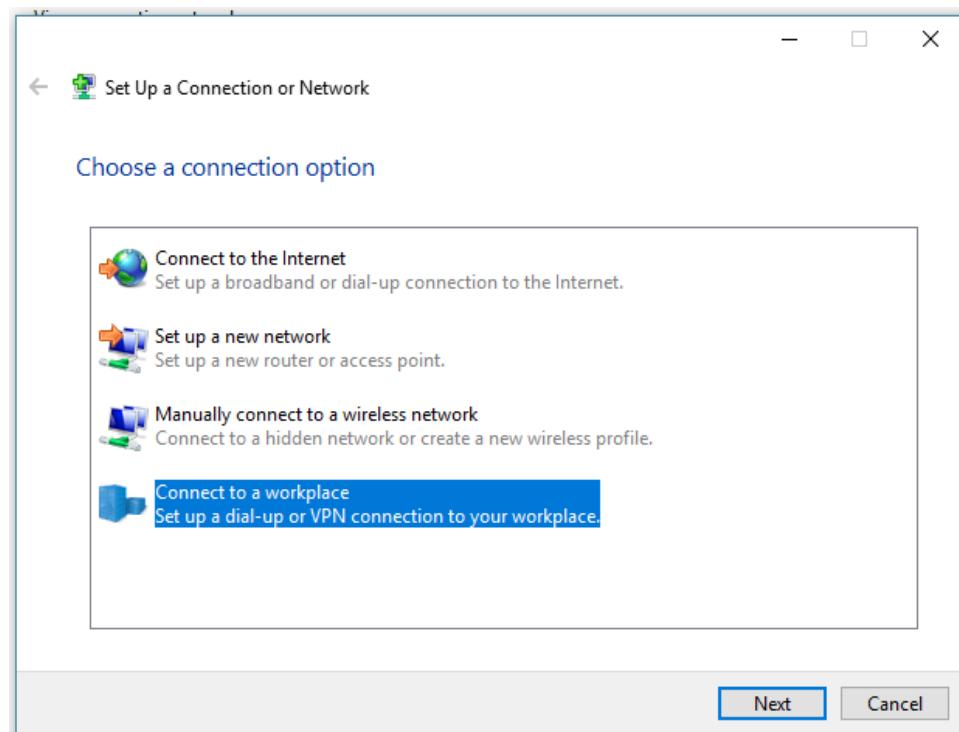


Figure 6. 105 : Set Up a Connection or Network

Step 6: Choose **No, create a new connection**. Then, click **Next**.

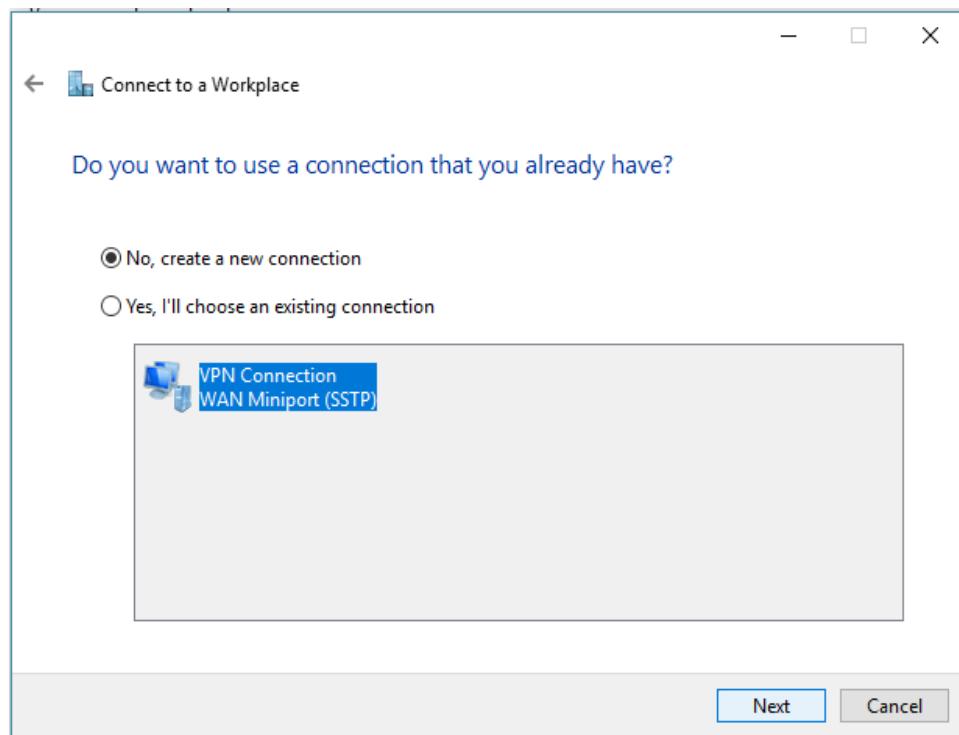


Figure 6. 106 : Connect to a Workplace

Step 7: Select **Use my Internet connection (VPN)**.

