



FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

SEMESTER 1 2018/19

BITU3923 - WORKSHOP II

BITC & BITZ

FINAL REPORT

VIRTUAL PRIVATE NETWORK (VPN)

GROUP NUMBER: 4

PREPARED BY:

NAME	MATRIC NO
MUHAMAD SYAFIQ AZLAN BIN MUSTAFA	B031610373
MUHAMMAD KIFLY BIN MOHD ZAN	B031610034
NUR JAMSYEIQQA BINTI JAMALUDDIN	B031610455
NURNASIHA BINTI MOHD ISA	B031610208
AHMAD SYARIFUDDIN BIN HARUN	B031610085
NUR SYAFIQAH BINTI NOR AZMI	B031610156
OOI XING CZEK	B031610125
NURDAYANA BINTI MOHD AIDI	B031610128

PREPARE FOR:

Dr. Zurina binti Sa'aya (M)

Dr. Robiah binti Yusof (S)

ACKNOWLEDGEMENTS

First and foremost, we would like to thank our supervisors of this project, Dr. Zurina binti Sa'aya and Dr. Robiah for their valuable guidance and advice. They inspired us greatly to work in this project. Their willingness to motivate us contributed tremendously to our project. We also would like to thank both of our supervisors for showing us some examples that are related to the services in our project which helped us a lot to understand our project. This helped us to complete our project on time. We would also like to thank our evaluator for this workshop, Dr Zaheera for taking the time to evaluate us. This evaluation gave us deeper understanding of our services and network infrastructure.

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

ABSTRACT

The main objectives for this Workshop 2 are designing a secured network infrastructure by using the available equipment, implementing designated secured network services and configuration into the network infrastructure, installing and integrating network infrastructure, services and configuration based on the requirement of secured network environment, and managing the secured network infrastructure, services and configuration. Our group consists of 9 students, 6 students from BITC and 3 students from BITZ. BITC students are required to install 18 designated network infrastructures includes DNS (IPv4 & IPv6), DHCP (IPv4 & IPv6), Inter VLAN and VLSM addressing, Routing and NAT, Active Directory (AD), Proxy Server, Samba, Network Management System, Server Virtualization, AAA (Authentication, Authorization and Accounting) using Radius, Access Control List (ACL), Secured FTP (with authentication and encryption), Web, SSL & Virtual Hosting, Linux Email Server, IPv6 Web with IPv6 Tunnelling (testing IPv6 Web from remote site), Media Streaming Server and Cloud Server. Meanwhile for BITZ students, a security policy should be designed, 12 security services and configuration required to be implemented. The 12 security services and configuration are Router Security (router hardening and remote login using SSH), Server Hardening (Linux server1 hardening and Windows server hardening), Security Service (Authentication user by integrating AD with Linux, Wireless user authentication using Radius server, IDS with port mirror, IPsec VPN for remote employees (between server and user) and Samba security services) and LAN Security (Port security and VLAN security). A project manager has been assigned from the group to lead the group members throughout the workshop. We have been provided with the equipment which are three (3) servers, one (1) Cisco 2800 router (2 Fast Ethernet), one (1) Cisco 2960 manageable switch, 15 meters UTP cable, 12 pieces RJ-45, NIC card, Access Point (AP) and one set crimping tool. The operating system used in servers are Windows Server 2012, Fedora 27 and Ubuntu 16.04. After setting up all the network configuration, infrastructure and services, several tests will be done to ensure they are working properly. At the end of workshop II, we are required to demonstrate our work to supervisors and evaluator. We are also required to produce poster and video for exhibition based on our title which is IPsec VPN.

ABSTRAK

Objektif utama Bengkel 2 ini adalah untuk mereka bentuk infrastruktur rangkaian yang selamat dengan menggunakan peralatan yang disediakan, mengaplikasikan servis rangkaian yang ditetapkan dan konfigurasi yang ditetapkan ke dalam infrastruktur rangkaian, memasang dan mengintegrasikan infrastruktur rangkaian, servis dan konfigurasi berdasarkan keperluan persekitaran rangkaian terjamin, dan menguruskan infrastruktur rangkaian, servis dan konfigurasi rangkaian yang dijamin. Kumpulan kami terdiri daripada 9 pelajar, 6 pelajar dari BITC dan 3 pelajar dari BITZ. Pelajar BITC perlu memasang 18 prasarana rangkaian yang ditetapkan termasuk *DNS (IPV4 & IPV6), DHCP (IPV4 & IPV6), InterVLAN and VLSM, Routing and NAT, Active Directory (AD), Proxy Server, Samba, Network Management System, Server Virtualization, AAA (Authentication, Authorization and Accounting) using Radius, Access Control List (ACL), Secured FTP (with authentication and encryption), Web, SSL \$ Virtual Hosting, Linux Email Server, IPv6 Web with IPv6 Tunnelling (testing IPv6 Web from remote site), Media Streaming Server and Cloud Server.* Selain itu, untuk pelajar BITZ, satu polisi keselamatan perlu direka, 12 servis keselamatan dan konfigurasi yang perlu dilaksanakan. 12 servis dan konfigurasi adalah *Router Security (router hardening and remote login using SSH), Server Hardening (Linux server1 hardening and Windows Server Hardening), Security Service (Authentication user by integrating AD with Linux, Wireless user authentication using Radius server, IDS with port mirror, IPsec VPN for remote employees (between server and user) and Samba security services) and LAN Security (Port security and VLAN Security).* Seorang pengurus projek dari kumpulan telah ditugaskan untuk memimpin ahli-ahli kumpulan di seluruh bengkel tersebut. Kami telah dilengkapi dengan peralatan yang terdiri daripada tiga (3) server, satu (1) Cisco 2800 router (2 Fast Ethernet), satu (1) Cisco 2960 manageable switch, 15 meters UTP cable, 12 pieces RJ-45, NIC card, Access Point (AP) and one set crimping tool. Sistem operasi yang digunakan dalam server adalah Windows Server 2012, Fedora 27 dan Ubuntu 16.04. Selepas melaraskan semua konfigurasi rangkaian, infrastruktur dan servis, beberapa ujian akan dilakukan untuk memastikan ia berfungsi dengan baik. Pada akhir bengkel II, kami dikehendaki menunjukkan kerja kami kepada penyelia dan penilai. Kami juga dikehendaki menghasilkan poster dan video untuk pameran berdasarkan tajuk kami iaitu IPsec VPN.

TABLE OF CONTENT

ACKNOWLEDGEMENTS	i
ABSTRACT	ii
ABSTRAK	iii
TABLE OF CONTENT	iv
LIST OF FIGURES	xii
LIST OF TABLES	xxxvii
1.0 CHAPTER 1: INTRODUCTION	1
1.1 Introduction	1
1.2 Objective	2
1.3 Project Plan/ Schedule	3
1.4 Conclusion	4
2.0 CHAPTER 2: PROJECT REQUIREMENT	5
2.1 Introduction	5
2.2 Types of Operating System Use in the Project	5
2.3 Operating System Background	6
2.3.1 Windows Server 2012 R2	6
2.3.2 Ubuntu 16.04	6
2.3.3 Fedora 27	7
2.4 Operating System Justification	7
2.4.1 Windows Server 2012 R2	7
2.4.2 Ubuntu 16.04	8
2.4.3 Fedora 27	8

2.5 Hardware Requirement	9
2.6 Hardware Justification	9
2.6.1 Servers	9
2.6.2 NIC (Network Interface Card)	10
2.6.3 UTP (Unshielded Twisted Pair) Cable	11
2.6.4 RJ-45 (Registered Jack-45) Connector	12
2.6.5 Ethernet Cable	12
2.6.6 Switch	14
2.6.7 Router	14
2.7 Conclusion	15
3.0 CHAPTER 3: SECURITY POLICY AND NETWORK DESIGN	16
3.1 Introduction	16
3.2 Security Policy	16
3.2.1 General	16
3.2.2 Password Creation	16
3.2.3 Password Protection	16
3.2.4 Server Security Policy	17
3.2.4.1 General Requirements	17
3.2.4.2 Configuration Requirements	18
3.2.5 Network Security	18
3.2.5.1 Router and Switch Security Policy	18
3.2.6 Application Security	21
3.2.6.1 IPv6 Web Policy	21

3.2.6.2 Remote Login using SSH Policy	21
3.2.6.3 Samba Policy	22
3.2.6.4 Hardening Services Policy	22
3.2.6.4.1 Access security	22
3.2.6.4.2 File system permissions	23
3.2.6.4.3 User accounts and passwords	23
3.2.6.4.4 Software and application image/ patching and updates	23
3.2.6.4.5 LAN services policy	24
3.2.6.4.6 Proxy server security	24
3.2.6.4.7 ACL policy	24
3.2.6.4.8 Hardening server policy	25
3.2.6.4.9 Router policy	26
3.2.6.4.10 Physical Policy	27
3.3 Physical Design	28
3.4 Logical Design	29
3.5 VLAN	30
3.6 Conclusion	30
4.0 CHAPTER 4: SERVICES	31
4.1 Introduction	31
4.2 List of Services	31
4.2.1 Services for Computer Networking (BITC)	31
4.2.2 Services/Configuration for Computer Security (BITZ)	31
4.3 Overview of Services	32

4.3.1 Domain Name Services (DNS)	32
4.3.2 Dynamic Host Configuration Protocol (DHCP)	32
4.3.3 Inter VLAN and VLSM Addressing	32
4.3.4 Routing & NAT	33
4.3.5 Active Directory (AD)	33
4.3.6 Proxy Server	34
4.3.7 Samba	34
4.3.8 Network Management System	34
4.3.9 Server Virtualization	34
4.3.10 AAA (Authentication, Authorization and Accounting) using Radius	35
4.3.11 Access Control List (ACL)	35
4.3.12 Secured FTP	36
4.3.13 Web, SSL & Virtual Hosting	36
4.3.14 Linux Email Server	36
4.3.15 IPv6 Web with IPv6 Tunneling	37
4.3.16 Media Streaming Server	37
4.3.17 Cloud Server	37
4.4 Services for BITZ	38
4.4.1 Security Policy	38
4.4.2 Router Hardening	38
4.4.3 Remote Login using SSH	38
4.4.4 Linux server1 Hardening	39

4.4.5 Windows Server Hardening	39
4.4.6 Authentication User by Integrating AD with Linux	39
4.4.7 Wireless User Authentication using Radius Server	40
4.4.8 IDS with Port Mirror	40
4.4.9 IPsec VPN for Remote Employees	41
4.4.10 Samba Security Services	41
4.4.11 Port Security	42
4.4.12 VLAN Security	42
4.5 Conclusion	43
5.0 CHAPTER 5: SERVICES INSTALLATION AND CONFIGURATION	44
5.1 Introduction	44
5.2 Services and Corresponding Person-In-Charge (BITC & BITZ)	44
5.3 Installation and Configuration	46
5.3.1 Domain Name System (DNS)	46
5.3.2 Dynamic Host Configuration Protocol (DHCP) IPv4	59
5.3.3 Dynamic Host Configuration Protocol (DHCP) IPv6	63
5.3.4 Inter VLAN and VLSM Addressing	68
5.3.5 Routing & NAT	72
5.3.6 Active Directory (AD)	73
5.3.7 Authentication User by Integrating AD with Linux	82
5.3.8 Proxy Server	85
5.3.9 Samba	91
5.3.10 Samba Security Services	95

5.3.11 Network Management System (NMS)	98
5.3.12 Server Virtualization	119
5.3.13 AAA (Authentication, Authorization and Accounting) using Radius	130
5.3.14 Wireless User Authentication using Radius Server	136
5.3.15 Access Control List (ACL)	163
5.3.16 Secured FTP	164
5.3.17 Web, SSL and Virtual Hosting	168
5.3.17.1 Web	168
5.3.17.2 Secure Socket Layer (SSL)	171
5.3.17.3 Virtual Hosting	174
5.3.18 Linux Email Server	180
5.3.19 IPv6 Web with IPv6 Tunneling	195
5.3.20 Media Streaming Server	201
5.3.21 Cloud Server	207
5.3.22 Remote Login using SSH	212
5.3.23 IDS with Port Mirror	215
5.3.24 IPsec VPN for Remote Employees	220
5.3.25 Port Security	232
5.3.26 VLAN Security	234
5.3.27 Router Hardening	235
5.3.28 Linux Server1 Hardening	240
5.3.29 Windows Server Hardening	245
5.4 Conclusion	271

6.0 CHAPTER 6: SERVICE TESTING	272
6.1 Introduction	272
6.2 Service Testing	272
6.2.1 Domain Name System (IPv4 & IPv6)	272
6.2.2 Dynamic Host Configuration Protocol (DHCP) IPv4 & IP v6	273
6.2.3 Inter VLAN and VLSM Addressing	274
6.2.4 Routing & NAT	276
6.2.5 Active Directory (AD)	276
6.2.6 Authentication User by Integrating AD with Linux	280
6.2.7 Proxy Server	281
6.2.8 Samba	282
6.2.9 Samba Security Services	285
6.2.10 Network Management System (NMS)	288
6.2.11 Server Virtualization	289
6.2.12 AAA (Authentication, Authorization and Accounting) using Radius	291
6.2.13 Wireless User Authentication using Radius Server	291
6.2.14 Access Control List (ACL)	292
6.2.15 Secured FTP	295
6.2.16 Web, SSL & Virtual Hosting	298
6.2.17 Linux Email Server	299
6.2.18 IPv6 Web with IPv6 Tunneling	303
6.2.19 Media Streaming Server	304
6.2.20 Cloud Server	308

6.2.21 Remote Login using SSH	310
6.2.22 IDS with Port Mirror	312
6.2.23 IPsec VPN for Remote Employees	314
6.2.24 Port Security	317
6.2.25 VLAN Security	318
6.2.26 Router Hardening	319
6.2.27 Linux Server (Fedora) Hardening	322
6.2.28 Windows Server Hardening	324
6.3 Conclusion	325
7.0 CHAPTER 7: CONCLUSION	326
7.1 Introduction	326
7.2 Project Advantages	327
7.3 Project Disadvantages	327
7.4 Project Limitation	328
7.5 Conclusion	329
BIBLIOGRAPHY	330
APPENDIX	331

LIST OF FIGURE

<i>Figure 1: Physical Design</i>	28
<i>Figure 2: Logical Design.</i>	29
<i>Figure 3: Create new DNS using Wizard</i>	46
<i>Figure 4: Select forward lookup zone</i>	46
<i>Figure 5: Select primary zone location</i>	47
<i>Figure 6: Enter zone name.</i>	47
<i>Figure 7: Select do not allow dynamic updates.</i>	48
<i>Figure 8: Host IP Address</i>	48
<i>Figure 9: Complete DNS Configuration</i>	49
<i>Figure 10: Create New Zone</i>	49
<i>Figure 11: Select Reverse Lookup Zone Name</i>	50
<i>Figure 12: Enter Network ID</i>	50
<i>Figure 1: New Zone Wizard Is completed</i>	51
<i>Figure 2: IPv6 Host</i>	51
<i>Figure 15: IPv6 Reverse Lookup Zone</i>	52
<i>Figure 16: IPv6 Address Prefix</i>	52
<i>Figure 3: DNS Resources</i>	53
<i>Figure 18: DNS Resources</i>	54
<i>Figure 4: DNS Resources</i>	54

<i>Figure 20: New Zone Wizard</i>	55
<i>Figure 21: Select the zone type</i>	56
<i>Figure 22: Select type of zone</i>	56
<i>Figure 23: Master DNS Server IP</i>	57
<i>Figure 24: New Zone Wizard is completed</i>	57
<i>Figure 25: Secondary DNS Resources</i>	58
<i>Figure 26: Adding role for DHCP</i>	59
<i>Figure 27: Select features for DHCP</i>	59
<i>Figure 28: DHCP role to be completed</i>	60
<i>Figure 29: DHCP configuration page</i>	60
<i>Figure 30: Create scope name for New Scope Wizard</i>	61
<i>Figure 31: Set the lease duration</i>	61
<i>Figure 32: Results of DHCP page</i>	62
<i>Figure 33: IP Helper command</i>	62
<i>Figure 34: Install DHCP from server manager</i>	63
<i>Figure 35: Choose New Scope</i>	63
<i>Figure 36: Add name in New Scope Wizard</i>	64
<i>Figure 37: Insert prefix</i>	64
<i>Figure 38: Scope Lease</i>	65
<i>Figure 39: New Scope Wizard completed</i>	65
<i>Figure 40: Choose New Scope</i>	66
<i>Figure 41: Add name in New Scope Wizard</i>	66

<i>Figure 42: Insert Prefix</i>	67
<i>Figure 43: Scope Lease</i>	67
<i>Figure 44: New Scope Wizard completed</i>	68
<i>Figure 45: Creating VLAN for Window Server</i>	68
<i>Figure 46: Creating VLAN for Ubuntu Server</i>	69
<i>Figure 47: Creating VLAN for Fedora Server</i>	69
<i>Figure 48: Creating VLAN for AP</i>	69
<i>Figure 49: Creating VLAN for User</i>	69
<i>Figure 50: Creating trunk from Switch to Router</i>	70
<i>Figure 51: Configure trunking for VLAN 10</i>	70
<i>Figure 52: Configure trunking for VLAN 20</i>	70
<i>Figure 53: Configure trunking for VLAN 30</i>	70
<i>Figure 54: Configure trunking for VLAN 50</i>	71
<i>Figure 55: Configure trunking for VLAN 51</i>	71
<i>Figure 56: Configure trunking for VLAN 3</i>	71
<i>Figure 57: IP NAT Outside</i>	72
<i>Figure 58: IP NAT inside</i>	72
<i>Figure 59: Static NAT public IP to all servers</i>	72
<i>Figure 60: NAT Setup</i>	72
<i>Figure 61: AD server roles selection</i>	73
<i>Figure 62: Installation progress for AD</i>	73
<i>Figure 63: AD DS roles in Dashboard</i>	74

<i>Figure 64: Tools at menu bar and click AD Users and Computer</i>	74
<i>Figure 65: Creating New User</i>	75
<i>Figure 66: Creating new user</i>	75
<i>Figure 67: Detailed of user data</i>	76
<i>Figure 68: Selecting groups</i>	76
<i>Figure 69: GPO Management Dashboard</i>	77
<i>Figure 70: GPO Status</i>	77
<i>Figure 71: Create GPO in this domain</i>	78
<i>Figure 72: Creating new GPO</i>	78
<i>Figure 73: GPO Status of Client policy</i>	79
<i>Figure 74: GPO Management Editor</i>	79
<i>Figure 75: Personalization of GPO</i>	80
<i>Figure 76: Personalization policy for the client</i>	80
<i>Figure 77: Policy update</i>	81
<i>Figure 78: Install apache2</i>	82
<i>Figure 79: Apache2 configuration</i>	82
<i>Figure 80: PBIS download and installation</i>	83
<i>Figure 81: Command to join domain</i>	83
<i>Figure 82: AD Users and Computer addition of Ubuntu</i>	84
<i>Figure 83: Command to install squid package</i>	85
<i>Figure 84: Edit squid configuration</i>	85
<i>Figure 85: Change http access in configuration file</i>	86

<i>Figure 86: Http access change to allow</i>	86
<i>Figure 87: Start Squid service.</i>	87
<i>Figure 88: Decide to block which need to be blocked</i>	87
<i>Figure 89: Insert domain/keyword that need to be blocked</i>	88
<i>Figure 90: Configure squid configuration</i>	88
<i>Figure 91: Squid status</i>	89
<i>Figure 92: Connection Settings</i>	89
<i>Figure 93: Network proxy setting</i>	90
<i>Figure 94: Samba package installation in Fedora</i>	91
<i>Figure 95: Download result</i>	91
<i>Figure 96: Enabling samba services</i>	92
<i>Figure 97: Opening port using service file of firewalld-cmd</i>	92
<i>Figure 98: Enabling access to home directory</i>	92
<i>Figure 99: Creating new user and password in Fedora</i>	93
<i>Figure 100: Home directory for each user by default</i>	93
<i>Figure 101: Editing configuration file</i>	93
<i>Figure 102: Permission sharing</i>	94
<i>Figure 103: Samba file location</i>	94
<i>Figure 104: Creating new group</i>	95
<i>Figure 105: Creating new directory</i>	95
<i>Figure 106: Operating security on the directory</i>	95
<i>Figure 107: Setting the permission file</i>	96

<i>Figure 108: Specify host allowed and host denied.</i>	96
<i>Figure 109: Starting samba service</i>	97
<i>Figure 110: Adding user authentication</i>	97
<i>Figure 111: Usermod of Security pelajar</i>	97
<i>Figure 112: Root login</i>	98
<i>Figure 113: Updating the system</i>	98
<i>Figure 114: Installing the update</i>	99
<i>Figure 115: Updating the package index</i>	99
<i>Figure 116: Installing Zabbix server</i>	100
<i>Figure 117: Creating new MySQL database</i>	100
<i>Figure 118: Creating database zabbixdb</i>	101
<i>Figure 119: Continuing creating database zabbixdb</i>	101
<i>Figure 120: Importing the initial schema and data</i>	101
<i>Figure 121: Configuring zabbix-server</i>	102
<i>Figure 122: Start Apache server</i>	102
<i>Figure 123: Zabbix installation process created</i>	103
<i>Figure 124: Replacing time zone</i>	103
<i>Figure 125: Install PHP modules that Zabbix needs</i>	104
<i>Figure 126: Continuing to install</i>	104
<i>Figure 127: Zabbix Server Web Installer</i>	105
<i>Figure 128: Zabbix database configuration screen</i>	105
<i>Figure 129: Configuration Zabbix DB connection</i>	106

<i>Figure 130: Summary of Pre-Installation</i>	106
<i>Figure 131: Pre-Installation summary to verify</i>	107
<i>Figure 132: Installation of repository configuration package</i>	107
<i>Figure 133: Updating package index</i>	108
<i>Figure 134: Zabbix agent installation</i>	108
<i>Figure 135: Zabbix agent configuration file</i>	109
<i>Figure 136: Start agent service</i>	109
<i>Figure 137: Installing package on Fedora</i>	110
<i>Figure 138: Installing Zabbix agent in Fedora</i>	110
<i>Figure 139: Continuing installing Zabbix agent in Fedora</i>	111
<i>Figure 140: Zabbix agent configuration file editing</i>	111
<i>Figure 141: Continuing editting Zabbix agent</i>	112
<i>Figure 142: Entering Zabbix Server</i>	112
<i>Figure 143: Opening port to allow Zabbix server with agent</i>	113
<i>Figure 144: Restarting agent service to reload new setting</i>	113
<i>Figure 145: Downloading latest windows zabbix agent</i>	114
<i>Figure 146: Making copy of sample configuration file</i>	114
<i>Figure 147: Edit configuration files and update the values</i>	115
<i>Figure 148: Installation of Zabbix ad Windows server</i>	116
<i>Figure 149: Services.msc window</i>	116
<i>Figure 150: Allowing apps to communicate through Windows firewall</i>	117
<i>Figure 151: Login screen of Zabbix</i>	118

<i>Figure 152: Zabbix Dashboard</i>	118
<i>Figure 153: Installation of Hyper-V</i>	119
<i>Figure 154: Installation of virtual windows server in Hyper-V</i>	119
<i>Figure 155: Results of Window Server</i>	120
<i>Figure 156: Server manager dashboard</i>	120
<i>Figure 157: Installation progress in virtual Windows server</i>	121
<i>Figure 158: Start page of IIS Manager</i>	122
<i>Figure 159: Creating new site in IIS</i>	122
<i>Figure 160: Adding new file document</i>	123
<i>Figure 161: Website that have been added in IIS Manager</i>	123
<i>Figure 162: Adding new zone at DNS Manager</i>	124
<i>Figure 163: Dynamic update</i>	124
<i>Figure 164: New Zone Wizard completed</i>	125
<i>Figure 165: DNS Manager to choose for new host</i>	125
<i>Figure 166: Adding new host and IP Address</i>	126
<i>Figure 167: Certificate chosen in IIS Manager</i>	126
<i>Figure 168: Server Certificates in IIS Manager</i>	127
<i>Figure 169: Adding SSL Name</i>	127
<i>Figure 170: Result of certificate that has been created</i>	128
<i>Figure 171: Website Addition</i>	128
<i>Figure 172: Default Document in IIS Manager</i>	129
<i>Figure 173: Installation progress of NPS, Routing and Remote Access</i>	130

<i>Figure 174: Admin Properties</i>	131
<i>Figure 175: Adding new RADIUS client</i>	131
<i>Figure 176: Group4 Properties</i>	132
<i>Figure 177: Vendor name of new RADIUS client</i>	132
<i>Figure 178: Specify connection request policy</i>	133
<i>Figure 179: Condition Selection</i>	133
<i>Figure 180: Specify connection request forwarding</i>	134
<i>Figure 181: Network Policy</i>	134
<i>Figure 182: Command AAA at router</i>	135
<i>Figure 183: IP Address of the AP</i>	136
<i>Figure 184: Wireless configuration inside the Linksys</i>	136
<i>Figure 185: Confirmation to continue updating network setting</i>	137
<i>Figure 186: Symbol to create new group</i>	137
<i>Figure 187: Creating new object – Group</i>	138
<i>Figure 188: Symbol to create new object – User</i>	138
<i>Figure 189: Creating new user</i>	139
<i>Figure 190: Creating password to the user</i>	140
<i>Figure 191: Confirmation of User</i>	140
<i>Figure 192: Members of group4wifi</i>	141
<i>Figure 193: Add Roles and Features Wizard</i>	142
<i>Figure 194: Select installation type</i>	142
<i>Figure 195: Select destination server</i>	143

<i>Figure 196: Adding features for AD CS</i>	143
<i>Figure 197: Selecting Server Roles</i>	144
<i>Figure 198: Installation progress of the additional features</i>	144
<i>Figure 199: Role services configuration</i>	145
<i>Figure 200: Role service selection for AD CS configuration</i>	145
<i>Figure 201: Setup type of CA</i>	146
<i>Figure 202: CA type specification</i>	146
<i>Figure 203: Choosing the private key</i>	147
<i>Figure 204: Selecting cryptography for CA</i>	147
<i>Figure 205: Specify CA name</i>	148
<i>Figure 206: Specify validity period</i>	148
<i>Figure 207: Specify database location</i>	149
<i>Figure 208: Confirmation of AD CS configuration</i>	149
<i>Figure 209: Results of AD CS Configuration</i>	150
<i>Figure 210: Console root page</i>	150
<i>Figure 211: Adding or Remove snap-ins</i>	151
<i>Figure 212: Choosing certificates snap in</i>	151
<i>Figure 213: Select the computer to manage snap-in</i>	152
<i>Figure 214: Loading the certificate into console</i>	152
<i>Figure 215: Beginning of certificate enrollment</i>	153
<i>Figure 216: Selecting certificate enrollment policy</i>	153
<i>Figure 217: Requesting certificates</i>	154

<i>Figure 218: Installation of certificate</i>	154
<i>Figure 219: Network Policy Server page</i>	155
<i>Figure 220: Select 802.1X connections type</i>	156
<i>Figure 221: Setting up new RADIUS client</i>	157
<i>Figure 222: Select the EAP type for the policy</i>	158
<i>Figure 223: Specify user group</i>	158
<i>Figure 224: Completing the RADIUS client</i>	159
<i>Figure 225: Certificate Export Wizard</i>	160
<i>Figure 226: Choose whether to export the private key or not</i>	160
<i>Figure 227: Selecting export file format</i>	161
<i>Figure 228: Specify the name of the file that wanted to be exported</i>	161
<i>Figure 229: Completing the certificate export wizard</i>	162
<i>Figure 230: Configuring ACL at Router</i>	163
<i>Figure 231: Showing ACL configuration</i>	163
<i>Figure 232: Updating all package before installation</i>	164
<i>Figure 233: Installing vsftpd service</i>	164
<i>Figure 234: Get in vsftpd configuration</i>	165
<i>Figure 235: Restarting and enabling service</i>	165
<i>Figure 236: Adding port 21 to secure ftp</i>	165
<i>Figure 237: Create group and user</i>	166
<i>Figure 238: Making directory</i>	166
<i>Figure 239: Changing the mode of secure ftp</i>	166

<i>Figure 240: Get into sshd config</i>	166
<i>Figure 241: Inserting comment at subsystem sftp</i>	167
<i>Figure 242: Restarting SSH service</i>	167
<i>Figure 243: Installing http service packet</i>	168
<i>Figure 244: Edit the configuration file of httpd</i>	168
<i>Figure 245: Configure the httpd</i>	168
<i>Figure 246: Changing the status</i>	169
<i>Figure 247: Configuration file of httpd</i>	170
<i>Figure 248: Restart http service and allow the firewall</i>	179
<i>Figure 249: Status of httpd</i>	171
<i>Figure 250: Creating key for web server in certification folder</i>	171
<i>Figure 251: Creating csr for the group</i>	172
<i>Figure 252: Setting all the implementation</i>	172
<i>Figure 253: Making SSL certificate at correct location</i>	173
<i>Figure 254: Reloading the SSL</i>	173
<i>Figure 255: Setting the SSL protocols</i>	173
<i>Figure 256: Server Manager and click on DNS</i>	174
<i>Figure 257: DNS Manager</i>	174
<i>Figure 258: Forward Lookup zone</i>	175
<i>Figure 259: New Zone Wizard page</i>	175
<i>Figure 260: Selecting the zone type</i>	176
<i>Figure 261: Insert new zone name for virtual host</i>	176

<i>Figure 262: Selecting dynamic update</i>	177
<i>Figure 263: Completing new zone wizard</i>	177
<i>Figure 264: Create new Host in the new zone</i>	178
<i>Figure 265: Inserting the name and IP Address for new host</i>	178
<i>Figure 266: Open Terminal in Fedora and edit the configuration file</i>	179
<i>Figure 267: Checking all port and path directory</i>	179
<i>Figure 268: Restart the httpd service</i>	179
<i>Figure 269: Install the postfix using this command</i>	180
<i>Figure 270: Postfix configuration</i>	180
<i>Figure 271: Postfix configuration</i>	180
<i>Figure 272: Installing Dovecot core package</i>	181
<i>Figure 273: Checking Dovecot package</i>	181
<i>Figure 274: Edit main config file</i>	181
<i>Figure 275: Edit main config file</i>	182
<i>Figure 276: Find email spool directory</i>	182
<i>Figure 277: Configuring authentication mechanism</i>	183
<i>Figure 278: Configuring authentication mechanism</i>	183
<i>Figure 279: Adding dovecot to mail group</i>	184
<i>Figure 280: Edit the authentication file</i>	185
<i>Figure 281: Edit the authentication file</i>	186
<i>Figure 282: Edit SSL/TLS config</i>	186
<i>Figure 283: Continuing editing SSL/TLS file</i>	187
<i>Figure 284: Edit the file so that Postfix can find dovecot authentication server</i>	187

<i>Figure 285: Continuation of editing file</i>	188
<i>Figure 286: Edit and auto create a folder</i>	189
<i>Figure 287: Restarting Dovecot and restart Postfix</i>	190
<i>Figure 288: Installing Rainloop</i>	190
<i>Figure 289: See the rainloop installation status</i>	191
<i>Figure 290: Unzip Rainloop</i>	191
<i>Figure 291: See the entire file.</i>	192
<i>Figure 292: Changing mode of the rainloop</i>	192
<i>Figure 293: Creating new file</i>	193
<i>Figure 294: Restart the Apache</i>	193
<i>Figure 295: Mail page at browser</i>	193
<i>Figure 296: Changing the password</i>	194
<i>Figure 297: Adding new website</i>	195
<i>Figure 298: Set the document that want to display on website</i>	195
<i>Figure 299: Adding new zone at DNS Manager</i>	196
<i>Figure 300: Specify the Dynamic Update</i>	196
<i>Figure 301: Completing new zone wizard</i>	197
<i>Figure 302: Adding new host for the domain</i>	197
<i>Figure 303: Add new host and IP Address</i>	198
<i>Figure 304: Check the Site Binding</i>	198
<i>Figure 305: Create tunnel interface at router</i>	199
<i>Figure 306: Set the IPv6 Router OSPF</i>	199
<i>Figure 307: Insert IPv6 address into terminal configuration</i>	199