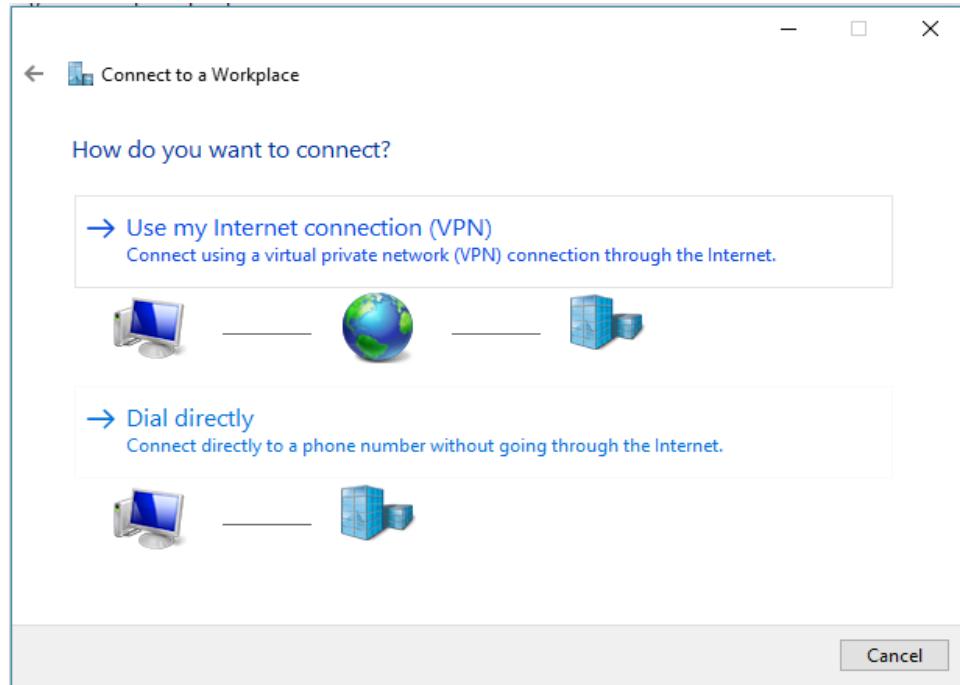


Figure 6. 107 : Connect to a Workplace

Step 8: Key in the **Internet address of VPN server** which is **vpn521660654.vpnazure.net**. Then, click **Create**.