<i>Figure 308: Set the OSPF and area of each inter-VLAN</i>	200
<i>Figure 309: Create new repo file</i>	201
<i>Figure 310: Downloads the plex</i>	201
<i>Figure 311: Installing plex media server</i>	202
<i>Figure 312: Start plex service</i>	202
<i>Figure 313: Start and enable plex media server</i>	203
<i>Figure 314: Check the status of media plex server</i>	203
<i>Figure 315: Enabling Firewall services</i>	204
<i>Figure 316: Start firewall service</i>	204
<i>Figure 317: Add new firewall for plex</i>	205
<i>Figure 318: Add plex media server to firewalld service</i>	206
<i>Figure 319: Check the status</i>	206
<i>Figure 320: Installing Lamp Server</i>	207
<i>Figure 321: Configuring root password for MySQL</i>	207
<i>Figure 322: Install related dependencies</i>	208
<i>Figure 323: Download Nextcloud zip files</i>	208
<i>Figure 324: Extract Nextcloud.zip</i>	209
<i>Figure 325: Move the extracted file</i>	209
<i>Figure 326: Change the ownership and setup MySQL</i>	210
<i>Figure 327: Create database Nextcloud and admin user</i>	210
<i>Figure 328: Setup Nextcloud configuration file</i>	211
<i>Figure 329: Enable module rewrite and restart apache2</i>	211
<i>Figure 330: SSH configuration in router</i>	212

<i>Figure 331: SSH configuration in switch</i>	212
<i>Figure 332: SSH configuration in Ubuntu</i>	213
<i>Figure 333: Check the status of the SSH</i>	213
<i>Figure 334: Change user to root</i>	214
<i>Figure 335: SSH command to install</i>	214
<i>Figure 336: Start the SSH Service</i>	214
<i>Figure 337: Check the status of SSH service</i>	214
<i>Figure 338: Install the library needs for snort</i>	215
<i>Figure 339: Install and build DAQ</i>	215
<i>Figure 340: Extract the file</i>	215
<i>Figure 341: Configure, make and install the file</i>	215
<i>Figure 342: Install the Snort</i>	216
<i>Figure 343: Extract the downloaded file</i>	216
<i>Figure 344: Repeat step for DAQ installation</i>	216
<i>Figure 345: Create a log directory and give ownership to Snort</i>	216
<i>Figure 346: Download snort rule</i>	217
<i>Figure 347: Create white list and black list rule</i>	217
<i>Figure 348: Create directory for dynamic rule</i>	217
<i>Figure 349: Change the ownership</i>	218
<i>Figure 350: Edit default snort configuration</i>	218
<i>Figure 351: Change to network that we are protecting</i>	218
<i>Figure 352: Change the rules path</i>	218
<i>Figure 353: Configuring port monitor at switch</i>	219

<i>Figure 354: Display monitor session</i>	219
<i>Figure 355: SoftEther Setup Wizard</i>	220
<i>Figure 356: Specify directory to install</i>	221
<i>Figure 357: Install SoftEther VPN server</i>	222
<i>Figure 358: Click on Localhost</i>	223
<i>Figure 359: SoftEther VPN server/ Bridge Easy Setup</i>	224
<i>Figure 360: Create IPsec pre-shared key</i>	224
<i>Figure 361: Create a group and full name</i>	225
<i>Figure 362: Manage virtual hub</i>	225
<i>Figure 363: Create User</i>	226
<i>Figure 364: Manage Virtual NAT and DHCP</i>	226
<i>Figure 365: Enabling Secure NAT</i>	227
<i>Figure 366: Specify IP Address range</i>	228
<i>Figure 367: Install SoftEther client on client's PC</i>	228
<i>Figure 368: Finish installation</i>	229
<i>Figure 369: SoftEther VPN Client Manager</i>	229
<i>Figure 370: Creating virtual network adapter</i>	230
<i>Figure 371: Enter all details in of server IP</i>	230
<i>Figure 372: Establishing VPN connection</i>	231
<i>Figure 373: VPN is now connected</i>	231
<i>Figure 374: Errdisable command</i>	232
<i>Figure 375: Port security on Windows server interface</i>	232
<i>Figure 376: Port security on Ubuntu server interface</i>	232

<i>Figure 377: Port security on Fedora server interface</i>	233
<i>Figure 378: VLAN allowed for trunk</i>	234
<i>Figure 379: Setting native VLAN</i>	234
<i>Figure 380: VLAN hopping prevention</i>	234
<i>Figure 381: Putty Login</i>	235
<i>Figure 382: Banner motd</i>	236
<i>Figure 383: System Log</i>	237
<i>Figure 384: Disable console and monitor logs</i>	237
<i>Figure 385: Enable syslog</i>	238
<i>Figure 386: Show Archive log config</i>	239
<i>Figure 387: Change user to root</i>	240
<i>Figure 388: Installing the new updates</i>	240
<i>Figure 389: View the current status</i>	241
<i>Figure 390: Edit the details command</i>	241
<i>Figure 391: Checking the changes</i>	241
<i>Figure 392: Install the Nmap</i>	242
<i>Figure 393: Display list of scan port</i>	242
<i>Figure 394: Disable CUPS service</i>	244
<i>Figure 395: Checking the status</i>	244
<i>Figure 396: Server Manager Dashboard</i>	245
<i>Figure 397: Security configuration wizard</i>	245
<i>Figure 398: Create new security policy</i>	246
<i>Figure 399: Insert server name</i>	246

<i>Figure 400: Complete the processing</i>	247
<i>Figure 401: Role based service configuration</i>	247
<i>Figure 402: Select server roles</i>	248
<i>Figure 403: Select server roles</i>	248
<i>Figure 404: Select client features</i>	249
<i>Figure 405: Select options used to administrate the selected server</i>	249
<i>Figure 406: Select additional services</i>	250
<i>Figure 407: Select Handling Unspecified services</i>	250
<i>Figure 408: Confirm service changes</i>	251
<i>Figure 409: Network security first page</i>	251
<i>Figure 410: Select network security rules</i>	252
<i>Figure 411: Registry setting first page</i>	252
<i>Figure 412: Select attributes needed for SMB Security Signature</i>	253
<i>Figure 413: Determine LDAP Signing</i>	253
<i>Figure 414: Select outbound authentication method</i>	254
<i>Figure 415: Select outbound authentication using Domain Accounts</i>	254
<i>Figure 416: Registry setting summary</i>	255
<i>Figure 417: First page of audit policy</i>	255
<i>Figure 418: Select system audit policy</i>	256
<i>Figure 419: Summary of audit policy</i>	256
<i>Figure 420: Security policy that has need to be save</i>	257
<i>Figure 421: Save the name and location</i>	257
<i>Figure 422: Select to apply security policy</i>	258

<i>Figure 423: Security configuration Wizard has completed</i>	258
<i>Figure 424: Security configuration wizard is complete</i>	259
<i>Figure 425: Server Manager dashboard</i>	259
<i>Figure 426: Disable account for guest</i>	260
<i>Figure 427: Local security policy</i>	260
<i>Figure 428: Audit policy</i>	261
<i>Figure 429: Local security setting for audit privilege use</i>	261
<i>Figure 430: Search for Windows Update</i>	262
<i>Figure 431: Change the setting of Installation updates</i>	262
<i>Figure 432: Check for available updates</i>	263
<i>Figure 433: Choose the updates that need to be installed</i>	263
<i>Figure 434: Server Manager dashboard</i>	264
<i>Figure 435: Enabling Firewall</i>	264
<i>Figure 436: Search for services.msc</i>	265
<i>Figure 437: Change the Startup Type of Distributed Transaction Coordinator Properties</i>	265
<i>Figure 438: Change the Startup Type of KtmRm for Distributed Transaction Coordinator Properties</i>	266
<i>Figure 439: Change the Startup Type of Print Spooler Properties</i>	267
<i>Figure 440: Search for services.msc</i>	267
<i>Figure 441: Change the Startup Type of Windows Error Reporting Service</i>	268
<i>Figure 442: Change the Startup Type of Secure Socket Tunneling Protocol Service Properties</i>	268
<i>Figure 443: Change the Startup Type of Certificate Propagation Properties</i>	269
<i>Figure 444: Change the Startup Type of NetLogon</i>	269

<i>Figure 445: Windows Error Reporting Service</i>	270
<i>Figure 446: Check the status of Certificate Propagation</i>	270
<i>Figure 447: Ensure NetLogon startup type</i>	271
<i>Figure 448: Nslookup</i>	272
<i>Figure 449: DHCP Testing</i>	273
<i>Figure 450: wired_user_ipv6 connected</i>	273
<i>Figure 451: wireless_user_ipv6 connected</i>	274
<i>Figure 452: Command to see VLAN Configuration</i>	274
<i>Figure 453: Command to see trunking configuration</i>	275
<i>Figure 454: Show IP NAT Translation</i>	276
<i>Figure 455: System properties</i>	276
<i>Figure 456: Computer Name/Domain Changes</i>	277
<i>Figure 457: AD user account</i>	277
<i>Figure 458: Login User Account</i>	278
<i>Figure 459: File Explorer</i>	278
<i>Figure 460: Connect to external hard disk/USB</i>	279
<i>Figure 461: Pop-up Access Denied</i>	279
<i>Figure 462: Log in username</i>	280
<i>Figure 463: Enter the password</i>	280
<i>Figure 464: Successfully access</i>	281
<i>Figure 465: Proxy Status</i>	281
<i>Figure 466: Blocked Website by Proxy</i>	282
<i>Figure 467: Enter username and password for authorized to access Samba</i>	282

<i>Figure 468: Shared files in Samba Folder</i>	283
<i>Figure 469: Connect to Samba Server</i>	283
<i>Figure 470: The shared folder is visible</i>	284
<i>Figure 471: Enter username and password</i>	284
<i>Figure 472: Shared files in Samba shared folder</i>	285
<i>Figure 473: Enter IP Address and connect</i>	285
<i>Figure 474: Input username and password</i>	286
<i>Figure 475: Failed to open file</i>	286
<i>Figure 476: Open Secure Folder in Windows</i>	287
<i>Figure 477: Samba can be opened in Windows</i>	287
<i>Figure 478: Open browser and login a username and password</i>	288
<i>Figure 479: Zabbix NMS</i>	289
<i>Figure 480: Web Hyper-V testing</i>	290
<i>Figure 481 Secure Browsing Hyper-V Testing</i>	290
<i>Figure 482: Result at putty when user trying to login into the router</i>	291
<i>Figure 483: Insert identity and password</i>	291
<i>Figure 484: Wireless authentication successful</i>	292
<i>Figure 485: ACL Configuration</i>	292
<i>Figure 486: Open browser</i>	293
<i>Figure 487: Display on other group browser.</i>	293
<i>Figure 488: Folder Samba can't be access</i>	294
<i>Figure 489: Samba can't be access</i>	294
<i>Figure 490: Command for access “sftp sftpuser2@192.168.30.4”</i>	295

<i>Figure 491: List only one folder that name files</i>	295
<i>Figure 492: Get File FedoraSFTP.txt</i>	295
<i>Figure 493: Command for access “<code>sftp sftpuser2@192.168.30.4</code>”</i>	296
<i>Figure 494: List only one folder that name files</i>	296
<i>Figure 495: Send file FedoraSFTP.txt</i>	296
<i>Figure 496: Command for access “<code>ssh sftpuser2@192.168.30.4</code>”</i>	296
<i>Figure 497: Close the connection SSH for secure ftp user</i>	297
<i>Figure 498: FileZilla Client software and connect to group4 network</i>	297
<i>Figure 499: Web browser</i>	298
<i>Figure 500: SSL secure browser</i>	298
<i>Figure 501: Virtual hosting browser</i>	299
<i>Figure 502: user login and password</i>	299
<i>Figure 503: change and update password</i>	300
<i>Figure 504: Rainloop – Admin Panel</i>	300
<i>Figure 505: Send email to user</i>	301
<i>Figure 506: Add user account</i>	301
<i>Figure 507: Add account by adding email and password</i>	302
<i>Figure 508: Successfully received email</i>	302
<i>Figure 509: Web testing using domain name</i>	303
<i>Figure 510: Group 3 access website</i>	304
<i>Figure 511: Plex Web</i>	304
<i>Figure 512: Add library for add media files</i>	305
<i>Figure 513: Choose media to upload</i>	305

<i>Figure 514: Browse media folder</i>	306
<i>Figure 515: Add the media</i>	306
<i>Figure 516: Add Library</i>	307
<i>Figure 517: Successfully photo uploaded</i>	307
<i>Figure 518: Login to NextCloud</i>	308
<i>Figure 519: Homepage upon login success</i>	308
<i>Figure 520: Access NextCloud from Windows Server</i>	309
<i>Figure 521: Test to access the content</i>	309
<i>Figure 522: Start SSH</i>	310
<i>Figure 523: Login and create files</i>	310
<i>Figure 524: Check file at Fedora</i>	310
<i>Figure 525: start and check status SSH</i>	311
<i>Figure 526: Login Ubuntu from Fedora</i>	311
<i>Figure 527: Create Ubuntu file from Fedora</i>	312
<i>Figure 528: Check existing file at Desktop</i>	312
<i>Figure 529: Monitor session interface</i>	312
<i>Figure 530: Command to start the IDS</i>	313
<i>Figure 531: ping from HOME_NET to other host</i>	313
<i>Figure 532: type correct information to add VPN on PC client</i>	314
<i>Figure 533: Type correct information</i>	315
<i>Figure 534: VPN is connected</i>	316
<i>Figure 535: VPN in Client Manager Connected</i>	317
<i>Figure 536: Check port-security status</i>	317

<i>Figure 537: Trunk setting in port</i>	318
<i>Figure 538: Display sh run command</i>	318
<i>Figure 539: Options controlling session logging</i>	319
<i>Figure 540: save log file name</i>	320
<i>Figure 541: Create log file in router</i>	320
<i>Figure 542: Location and save of log file</i>	321
<i>Figure 543: Show the configuration of log file</i>	321
<i>Figure 544: Before change the password expiry</i>	322
<i>Figure 545: After change the password expiry</i>	322
<i>Figure 546: Before disabling port</i>	323
<i>Figure 547: After disabling port 631</i>	323
<i>Figure 548: Services start-up type started and automatic</i>	324
<i>Figure 549: Status of Certificate Propagation</i>	324
<i>Figure 550: Net Logon information services</i>	325

LIST OF TABLE

Table 1: Server Configuration Ubuntu 16.04 LTS	8
Table 2: Server configuration Fedora 27	9
Table 3: VLAN	30
Table 4: Services distribution.	45
Table 5: Gantt Chart	331

1.0 INTRODUCTION

1.1 Introduction

The subject BITU 3923, Workshop II is taken by BITC and BITZ student before graduation as a platform for them to train and prepare for their Industrial Training and Final Year Project. During Workshop II, students are divided into a group consists of 8 members which are 6 students from BITC and 3 students from BITZ. This is to develop a project based on their majoring. Workshop II provides an opportunity to students to practice their knowledge and experiences gained from previous subjects.

Basically, BITC student need to develop a network infrastructure with a minimum of 18 services and BITZ student must perform 12 security services/configuration and draft the Security Policy. This project also required the student to analyze, design, built, manage and integrate network services infrastructure to suit the network environment while maintain and control the network services infrastructure. Therefore, students can develop their understanding of problem-solving techniques to solve the particular problem based on their respective project.

We have been provided with the equipment which are three (3) servers which are Ubuntu 16.04, Windows Server 2012 and Fedora 27, one (1) Cisco 2800 router (2 Fast Ethernet), one (1) Cisco 2960 manageable switch, 15 meters UTP cable, one (1) NIC, 12 pieces of RJ-45 and one set crimping tool. By using the equipment above, we are required to design, setup, maintain and monitor a network environment with basic server applications and fundamental services. Finally, after the network is up to service, we need to ensure that our domain can communicate with another group's domain.

1.2 Objective

Our main objective for Workshop II is to build a network in a difference operating system in LAN and WAN connection and develop an understanding of problem-solving techniques to solve a particular problem or services. Besides, the objective of the network development is:

- i. To design network infrastructure by using the provided equipment and tools.
- ii. To ensure that our network environment will be able to communicate to another network environment.
- iii. To be able to maintain and control the network services infrastructure.
- iv. To ensure the learners get the necessary skills and knowledge that is required to design, set up and configure network equipment.
- v. To ensure the security services installed will work efficiently.

1.3 Project Plan/ Schedule

In week 1 and week 2, we will be assigned to the respective supervisors. Then, we borrow the equipment needed such as router, switch and servers from the faculty. We will prepare the project proposal that includes the details of the project such as the executive summary, logical and physical network design to show the network topology, Gantt chart is developed to show the timeline of the project and project distribution where the project manager will distribute the tasks to all the members accordingly. We will submit the finalized proposal by the end of week 2.

After the submission of the project proposal, we will proceed to set up the services needed for this project. There are 5 services that we plan to install during this period. The services include VLAN, IPv6, DNS, DHCP and the service for video (IPsec VPN). Our group starts to install and configure the services planned before week 5 to accomplish the progress 1.

From week 6 to week 10, we plan to proceed to set up the 25 other services. The examples are setting up IPsec between server and user, proxy server, install Samba Security services, set up web, SSL and virtual hosting and radius server for network accounting. Our group completed to install and configure 25 services within 4 weeks and accomplished the progress II.

During week 11 to week 13, we will proceed towards completing the setup of the whole network and setup of all services required. At the same time, we will prepare a video and a poster based on our project title IPsec VPN. After the completion of the network setup, we will demonstrate our respective task individually to the supervisor and evaluator at the week 12 and week 13 respectively.

At week 14, the final report and individual log book will be revised if there is any error and improved. The video and poster produced during week 11 to week 12 will be used in the video and poster exhibition during the showcase. The completed video and poster will be evaluated by the supervisors and evaluator. The finalized final report and individual log book will be submitted during study week which is equivalent to week 15.

1.4 Conclusion

Upon the completion of workshop II, we are able to install, configure, set up, monitor and maintain a complete network given the necessary network equipment and services. We are also exposed to different operating system environment. We should be able to design our own network and maintain a good network environment. Moreover, we will learn to build up a crucial security system to secure and protect the network from being attacked and compromised. This is very important because we can train our team to work not only for industrial training but in the future as well. Besides, we will be able to apply teamwork and project management skills in the future. All of these are the basic requirements that prepare us for the real working environment. In addition, we can apply our knowledge we gained in class through practical and find out our weaknesses and improve them. Finally, we can gain extra knowledge, experience and confidence to face the future challenges in final year project and industrial training.

2.0 PROJECT REQUIREMENT

2.1 Introduction

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

In this workshop, we have been provided with the equipment which are three (3) servers, one (1) Cisco 2800 router (2 Fast Ethernet), one (1) Cisco 2960 manageable switch, 15 meters UTP cable, 12 pieces RJ-45 and one set crimping tool. By using the equipment listed, we are required to design, set up, maintain and monitor a network environment with basic server applications and fundamental services.

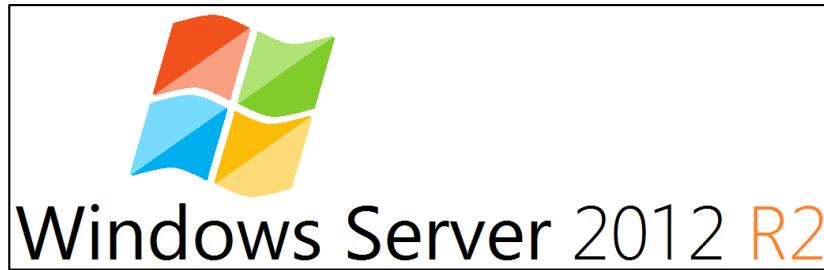
2.2 Types of Operating System use in the project

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

1. Window Server 2012 R2
2. Ubuntu 16.04 LTS (Linux-Based)
3. Fedora 27

2.3 Operating System Background

2.3.1 Window Server 2012 R2



Windows Server 2012 R2 is the server operating system developed by Microsoft. It is the sixth release of Windows Server. It is the server version of version of Windows 8 and succeeds Windows Server 2008 R2.

Unlike its predecessor, Windows Server 2012 has no support for Itanium-based computers and has four editions. Various features were added or improved over Windows Server 2008 R2 such as Hyper-V, an IP address management role, a new version of Windows Task Manager, and ReFS; a new file system.

2.3.2 Ubuntu 16.04 LTS (Linux-Based)



Ubuntu is a Debian-based Linux operating system for personal computers, tablets and smart phones, where Ubuntu Touch edition is used; and also runs network servers, usually with the Ubuntu Server edition, either on physical or virtual servers. Ubuntu 16.04 runs on all major architectures – x86, x86-64, ARM v7, ARM64, POWER8 and IBM System z mainframes via LinuxONE.

For the Ubuntu desktop release 16.04 LTS, a PC with at least 2 GHz dual-core processor, 2 GB of RAM and 25 GB of free disk space is recommended. For less powerful computers, there are other Ubuntu distributions such as Lubuntu

and Xubuntu. Since version 12.04, Ubuntu supports the ARM architecture. Ubuntu is also available on Power, older PowerPC architecture was at one point unofficial supported, and now newer Power Architecture CPUs (POWER8) are supported.

2.3.3 Fedora 27



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-sources licenses and aims to be on the leading edge of such technologies. Fedora is the upstream sources of the commercial Red Hat Enterprise Linux distribution.

Since the release of Fedora 21, three different editions are currently available which are Workstation (focused on the personal computer), Server (for servers) and Atomic (focus on cloud computing).

2.4 Operating System Justification

2.4.1 Windows Server 2012 R2

Windows Server 2012 R2 is the server operating system developed by Microsoft. It is the sixth release of Windows Server. It is the server version of version of Windows 8 and succeeds Windows Server 2008 R2. Unlike its predecessor, Windows Server 2012 has no support for Itanium-based computers and has four editions. Various features were added or improved over Windows Server 2008 R2 such as Hyper-V, an IP address management role, a new version of Windows Task Manager, and ReFS; a new file system.

2.4.2 Ubuntu 16.04 LTS

Ubuntu is an entire Linux working framework, unreservedly accessible with both network and expert help. The Ubuntu people group is based on the

thoughts cherished in the Ubuntu Manifesto: that product ought to be accessible gratis, that product devices ought to be usable by individuals in their nearby dialect and in spite of any incapacities, and that individuals ought to have the flexibility to modify and adjust their product in the manner in which they see fit. Ubuntu incorporates a huge number of bits of programming, beginning with the Linux bit rendition 4.15 and GNOME 3.28, and covering each standard work area application from word preparing and spreadsheet applications to web get to applications, web server programming, email programming, programming dialects and apparatuses and obviously a few diversions.

Server Configuration

Processor	2 GHz or faster
Memory	2 GB
Operating System	Ubuntu 16.04 64bit
Chassis Configuration	Tower Chassis Orientation
Hard Drive	25 GB or greater

Table 1: Server Configuration

2.4.3 Fedora 27

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.

Since the release of Fedora 21, three different editions are currently available: Workstation, focused on the personal computer, Server for servers, and Atomic focused on cloud computing. As of February 2016, Fedora has an estimated 1.2 million users, including Linus Torvalds, creator of the Linux kernel.

Server configuration

1 GHz or faster	1 GHz or faster
Memory	3.8GB
Operating System	64-bit
Disk	17.0GB
Graphic	Intel@ HD Graphic 400
GNOME	Version 3.2

Table 2: Server configuration

2.5 Hardware Requirement

In Workshop II, we have been provided with the equipment which are four desktop computers, one (1) Cisco 1941 Router (2 Fast Ethernet), one (1) Cisco 2960 manageable Switch, 15 meters UTP cable, one (1) set crimping tool, one (1) NIC and one (1) Access Point. This hardware is required to complete Workshop II. The equipment given is not brand new. Therefore, there are several preparations have been taken before we start the configuration.

1. Check all the equipment given whether failure to function.
2. Format the hard drive of the desktops.
3. Erase the configuration of the switch and router.

2.6 Hardware Justification

2.6.1 Servers

There are four (4) desktop given. Three (3) of the desktop acts as servers and the other one acts as client. One of the servers will be installed with Windows Server 2012 R2 and the rest will be installed with Linux-based which are Ubuntu 16.04 LTS and Fedora 27. There are minimum 5 services need to be installed into each server.

Windows Server 2012 R2:

1. Domain Name System (DNS)
2. Dynamic Host Configuration Protocol (DHCP) IPv4
3. Dynamic Host Configuration Protocol (DHCP) IPv6
4. Web, SSL & Virtual Hosting
5. AAA (Authentication, Authorization and Accounting) using Radius
6. Wireless User Authentication using Radius Server

7. IPsec VPN for Remote Employees
8. Active Directory (AD)
9. Server Virtualization
10. Windows Server Hardening

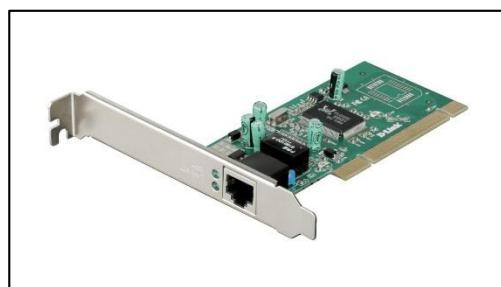
Ubuntu Server 16.04 LTS

1. Linux Email Server
2. Network Management System (NMS)
3. Authentication User by Integrating AD with Linux
4. IDS with Port Mirror
5. Cloud Server
6. Remote Login using SSH

Fedora 27

1. Samba
2. Samba Security Services
3. Remote Login using SSH
4. Secured FTP
5. Proxy Server
6. Media Streaming Server
7. Linux Server1 Hardening

2.6.2 NIC (Network Interface Card)



Network Interface Card (NIC) functions as a middleman between your computer and the data network. For example, when you log in to a website, the PC passes the site information to the network card, which converts the address into electrical impulses. Network cables carry these impulses to a Web server somewhere on the Internet, which responds by sending a Web page back to you, once again in the form of electronic signals. The card receives these signals and turns them into data that your PC displays. NIC is an add-on device that enables a computer to communicate with not only computers but router and switch. When

multiple computers are linked together using NIC or other devices, the resulting group is called a "network". NIC has the ability of supplying a basic addressing system that can be used to get data from one computer to another on the network. This function will help port mirror to capture the data from the other server on the same network.

2.6.3 UTP (Unshielded Twisted Pair) Cable



We are given 15 meters of UTP Cable for Workshop II. UTP cable is a type of wiring in which two conductors of a single circuit are twisted together for the purpose of cancelling out Electromagnetic Interference (EMI) from external sources. UTP is also a type of cable that can transmit voice or data signals. It acts as a medium between devices. In a wired connection, it is very important to connect among the devices.

2.6.4 RJ-45 (Registered Jack-45) Connector



RJ-45 is an 8-pin/8-position plug or jack is commonly used to connect computers onto Ethernet-based local area networks (LAN). Two (2) wiring schemes which are T568A and T568B are used to terminate the twisted-pair cable onto the connector interface.

2.6.5 Ethernet Cable



An Ethernet cable is one of the most popular forms of network cable used on wired networks. Ethernet cables connect devices together within a local area network, like PCs, routers, and switches. There are two standards released by the EIA/TIA group about UTP wiring which used in Workshop II:

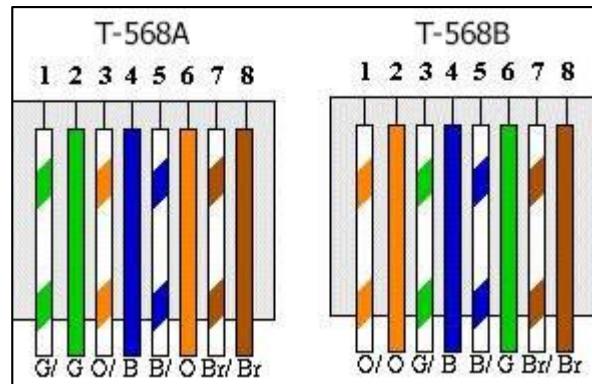
1. T568A (Cross-Over cable)

- Connect between router and router for Routing and NAT
- Connect between servers for Services Testing

2. T568B (Straight Through Cable)

- Connect between servers and switch
- Connect between switch and router

UTP cable, RJ-45 connector and crimping tool set are necessary to create a Ethernet Cable.



How to make an Ethernet cable:

- Step 1 : Strip the cable jacket about 1.5 inch down from the end.
- Step 2 : Spread the four pairs of twisted wire apart.
- Step 3 : Untwist the wire pairs and neatly align them in the T568B orientation. Be sure not to untwist them any farther down the cable than where the jacket begins; we want to leave as much of the cable twisted as possible.
- Step 4 : Cut the wires as straight as possible, about 0.5 inch above the end of the jacket
- Step 5 : Carefully insert the wires all the way into the modular connector, making sure that each wire passes through the appropriate guides inside the connector.
- Step 6 : Push the connector inside the crimping tool and squeeze the crimping tool all the way down.
- Step 7 : Repeat steps 1-6 for the other end of the cable.

2.6.6 Switch



A switch is a device in a computer network that connects together other devices. Multiple data cables are plugged into a switch to enable communication between different networked devices. Switches manage the flow of data across a network by transmitting a received network packet only to the one or more devices for which the packet is intended. Each networked device connected to a switch can be identified by its network address, allowing the switch to direct the flow of traffic maximizing the security and efficiency of the network. Segmentation involves the use of a switch to split a larger collision domain into smaller ones in order to reduce collision probability, and to improve overall network throughput. In Workshop II, our group choose Switch Cisco 2960 instead of Switch Cisco 2950. Because Switch Cisco 2960 does allow SSH, but Switch Cisco 2950 does not unless downloaded a IOS named “k9” in it. Switch Cisco 2960 is supported port mirroring which is the services need to be carried out in Workshop II.

2.6.7 Router

A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. A data packet is typically forwarded from one router to another router through the networks that constitute an internetwork until it reaches its destination node. A router is connected to two or more data lines from different networks. (NAT and Routing). Our group has Router Cisco 2800 in Workshop II. This model is have not seen before and our group need to do more research on it.

2.7 Conclusion

In Workshop II, we do the research immediately about the hardware given and the operating system that we chose. Network Infrastructure of Workshop II is built up with hardware requirement mentioned above and the operating system. Hence, we are very discreet in choosing operating system applied and checking the hardware given.

3.0 DESIGN

3.1 Introduction

In this workshop II, we have to define, design, implement and manage the network services. Each group in Workshop II should be implementing their own network design. According to the requirements of Workshop II, we need to set up a LAN (Local Area Network) which consists of three servers, one router, one switch and one client based on network design that we did. As mentioned before, our group set up a network with three servers (1 Fedora 27, 1 Ubuntu 16.04 LTS and 1 Windows Server 2012), one VM VirtualBox Machine (Windows Server 2012 R2), one Router Cisco 2800, one Switch Cisco Catalyst 2960, one AP (Access Point), and one client (Windows 7).

3.2 Security Policy

3.2.1 General

1. Acceptable Encryption Policy

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

2. Password Protection Policy

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

3.2.2 Password Creation

1. Password **MUST** contain alphabet (lower or uppercase) and symbol or numbers.
2. Password must at least have minimum of 8 characters.

3.2.3 Password Protection

1. Passwords **MUST NOT** be shared with anyone. All passwords are to be treated as sensitive, confidential group information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place.

2. Passwords **MUST NOT** be inserted into email messages, Alliance cases or other forms of electronic communication.
3. Passwords **MUST NOT** be revealed over the phone to anyone.
4. **DO NOT** reveal a password on questionnaire or security forms.
5. **DO NOT** hint at the format of a password.
6. **DO NOT** share group password with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation or with family members.
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.
8. **DO NOT** use the “Remember Password” feature of applications.

3.2.4 Server Security Policy

3.2.4.1 General Requirements

1. All internal servers deployed at <Group 4> must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by InfoSec. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by InfoSec. The following items must be met:
 - Server must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
 - i. Server contact(s) and location, and a backup contact
 - ii. Hardware and Operating System/Version
 - iii. Main functions and applications, if applicable
 - iv. Information in the corporate enterprise management system must be kept up-to-date

- v. Configuration changes for production servers must follow the appropriate change management procedures
2. For security, compliance and maintenance purposes, authorized personnel may monitor and audit equipment, system, processes and network traffic per the Audit Policy.

3.2.4.2 Configuration Requirements

1. Operating System configuration should be in accordance with approved InfoSec guidelines
2. Services and applications that will not be used must be disabled where practical
3. Access to services should be logged and/or protected through access-control methods such as web application firewall
4. The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements
5. Always use standard security principles of least required access to perform function
6. Do not use root when a non-privileged account
7. Servers should be physically located in an access-controlled environment
8. Servers are specifically prohibited operating from uncontrolled cubicle areas

3.2.5 Network Security

3.2.5.1 Router and Switch Security Policy

Every router must meet the following configuration standards:

1. No local user accounts are configured on the router. Routers and switches must use TACACS+ for all user authentication (RADIUS)
2. The enable password on the router or switch must be kept in secure encrypted form. The router or switch must have the enable

password set to the current production router/switch password from the device's support organization

3. The following service must be configured:
 - i. Password-encryption
4. All routing updates shall be done using secure routing updates
5. Access control list must be used to limit source and type of traffic that can terminate on the device itself
6. Access control list for transiting the device are to be added as business needs arise
7. Each router and switch must have the following statement presented for all forms whether remote or local:

"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."
8. SSH may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol
9. Dynamic routing protocols must use authentication in routing updates sent to neighbours. Password hashing for the authentication string must be enabled when supported
10. The corporate router configuration standard will define the category of sensitive routing and switching devices, require additional services or configuration on sensitive devices including:
 - i. IP access list accounting
 - ii. Device logging

- iii. Incoming packets at the router sourced with invalid addresses, such as the address that could be used to spoof network traffic shall be dropped.
- iv. Router console and modem access must be retrieved by additional security controls.

3.2.6 Application Security

3.2.6.1 IPv6 Web Policy

IPv6 can run end-to-end encryption. While this technology was retrofitted into IPv4, it remains an optional extra that isn't universally used. The encryption and integrity-checking used in current VPNs is a standard component in IPv6, available for all connections and supported by all compatible devices and systems. Widespread adoption of IPv6 will therefore make man-in-the-middle attacks significantly more difficult.

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

This added security depends entirely on proper design and implementation, and the more complex and flexible infrastructure of IPv6 makes for more work. Nevertheless, properly configured, IPv6 networking will be significantly more secure than its predecessor.

3.2.6.2 Remote Login using SSH Policy

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

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

3.2.6.3 Samba Policy

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

3.2.6.4 Hardening Services Policy

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

3.2.6.4.1 Access security

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

3.2.6.4.2 File system permissions

- i. For Linux Servers, permissions are on key security files such as /etc/passwd or /etc/shadow set in accordance with best practice in harden
- ii. Sudo being used, and are only root when members are allowed to use it
- iii. For Windows Server, the key must executable, DLLs and drivers protected in the System32 and SysWOW64

3.2.6.4.3 User accounts and passwords

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

3.2.6.4.4 Software and application image/ patching and updates

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

3.2.6.4.5 LAN services policy

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

network connection point, so it belongs to the original VLAN we had.

One solution to this problem is the use of the VTP protocol together with the Cisco VMPS (VLAN Management Policy Server) service, which provides a first approximation to a solution of network access control such as the ones offered by manufacturers today. Among other features, VMPS allows to dynamically associate devices to VLANs based on MAC address (with the security issues this involves). This way, we can connect our laptop to any network point of the office and it will always belong to the same correct VLAN.

3.2.6.4.6 Proxy server security

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

3.2.6.4.7 ACL policy

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

- i. The names of users and groups whose access to the object is explicitly controlled
- ii. The specific operations permitted to each user, group, or role
- iii. The specific operations permitted to the special any-other and unauthenticated user categories

For our group, we had permitted the Linux email server, web server, FTP to allow accessing to the window only. Other service then the stated service cannot access to the window server.

3.2.6.4.8 Hardening server policy

All internal servers deployed at must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides.

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

3.2.6.4.9 Router policy

Every router must meet the following configuration standards:

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

3.2.6.4.10 Physical Policy

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

1. Computer
 - i. Computers shall be inventoried before being put into service. Inventory list shall be available to all Systems Administrators.
 - ii. Each unit shall be distinctly and uniquely identified on all visible sides. Machines shall be housed in secured facilities (caged or locked).
2. Media
 - i. Provisioning

- Storage media (disk drives, tapes and removable media) are inventoried upon acquisition and tracked in their use.
- New storage media (whether disk or removable) shall be securely erased and reformatted before use.

3. Physical Access

- i. In accordance with the principle of dual control, at least two persons authorized for access must be on site at the same time for physical access to be granted.
- ii. Access cards and keys must be appropriately protected, not shared or transferred and returned when no longer needed. Lost or stolen cards/keys must be reported immediately.
- iii. Access Authorization (Access to physical equipment must be authorized.)
- iv. Access Logging (All physical accesses are logged and reported to all.)

3.3 Physical Design

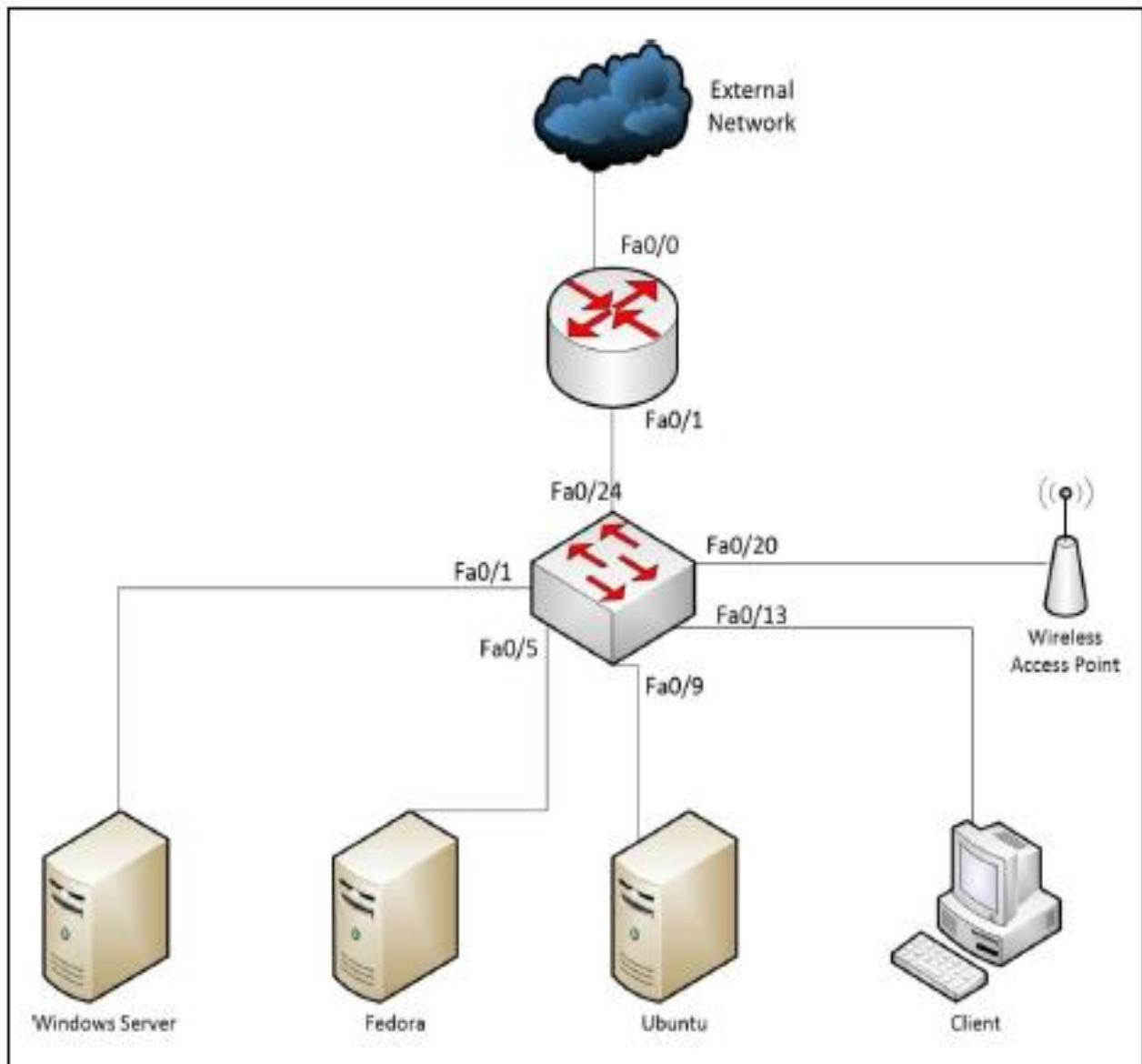


Figure 1: Physical Design

3.4 Logical Design

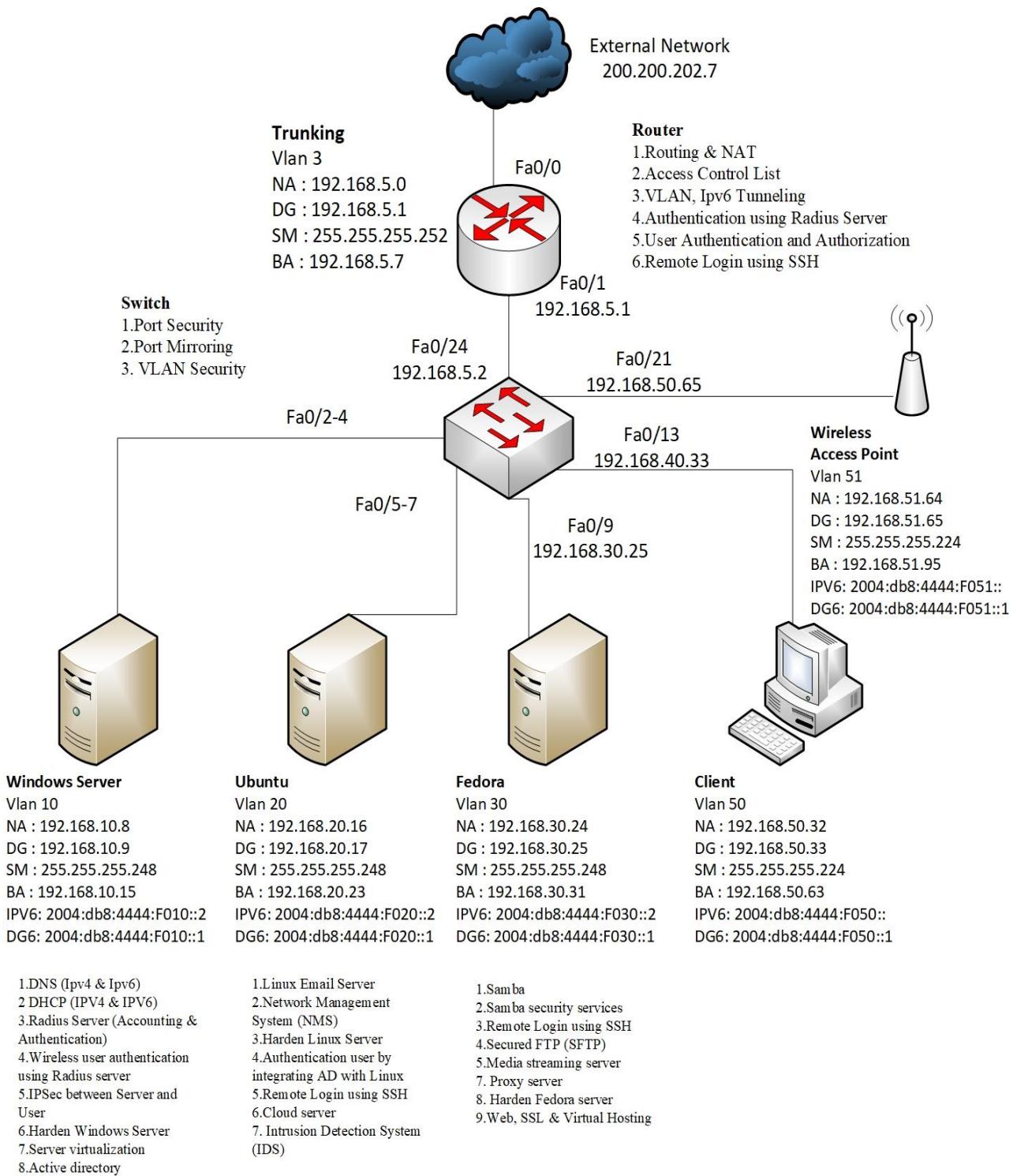


Figure 2: Logical Design.

3.5 VLAN

VLAN	No of IP	CIDR	Interface	Range
5	8	/29	Fa0/24	192.168.4.0 – 192.168.4.7
10	8	/29	Fa0/1 – Fa0/4	192.168.4.08 – 192.168.4.15

20	8	/29	Fa0/5 – Fa0/8	192.168.4.16 – 192.168.0.23
30	8	/29	Fa0/9 – Fa0/12	192.168.4.24 – 192.168.4.31
40	32	/27	Fa0/13 – Fa0/23	192.168.4.32 – 192.168.0.63
50	32	/27	Fa0/21 – Fa0/23	192.168.4.64 – 192.168.4.95

Table 3: VLAN

3.6 Conclusion

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

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

4.0 SERVICES

4.1 Introduction

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

4.2 List of Services

Service for Networking

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

Service for Security

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
8. IDS with Port Mirror
9. IPsec VPN for Remote Employees

10. Samba Security Services
11. Port Security
12. VLAN Security

4.3 Brief Overview for Services (Networking Services)

4.3.1 Domain Name Services (DNS)

The Domain Name System (DNS) is the phonebook of the Internet. People get to data online through area names, as nytimes.com or espn.com. Internet browsers cooperate through Internet Protocol (IP) addresses. DNS makes an interpretation of area names to IP addresses so programs can stack Internet assets. Every gadget associated with the Internet has a special IP address which different machines use to discover the gadget. DNS servers dispose of the requirement for people to remember IP tends to, for example, 192.168.1.1 (in IPv4), or more unpredictable more current alphanumeric IP tends to, for example, 2400:cb00:2048:1::c629:d7a2 (in IPv6).

4.3.2 Dynamic Host Configuration Protocol (DHCP)

DHCP (Dynamic Host Configuration Protocol) is a convention used to give snappy, programmed, and focal administration for the conveyance of IP addresses inside a system. DHCP is likewise used to arrange the best possible subnet veil, default passage, and DNS server data on the gadget.

A DHCP server is utilized to issue interesting IP addresses and naturally design other system data. In many homes and private ventures, the switch goes about as the DHCP server. In extensive systems, a solitary PC may go about as the DHCP server.

4.3.3 Inter VLAN and VLSM Addressing

VLAN is an intelligent gathering of gadgets that give off an impression of being on a similar LAN or distinctive LAN notwithstanding their graphical circulation. It permits the division of the system without utilizing numerous switch ports. Ipv6 Transition Mechanism is an innovation that encourages the changing of the Internet from the Internet Protocol variant 4 (Ipv4) to the successor tending to and directing arrangement of Internet Protocol Version 6 (Ipv6). As Ipv4 and Ipv6 systems are not straightforwardly interoperable, progress advances are intended to allow has on either arrange sort to speak with some other host.

4.3.4 Routing & 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. The routing process directs forwarding on the basis of routing tables which maintain a record of the routes to various network destinations. The routing service provided by the router allows a client to access and receive resources from remote networks. Network Address Translation is the act of translating an address from one to another within the packet. A router that acts as intermediary between networks performs the NAT function. One network is designated the inside network and the other is the outside. The local inside network addresses maps to one or more global outside IP addresses and unmaps 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.

4.3.5 Active Direction (AD)

Active Directory (AD) is a directory service that Microsoft developed for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services. Initially, Active Directory was only in charge of centralized domain management. Starting with Windows Server 2008, however, Active Directory became an umbrella title for a broad range of directory-based identity-related services.

4.3.6 Proxy Server

A proxy server is associated with a part of a gateway server that separates the enterprise network from the outside network and a firewall server that protects the enterprise network from outside intrusion. The client forwards request for resource to the proxy server and the proxy server will require the resource on behalf of the client and deliver back to the client. As the network traffic is intercepted from inside to outside or vice versa, a proxy server can also be one of the components of firewall. Proxy server provides security and able to improve performance through caching in the network.

4.3.7 Samba

Samba is the standard Windows interoperability suite of projects for Linux and Unix. Since 1992, Samba has given secure, steady and quick document and print administrations for all customers utilizing the SMB/CIFS convention, for example, all forms of DOS and Windows, OS/2, Linux and numerous others.

Samba is an essential segment to flawlessly coordinate Linux/Unix Servers and

Desktops into Active Directory conditions. It can work both as a space controller

or as a general area part. Samba is a product bundle that gives organize overseer's adaptability and opportunity as far as setup, design, and selection of frameworks and gear.

4.3.8 Network Management System (NMS)

System administration alludes to the expansive subject of overseeing PC

systems. There exists a wide assortment of programming and equipment items that assistance organizes framework executives deal with a network security. Ensuring that the system is shielded from unapproved clients.

4.3.9 Server Virtualization

Server virtualization is the masking of server resources, including the number and identity of individual physical servers, processors, and operating systems, from server users. The server administrator uses a software application to divide one physical server into multiple isolated virtual

environments. The virtual environments are sometimes called virtual private servers, but they are also known as guests, instances, containers or emulations.

4.3.10 AAA (Authentication, Authorization and Accounting) using Radius

Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or within an authentication server. If the credentials match, the process is completed, and the user is granted authorization for access.

Authorization is the function of specifying access rights to resources related to information security and computer security in general and to access control in particular. More formally, "to authorize" is to define an access policy.

RADIUS is the abbreviation for Remote Authentication Dial-In Service. It is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service. The client that needs to be authenticated will send a message to the RADIUS server and the server will respond with „accept“ or „reject“ message back to the client based on the client authenticity. RADIUS server needs to be implemented in the project because it is a systematic way for authenticating network client or devices thus enhances the security level of the network.

4.3.11 Access Control List (ACL)

An entrance control list (ACL) is a table that tells a PC working framework which get to right every client has to a specific framework question, for example, a record catalogue or individual document. Each question has a security quality that recognizes its entrance control list. The rundown has a passage for every framework client with get to benefits. The most well-known benefits incorporate the capacity to peruse a record (or every one of the documents in a registry), to keep in touch with the document or records, and to execute the record (in the event that it is an executable document, or program). Microsoft Windows NT/2000, Novell's NetWare, Digital's OpenVMS, and UNIX-based frameworks are among the working frameworks that utilization get to control records. The rundown is actualized contrastingly by each working framework.

4.3.12 Secured FTP

SFTP typically relies upon SSH, a very common and well-tested protocol that provides secure communications using a key-based encryption scheme. It fully encrypts the file transfer process, from start to finish with limited threat exposure for the user and proven secure method to transmit files. Ftp user may authenticate them using a clear-text-sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission it hides username and password and encrypts the content. SFTP is essential as a mean to transfer files between servers and client or network equipment without compromising on security and confidentiality. Also known as SSH FTP (SFTP) and FTP Secure (FTPS. Both supply mechanisms for secure file transfer but vary in method.

- FTPS – uses SSL or TLS for traffic flow encryption
- SFTP – uses SSH to tunnel an FTP session to a SFTP server

4.3.13 Web, SSL & Virtual Hosting

Web server is a PC that conveys Web pages. Web server are introducing in Windows Server by including Web Server (ISS) part. The webpage name is

groupeightweb.com and IP address is 192.168.10.3. Web server is a server that oversee site that are transferred by client. A site must be situated on a web server. Site can be anchored by utilizing testament and is called Secure Socket Layer (SSL). SSL can be introducing utilizing Server Certificate in the ISS Manager. This will guarantee that all information go between the web server and program stays private and indispensable. A webserver can have progressively that one site. This strategy is called virtual facilitating, where every site has their own URL and page yet inside on a similar server. Virtual facilitating can be made in DNS server by including a New Zone.

4.3.14 Linux Email Server

A mail server (or email server) is a PC framework that sends and gets email. Mail servers send and get email utilizing standard email conventions. For instance, the SMTP convention sends messages and handles active mail demands. The IMAP and POP3 conventions get messages and are utilized to process approaching mail.

4.3.15 IPv6 Web with IPv6 Tunnelling

Web Protocol rendition 6 (IPv6) is the latest adaptation of the Internet Protocol (IP), the interchanges convention that gives an ID and area framework for PCs on systems and courses movement over the Internet. IPv6 is proposed to supplant

4.3.16 Media Streaming Server

A media server refers either to a dedicated computer appliance or to a specialized application software, ranging from an enterprise class machine providing video on demand, to, more commonly, a small computer or NAS (Network Attached Storage) for the home, dedicated for storing various digital media (meaning digital videos/movies, audio/music, and picture files).

By definition a media server is a device that simply stores and shares media. This definition is vague and can allow several different devices to be called Media Servers. It may be a simple Network-attached storage, a Home theater PC (HTPC) running Windows XP Media Center Edition, MediaPortal or MythTV, or a commercial web server that hosts media for a large web site. In a home setting, a media server acts as an aggregator of information: video, audio, photos, books, etc. These different types of media (whether they originated on DVD, CD, digital camera, or in physical form) are stored on the media server's hard drive. Access to these is then available from a central location. It may also be used to run special applications that allow the user(s) to access the media from a remote location via the internet.

4.3.17 Cloud Server

A cloud server is powerful physical or virtual infrastructure that performs application- and information-processing storage. Cloud servers are created using virtualization software to divide a physical (bare metal) server into multiple virtual servers. Organizations use an infrastructure-as-a-service (IaaS) model to process workloads and store information. They can access virtual server functions remotely through an online interface.

4.4 Brief Overview for Services (Security Services)

4.4.1 Security Policy

Security strategy is a protected for the framework, association or other element which arrive in an arrangement of tenets characterizing who is approved to get to what and under which conditions, and the criteria under which such approval is given or dropped. For frameworks, the security arrangement tends to limitations on capacities and stream among them, requirements on access by outer frameworks and enemies including projects and access by outside frameworks and foes including projects and access to information by individuals. For an association, it tends to the requirements on conduct of its individuals and in addition limitations forced on foes by components, for example, entryways, bolts, keys and dividers. For the most part, security arrangement will be refreshing every now and then, as innovation and framework prerequisites continually evolving.

4.4.2 Router Hardening

Hardening a router means that the router is secured against attacks as best as possible. From secure, tough-to-crack passwords that are encrypted in the configurations, to the shutting down of unnecessary ports and services, the router has few vulnerabilities for would-be attackers to exploit. By hardening a router, we make it difficult to penetrate and unyielding under the pressure of attacks.

4.4.3 Remote Login using SSH

SSH, short for Secure Shell is a UNIX-based command interface and protocol for getting secured access to a remote computer similar to telnet. SSH commands are encrypted and secure during transmission and the connection between the client and server is authenticated by using a digital certificate. It is used to access and control computer and equipment securely from remote location.

4.4.4 Linux server1 Hardening

Solidifying is a procedure of safely designing defencelessness purpose of a framework like there possibly unused port, administrations or futile programming running that may make helplessness point in the framework.

This defencelessness point might be utilized by others to enter the framework. primary ways to hardening Linux and to prevent attackers from gaining access to the systems:

- a. Minimize the amount of software installed and running in order to minimize vulnerability.
- b. Encrypt all data transmitted over the network.
- c. Use security-enhancing software and tools whenever available (e.e SELinux).

Hardening will lessen the security danger of Fedora Server as hardened servers

are more impervious to security issues than non-hardened servers. In Fedora, there are sure part that should be secure by hardening them like bit, root client,

authoritative records and others. Every one of them will be arranged to keep from a wide range of security assault. Utilize static ARP to set arp table and flush

pointless sections. Subsequent to hardening, the Solaris Server will be more sheltered and secure.

4.4.5 Windows Server Hardening

The purpose of hardening is eliminated as many security risks as possible. Techniques to harden systems are protecting accounts with passwords, disabling unnecessary accounts, disabling unnecessary services and protecting management interfaces and application. Hardening the Microsoft Windows Server 2008 R2 operating system reduces the attack surface by disabling functionality that is not required while maintaining the minimum functionality that is required.

4.4.6 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.

The realmd system will be used to allow Linux user to be authenticated using Active Directory. It configures underlying Linux system services, such as SSSD or Winbind, to connect to the domain

4.4.7 Wireless User Authentication using Radius Server

WPA2-Enterprise with 802.1x authentication can be used to authenticate users or computers in a domain. The supplicant (wireless client) authenticates against the RADIUS server (authentication server) using an EAP method configured on the RADIUS server. The gateway APs (authenticator) role is to send authentication messages between the supplicant and authentication server. This means the RADIUS server is responsible for authenticating users.

APs perform EAPOL exchanges between the supplicant and convert these to RADIUS Access-requests messages, which are sent to the RADIUS server's IP address and UDP port specified in Dashboard. Gateway APs need to receive a RADIUS Access-accept message from the RADIUS server in order to grant the supplicant access to the network.

4.4.8 IDS with Port Mirror

The IDS manager provides a graphical interface for managing security across a distributed network. The IDS module performs network sensing. The IDS module searches for patterns of misuse by examining either the data portion and/or the header portion of network packets. Content-based attacks derive from the data portion, and context-based attacks derive from the header portion. To avoid from affecting the production, IDS usually gets the network traffic by mirroring the port. With port mirroring enabled, the switch sends a copy of all network packets seen on one port (or an entire VLAN) to another port, where the packet can be analysed.

4.4.9 IPsec VPN for Remote Employees

A VPN provides a means by which remote computers communicate securely across a public WAN such as the Internet. A VPN connection can link two LANs (site-to-site VPN) or a remote dial-up user and a LAN. The traffic that flows between these two points passes through shared resources such as routers, switches, and another network equipment that make up the public WAN. To secure VPN communication while passing through the WAN, the two participants create an IP Security (IPsec) tunnel.

IPsec is a suite of related protocols for cryptographically securing communications at the IP Packet Layer. IPsec also provides methods for the manual and automatic negotiation of security associations (SAs) and key distribution, all the attributes for which are gathered in a domain of interpretation (DOI). The IPsec DOI is a document containing definitions for all the security parameters required for the successful negotiation of a VPN tunnel—essentially, all the attributes required for SA and IKE negotiations.

4.4.10 Samba Security Services

Collectively, we call Samba implementations of the security levels security modes. They are known as share, user, domain, ADS and server modes. An SMB server informs the client, at the time of a session setup, the security level the server is running. There are two options which are share-level and user-level. Which of these two the client receives affects the way the client then tries to authenticate itself.

- **User- Level Security**

If we want to restrict access to our server to valid users only, then the following method may be of use. In the smb.conf [global] section put:

```
valid user = @secured
```

This restricts all server access either to the user secured or to members of the system group smbusers.

- **Share- Level Security**

In share-level security, the client authenticates itself separately for each share. It sends a password along with each tree connection request (share mount), but it does not explicitly send a username with this operation.

In the smb.conf [global] section put:

```
share ok = yes
```

4.4.11 Port Security

Port security is a layer two traffic control feature on Cisco Catalyst switches. It enables an administrator to configure individual switch ports to allow only a specified number of source MAC addresses engrossing the port. Its primary use is to deter the addition by users of "dumb" switches to illegally extend the reach of the network (e.g. so that two or three users can share a single access port). The addition of unmanaged devices complicates troubleshooting by administrators and is best avoided.

4.4.12 VLAN Security

The first principle in securing a VLAN network is physical security. If an organization does not want its devices tampered with, physical access must be strictly controlled. Core switches are usually safely located in a data centre with restricted access, but edge switches are often located in exposed areas. Just as physical security guidelines require equipment to be in a controlled space, VLAN-based security requires the use of special tools and following a few best security practices to achieve the desired result.

4.5 Conclusion

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

5.0 INSTALLATION AND CONFIGURATION

5.1 Introduction

In this chapter, we introduce the list of person-in-charge and their corresponding services. Also, the service installation and configuration will be explained in detail.

5.2 Services and Corresponding Person-In-Charge (BITC & BITZ)

Services (BITC)	Person-In-Charge (BITC)
1. Domain Name System (IPv4 & IPv6) 2. Cloud Server 3. Routing & NAT	Muhamad Syafiq Azlan bin Mustafa
1. Dynamic Host Configuration Protocol (DHCP) IPv4 2. Proxy Server 3. AAA (Authentication, Authorization and Accounting) using Radius	Ahmad Syarifuddin bin Harun
1. Inter VLAN and VLSM Addressing 2. Network Management System (NMS) 3. Access Control List (ACL)	Nurnasiha binti Mohd Isa
1. Server Virtualization 2. Samba 3. IPv6 Web with IPv6 Tunnelling)	Nur Jamsyeqa binti Jamaludin
1. Active Directory (AD) 2. Secured FTP; with authentication and encryption 3. Web, SSL & Virtual Hosting	Muhammad Kifly bin Mohd Zan
1. Linux Email Server 2. Dynamic Host Configuration Protocol (DHCP) IPv6 3. Media Streaming Server	Nur Anisa

Services (BITZ)	Person-In-Charge
1. VLAN Security 2. IPsec VPN for Remote Employees 3. Samba Security Services 4. Linux Server1 Hardening	Nur Dayana binti Mohd Aidi
1. IDS with Port Mirror 2. Authentication User by Integrating AD with Linux 3. Windows Hardening 4. Router Hardening	Ooi Xing Czek
1. Security Policy 2. Remote Login using SSH 3. Wireless User Authentication using Radius Server 4. Port Security	Nur Syafiqah binti Nor Azmi

Table 4: Services distribution.

5.3 Service Installation and Configuration

5.3.1 Domain Name System (IPv4 & IPv6)

5.3.1.1 Primary DNS

Step 1: Create new DNS server using wizard.

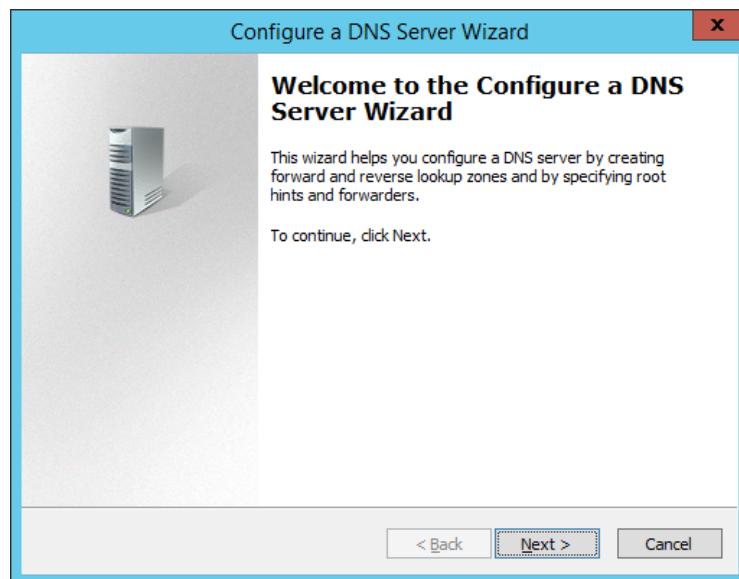


Figure 3: Create new DNS using Wizard

Step 2: Then, configure a DNS action by ticking at Create a forward lookup zone and click Next.

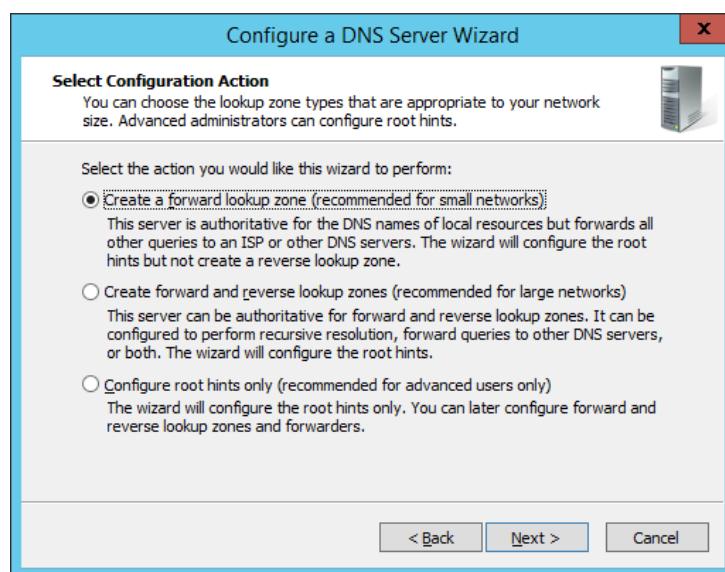


Figure 4: Select forward lookup zone

Step 3: For Primary Server Location, select This server maintains the zone and click Next.