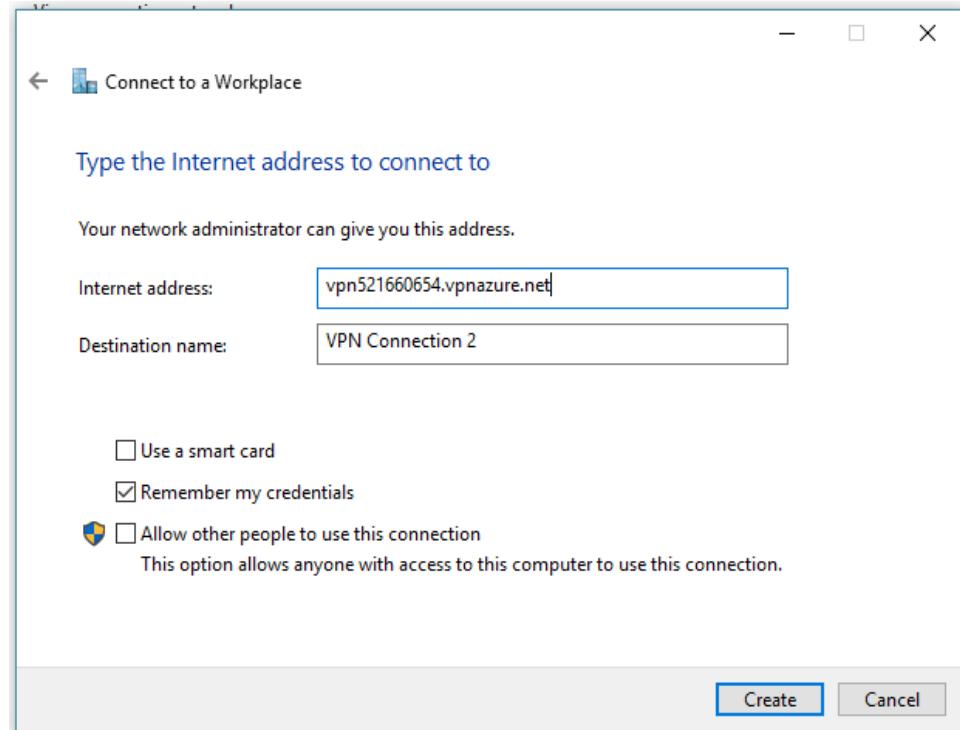


Figure 6. 108 : Connect to a Workplace

Step 9: Click Connect on VPN Connection.

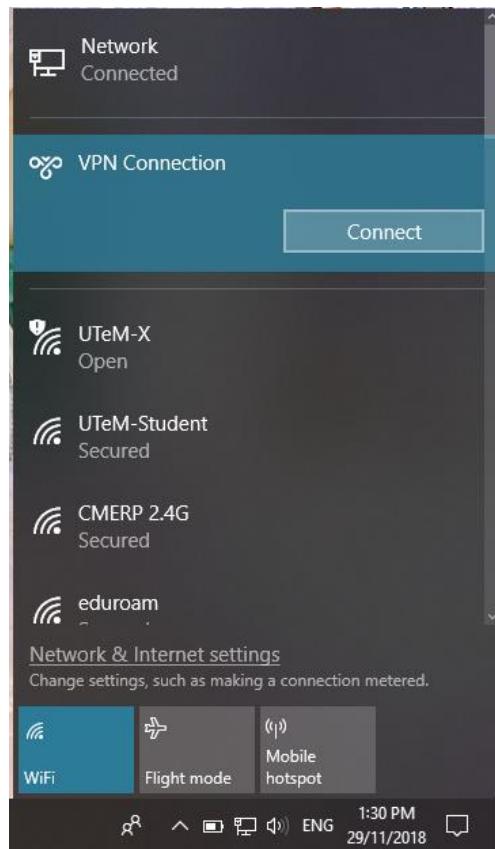


Figure 6. 109 : Pop-up window of WiFi

Step 10: Sign in by entering **Username** and **Password** that been created at VPN Server.

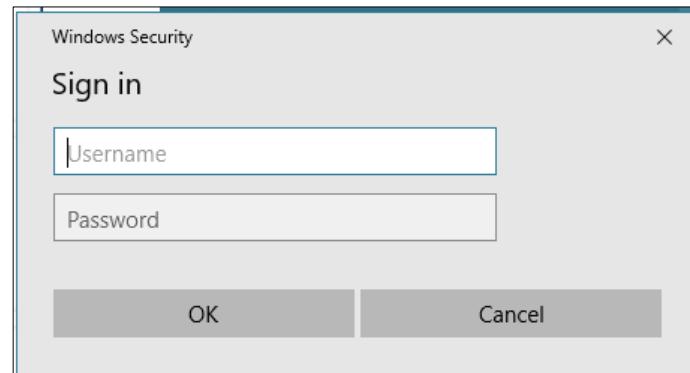


Figure 6. 110 : Windows Security

Step 11: VPN connection has been connected.

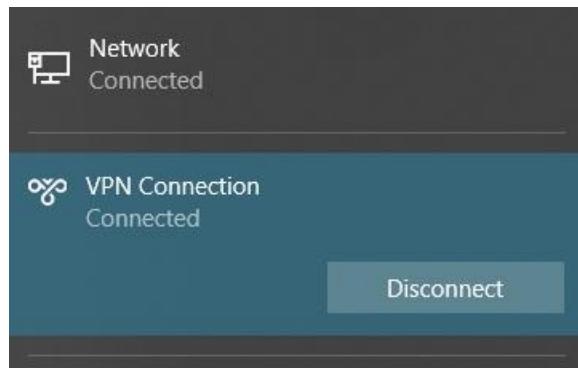


Figure 6. 111 : VPN Connection

Step 12: By using Command Prompt, ping IP address of server. The connection was successful as there were replies from server.

```
C:\> Command Prompt
Microsoft Windows [Version 10.0.17134.407]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\User>ping 10.73.39.98

Pinging 10.73.39.98 with 32 bytes of data:
Reply from 10.73.39.98: bytes=32 time=1ms TTL=128
Reply from 10.73.39.98: bytes=32 time<1ms TTL=128
Reply from 10.73.39.98: bytes=32 time<1ms TTL=128
Reply from 10.73.39.98: bytes=32 time<1ms TTL=128

Ping statistics for 10.73.39.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\User>
```

Figure 6. 112 : Command Prompt

6.2.28 Samba security services

Step 1: Open Run dialog by pressing Win + R and key in Fedora's IP.