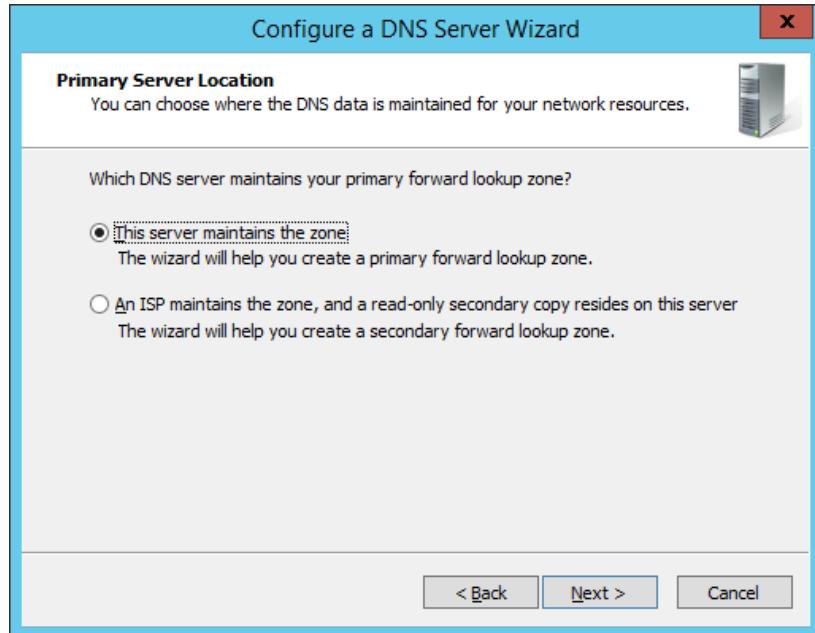


Figure 5: Select primary zone location

Step 4: Then, enter the zone name (example; group4.com).

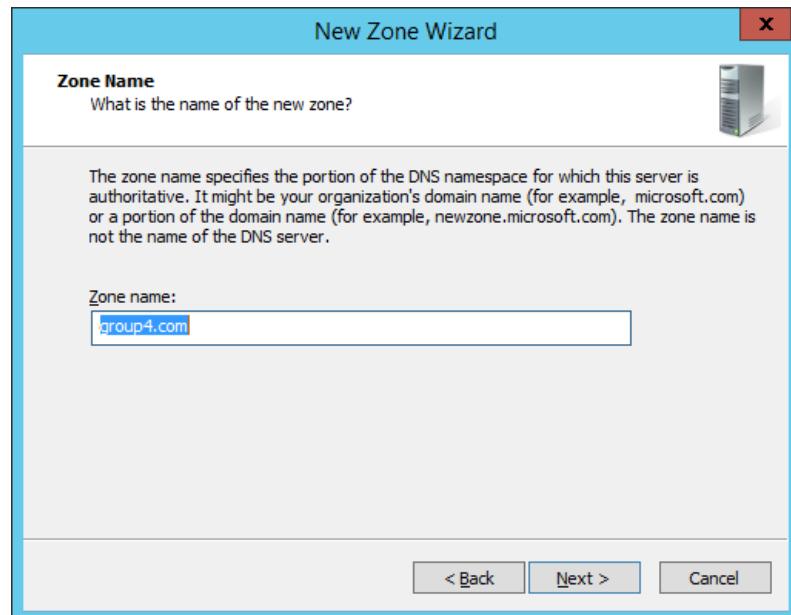


Figure 6: Enter zone name.

Step 5: For Dynamic Updates, select Do not allow dynamic updates. Then, click Next.

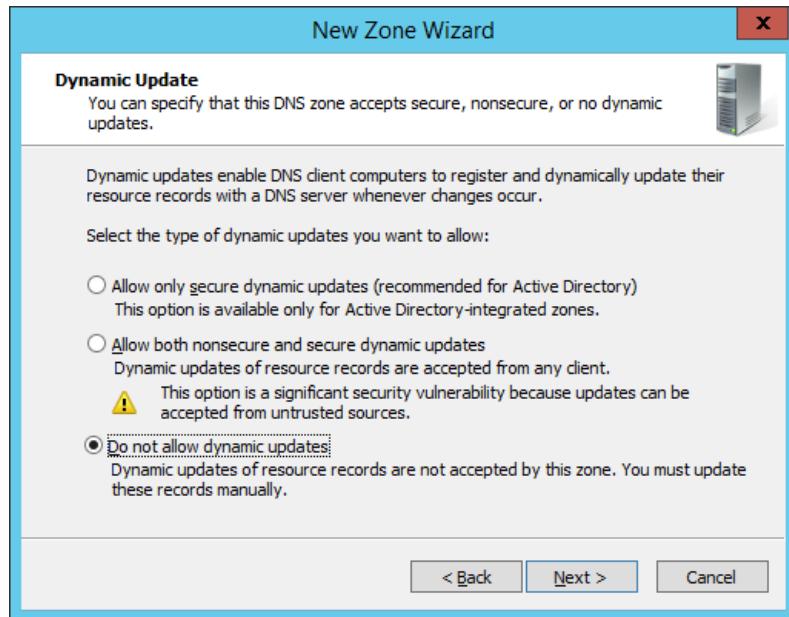


Figure 7: Select do not allow dynamic updates.

Step 6: After that, enter host IP Address for the Forwarders and click Next.

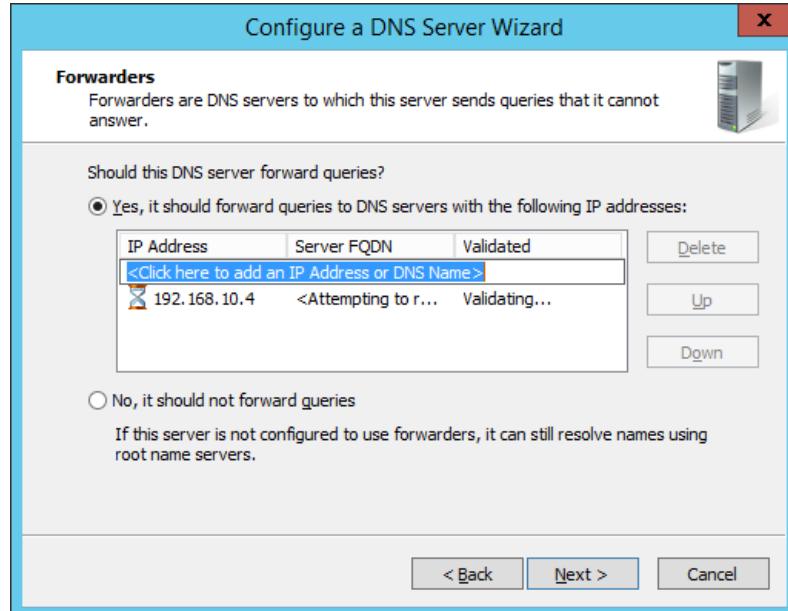


Figure 8: Host IP Address

Step 7: As a result of DNS configuration, it will show all the detail that you have enter.

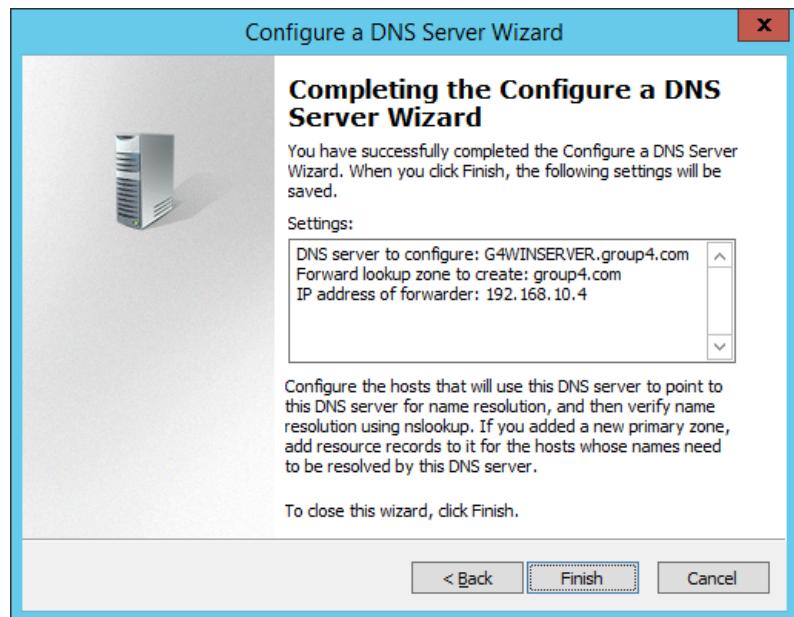


Figure 9: Complete DNS Configuration

Step 8: Then, create New Zone and click Next.



Figure 10: Create New Zone

Step 9: For Reverse Lookup Zone Name, select IPv4 Reverse Lookup Zone and click Next.

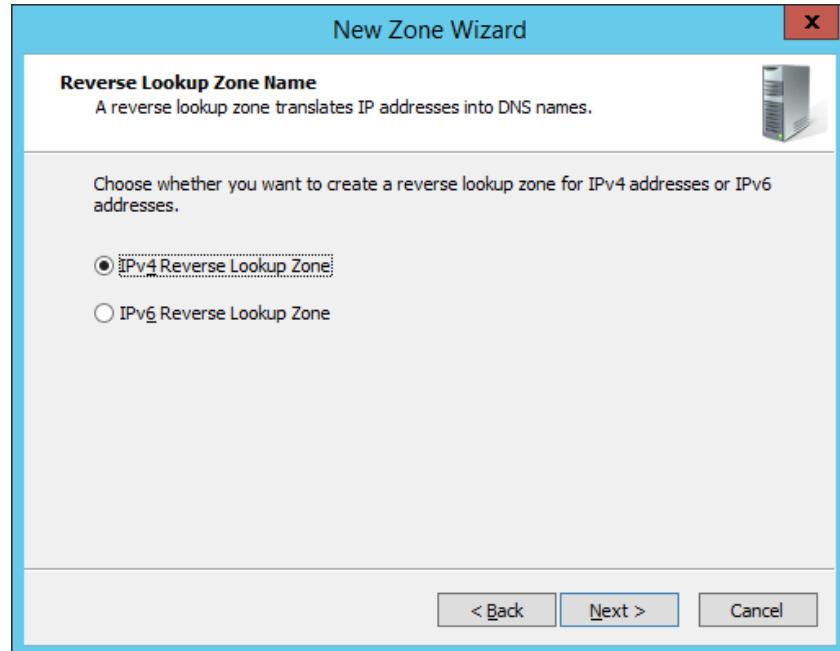


Figure 11: Select Reverse Lookup Zone Name

Step 10 : Enter Network ID for the zone and click Next button.

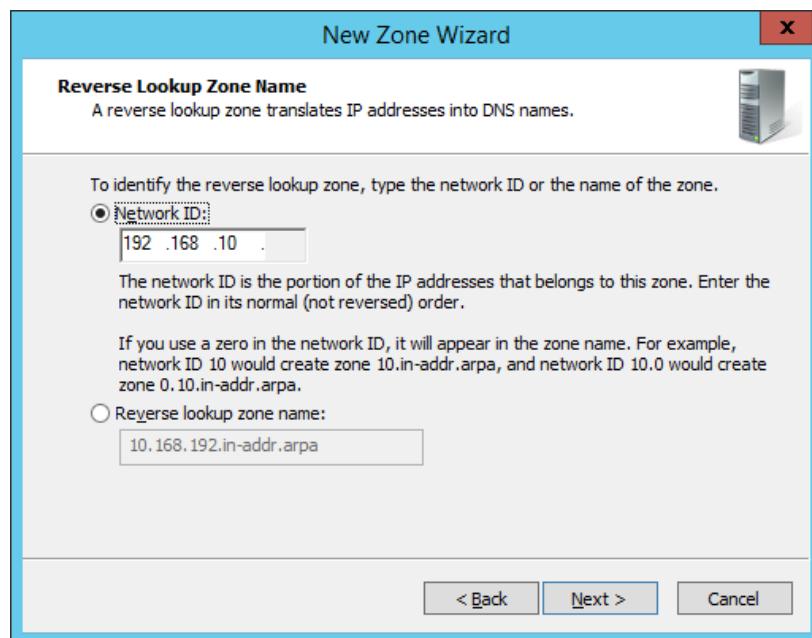


Figure 12: Enter Network ID

Step 11 : Upon completing the New Zone Wizard, it will show the specified settings that have been done. Then, click Finish to close.

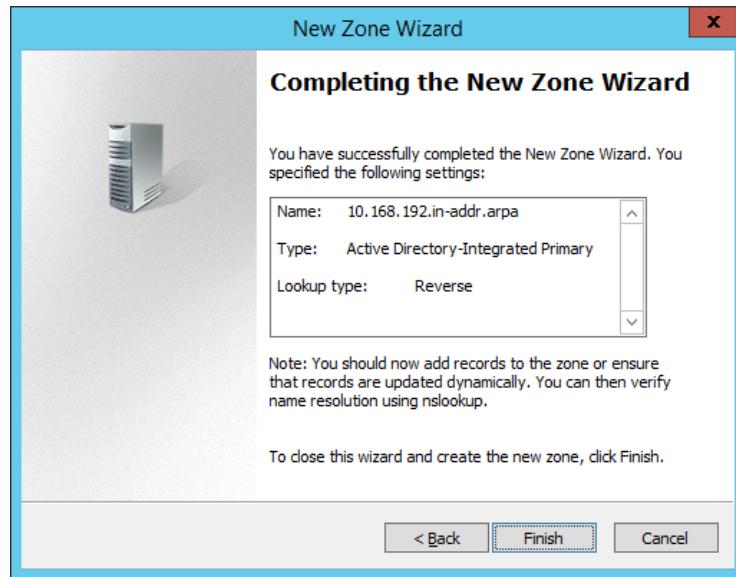


Figure 6: New Zone Wizard Is completed

Step 12 : Then, add IPv6 host in forward lookup zone.

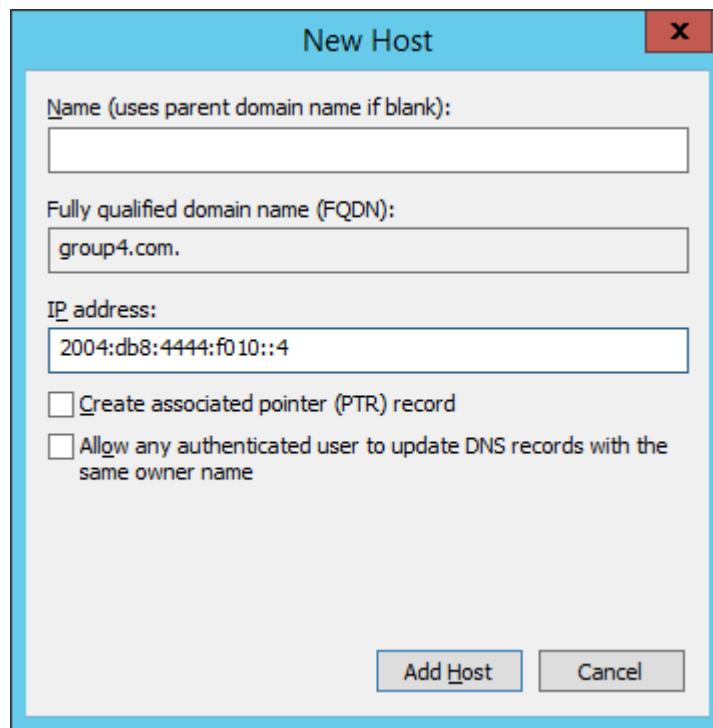


Figure 7: IPv6 Host

Step 13 : For Reverse Lookup Zone Name, select IPv6 Reverse Lookup Zone and click Next.

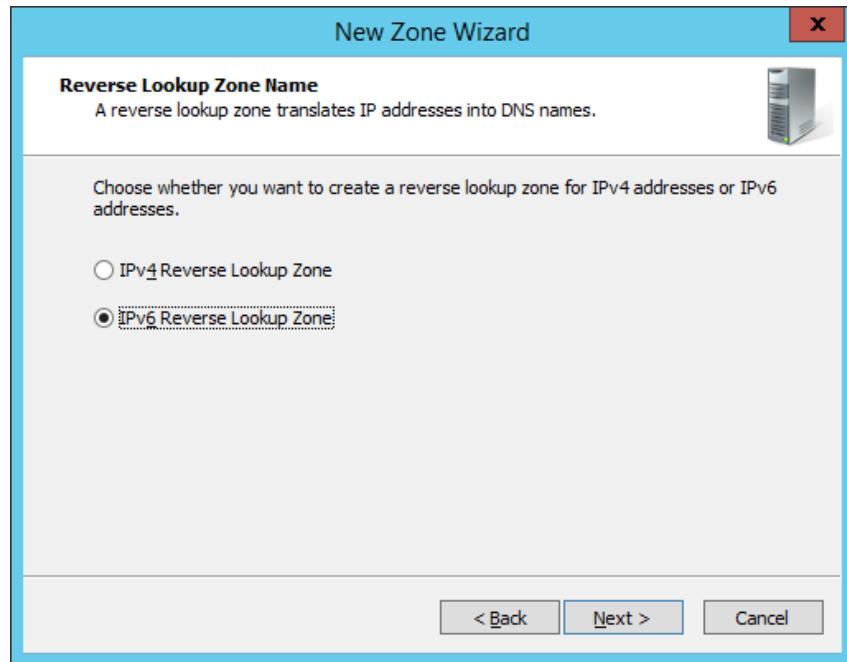


Figure 15: IPv6 Reverse Lookup Zone

Step 14 : Enter IPv6 Address Prefix and click Next.

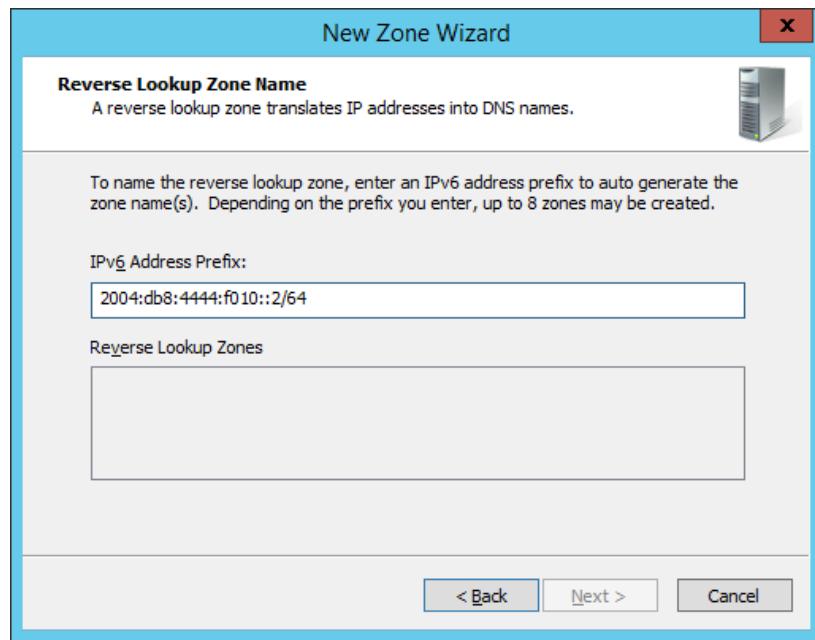


Figure 16: IPv6 Address Prefix

Step 15 : Then, verify Primary DNS resources.

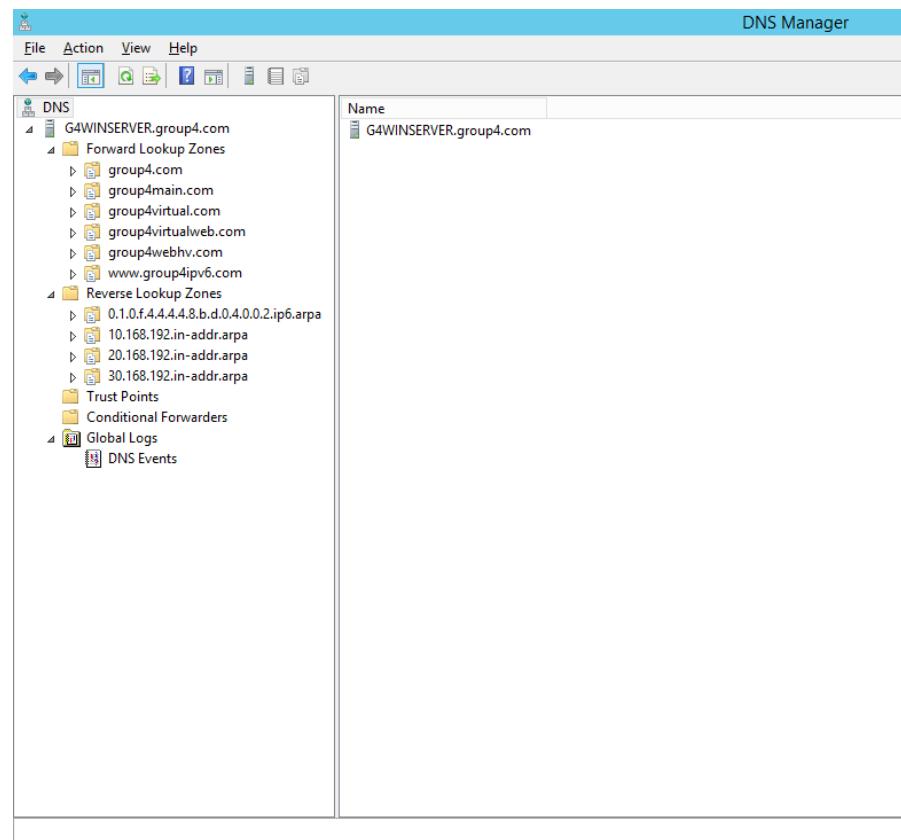


Figure 8: DNS Resources

DNS Manager

The screenshot shows the Windows DNS Manager interface. On the left, a tree view displays the DNS structure under 'G4WINSERVER.group4.com'. On the right, a table lists various DNS resources with columns for Name, Type, Data, and Timestamp.

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[2685], g4winserver.group4.com., hostmaster.group4...	static
(same as parent folder)	Name Server (NS)	g4winserver.group4.com.	static
(same as parent folder)	Name Server (NS)	group4.com.	static
(same as parent folder)	Name Server (NS)	g4winserver2.group4.com.	static
(same as parent folder)	Host (A)	192.168.10.4	11/27/2018 3:00:00 PM
(same as parent folder)	Host (A)	192.168.10.5	static
(same as parent folder)	IPv6 Host (AAAA)	2004:0db8:4444:f010:40f9:81f9:ebc4:9059	11/29/2018 4:00:00 PM
(same as parent folder)	IPv6 Host (AAAA)	2004:0db8:4444:f010:0000:0000:0000:0002	static
(same as parent folder)	IPv6 Host (AAAA)	2004:0db8:4444:f010:0000:0000:0000:0003	static
(same as parent folder)	IPv6 Host (AAAA)	2004:0db8:4444:f010:5531:c715:5345:7263	12/1/2018 10:00:00 AM
DESKTOP-JBUDNH-D	Host (A)	192.168.50.2	11/30/2018 1:00:00 PM
DESKTOP-JBUDNH-D	IPv6 Host (AAAA)	2004:0db8:4444:f050:8ec9:9fb8:a604:ee60	11/30/2018 1:00:00 PM
DESKTOP-SE7HRLH	Host (A)	192.168.50.2	10/23/2018 7:00:00 PM
email	Host (A)	192.168.20.4	static
email	Mail Exchanger (MX)	[10] email.group4.com.	static
g4winserver	Host (A)	192.168.10.4	static
g4winserver	IPv6 Host (AAAA)	2004:0db8:4444:f010:40f9:81f9:ebc4:9059	static
g4winserver	IPv6 Host (AAAA)	2004:0db8:4444:f010:0000:0000:0000:0002	static
g4winserver2	Host (A)	192.168.10.5	static
g4winserver2	IPv6 Host (AAAA)	2004:0db8:4444:f010:0000:0000:0000:0003	static
g4winserver2	IPv6 Host (AAAA)	2004:0db8:4444:f010:5531:c715:5345:7263	static
mail	Host (A)	192.168.20.4	static
nextcloud	Host (A)	192.168.20.4	static
plex	Host (A)	192.168.30.4	static
testing	Host (A)	192.168.10.4	static
WIN-252B0A9KDNJ	Host (A)	192.168.10.5	9/27/2018 2:00:00 PM
www	Host (A)	192.168.30.4	static
zabbix	Host (A)	192.168.20.4	static

Figure 18: DNS Resources

DNS Manager

The screenshot shows the Windows DNS Manager interface. On the left, a tree view displays the DNS structure under 'G4WINSERVER.group4.com'. On the right, a table lists various DNS resources with columns for Name, Type, Data, and Timestamp.

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[568], g4winserver.group4.com., hostmaster.group4.c...	static
(same as parent folder)	Name Server (NS)	g4winserver2.group4.com.	static
(same as parent folder)	Name Server (NS)	g4winserver.group4.com.	static
2004:0db8:4444:f010:0000:0000:0000:0002	Pointer (PTR)	g4winserver.group4.com.	12/1/2018 10:00:00 AM
2004:0db8:4444:f010:0000:0000:0000:0003	Pointer (PTR)	g4winserver2.group4.com.	12/1/2018 10:00:00 AM
2004:0db8:4444:f010:0000:0000:0001:0003	Pointer (PTR)	g4winserver2.group4.com.	10/1/2018 12:00:00 PM
2004:0db8:4444:f010:40f9:81f9:ebc4:9059	Pointer (PTR)	g4winserver.group4.com.	12/1/2018 10:00:00 AM
2004:0db8:4444:f010:5531:c715:5345:7263	Pointer (PTR)	g4winserver2.group4.com.	12/1/2018 10:00:00 AM
2004:0db8:4444:f010:7860:3417:ddf2:7a47	Pointer (PTR)	g4winserver.group4.com.	10/2/2018 3:00:00 PM

Figure 9: DNS Resources

5.3.1.2 Secondary DNS in Hyper-V

Step 1 : Setup the DNS same line the primary then create new zone.



Figure 20: New Zone Wizard

Step 2 : Select the Secondary zone for the Zone Type and click Next button.

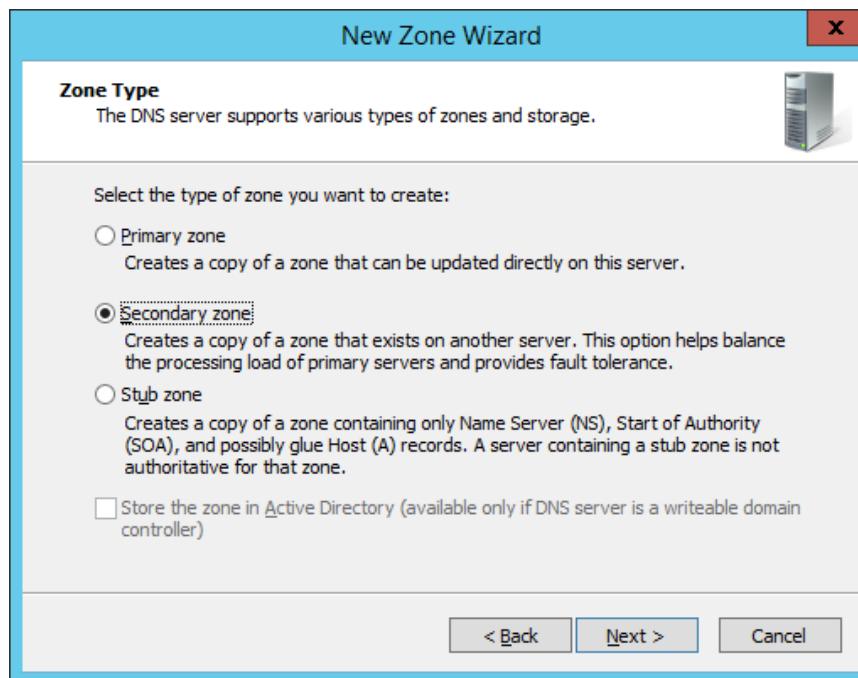


Figure 21: Select the zone type

Step 3 : Then, setup forward lookup zone same as the primary DNS and click Next.

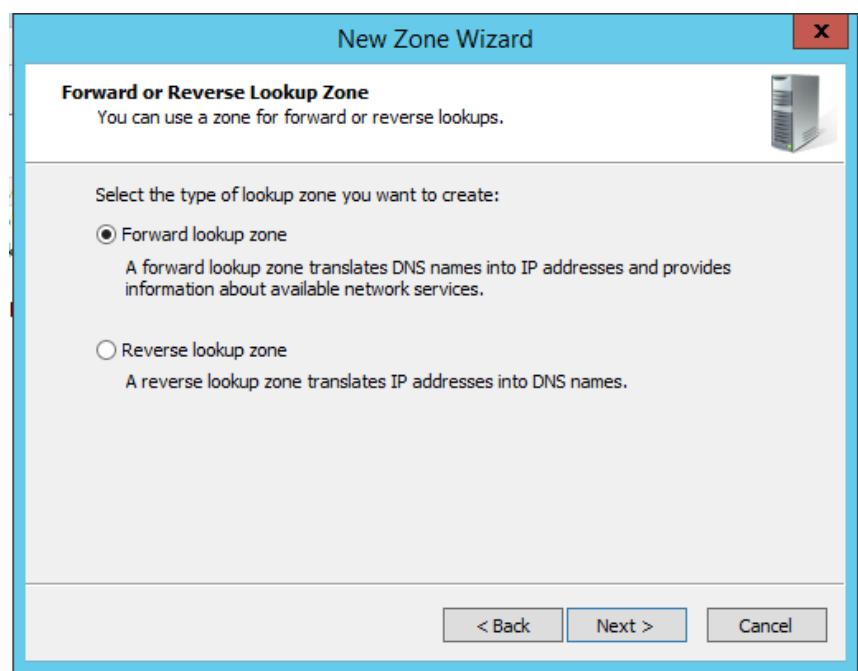


Figure 22: Select type of zone

Step 4 : For Master DNS Server, enter the Master DNS IP and click Next.

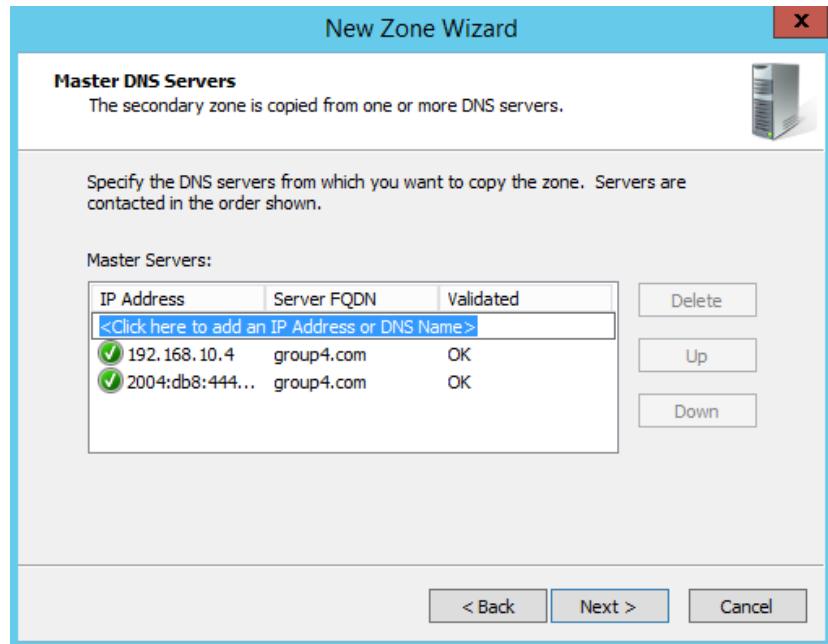


Figure 23: Master DNS Server IP

Step 5 : Then, the secondary zone setup is completed. Click Finish to close.

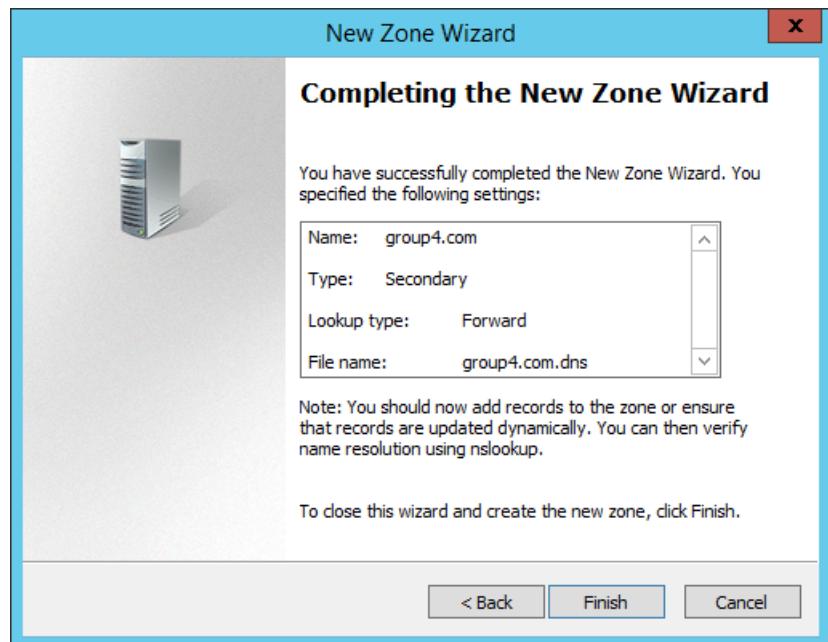


Figure 24: New Zone Wizard is completed

Step 6 : Repeat the step for reverse lookup zone of IPv4 and IPv6 forward and reverse lookup zones.