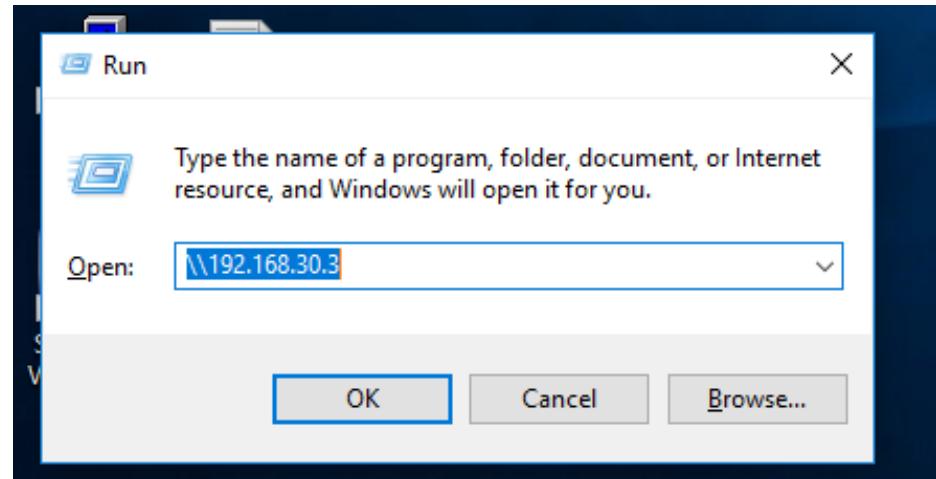


Figure 6. 113 : Run dialog box

It will show up a Windows Explorer as below.

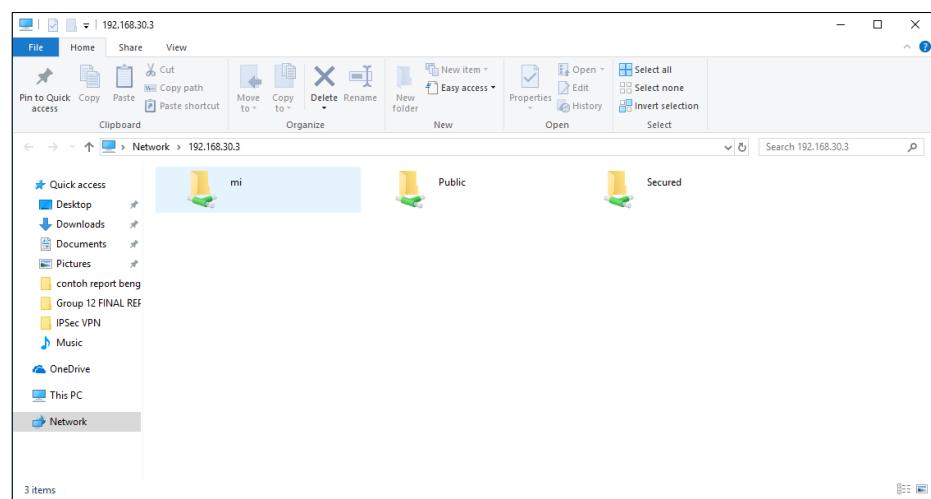


Figure 6. 114 : Samba's files

Step 2: Click folder “Secured” and it will prompt a dialog box requesting username and password.