Step 7 : Verify the secondary DNS resources. (It will be just the same as primary DNS as it is a read only copy from its master DNS).

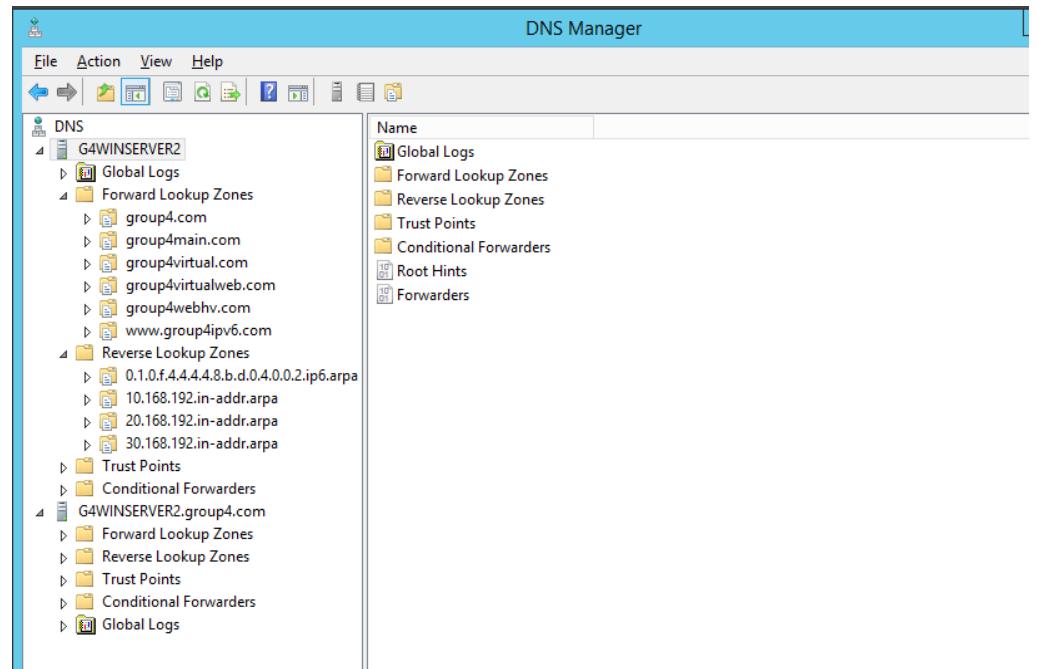


Figure 25: Secondary DNS Resources

5.3.2 Dynamic Host Configuration Protocol (DHCP) IPv4

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

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

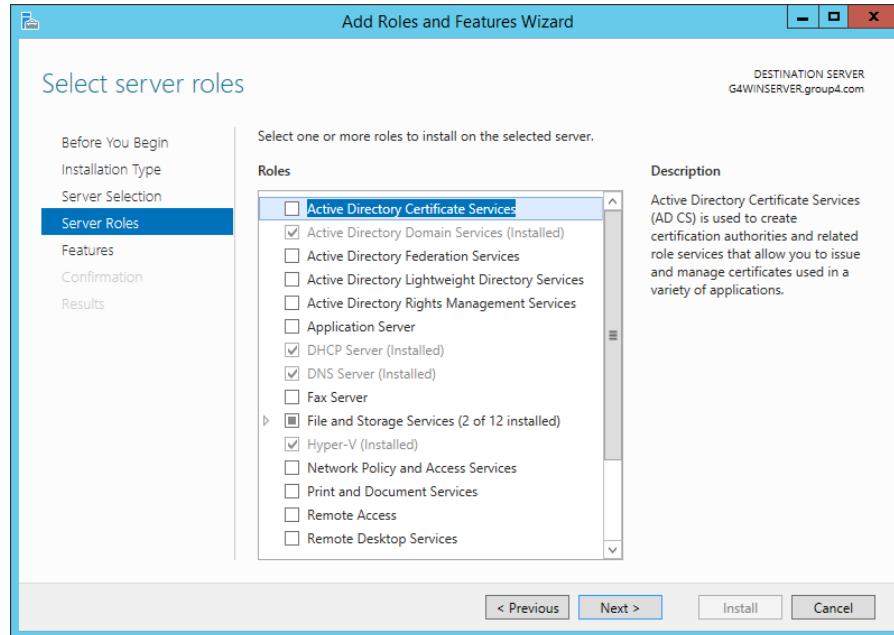


Figure 26: Adding role for DHCP

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

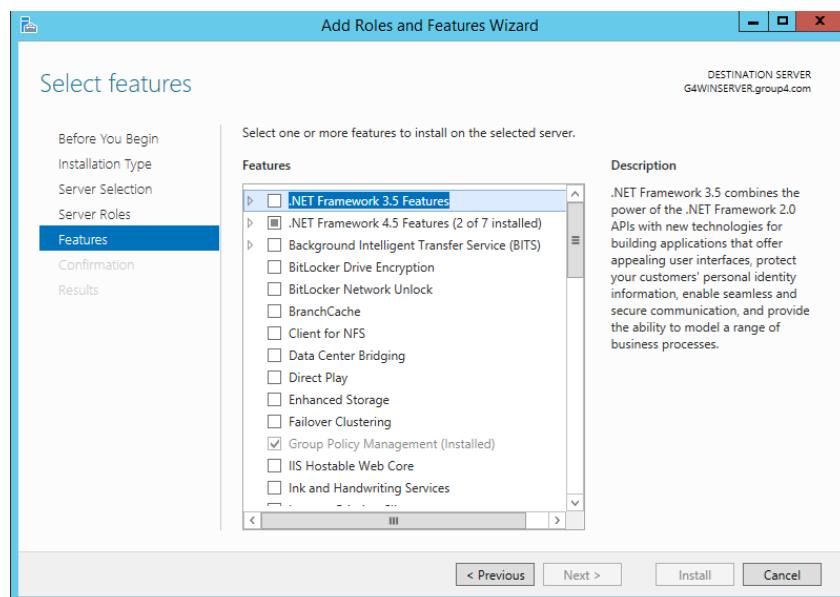


Figure 10: Select features for DHCP

Step 4: Then, wait until the installation completed.

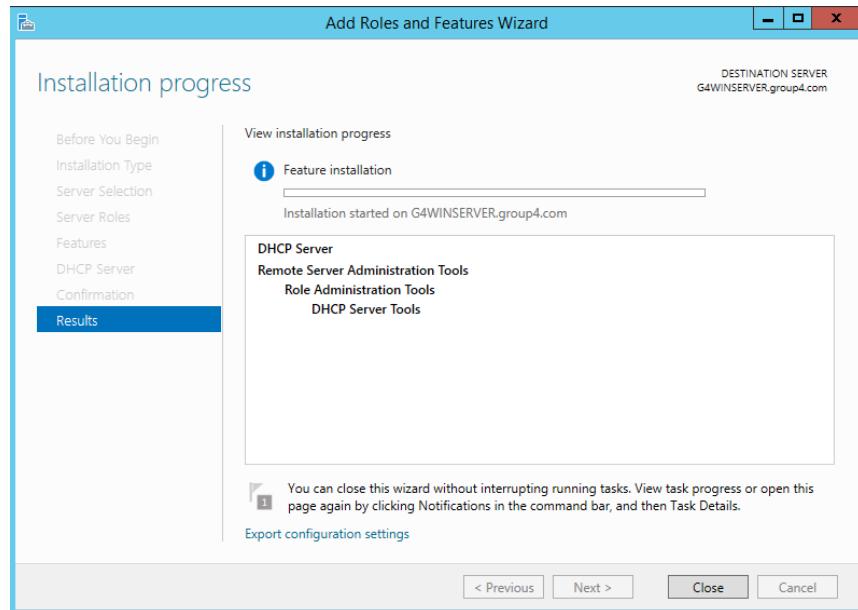


Figure 28: DHCP role to be completed

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

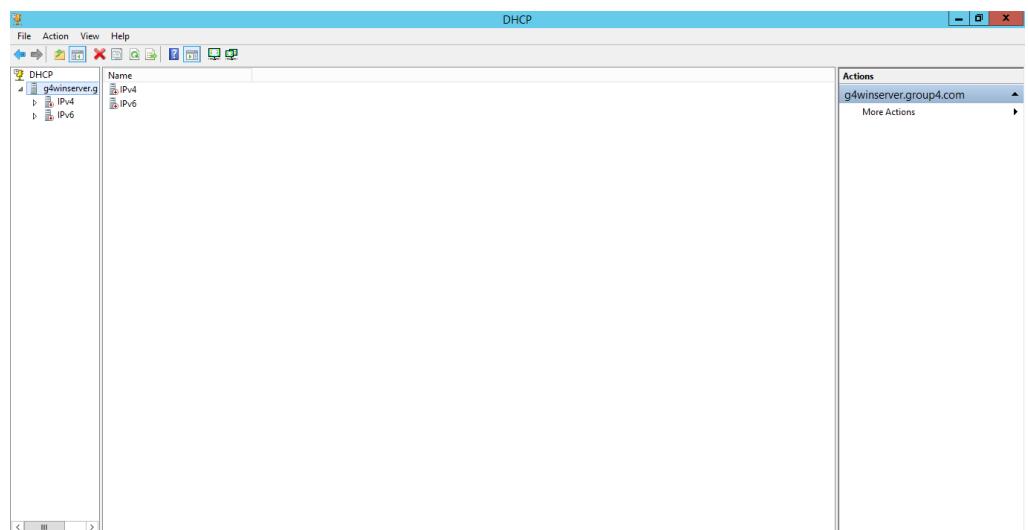


Figure 2911: DHCP configuration page

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

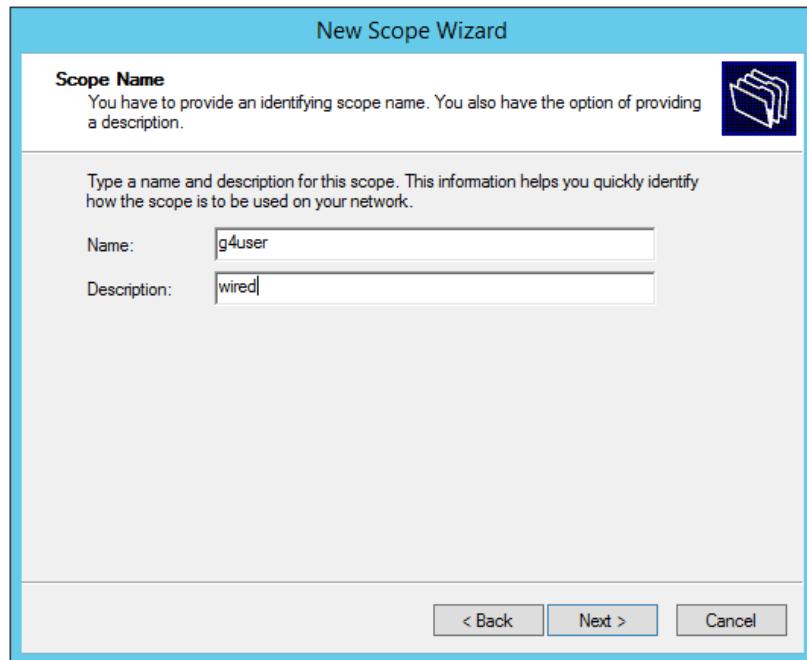


Figure 30: Create scope name for New Scope Wizard

Step 7: Then, set the lease duration. It is to specifies how long client can use and IP Address from this scope. After that, click Next.

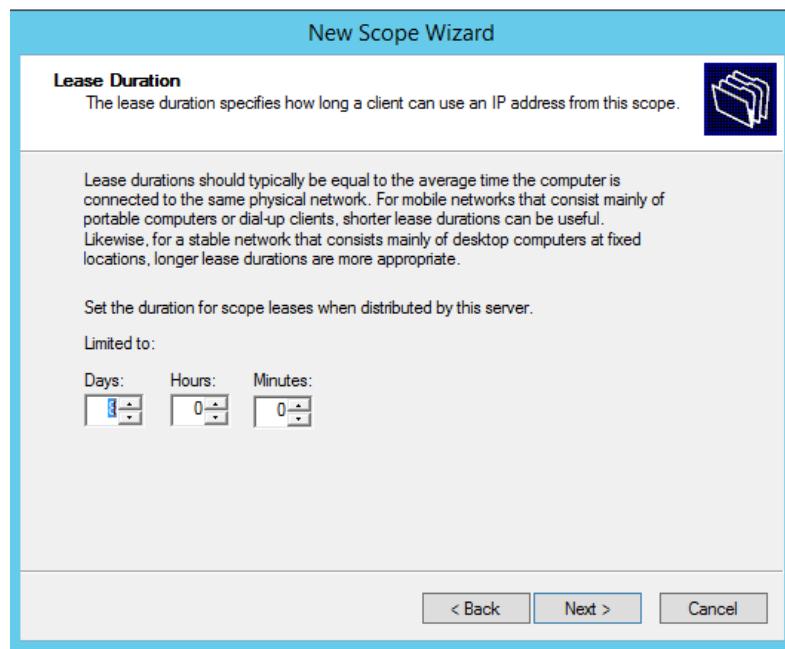


Figure 31: Set the lease duration

Step 8: As a result, it will show the Start IP Address, End IP Address and Description at the DHCP page.

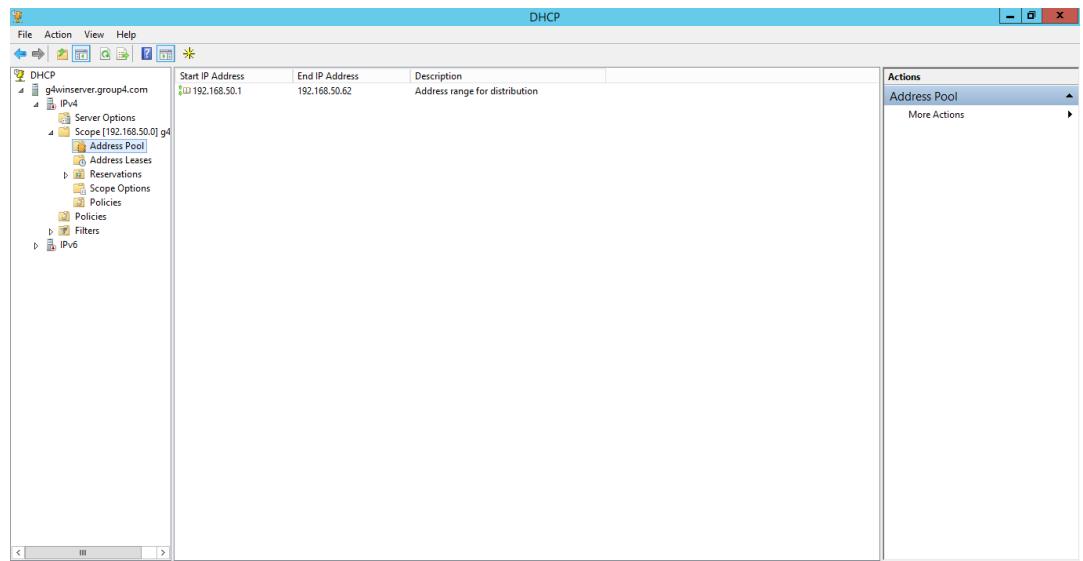


Figure 32: Results of DHCP page

```
G4Router(config)#int fa0/1.50
G4Router(config-subif)#ip helper-address 192.168.10.4
G4Router(config-subif)#exit
```

Figure 12: IP Helper command

5.3.3 Dynamic Host Configuration Protocol (DHCP) IPv6

Installation DHCP IPv6 (Wired)

Step 1: Open Tool and choose DHCP

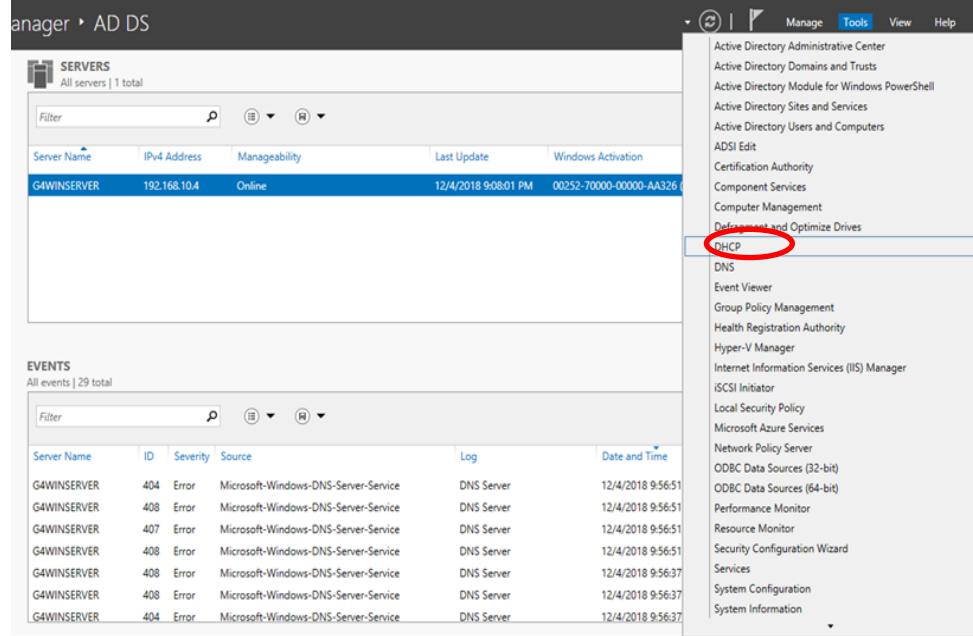


Figure 34: Install DHCP from server manager

Step 2: Right click IPv6 and choose New Scope.

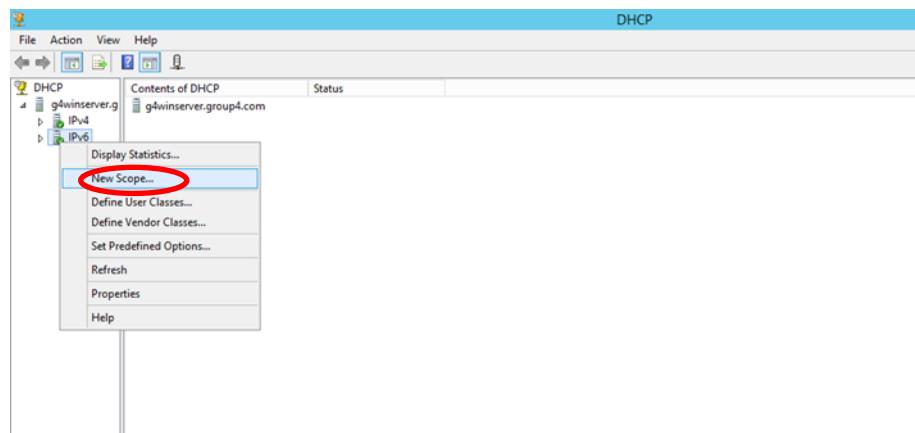


Figure 35: Choose New Scope

Step 3: Insert name as “wired_user_ipv6” then click Next.

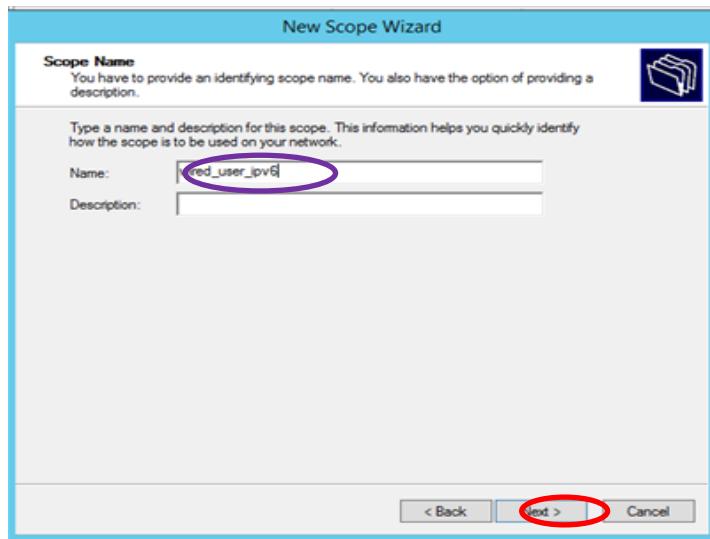


Figure 36: Add name in New Scope Wizard

Step 4: After that, insert prefix with (2004:db8:4444:F050::). Next, until it is completing the New Scope Wizard.

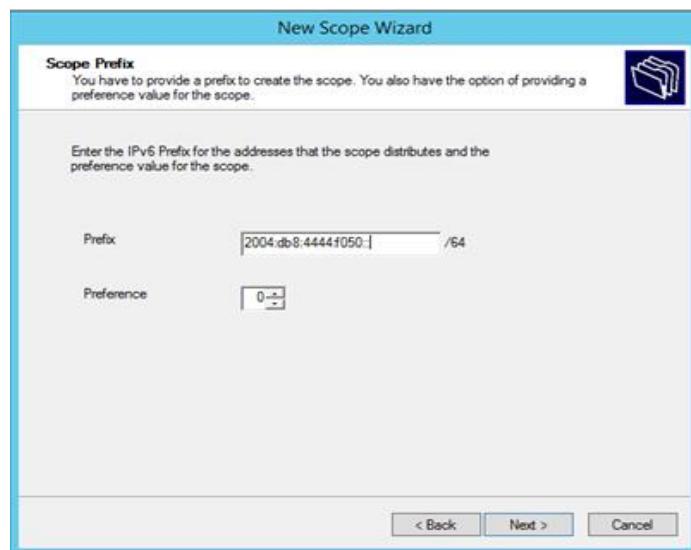


Figure 37: Insert prefix

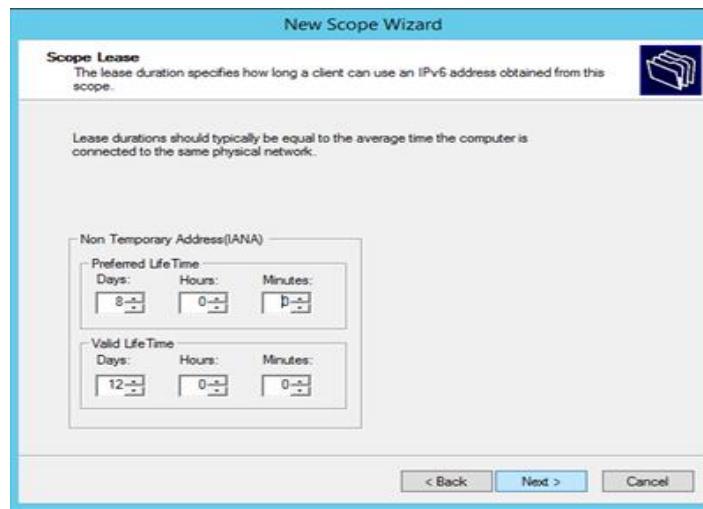


Figure 38: Scope Lease

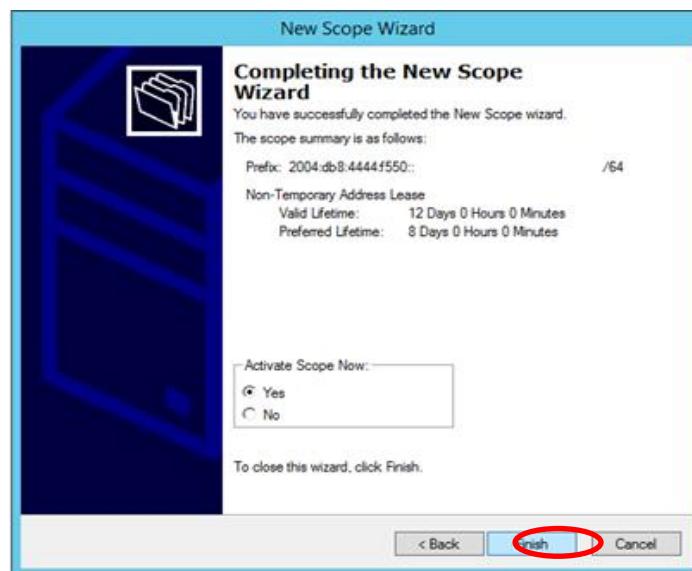


Figure 39: New Scope Wizard completed

Installation DHCP IPv6 (wireless)

Step 1: Right click IPv6 and choose New Scope

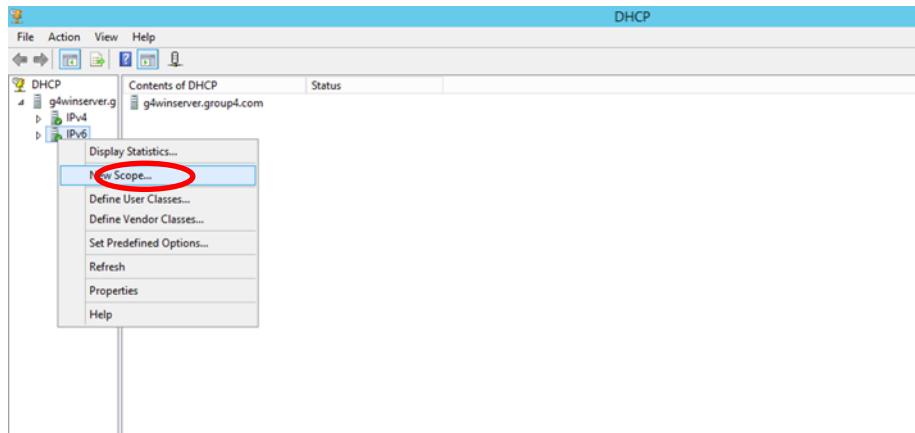


Figure 40: Choose New Scope

Step 2: Insert name as “*Wireless_user_ipv6*” then click next.

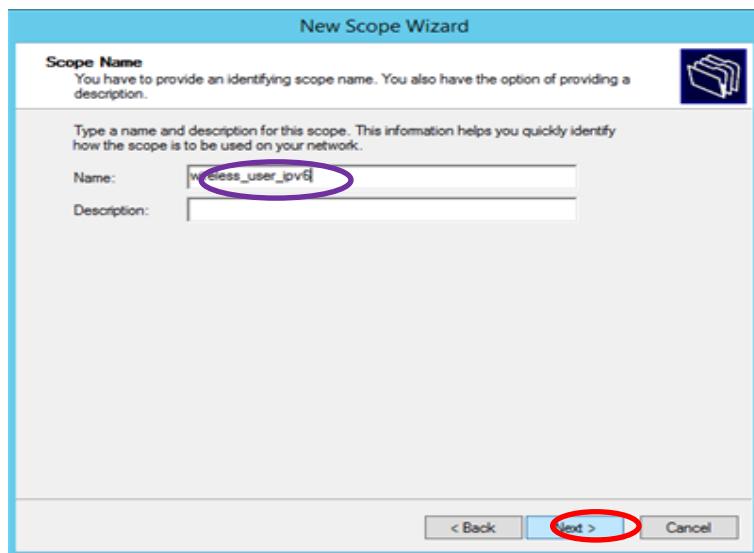


Figure 41: Add name in New Scope Wizard

Step 4: Insert prefix with (2004:db8:4444:F051::). Then, click next until it is finish.

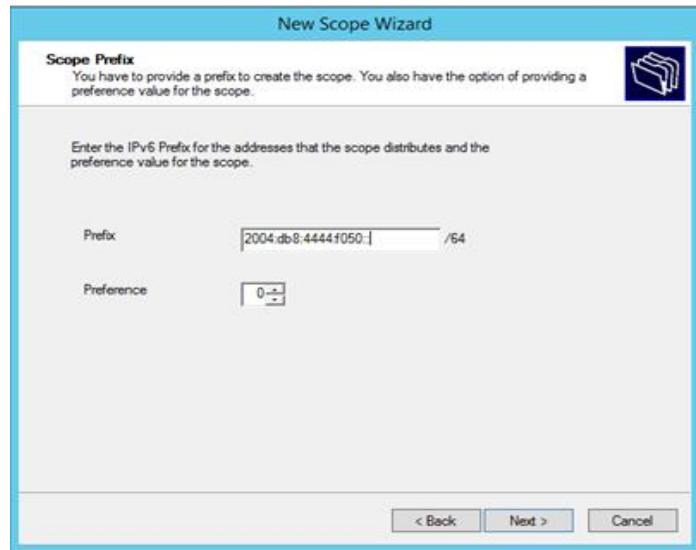


Figure 42: Insert Prefix

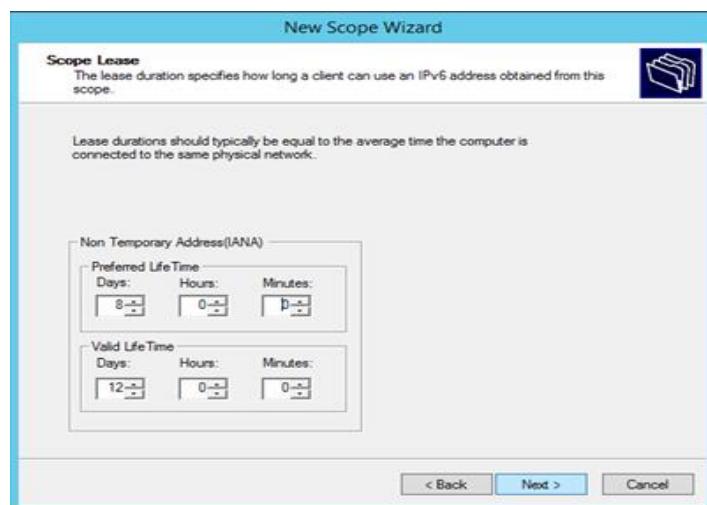


Figure 43: Scope Lease

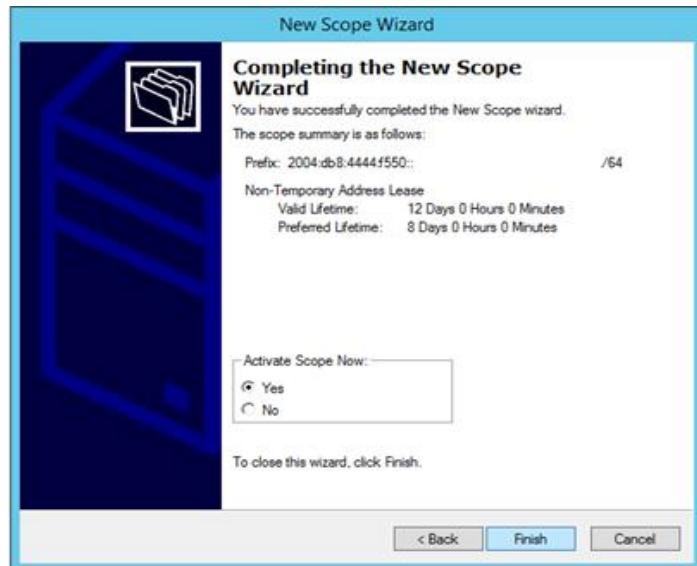


Figure 44: New Scope Wizard completed

5.3.4 Inter VLAN and VLSM Addressing

VLAN Configuration on Switch

Step 1 : Create VLAN and assign port number. Enables the VLAN to be used by using switchport mode access command.