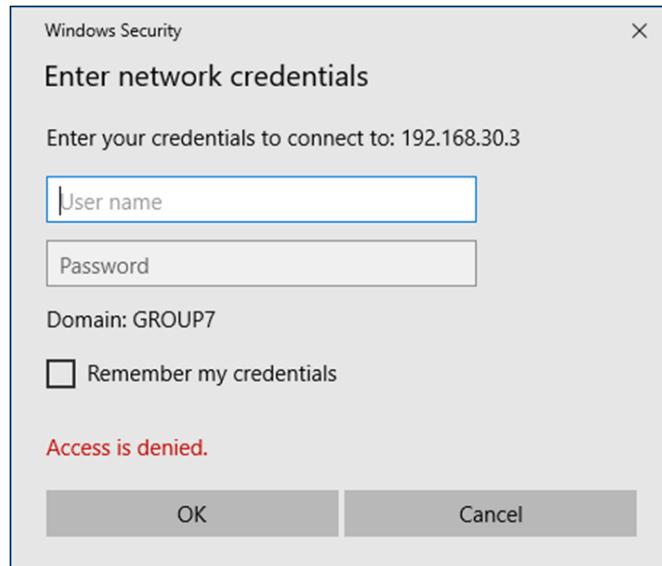


Figure 6. 115 : Login box

Key in username “yap” and its password when Samba account was created. New folder was seen named as “yap” and shows the user successfully login to Samba Secure.

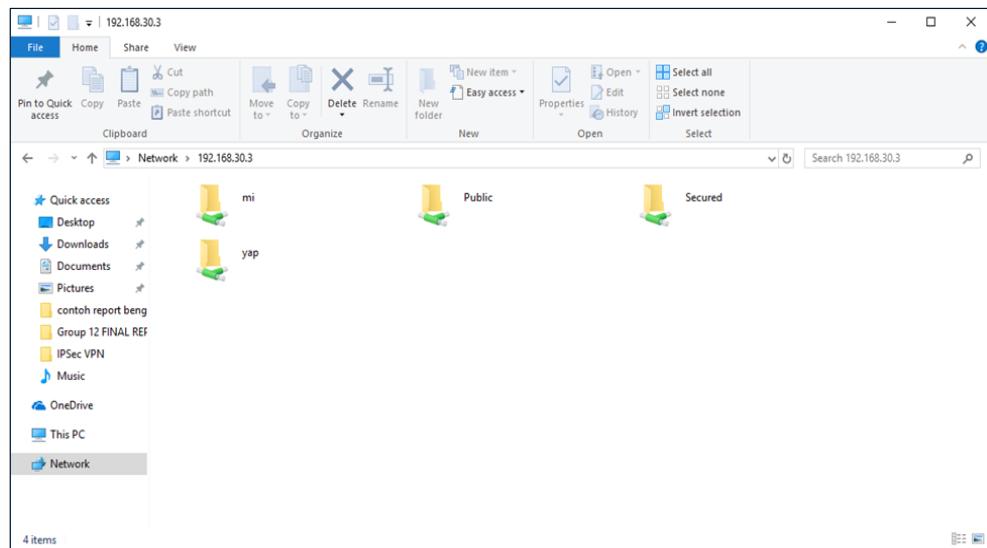


Figure 6. 116 : New folder shown

Enter yap folder and create a new text file named as yap.txt.

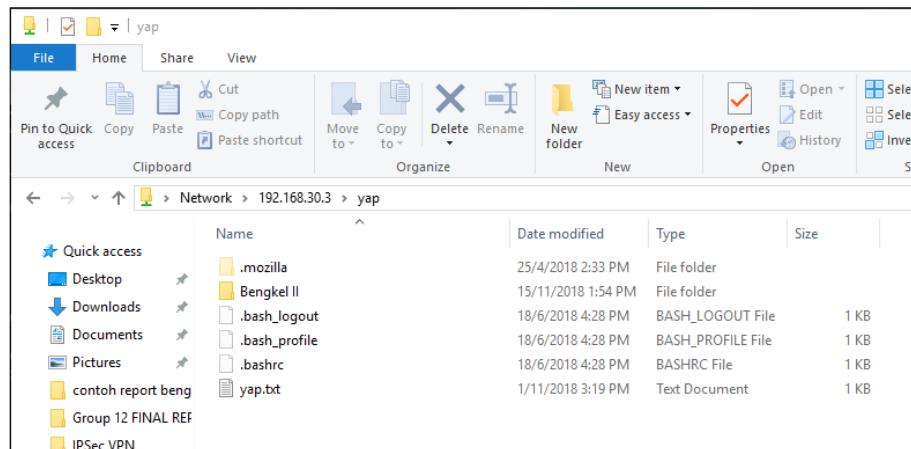


Figure 6. 117 : Yap 's file

Step 3: SSH to Fedora to check whether the file was created in Samba folder.

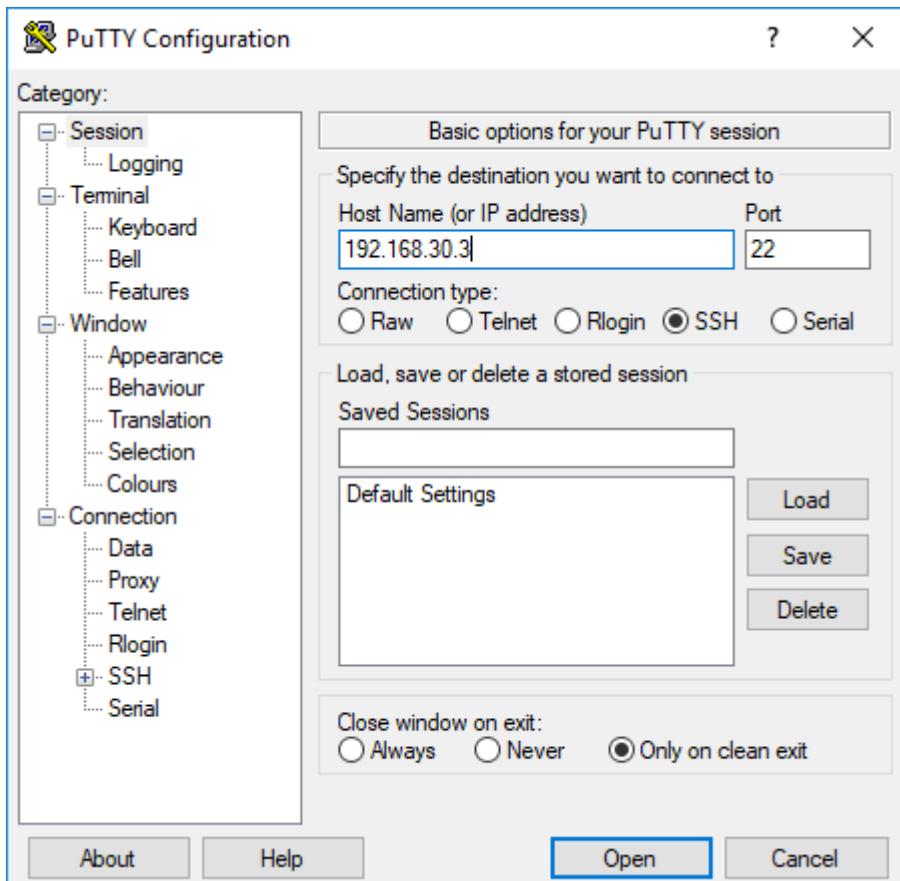


Figure 6. 118 : SSH to fedora

Login as g7 (local account) and g7's password.



Figure 6. 119 : Login box

Change working directory to Samba Secured folder which is at /var/lib/secured. As you can see, yap.txt was created.

A screenshot of a terminal window titled "g7@fedora-group7-com:~". It shows the command "ls -la /var/lib/secured/" being run, resulting in a permission denied error. Then, "sudo ls -la /var/lib/secured/" is run, prompting for a password. The output shows a file named "yap.txt" with permissions drwxr--r--. The file was created on Oct 30 17:39.

Figure 6. 120 : Samba's file directory

Step 4: Open yap.txt file.

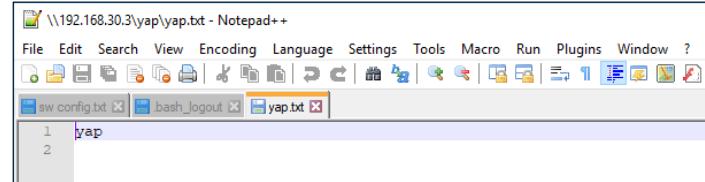


Figure 6. 121: yap.txt

6.2.29 Port Security

Step 1: Check either gi1/0/4 – 8 and gi1/0/10 – 12 is secure open or not

```
group7-SW#sh port-security int gi1/0/4
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   : 5
Configured MAC Addresses : 1
Sticky MAC Addresses  : 0
Last Source Address:Vlan : da3a.c543.88d2:10
Security Violation Count : 0
```