Step 2 : For Windows Server.

```
G4Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
G4Switch(config)#vlan 10
G4Switch(config-vlan)#name Window
G4Switch(config-vlan)#exit

G4Switch(config-vlan)#int range fa0/2-4
G4Switch(config-if-range)#switchport mode access
G4Switch(config-if-range)#switchport access vlan 10
G4Switch(config-if-range)#exit
```

Figure 45: Creating VLAN for Window Server

Step 3 For Ubuntu Server.

```
G4Switch(config)#vlan 20
G4Switch(config-vlan)#name Ubuntu
G4Switch(config-vlan)#exit
G4Switch(config)#int range fa0/5-7
G4Switch(config-if-range)#switchport mode access
G4Switch(config-if-range)#switchport access vlan 20
G4Switch(config-if-range)#exit
```

Figure 46: Creating VLAN for Ubuntu Server

Step 4 : For Fedora Server.

```
G4Switch(config)#vlan 30
G4Switch(config-vlan)#name Fedora
G4Switch(config-vlan)#exit

G4Switch(config)#int range fa0/8-10
G4Switch(config-if-range)#switchport mode access
G4Switch(config-if-range)#switchport access vlan 30
G4Switch(config-if-range)#exit
```

Figure 47: Creating VLAN for Fedora Server

Step 5 : For Access Point.

```
G4Switch(config)#vlan 51
G4Switch(config-vlan)#name AP
G4Switch(config-vlan)#exit

G4Switch(config)#int range fa0/11-12
G4Switch(config-if-range)#switchport mode access
G4Switch(config-if-range)#switchport access vlan 51
G4Switch(config-if-range)#exit
```

Figure 48: Creating VLAN for AP

Step 6 : For User.

```
G4Switch(config)#vlan 50
G4Switch(config-vlan)#name User
G4Switch(config-vlan)#exit

G4Switch(config)#int range fa0/14-17
G4Switch(config-if-range)#switchport mode access
G4Switch(config-if-range)#switchport access vlan 50
G4Switch(config-if-range)#exit
```

Figure 49: Creating VLAN for User

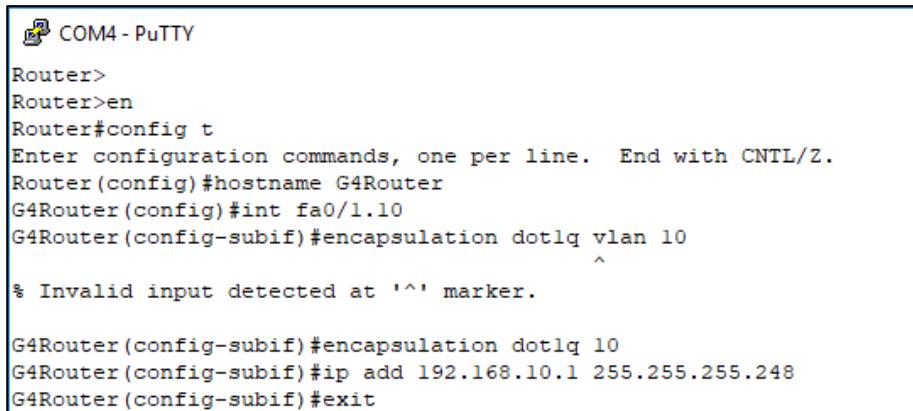
Step 7 : Create trunk from Switch to Router.

```
G4Switch(config)#int range fa0/23-24
G4Switch(config-if-range)#switchport mode access
G4Switch(config-if-range)#no switchport mode access
G4Switch(config-if-range)#switchport mode trunk
G4Switch(config-if-range)#switchport trunk native vlan 3
G4Switch(config-if-range)#exit
```

Figure 50: Creating trunk from Switch to Router

Step 8 : Configure trunking on port fa0/0 for VLAN 10, VLAN 20, VLAN 30 and VLAN 50 in router.

Step 9 : Configure trunking for VLAN 10 (int fa0/1.10)



```
COM4 - PuTTY
Router>
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname G4Router
G4Router(config)#int fa0/1.10
G4Router(config-subif)#encapsulation dot1q vlan 10
^
% Invalid input detected at '^' marker.

G4Router(config-subif)#encapsulation dot1q 10
G4Router(config-subif)#ip add 192.168.10.1 255.255.255.248
G4Router(config-subif)#exit
```

Figure 51: Configure trunking for VLAN 10

Step 10 : Configure trunking for VLAN 20 (int fa0/1.20)

```
G4Router(config)#int fa0/1.20
G4Router(config-subif)#encapsulation dot1q 20
G4Router(config-subif)#ip add 192.168.20.1 255.255.255.248
G4Router(config-subif)#no shut
G4Router(config-subif)#exit
```

Figure 52: Configure trunking for VLAN 20

Step 11 : Configure trunking for VLAN 30 (int fa0/1.30)

```
G4Router(config)#int fa0/1.30
G4Router(config-subif)#encapsulation dot1q 30
G4Router(config-subif)#ip add 192.168.30.1 255.255.255.248
G4Router(config-subif)#no shut
G4Router(config-subif)#exit
```

Figure 53: Configure trunking for VLAN 30

Step 12 : Configure trunking for VLAN 50 (int fa0/0.100)

```
COM4 - PuTTY
G4Router(config)#int fa0/1.50
G4Router(config-subif)#encapsulation dot1q 50
G4Router(config-subif)#ip add 192.168.50.1 255.255.255.192
G4Router(config-subif)#no shut
G4Router(config-subif)#exit
```

Figure 54: Configure trunking for VLAN 50

Step 13 : Configure trunking for VLAN 51 (int fa0/1.51)

```
G4Router(config)#int fa0/1.51
G4Router(config-subif)#encapsulation dot1q 521
G4Router(config-subif)#no encapsulation dot1q 521
G4Router(config-subif)#encapsulation dot1q 51
G4Router(config-subif)#ip add 192.168.51.1 255.255.255.192
G4Router(config-subif)#no shut
```

Figure 55: Configure trunking for VLAN 51

Step 14 : Configure trunking for VLAN 3 (int fa0/1.3)

```
G4Router(config)#int fa0/1.3
G4Router(config-subif)#encapsulation dot1q 3
G4Router(config-subif)#ip add 192.168.3.1 255.255.255.248
G4Router(config-subif)#no shut
G4Router(config-subif)#exit
```

Figure 56: Configure trunking for VLAN 3

5.3.5 Routing & NAT

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

```
interface FastEthernet0/0
ip address 200.200.202.7 255.255.255.240
ip nat outside
```

Figure 57: IP NAT Outside

Step 2: Set IP NAT Inside to all intervlans.

```
interface FastEthernet0/1.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.248
ip nat inside
```

Figure 58: IP NAT inside

Step 3: Set the F0/0 overload and set the static NAT public IP to all servers.

```
ip nat inside source list 11 interface FastEthernet0/0 overload
ip nat inside source static 192.168.10.4 200.200.202.4
ip nat inside source static 192.168.20.4 200.200.202.5
ip nat inside source static 192.168.30.4 200.200.202.6
```

Figure 59: Static NAT public IP to all servers

Step 4: Then, set the NAT setup.

```
ip nat pool G4-Pool 200.200.202.1 200.200.202.7 netmask 255.255.255.240
ip nat inside source list 1 pool G4-Pool overload
ip nat inside source list 11 interface FastEthernet0/0 overload
ip nat inside source static 192.168.10.4 200.200.202.4
ip nat inside source static 192.168.20.4 200.200.202.5
ip nat inside source static 192.168.30.4 200.200.202.6

access-list 1 permit 192.168.50.0 0.0.0.63
access-list 1 permit 192.168.51.0 0.0.0.63
access-list 11 permit 192.168.0.0 0.0.0.255
access-list 11 permit 192.168.0.0 0.0.127.255
```

Figure 60: NAT Setup

5.3.6 Active Directory (AD)

Step 1 : Open Server Manager in Windows Server and select Add Roles and Features Wizard.

Step 2 : Tick on Active Directory Domain Service and then click Next > Next until it required to click Install button.

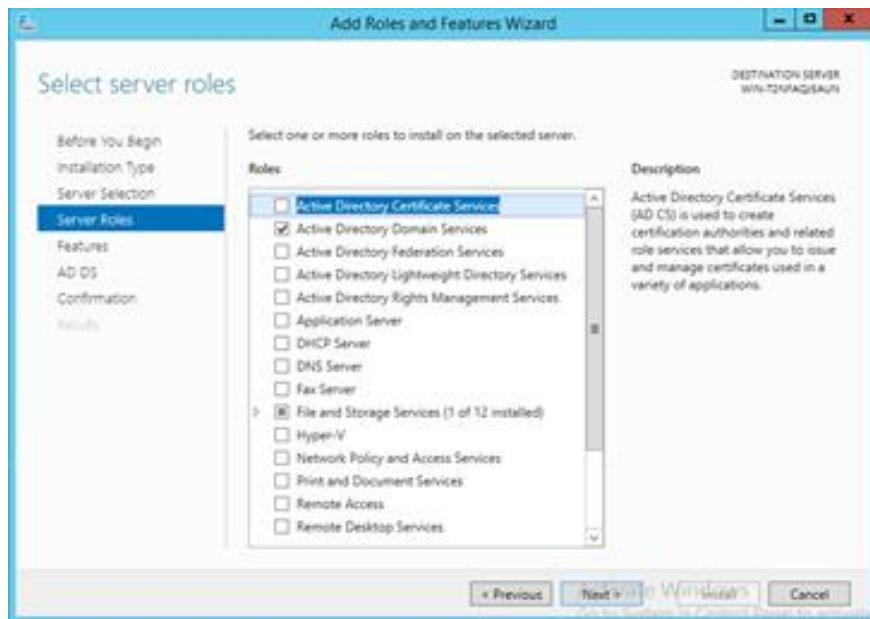


Figure 61: AD server roles selection

Step 3 : Then, wait until the installation of the features finish and click Close.

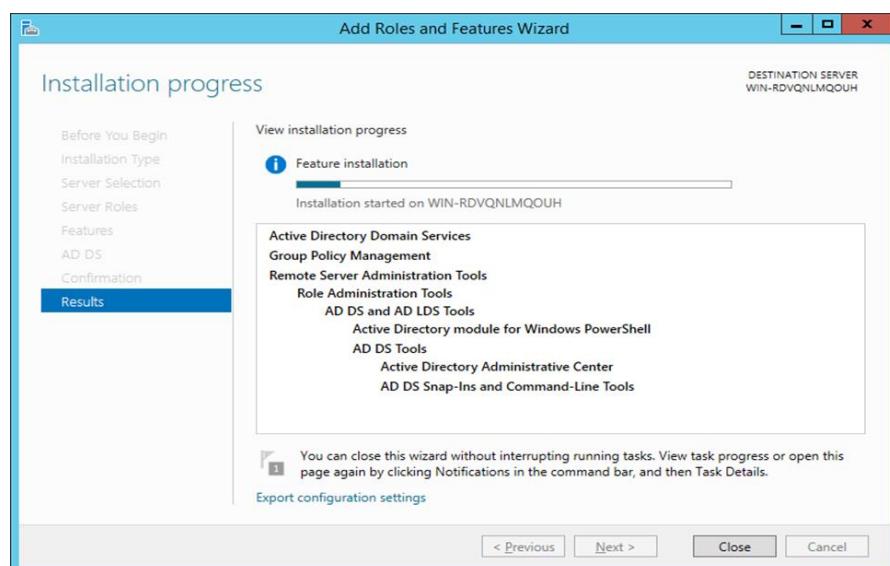


Figure 62: Installation progress for AD

Step 4 : After installation finished, check at the Dashboard. If success, it will display Active Directory Domain Services (AD DS) roles.

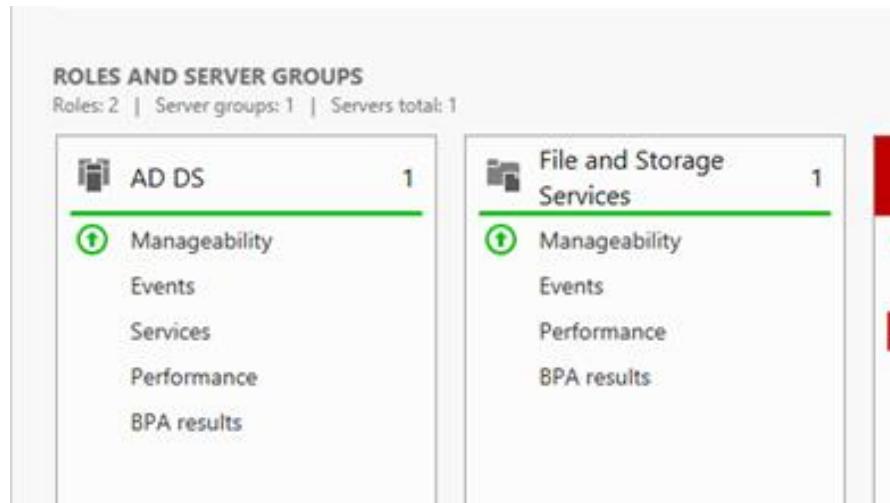


Figure 63: AD DS roles in Dashboard

Step 5 : Then, select Tools at menu bar on upper right and choose Active Directory Users and Computer.

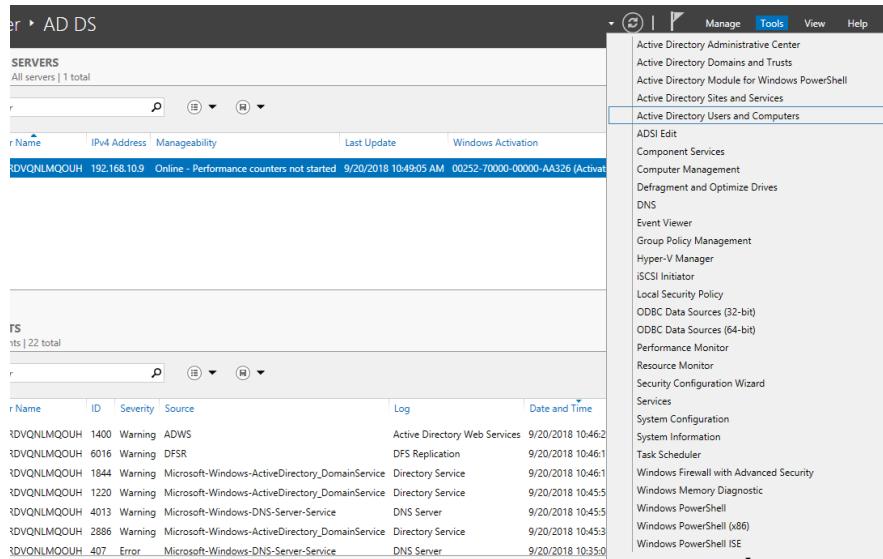


Figure 64: Tools at menu bar and click AD Users and Computer

Step 6 : Next, create a new user (in our group; KIFLYZAN). Then, right click at the Users and choose New > User.

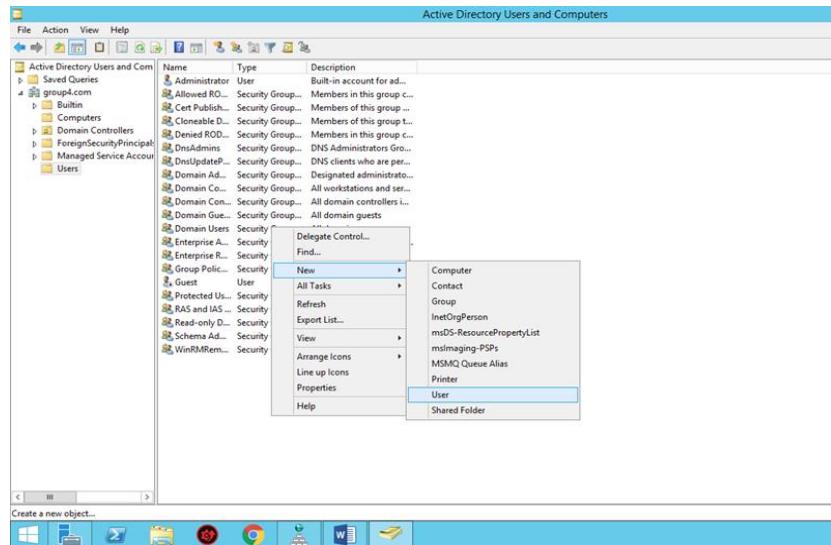


Figure 65: Creating New User

Step 7 : Next, create a new user named g4-17. After that, click Next button.

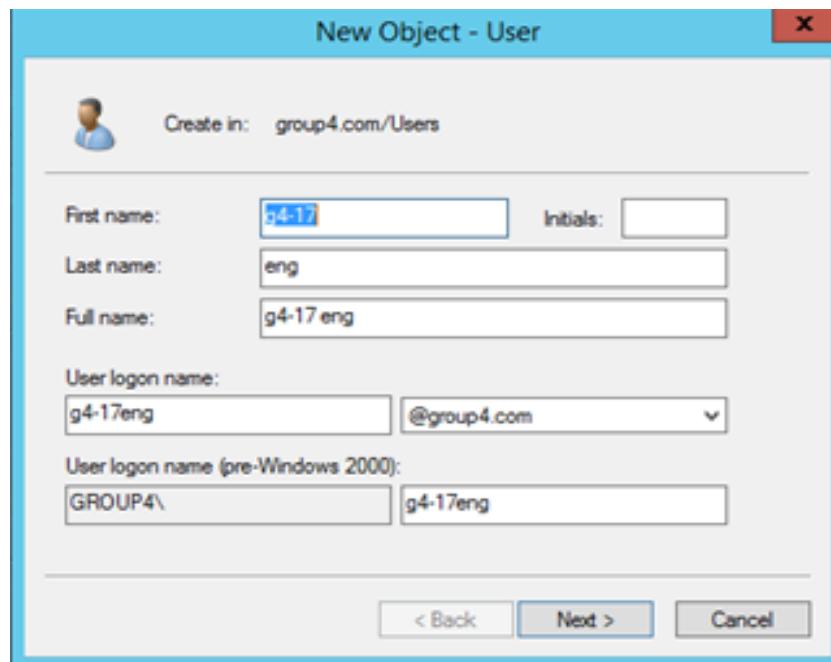


Figure 66: Creating new user

Step 8 : Then, it will show the detailed of the user data that have been created and click Finish.

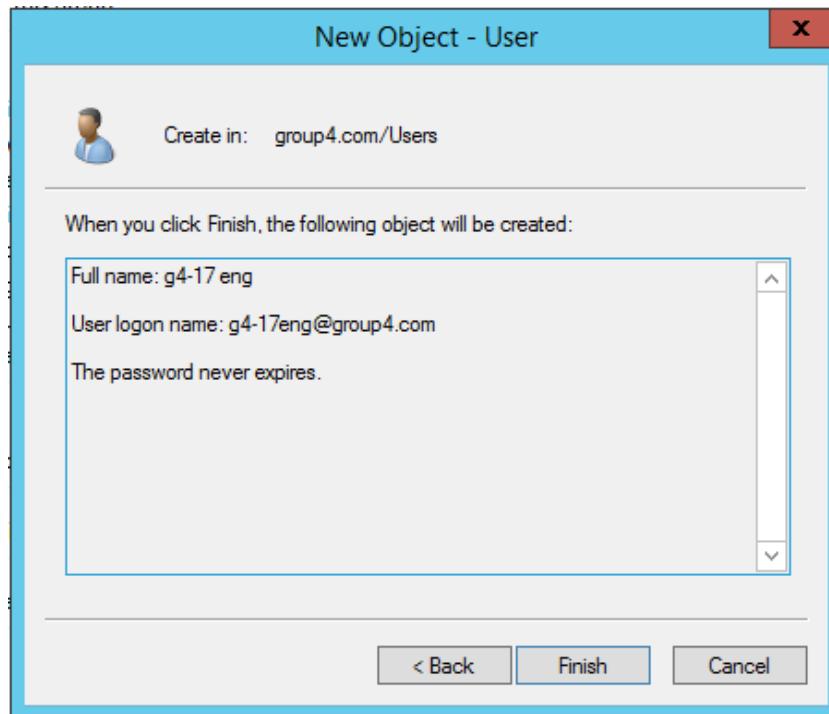


Figure 67: Detailed of user data

Step 9 : Now, create 9 more user (each of group members). Repeat same step from step 6 – step 8.

Step 10 : Next step, type Domain Admin in the object names and click OK button.

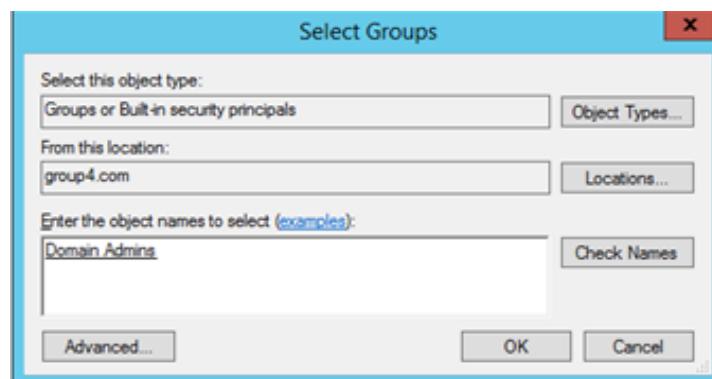


Figure 68: Selecting groups

Group Policy Object

Step 1 : Go to Icon window > Search Box > Group Policy Management.

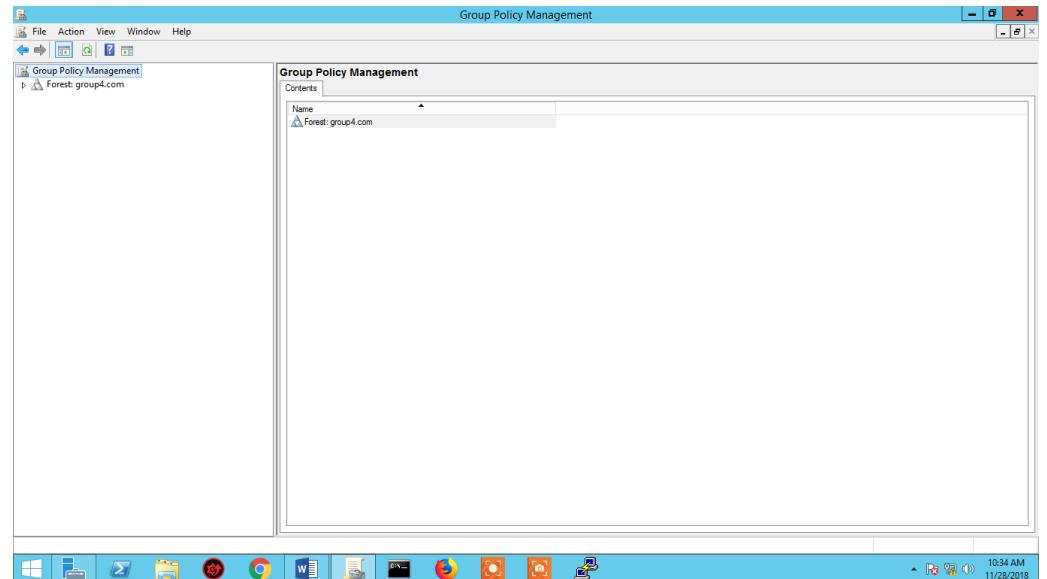


Figure 69: GPO Management Dashboard

Step 2 : Select on Forest group4.com > Domain > group4.com

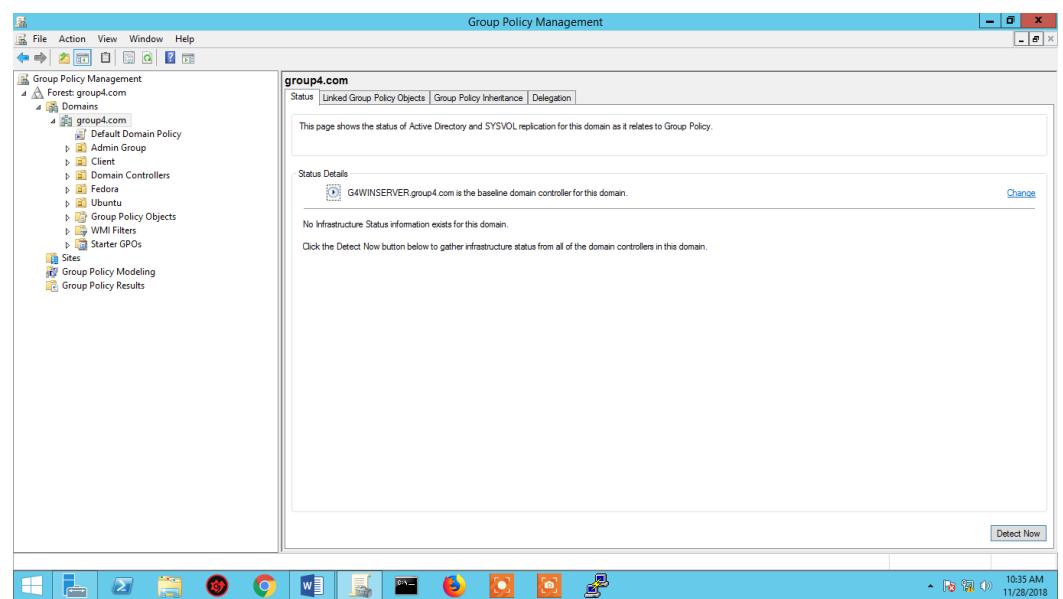


Figure 70: GPO Status

Step 3 : Right click on Client organizational unit and select Create GPO in this domain.

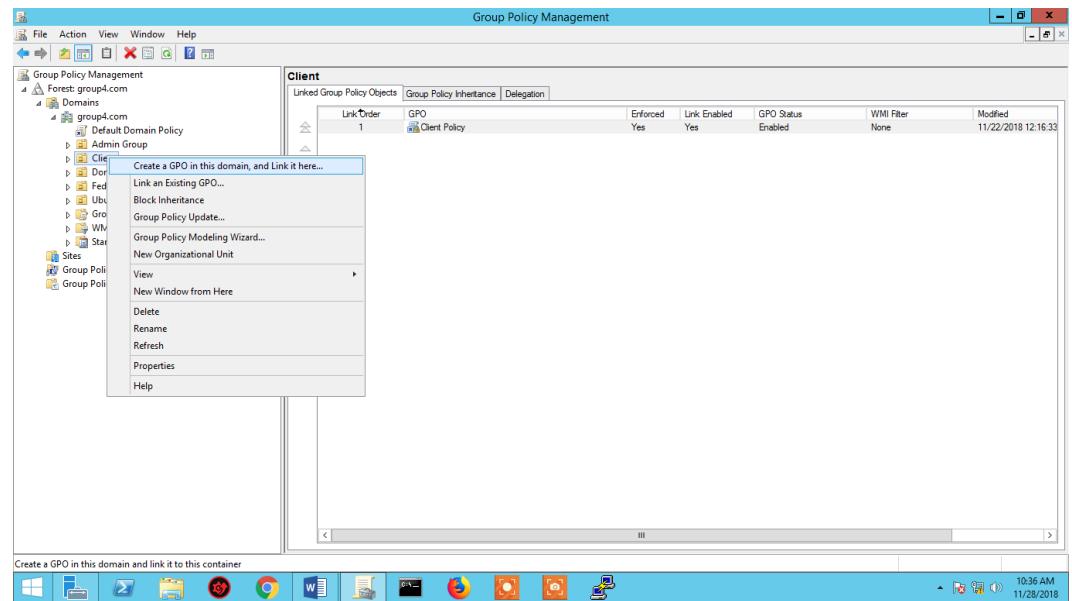


Figure 71: Create GPO in this domain

Step 4 : Insert Name (example: Client Policy) for the new GPO.

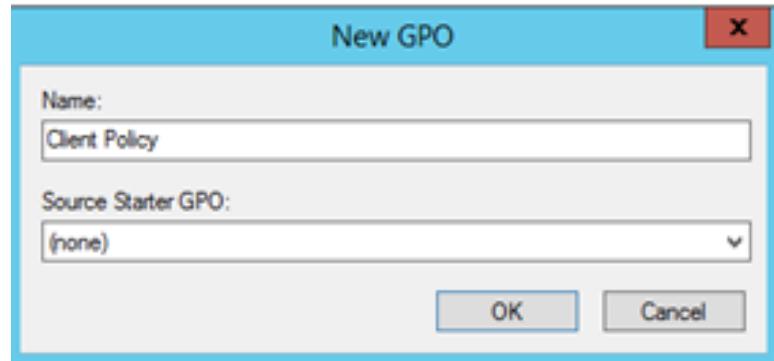


Figure 72: Creating new GPO

Step 5 : After creating the new GPO, we will see the new policy are Client Policy at GPO status.

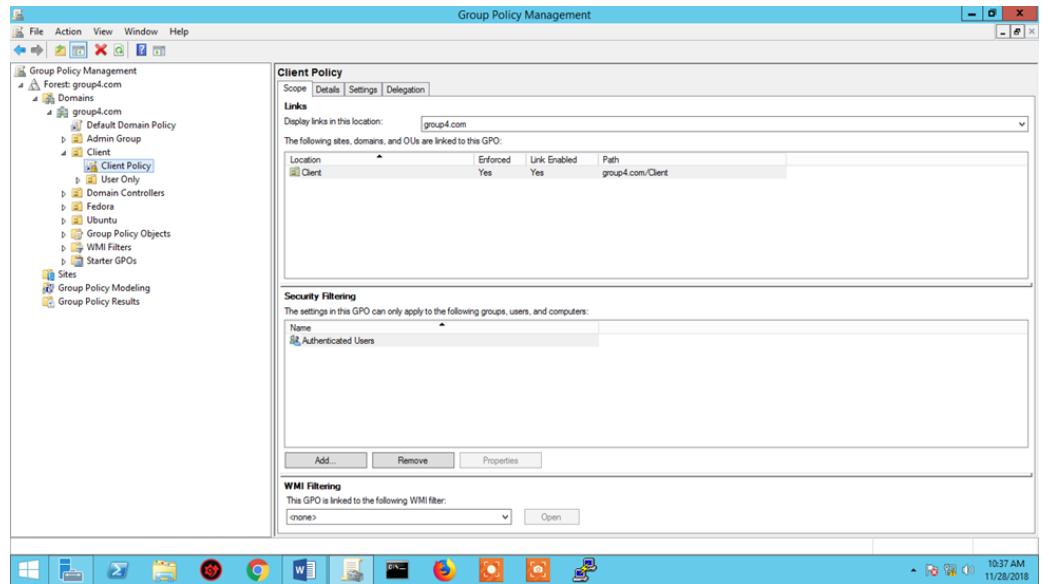


Figure 73: GPO Status of Client policy

Step 6 : Then, right click on Client Policy > Edit Policy > GPO Editor.

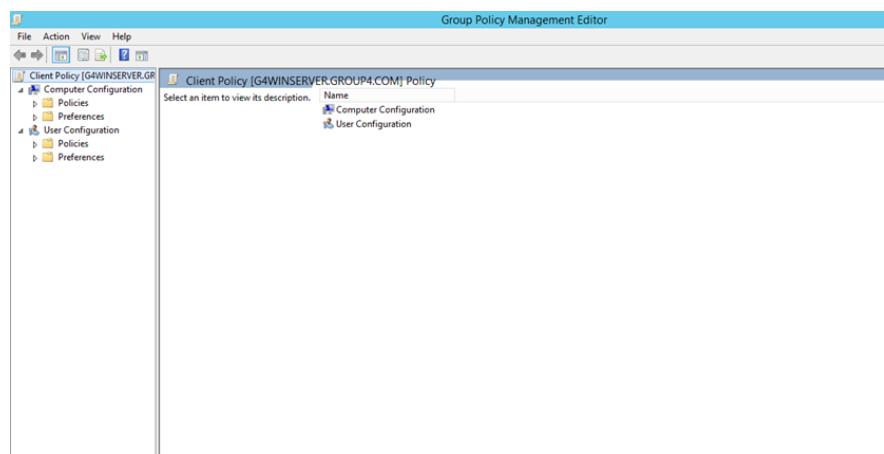


Figure 74: GPO Management Editor

Step 7 : After that, select User Configuration > Policies > Administrative Template > Control Panel > Personalization.