Figure 6. 122 : Testing the ports that have been configured

Step 2: Type the command **show port-security** to check all the ports that have been right shutdown or not.

```
group7-SW#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
(Count)      (Count)       (Count)       (Count)
-----
Gi1/0/4      10           5              0               Shutdown
Gi1/0/5      1             0              0               Shutdown
Gi1/0/6      1             0              0               Shutdown
Gi1/0/7      1             0              0               Shutdown
Gi1/0/8      1             1              0               Shutdown
Gi1/0/10     1             0              0               Shutdown
Gi1/0/11     1             1              0               Shutdown
Gi1/0/12     1             0              0               Shutdown
-----
Total Addresses in System (excluding one mac per port) : 4
Max Addresses limit in System (excluding one mac per port) : 4096
```

Figure 6. 123 : Summary of shutdown ports

Step 3: Type the command **show int status** to show the status of each interface

group7-SW#show int status						
Port	Name	Status	Vlan	Duplex	Speed	Type
Gil/0/12		notconnect	30	auto	auto	10/100/1000BaseTX
Gil/0/13		notconnect	60	auto	auto	10/100/1000BaseTX
Gil/0/14		notconnect	60	auto	auto	10/100/1000BaseTX
Gil/0/15		notconnect	60	auto	auto	10/100/1000BaseTX
Gil/0/16		connected	101	a-full	a-1000	10/100/1000BaseTX
Gil/0/17		notconnect	101	auto	auto	10/100/1000BaseTX
Gil/0/18		notconnect	101	auto	auto	10/100/1000BaseTX
Gil/0/19		notconnect	102	auto	auto	10/100/1000BaseTX
Gil/0/20		notconnect	102	auto	auto	10/100/1000BaseTX
Gil/0/21		notconnect	102	auto	auto	10/100/1000BaseTX
Gil/0/22		notconnect	1	auto	auto	10/100/1000BaseTX
Gil/0/23		notconnect	1	auto	auto	10/100/1000BaseTX
Port	Name	Status	Vlan	Duplex	Speed	Type
Gil/0/24		connected	trunk	a-full	a-1000	10/100/1000BaseTX
Gil/1/1		notconnect	1	auto	auto	unknown
Gil/1/2		notconnect	1	auto	auto	unknown
Gil/1/3		notconnect	1	auto	auto	unknown
Gil/1/4		notconnect	1	auto	auto	unknown

Figure 6. 124 : Status of all port interface

6.3 CONCLUSION

After all the installation the services in the network and configuration of all the services, we carry out testing to ensure all the services are configured correctly. Although, we made the correct configuration following step by step sometimes in the testing phase we might find it unsuccessful. Therefore, the testing phase is very important to troubleshoot any problem detected. After all the done, we carry out testing to ensure all the services are running smoothly and the network is up and make it in documentation.

CHAPTER 7 – CONCLUSION

7.1 INTRODUCTION

Workshop 2 is the prerequisite subject that preparing student before ongoing industrial training. In this workshop 2, student is more exposed the environment that working in a group with flexible schedule within a period time and all in real device instead of using simulation software such as GNS3 or packet tracer.

This also a good platform that provide knowledge exchange and sharing between computer securities students with networking students. Both courses of student are able to expose to each other expertise field knowledge that will provide greater advantage in future of student career. Workshop 2 also provided the platform for student to explore the knowledge of configuration that can be done with different tools and software.

We have to define, implement and manage starts from selecting a leader in leading this project from beginning until the end of the project. The overall performance of this workshop is acceptable. Although there are certain constraints arise while developing the workshop, the development of the workshop was able to meet the due date. A task has been given to each member and creates a schedule to get the task done. It is very important in managing and organizes every task in order not to face any problems and error at the future.

This network is suitable for Small and Medium Enterprise Business since it is easy to manage and implement. Furthermore, this network includes all the basic service (such as DNS, DHCP, Email, SFTP, Proxy Server and etc.) that needs to run the business. Hopefully we can achieve our goals or objective that is to make this project a success and able go through the obstacles and challenges faced in completing the task given. We are so grateful being given this as this will bring us more prepared for an industrial training.

7.2 PROJECT ADVANTAGES

There are many advantages that we get as long as we implement this project. The most important this project give us more experience that usually we can only be gained during working environment. Besides that, this project also give have others advantages to us. There are:

1. We have more knowledge about these services for this project.
2. We also know how to install and configure these services in a server.
3. We learn many ways to troubleshoot and overcome any problems during setup these services.
4. We learn how to develop a simple networking system where communicate between other computers and different platform.
5. We have to make it communicate and running by implementing some basic services.
6. We had learned how to design, set up, maintain, and monitor for a small networking infrastructure.
7. We learn how to manage time to complete all 27 services on time.
8. This project exposes us to find about the services that we never do.
9. We able to learn and adapt the real environment that preparing us for industrial training and also for career in future.
10. Others important benefit that we get during this project that we have an experienced how to work in a group and also how to tolerate with other group to share the server.