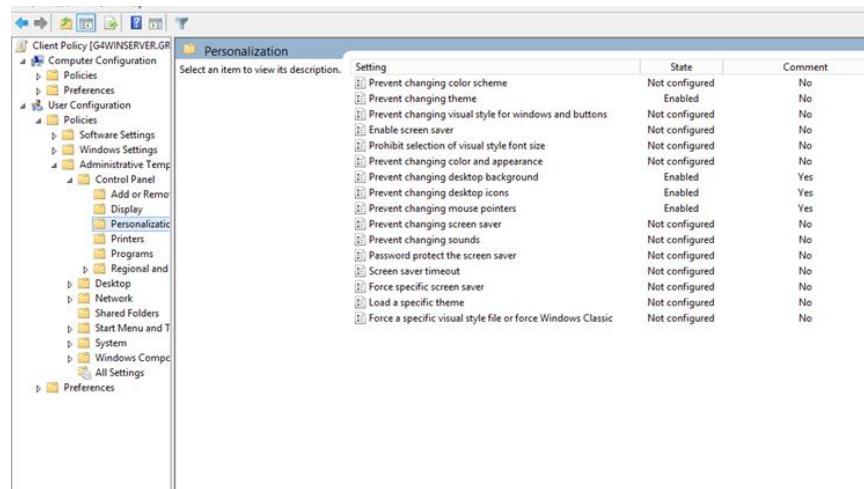


Figure 75: Personalization of GPO

Step 8 : Configure personalization policy for the client.

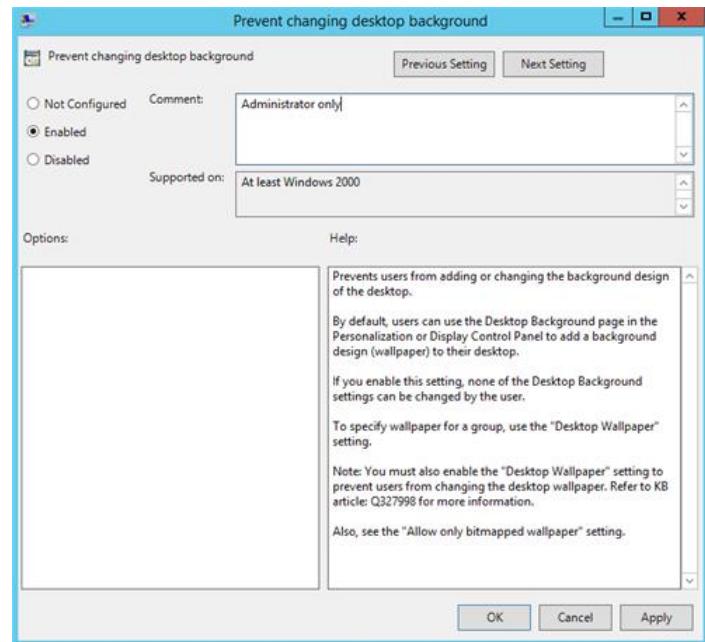
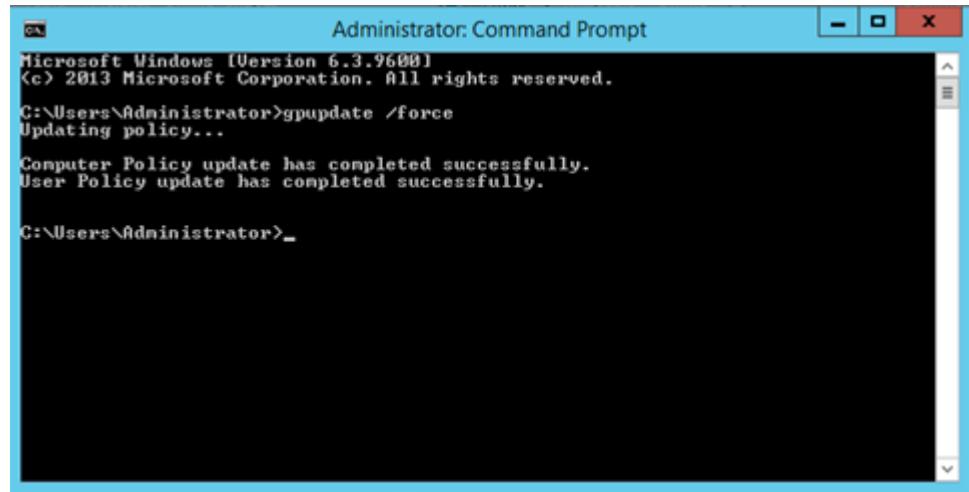


Figure 76: Personalization policy for the client

Step 9 : Open command prompt to update the policy



The image shows an 'Administrator: Command Prompt' window. The title bar reads 'Administrator: Command Prompt'. The content area displays the following text:

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

C:\Users\Administrator>gpupdate /force
Updating policy...

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

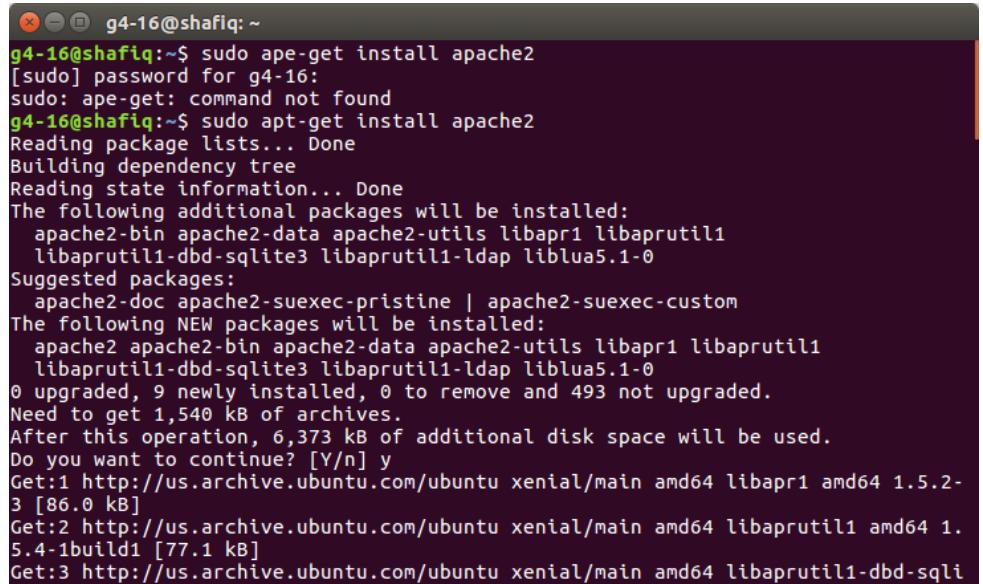
C:\Users\Administrator>
```

Figure 77: Policy update

5.3.7 Authentication User by Integrating AD with Linux

Step 1 : Open the Terminal in Ubuntu.

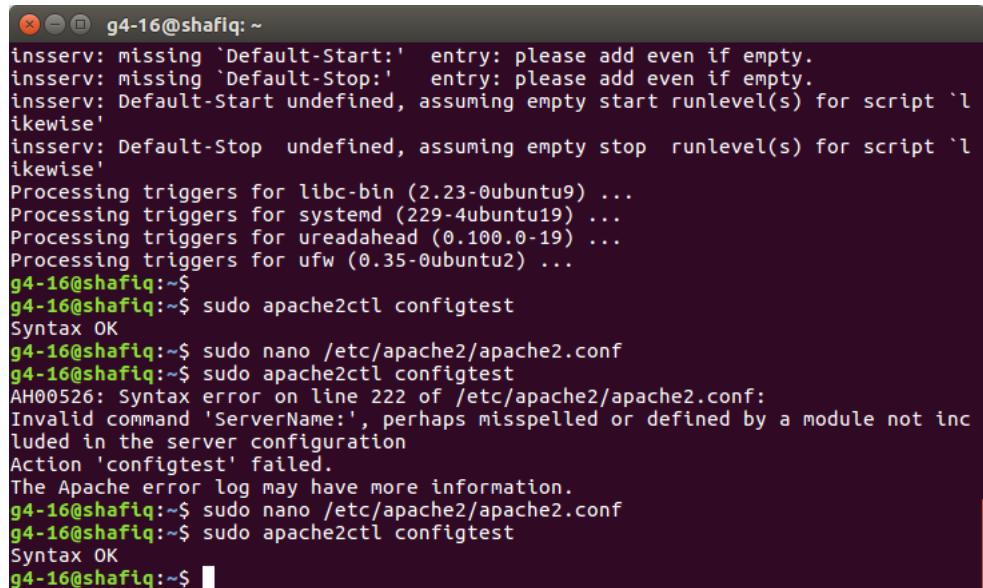
Step 2 : On the terminal, using command “sudo apt-get install apache2” to install apache2.



```
g4-16@shafiq:~$ sudo apt-get install apache2
[sudo] password for g4-16:
sudo: apt-get: command not found
g4-16@shafiq:~$ sudo apt-get install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.1-0
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.1-0
0 upgraded, 9 newly installed, 0 to remove and 493 not upgraded.
Need to get 1,540 kB of archives.
After this operation, 6,373 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 libapr1 amd64 1.5.2-3 [86.0 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 libaprutil1 amd64 1.5.4-1build1 [77.1 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 libaprutil1-dbd-sqlite3 [11.4 kB]
```

Figure 78: Install apache2

Step 3 : Then, configure apache2.



```
g4-16@shafiq:~$ insserv: missing 'Default-Start:' entry: please add even if empty.
insserv: missing 'Default-Stop:' entry: please add even if empty.
insserv: Default-Start undefined, assuming empty start runlevel(s) for script 'likewise'
insserv: Default-Stop undefined, assuming empty stop runlevel(s) for script 'likewise'
Processing triggers for libc-bin (2.23-0ubuntu9) ...
Processing triggers for systemd (229-4ubuntu19) ...
Processing triggers for ureadahead (0.100.0-19) ...
Processing triggers for ufw (0.35-0ubuntu2) ...
g4-16@shafiq:~$ g4-16@shafiq:~$ sudo apache2ctl configtest
Syntax OK
g4-16@shafiq:~$ g4-16@shafiq:~$ sudo nano /etc/apache2/apache2.conf
g4-16@shafiq:~$ sudo apache2ctl configtest
AH00526: Syntax error on line 222 of /etc/apache2/apache2.conf:
Invalid command 'ServerName:', perhaps misspelled or defined by a module not included in the server configuration
Action 'configtest' failed.
The Apache error log may have more information.
g4-16@shafiq:~$ g4-16@shafiq:~$ sudo nano /etc/apache2/apache2.conf
g4-16@shafiq:~$ sudo apache2ctl configtest
Syntax OK
g4-16@shafiq:~$
```

Figure 79: Apache2 configuration

Step 4 : After that, download PBIS latest version (pbis 8.5.6.375) and install it using “chmod+x ./pbis-open-8.5.6.375.linux.x86_64.deb.sh”.



```
root@g416-HP-ProDesk-600-G3-MT:/home/g4-16# chmod +x ./pbis-open-8.5.6.375.linux.x86_64.deb.sh
root@g416-HP-ProDesk-600-G3-MT:/home/g4-16# ./pbis-open-8.5.6.375.linux.x86_64.deb.sh
Creating directory pbis-open-8.5.6.375.linux.x86_64.deb
Verifying archive integrity... All good.
Uncompressing pbis-open-8.5.6.375.linux.x86_64.deb...
Installing packages and old packages will be removed...
Selecting previously unselected package pbis-open upgrade.
(Reading database ... 175354 files and directories currently installed.)
Preparing to unpack .../pbis-open-upgrade_8.5.6.375_amd64.deb ...
Preserving Likewise 6.1 configuration in /var/lib/pbis-upgrade.

Unpacking pbis-open-upgrade (8.5.6.375) ...
Setting up pbis-open-upgrade (8.5.6.375) ...
(Reading database ... 175355 files and directories currently installed.)
Removing likewise-open (6.1.0.406~Ubuntu10) ...
Processing triggers for man-db (2.7.5-1) ...
Processing triggers for libc-bin (2.23-0ubuntu9) ...
Selecting previously unselected package pbis-open.
(Reading database ... 175116 files and directories currently installed.)
Preparing to unpack .../pbis-open_8.5.6.375_amd64.deb ...
Unpacking pbis-open (8.5.6.375) ...
Setting up pbis-open (8.5.6.375) ...
Upgrading from Likewise Open 6.1

Importing registry...

Selecting previously unselected package pbis-open-gui.
(Reading database ... 175492 files and directories currently installed.)
Preparing to unpack .../pbis-open-gui_8.5.6.375_amd64.deb ...
Unpacking pbis-open-gui (8.5.6.375) ...
Setting up pbis-open-gui (8.5.6.375) ...
Installing Packages was successful

New libraries and configurations have been installed for PAM and NSS.
Please reboot so that all processes pick up the new versions.

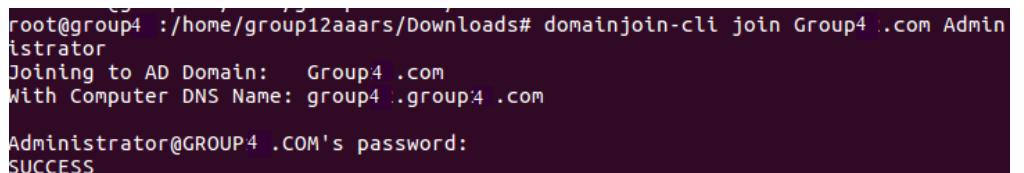
As root, run domainjoin-gui or domainjoin-cli to join a domain so you can log on
with Active Directory credentials. Example:
domainjoin-cli join MYDOMAIN.COM MyJoinAccount

root@g416-HP-ProDesk-600-G3-MT:/home/g4-16#
```

Figure 80: PBIS download and installation

Join Domain

Step 1 : Type command “domainjoin-cli join group4.com Administrator” and type password to join.

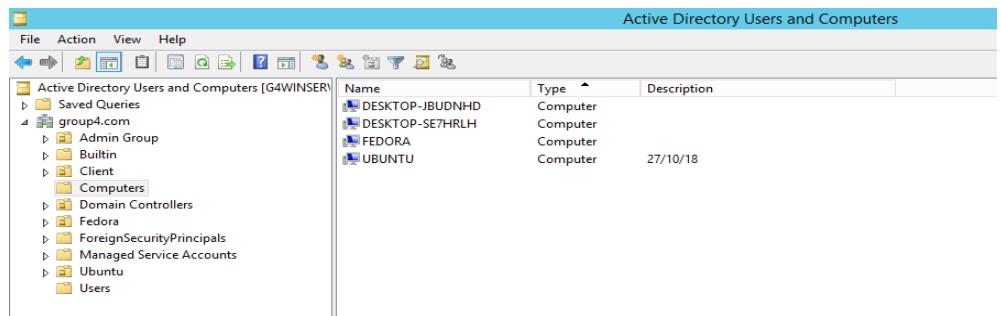


```
root@group4 :/home/group12aaars/Downloads# domainjoin-cli join Group4 .com Administrator
Joining to AD Domain: Group4 .com
With Computer DNS Name: group4 .group4 .com

Administrator@GROUP4 .COM's password:
SUCCESS
```

Figure 81: Command to join domain

Step 2 : Ubuntu 16.04 is added inside the computer file of Active Directory
Users and Computers in Windows Server 2012.



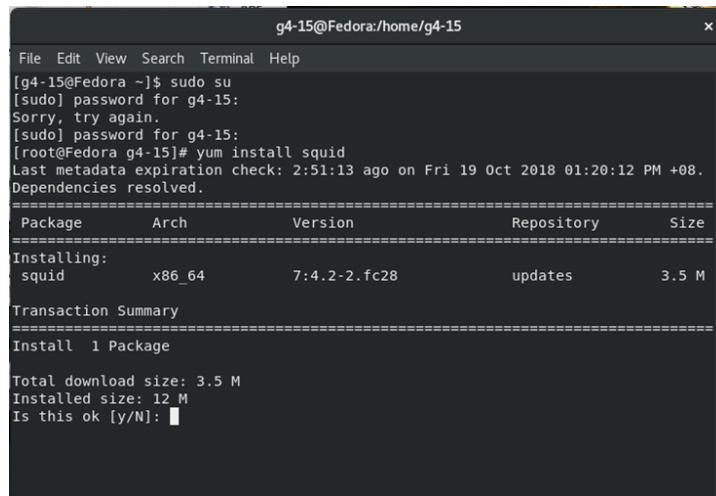
The screenshot shows the Windows Server 2012 Active Directory Users and Computers console. The left pane displays a tree view of the directory structure under 'Active Directory Users and Computers [G4WINSER]'. The 'Computers' node is selected. The right pane is titled 'Active Directory Users and Computers' and contains a table with three rows of data:

Name	Type	Description
DESKTOP-JBUDNHD	Computer	
DESKTOP-SE7HRLH	Computer	
FEDORA	Computer	
UBUNTU	Computer	27/10/18

Figure 82: AD Users and Computer addition of Ubuntu

5.3.8 Proxy Server

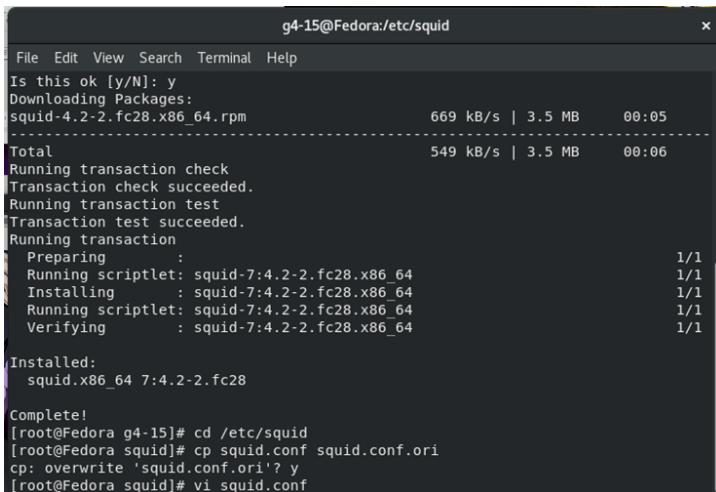
Step 1 : Firstly, Install the Squid Package using command as shown below.



```
g4-15@Fedora:~]$ sudo su
[sudo] password for g4-15:
Sorry, try again.
[sudo] password for g4-15:
[root@Fedora g4-15]# yum install squid
Last metadata expiration check: 2:51:13 ago on Fri 19 Oct 2018 01:20:12 PM +08.
Dependencies resolved.
=====
| Package      Arch   Version       Repository  Size
=====
| Installing:
|   squid        x86_64  7:4.2-2.fc28    updates     3.5 M
Transaction Summary
=====
Install 1 Package

Total download size: 3.5 M
Installed size: 12 M
Is this ok [y/N]:
```

Figure 83: Command to install squid package



```
g4-15@Fedora:/etc/squid
File Edit View Search Terminal Help
Is this ok [y/N]: y
Downloading Packages:
squid-4.2-2.fc28.x86_64.rpm          669 kB/s | 3.5 MB  00:05
-----
Total                                         549 kB/s | 3.5 MB  00:06
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing :                                                 1/1
Running scriptlet: squid-7:4.2-2.fc28.x86_64           1/1
Installing : squid-7:4.2-2.fc28.x86_64                1/1
Running scriptlet: squid-7:4.2-2.fc28.x86_64           1/1
Verifying  : squid-7:4.2-2.fc28.x86_64                1/1
Installed:
  squid.x86_64 7:4.2-2.fc28

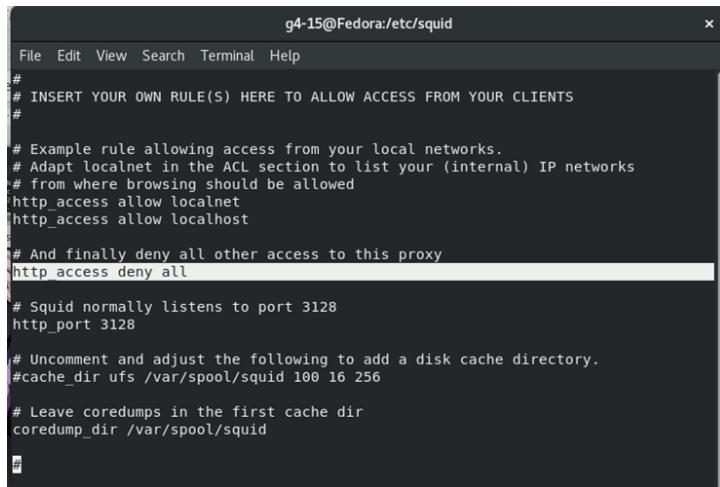
Complete!
[root@Fedora g4-15]# cd /etc/squid
[root@Fedora squid]# cp squid.conf squid.conf.orig
cp: overwrite 'squid.conf.orig'? y
[root@Fedora squid]# vi squid.conf
```

Figure 84: Edit squid configuration

Step 2 : Then, check the Squid Package Status using command “*service squid status*”

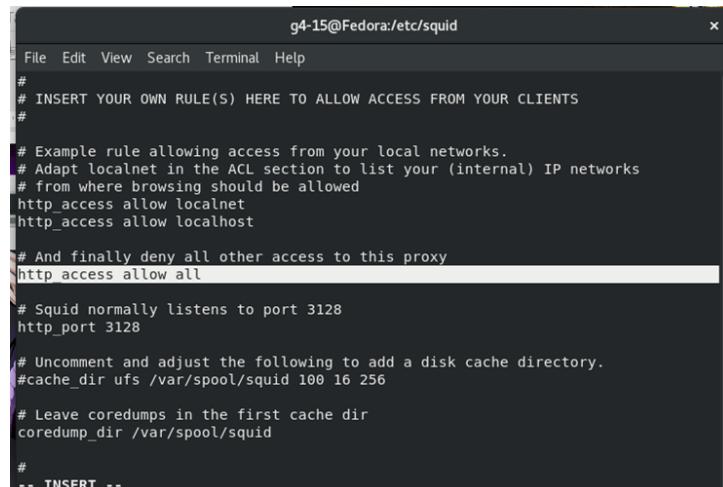
Step 3 : After that, to edit the squid configuration must use this command.

Step 4 : In the configuration file, change http access from “deny all” to “allow all”. Then, save the configuration file



```
g4-15@Fedora:/etc/squid
File Edit View Search Terminal Help
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
# 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 85: Change http access in configuration file



```
g4-15@Fedora:/etc/squid
File Edit View Search Terminal Help
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
# 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
#
# 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
#
# -- INSERT --
```

Figure 86: Http access change to allow

Step 5 : After that, start the Squid service using command “*systemctl start squid.service*”.

```
g4-15@Fedora:/etc/squid
File Edit View Search Terminal Help
Downloading Packages:
squid-4.2.2.fc28.x86_64.rpm          669 kB/s | 3.5 MB   00:05
-----
Total                                549 kB/s | 3.5 MB   00:06
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing :                                                 1/1
  Running scriptlet: squid-7:4.2-2.fc28.x86_64               1/1
  Installing  : squid-7:4.2-2.fc28.x86_64                   1/1
  Running scriptlet: squid-7:4.2-2.fc28.x86_64               1/1
  Verifying   : squid-7:4.2-2.fc28.x86_64                   1/1

Installed:
  squid.x86_64 7:4.2-2.fc28

Complete!
[root@Fedora g4-15]# cd /etc/squid
[root@Fedora squid]# cp squid.conf squid.conf.ori
cp: overwrite 'squid.conf.ori'? y
[root@Fedora squid]# vi squid.conf
[root@Fedora squid]# systemctl start squid.service
```

Figure 87: Start Squid service.

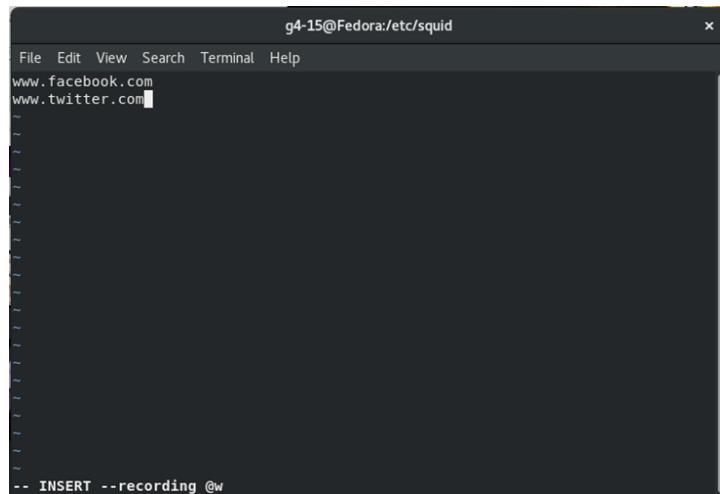
```
g4-15@Fedora:/etc/squid
File Edit View Search Terminal Help
squid-4.2.2.fc28.x86_64.rpm          669 kB/s | 3.5 MB   00:05
-----
Total                                549 kB/s | 3.5 MB   00:06
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing :                                                 1/1
  Running scriptlet: squid-7:4.2-2.fc28.x86_64               1/1
  Installing  : squid-7:4.2-2.fc28.x86_64                   1/1
  Running scriptlet: squid-7:4.2-2.fc28.x86_64               1/1
  Verifying   : squid-7:4.2-2.fc28.x86_64                   1/1

Installed:
  squid.x86_64 7:4.2-2.fc28

Complete!
[root@Fedora g4-15]# cd /etc/squid
[root@Fedora squid]# cp squid.conf squid.conf.ori
cp: overwrite 'squid.conf.ori'? y
[root@Fedora squid]# vi squid.conf
[root@Fedora squid]# systemctl start squid.service
[root@Fedora squid]# vi block.domain.acl
```

Figure 88: Decide to block which need to be blocked

Step 6: Block the domain that need to be block.

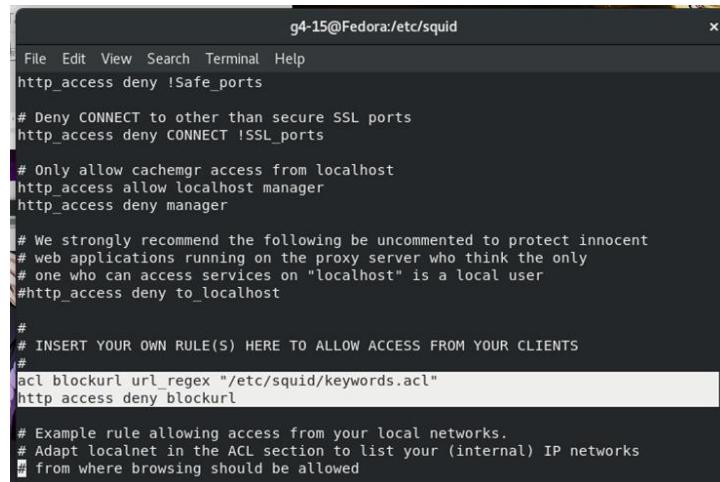


A screenshot of a terminal window titled "g4-15@Fedora:/etc/squid". The window shows a command-line interface with the following text:
www.facebook.com
www.twitter.com
-- INSERT --recording @w

Figure 89: Insert domain/keyword that need to be blocked

Step 7: Insert the domain/keyword that you to block.

Step 8: Go into squid.conf once again and insert the command below



A screenshot of a terminal window titled "g4-15@Fedora:/etc/squid". The window shows a configuration file with the following content:
http_access deny !safe_ports
Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports
Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager
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

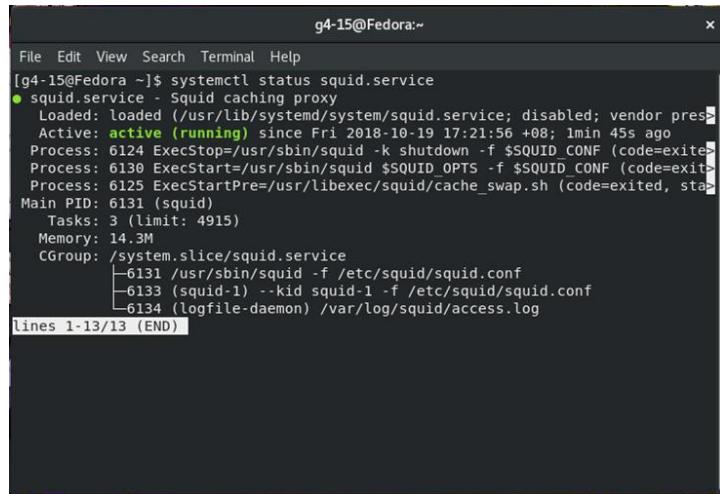
INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

acl blockurl url_regex "/etc/squid/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

Figure 90: Configure squid configuration

Step 9: Check the squid status. For every change of configuration that has been made, the squid proxy must be restarted.



```
g4-15@Fedora ~]$ systemctl status squid.service
● squid.service - Squid caching proxy
   Loaded: loaded (/usr/lib/systemd/system/squid.service; disabled; vendor pres>
   Active: active (running) since Fri 2018-10-19 17:21:56 +08; 1min 45s ago
     Process: 6124 ExecStop=/usr/sbin/squid -k shutdown -f $SQUID_CONF (code=exit>
     Process: 6130 ExecStart=/usr/sbin/squid $SQUID_OPTS -f $SQUID_CONF (code=exit>
     Process: 6125 ExecStartPre=/usr/libexec/squid/cache_swap.sh (code=exited, sta>
Main PID: 6131 (squid)
   Tasks: 3 (limit: 4915)
      Memory: 14.3M
         CPU: 0.000 CPU(s) since start
        CGroup: /system.slice/squid.service
                  ├─6131 /usr/sbin/squid -f /etc/squid/squid.conf
                  ├─6133 (squid-1) --pid squid-1 -f /etc/squid/squid.conf
                  └─6134 (logfile-daemon) /var/log/squid/access.log
lines 1-13/13 (END)
```

Figure 91: Squid status

Step 10: Open Your Browser.

Step 11: At the top right bar, click and select “Preferences” option.

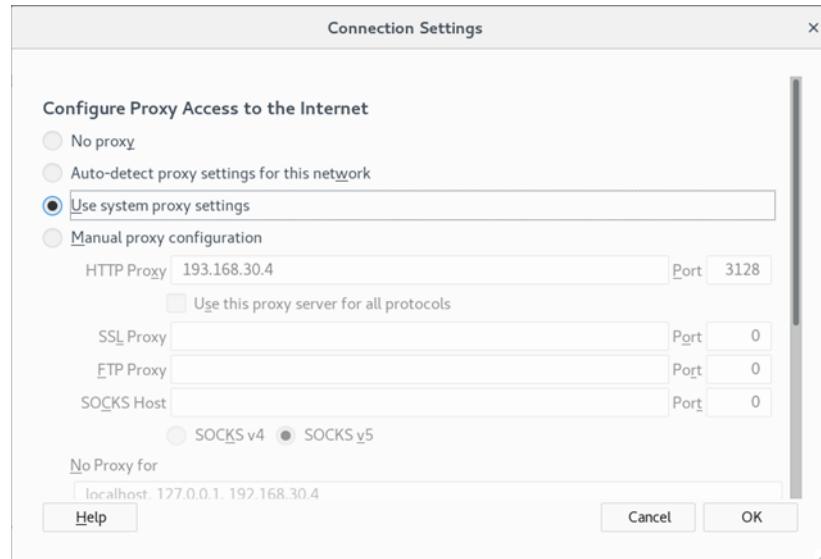


Figure 92: Connection Settings

Step 12: Select “Advance” option, “Network” and “Setting” button.

Step 13: Select “Use system proxy settings” and fill in as below.

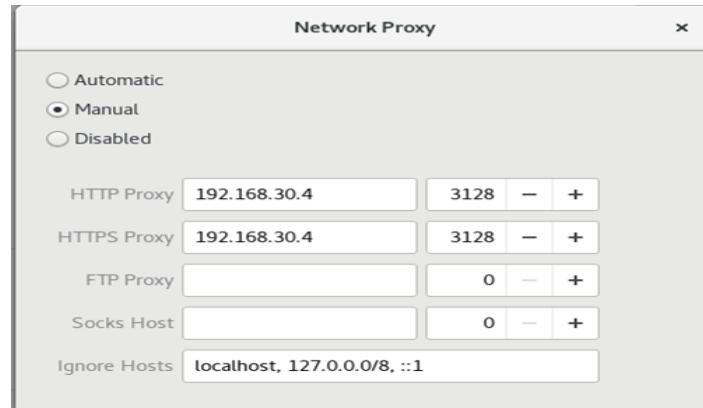
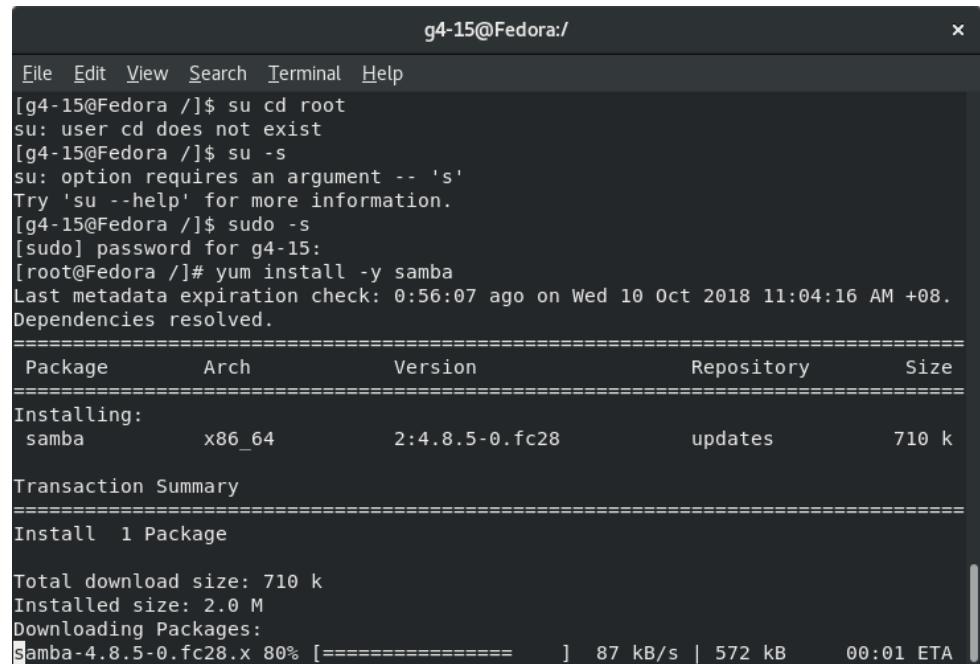


Figure 93: Network proxy setting

Step 14: Change the network proxy settings to manual.