7.3 PROJECT DISADVANTAGES

However, there were some disadvantages in this project. This workshop requires us to set up a network with 30 services. However, most of these services we have no idea on what are they and how to configure them. Services like IPv6 transition mechanism, RADIUS, proxy we have never heard before in our first two years of study. We suggest that faculty should revise the course's subject and include some basic server configuration hands on before the Workshop 2.

7.4 PROJECT LIMITATION

The limitations of this workshop include but not limited to:

1. Workshop 2 deserve more than 3 credit hours. Time spent on Workshop 2 is definitely more than 3 hours per week. It really takes a lot of effort to get it done well. This is the reason why some students are not willing to spend hours and hours in this workshop. Because by doing so, it will cost them other subject's grade.
2. Lack of current enterprise technique. Most of the enterprises are implementing switch stacking, load balancing, and server failover. Maybe faculty can introduce these technique into workshop as it will be useful for students in their future working environment.

7.5 CONCLUSION

Last but not least, we are able to configure and set up our network using the basic network equipment through the workshop 2. We are also exposed with the operating system knowledge that will help us in choosing operating system for our server in future. We are able to design our own network infrastructure and maintain it in a good condition at all time. We are also exposed with the knowledge of security vulnerability on the operating system and network and solve it using hardening in order to ensure the whole network that had been setup are secure and ready to be used.

In this workshop 2, one of the main objective is to provide the environment for student to work in a team. Through this project, we learnt to plan among our team and give full cooperation among each other's along the project progression. This also enable us to prepare for facing the real environment of career and industrial training. We are also able to share our knowledge each other to ensure everyone able to gain new knowledge and experience that will be useful in future.

As a conclusion, this workshop has successfully given the real working environment exposure to us at the end of this workshop 2 project and we are managed to complete all the tasks given and setup the network as required.

BIBLIOGRAPHY

- BIND 9 Administrator Reference Manual.* (2008). Retrieved from
<https://ftp.isc.org/www/bind/arm95/Bv9ARM.html>
- Build Your Own Email.* (05 October, 2018). Retrieved from LinuxBabe:
<https://www.linuxbabe.com/>
- Computer Network. (2000). In L. P. Davie, *A System Approach*. Morgan Kaufman Publisher.
- Monitoring Windows Machines.* (03 August, 2016). Retrieved from Nagios Docs:
<https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/monitoring-windows.html>
- PacketLife.net.* (03 May, 2010). Retrieved from Port Security:
<http://packetlife.net/blog/2010/may/3/port-security/>
- Ravi Saive, G. C. (2012 August, 2012). *Techmint.* Retrieved from How to Add Windows Host to Nagios Monitoring Server: <https://www.tecmint.com/how-to-add-windows-host-to-nagios-monitoring-server/>
- Richard. (2018). *Install Nextcloud Server.* Retrieved from Website for student:
<https://websiteforstudents.com/install-nextcloud-server-using-composer-on-ubuntu-16-04-18-04-with-apache2-mariadb-and-php-7-2-support/>
- SoftEther.* (April, 2004). Retrieved from SoftEther VPN: <https://www.softether.org/3-screens>
- Spiceworks.* (2006). Retrieved from Integrate Linux with Active Directory:
https://community.spiceworks.com/how_to/445-integrate-linux-with-active-directory-using-samba-winbind-and-kerberos
- Sublime Robots.* (December, 2014). Retrieved from Snort 2.9.9.9.x on Ubuntu:
<http://sublimerobots.com/2017/01/snort-2-9-9-x-ubuntu-installing-snort/>
- Web Proxy Caching: the devil is in details. (1998). In F. A. R. Caceres, *Workshop on ISP held with SIGMETRICS.*

APPENDIX

No	Task Name	Week														
		1	2	3	4	5	6	7	8	9	MID Semester break	10	11	12	13	14
1	Attend workshop 2 speech															
2	Discussion with Group Member															
3	Proposal preparation and writing proposal															
4	Submit project proposal															
5	Preparation Hardware and setup device															
6	Progress report 1															
7	Progress report 2															
8	Progress report 3															
9	Preparation of Video and Poster															
10	Revision Final Report & Log Book															
11	Final presentation															
12	Submission of Final Report & Log Book															