5.3.9 Samba

Step 1 : Firstly, installed the Samba package in the Fedora terminal.

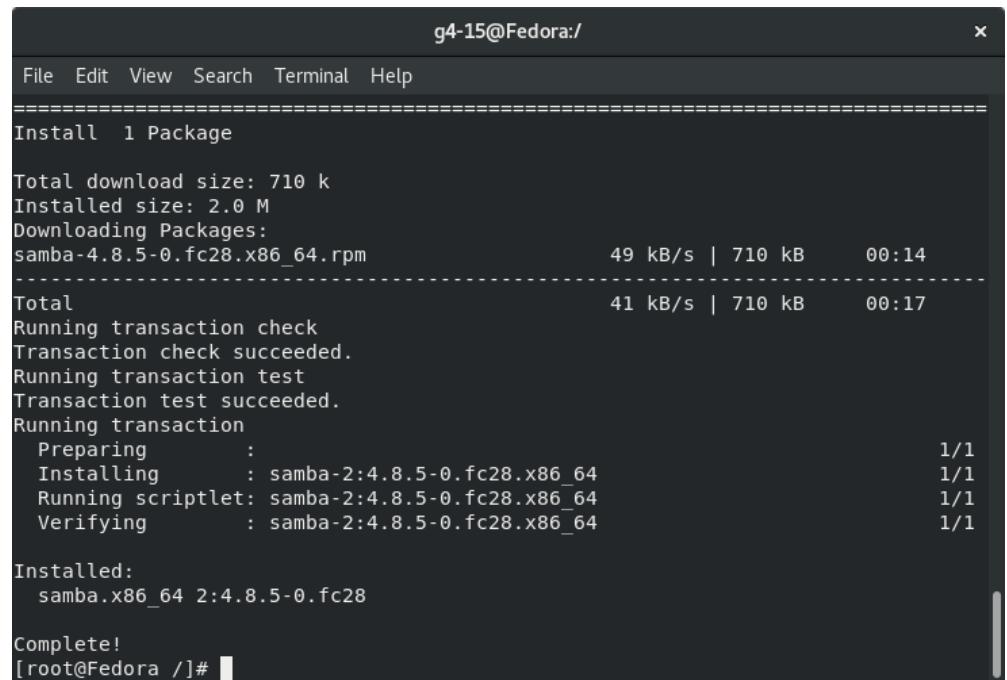


```
g4-15@Fedora:/ 
File Edit View Search Terminal Help
[g4-15@Fedora /]$ su cd root
su: user cd does not exist
[g4-15@Fedora /]$ su -s
su: option requires an argument -- 's'
Try 'su --help' for more information.
[g4-15@Fedora /]$ sudo -s
[sudo] password for g4-15:
[root@Fedora /]# yum install -y samba
Last metadata expiration check: 0:56:07 ago on Wed 10 Oct 2018 11:04:16 AM +08.
Dependencies resolved.
=====
Package           Arch      Version       Repository   Size
=====
Installing:
  samba          x86_64    2:4.8.5-0.fc28     updates      710 k

Transaction Summary
=====
Install 1 Package

Total download size: 710 k
Installed size: 2.0 M
Downloading Packages:
Samba-4.8.5-0.fc28.x8 80% [=====] 87 kB/s | 572 kB      00:01 ETA
```

Figure 94: Samba package installation in Fedora



```
g4-15@Fedora:/ 
File Edit View Search Terminal Help
=====
Install 1 Package

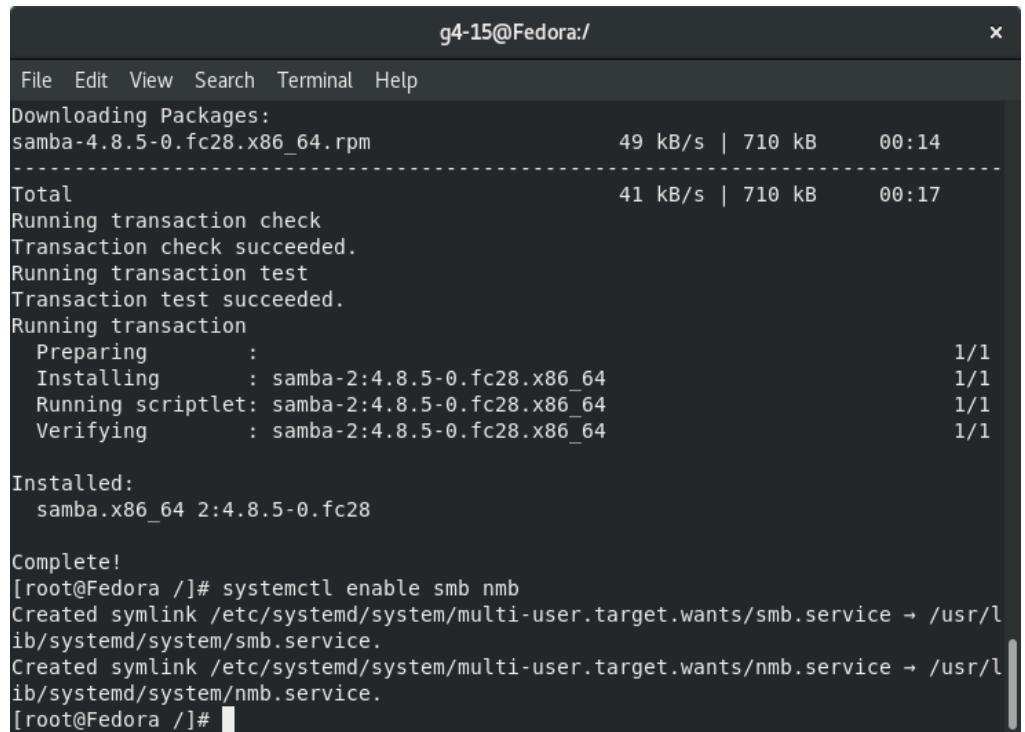
Total download size: 710 k
Installed size: 2.0 M
Downloading Packages:
samba-4.8.5-0.fc28.x86_64.rpm      49 kB/s | 710 kB      00:14
-----
Total                      41 kB/s | 710 kB      00:17
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing          : 1/1
  Installing        : samba-2:4.8.5-0.fc28.x86_64 1/1
  Running scriptlet: samba-2:4.8.5-0.fc28.x86_64 1/1
  Verifying         : samba-2:4.8.5-0.fc28.x86_64 1/1

Installed:
  samba.x86_64 2:4.8.5-0.fc28

Complete!
[root@Fedora /]#
```

Figure 95: Download result

Step 2 : After samba package is already installed, enabled the samba services.



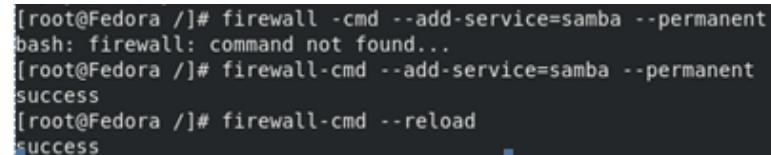
The screenshot shows a terminal window titled "g4-15@Fedora:/". It displays the output of a package manager (likely yum) showing the download and installation of the "samba-4.8.5-0.fc28.x86_64.rpm" package. The package is downloaded at 49 kB/s and installed at 41 kB/s. The transaction check and test both succeed. The service is then enabled with the command "systemctl enable smb nmb". Symlinks are created in /etc/systemd/system/multi-user.target.wants/ for both services.

```
g4-15@Fedora:/
File Edit View Search Terminal Help
Downloading Packages:
samba-4.8.5-0.fc28.x86_64.rpm          49 kB/s | 710 kB   00:14
-----
Total                                         41 kB/s | 710 kB   00:17
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing           : 1/1
Installing         : samba-2:4.8.5-0.fc28.x86_64 1/1
Running scriptlet: samba-2:4.8.5-0.fc28.x86_64 1/1
Verifying          : samba-2:4.8.5-0.fc28.x86_64 1/1
-----
Installed:
  samba.x86_64 2:4.8.5-0.fc28

Complete!
[root@Fedora /]# systemctl enable smb nmb
Created symlink /etc/systemd/system/multi-user.target.wants/smb.service → /usr/lib/systemd/system/smb.service.
Created symlink /etc/systemd/system/multi-user.target.wants/nmb.service → /usr/lib/systemd/system/nmb.service.
[root@Fedora /]#
```

Figure 96: Enabling samba services

Step 3 : Next, open port with using service file of firewall-cmd.

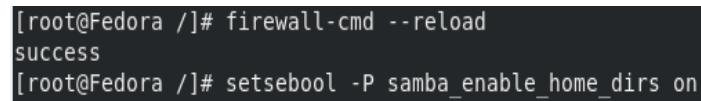


The screenshot shows a terminal window with root privileges. The user attempts to use the command "firewall -cmd --add-service=samba --permanent" but receives an error message stating "bash: firewall: command not found...". The user then successfully uses the command "firewall-cmd --add-service=samba --permanent" followed by "firewall-cmd --reload" to open the port.

```
[root@Fedora /]# firewall -cmd --add-service=samba --permanent
bash: firewall: command not found...
[root@Fedora /]# firewall-cmd --add-service=samba --permanent
success
[root@Fedora /]# firewall-cmd --reload
success
```

Figure 97: Opening port using service file of firewalld-cmd

Step 4 : Then, Enable access to home directory without samba_share_t label.



The screenshot shows a terminal window with root privileges. The user reloads the firewall configuration with "firewall-cmd --reload" and then enables the "samba_enable_home_dirs" boolean with "setsebool -P samba_enable_home_dirs on".

```
[root@Fedora /]# firewall-cmd --reload
success
[root@Fedora /]# setsebool -P samba_enable_home_dirs on
```

Figure 98: Enabling access to home directory

Step 5 : After that, create the new user with a password in Fedora terminal which will be added as samba user. In this case, the user name is **jamsyeiqa** and the password already set as **g4123456@.**

```
[root@Fedora /]# pdbedit -a jamsyeiqa  
new password:  
retype new password:  
Failed to add entry for user jamsyeiqa.  
[root@Fedora /]# pdbedit -a
```

```
[root@Fedora /]# smbpasswd -a jamsyeiqa  
New SMB password:  
Retype new SMB password:  
Added user jamsyeiqa.
```

Figure 99: Creating new user and password in Fedora

Step 6 : The Samba in Fedora provides home directory for each user by default. A <username> added by pdbedit can access to /home/<username>. Open and edit the configuration file into **smb.conf** which is can edit smb.conf file and create a share directory.

```
[root@Fedora /]# diff -uprN /etc/smbsa/smb.conf{.org,}  
diff: /etc/smbsa/smb.conf.org: No such file or directory  
diff: /etc/smbsa/smb.conf: No such file or directory  
[root@Fedora /]# nano /etc/smbsa/smb.conf{.org,}  
[root@Fedora /]# nano /etc/smbsa/smb.conf  
[root@Fedora /]# nano /etc/samba/smb.conf
```

Figure 100: Home directory for each user by default

```
[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  
writable = yes  
  
[jamsyeiqa]  
comment = Jamsyeiqa's file  
path = /var/lib/jamsyeiqa  
read only = no  
guest only = no  
writable = yes
```

Figure 101: Editing configuration file

Step 7 : Share the permission 0777 directory with multiple user added by pdbedit. Change **/var/lib/share**'s permission to 0777. Change the file permission to ensure that the file shared could be read, modified and executed by anyone who has access to the file. Then, add samba_share_t label to **/var/lib/share**.

```
[root@Fedora /]# mkdir /var/lib/share  
[root@Fedora /]# chmod 0777 /var/lib/share  
[root@Fedora /]# chcon -R -t samba_share_t /var/lib/share  
[root@Fedora /]#
```

Figure 102: Permission sharing

Step 8 : Lastly, go to **/var/lib/share** folder which is the location of file Samba that already configured in Fedora terminal. Admin can add, edit, delete the file and the user can view the file that already shared by entering username and password.

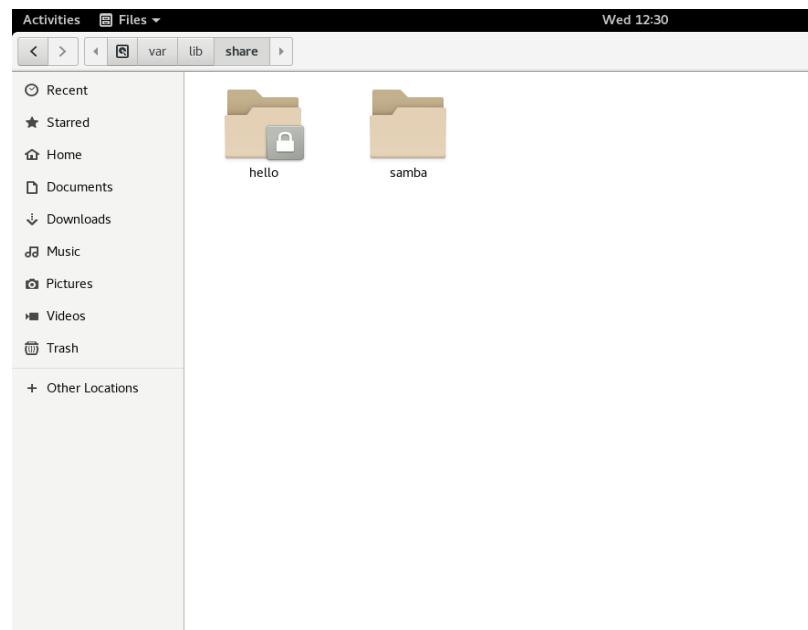
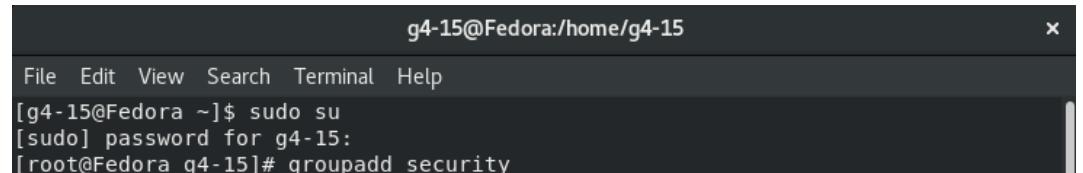


Figure 103: Samba file location

5.3.10 Samba Security Services

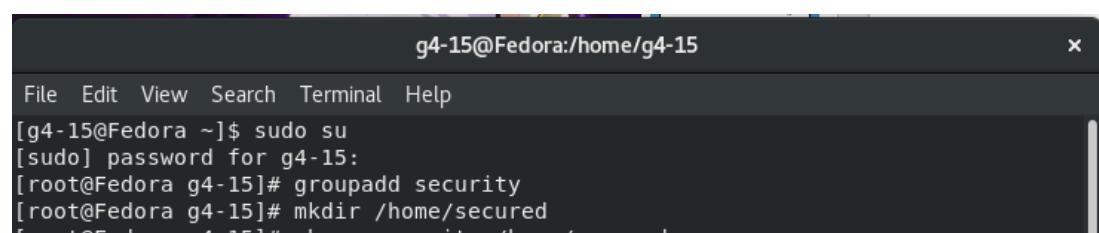
Step 1 : Create a new group which name “security” by type this command “groupadd security” on the terminal.



```
g4-15@Fedora:/home/g4-15
File Edit View Search Terminal Help
[g4-15@Fedora ~]$ sudo su
[sudo] password for g4-15:
[root@Fedora g4-15]# groupadd security
```

Figure 134: Creating new group

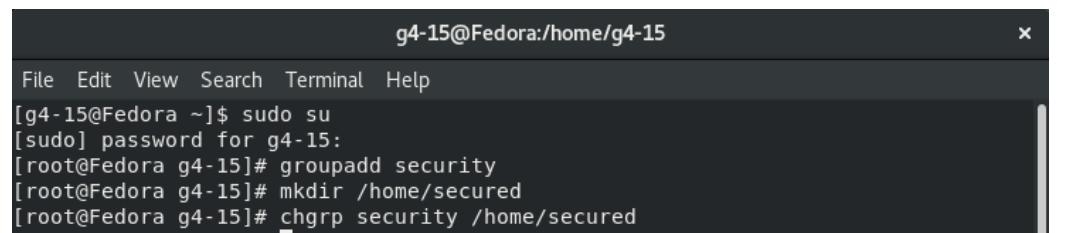
Step 2 : Create a new directory for file sharing by enter this command “mkdir /home/secured”.



```
g4-15@Fedora:/home/g4-15
File Edit View Search Terminal Help
[g4-15@Fedora ~]$ sudo su
[sudo] password for g4-15:
[root@Fedora g4-15]# groupadd security
[root@Fedora g4-15]# mkdir /home/secured
```

Figure 105: Creating new directory

Step 3 : Operate security on the directory that has been created on folder/home/security/ by type command “chgrp security /home/secured”.



```
g4-15@Fedora:/home/g4-15
File Edit View Search Terminal Help
[g4-15@Fedora ~]$ sudo su
[sudo] password for g4-15:
[root@Fedora g4-15]# groupadd security
[root@Fedora g4-15]# mkdir /home/secured
[root@Fedora g4-15]# chgrp security /home/secured
```

Figure 106: Operating security on the directory

Step 4 Set the option permissions file/directory on /home/secured by type this command “chmod –R 770 /home/secured”.

```
g4-15@Fedora:/home/g4-15
File Edit View Search Terminal Help
[g4-15@Fedora ~]$ sudo su
[sudo] password for g4-15:
[root@Fedora g4-15]# groupadd security
[root@Fedora g4-15]# mkdir /home/secured
[root@Fedora g4-15]# chgrp security /home/secured
[root@Fedora g4-15]# chmod -R 770 /home/secured
```

Figure 107: Setting the permission file

Step 5 : Open samba config by typing sudo nano/etc/samba/smb.conf and add the [SecureFolder] section. Specify host ip that is allowed to access the file in ‘host allow’ and enter the host that is denied from accessing the file in ‘host deny’. Also, specify the path for the file.

```
g4-15@Fedora:/home/share
File Edit View Search Terminal Help
GNU nano 2.9.8 /etc/samba/smb.conf

valid users = %S, %D%w%S
browseable = No
read only = No
inherit acls = Yes

[Group4]
comment = File sharing to public users
path = /home/share
writable = yes
guest ok = yes
guest only = yes
create mode = 0777
directory mode = 0777

#[securityfolder]
#path = /home/secured
#writable = yes
#create mode = 0770
#directory mode = 0770
#guest ok = no
#read only = no
#valid users = @security

[SecureFolder]
comment = file sharing to specific host
path = /home/ClientFolder
host allow = 192.168.50. localhost
hosts deny = 0.0.0./0
writable = yes
guest ok = yes
```

Figure 108: Specify host allowed and host denied.

Step 6 : Start samba service by type this command “systemctl start smb nmb” and enable the samba service by type this command “systemctl enable smb nmb”.

```
[root@Fedora g4-15]# systemctl start smb nmb  
[root@Fedora g4-15]# systemctl enable smb nmb
```

Figure 14: Starting samba service

Step 7 : Add a user authentication which is username and password in Samba by type this command “useradd pelajar” for add user and “smbpasswd – pelajar” to add password to user.

```
[root@Fedora g4-15]# useradd pelajar  
[root@Fedora g4-15]# smbpasswd -a pelajar  
New SMB password:  
Retype new SMB password:  
Added user pelajar.
```

Figure 110: Adding user authentication

Step 8 : New list of supplementary groups by type this command “usermod – G security pelajar” to make user which is pelajar will follow rule security in configuration file.

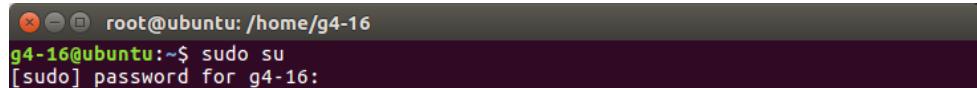
```
[root@Fedora g4-15]# usermod -G security pelajar
```

Figure 111: Usermod of Security pelajar

5.3.11 Network Management System (NMS)

Installing Zabbix- Server

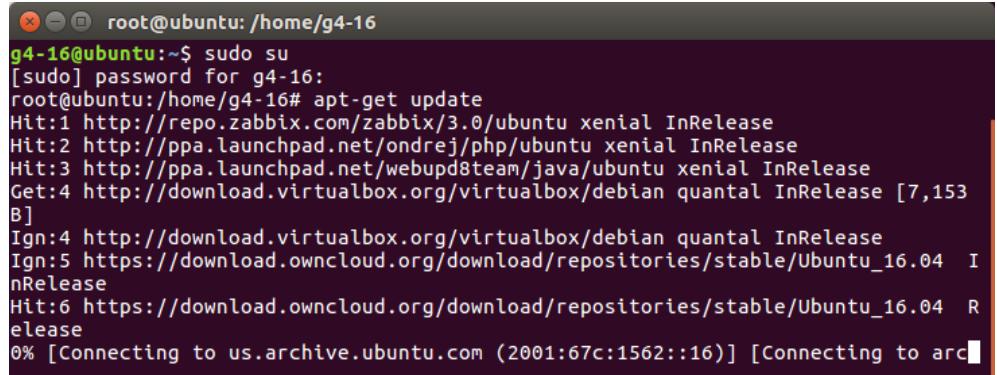
Step 1 : Login with root.



```
root@ubuntu:/home/g4-16
g4-16@ubuntu:~$ sudo su
[sudo] password for g4-16:
```

Figure 15: Root login

Step 2 : Before install Zabbix, we need to install a few PHP modules that Zabbix needs. First, update the system's list of available packages by running the following command:



```
root@ubuntu:/home/g4-16
g4-16@ubuntu:~$ sudo su
[sudo] password for g4-16:
root@ubuntu:/home/g4-16# apt-get update
Hit:1 http://repo.zabbix.com/zabbix/3.0/ubuntu xenial InRelease
Hit:2 http://ppa.launchpad.net/ondrej/php/ubuntu xenial InRelease
Hit:3 http://ppa.launchpad.net/webupd8team/java/ubuntu xenial InRelease
Get:4 http://download.virtualbox.org/virtualbox/debian quantal InRelease [7,153
B]
Ign:4 http://download.virtualbox.org/virtualbox/debian quantal InRelease
Ign:5 https://download.owncloud.org/download/repositories/stable/Ubuntu_16.04_I
nRelease
Hit:6 https://download.owncloud.org/download/repositories/stable/Ubuntu_16.04_R
elease
0% [Connecting to us.archive.ubuntu.com (2001:67c:1562::16)] [Connecting to arc...
```

Figure 113: Updating the system

Step 3 : Install the Lamp server

Step 4 : Zabbix is available in Ubuntu's package manager, but it's outdated, so we'll use the official Zabbix repository to install the latest stable version. Download and install the repository configuration package:

```

root@ubuntu:/home/g4-16# wget http://repo.zabbix.com/zabbix/3.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_3.0-1+xenial_all.deb
--2018-10-25 17:13:27--  http://repo.zabbix.com/zabbix/3.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_3.0-1+xenial_all.deb
Resolving repo.zabbix.com (repo.zabbix.com)... 162.243.159.138
Connecting to repo.zabbix.com (repo.zabbix.com)|162.243.159.138|:80... connected
.
HTTP request sent, awaiting response... 200 OK
Length: 3842 (3.8K) [application/octet-stream]
Saving to: 'zabbix-release_3.0-1+xenial_all.deb.1'

zabbix-release_3.0- 100%[=====] 3.75K ---KB/s   in 0s

2018-10-25 17:13:28 (236 MB/s) - 'zabbix-release_3.0-1+xenial_all.deb.1' saved [3842/3842]

root@ubuntu:/home/g4-16# 

root@ubuntu:/home/g4-16# dpkg -i zabbix-release_3.0-1+xenial_all.deb
(Reading database ... 251499 files and directories currently installed.)
Preparing to unpack zabbix-release_3.0-1+xenial_all.deb ...
Unpacking zabbix-release (3.0-1+xenial) over (3.0-1+xenial) ...
Setting up zabbix-release (3.0-1+xenial) ...
root@ubuntu:/home/g4-16# 

```

Figure 114: Installing the update

Step 5 : Update the package index so the new repository is included:

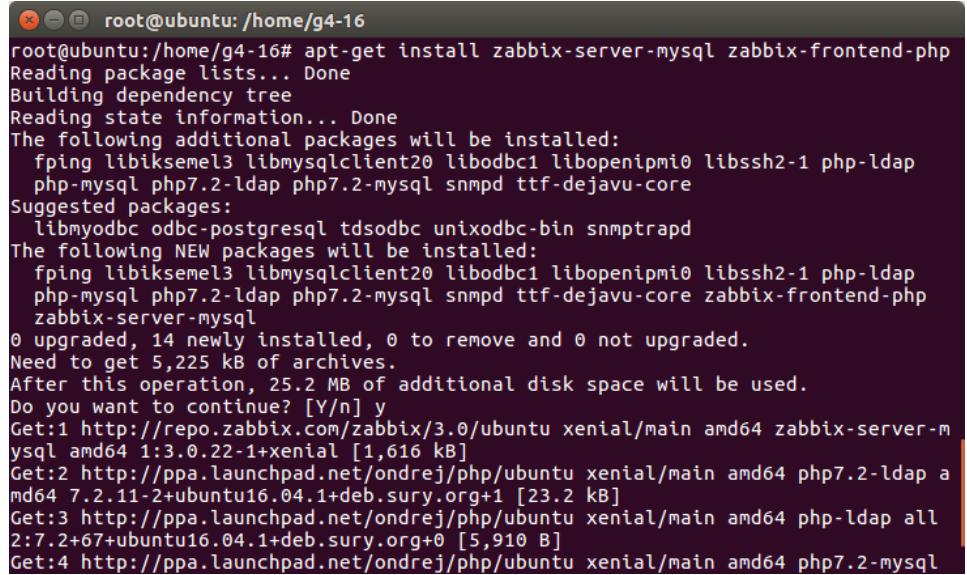
```

root@ubuntu:/home/g4-16# apt-get update
Hit:1 http://repo.zabbix.com/zabbix/3.0/ubuntu xenial InRelease
Hit:2 http://ppa.launchpad.net/ondrej/php/ubuntu xenial InRelease
Hit:3 http://ppa.launchpad.net/webupd8team/java/ubuntu xenial InRelease
Get:4 http://download.virtualbox.org/virtualbox/debian quantal InRelease [7,153
B]
Ign:4 http://download.virtualbox.org/virtualbox/debian quantal InRelease
Ign:5 https://download.owncloud.org/download/repositories/stable/Ubuntu_16.04 I
nRelease
Hit:6 https://download.owncloud.org/download/repositories/stable/Ubuntu_16.04 R
elease
Ign:8 http://debian.opennms.org stable InRelease
Ign:9 http://debian.OpenNMS.org stable InRelease
Hit:10 http://debian.opennms.org stable Release
Hit:11 http://debian.OpenNMS.org stable Release
0% [Connecting to us.archive.ubuntu.com (91.189.91.23)] [Connecting to archive.]

```

Figure 115: Updating the package index

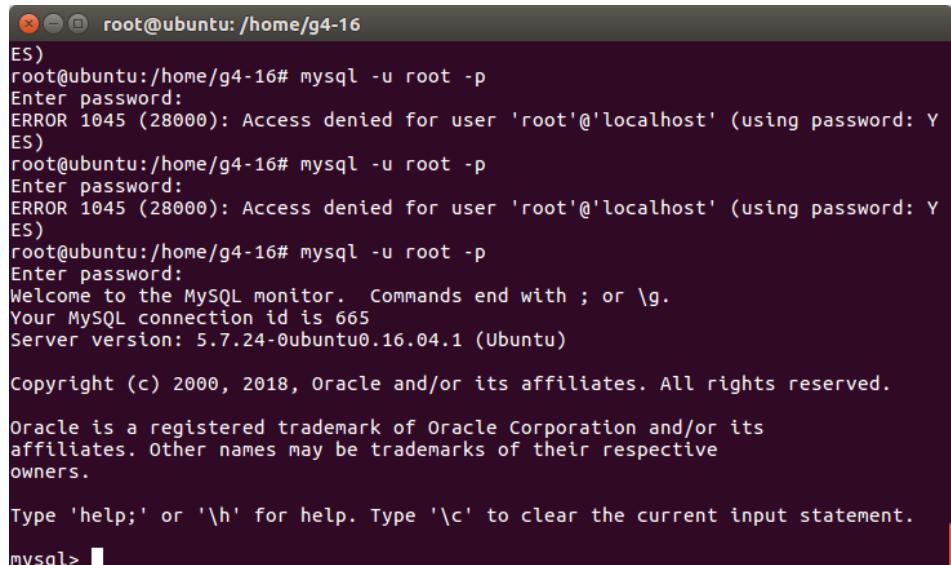
Step 6 Then install the Zabbix server and web frontend with MySQL database support:



```
root@ubuntu:/home/g4-16# apt-get install zabbix-server-mysql zabbix-frontend-php
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  fping libiksemel3 libmysqlclient20 libodbc1 libopenipmi0 libssh2-1 php-ldap
  php-mysql php7.2-ldap php7.2-mysql snmpd ttf-dejavu-core
Suggested packages:
  libmyodbc odbc-postgresql tdsodbc unixodbc-bin snmptrapd
The following NEW packages will be installed:
  fping libiksemel3 libmysqlclient20 libodbc1 libopenipmi0 libssh2-1 php-ldap
  php-mysql php7.2-ldap php7.2-mysql snmpd ttf-dejavu-core zabbix-frontend-php
  zabbix-server-mysql
0 upgraded, 14 newly installed, 0 to remove and 0 not upgraded.
Need to get 5,225 kB of archives.
After this operation, 25.2 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://repo.zabbix.com/zabbix/3.0/ubuntu xenial/main amd64 zabbix-server-mysql amd64 1:3.0.22-1+xenial [1,616 kB]
Get:2 http://ppa.launchpad.net/ondrej/php/ubuntu xenial/main amd64 php7.2-ldap all 7.2.11-2+ubuntu16.04.1+deb.sury.org+1 [23.2 kB]
Get:3 http://ppa.launchpad.net/ondrej/php/ubuntu xenial/main amd64 php-ldap all 2:7.2+67+ubuntu16.04.1+deb.sury.org+0 [5,910 B]
Get:4 http://ppa.launchpad.net/ondrej/php/ubuntu xenial/main amd64 php7.2-mysql
```

Figure 116: Installing Zabbix server

Step 7 : We need to create a new MySQL database and populate it with some basic information in order to make it suitable for Zabbix. We'll also create a specific user for this database so Zabbix isn't logging into MySQL with the root account. Log into MySQL as the root user using the root password that you set up during the MySQL server installation:



```
root@ubuntu:/home/g4-16#
ES)
root@ubuntu:/home/g4-16# mysql -u root -p
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: Y
ES)
root@ubuntu:/home/g4-16# mysql -u root -p
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: Y
ES)
root@ubuntu:/home/g4-16# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 665
Server version: 5.7.24-0ubuntu0.16.04.1 (Ubuntu)

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

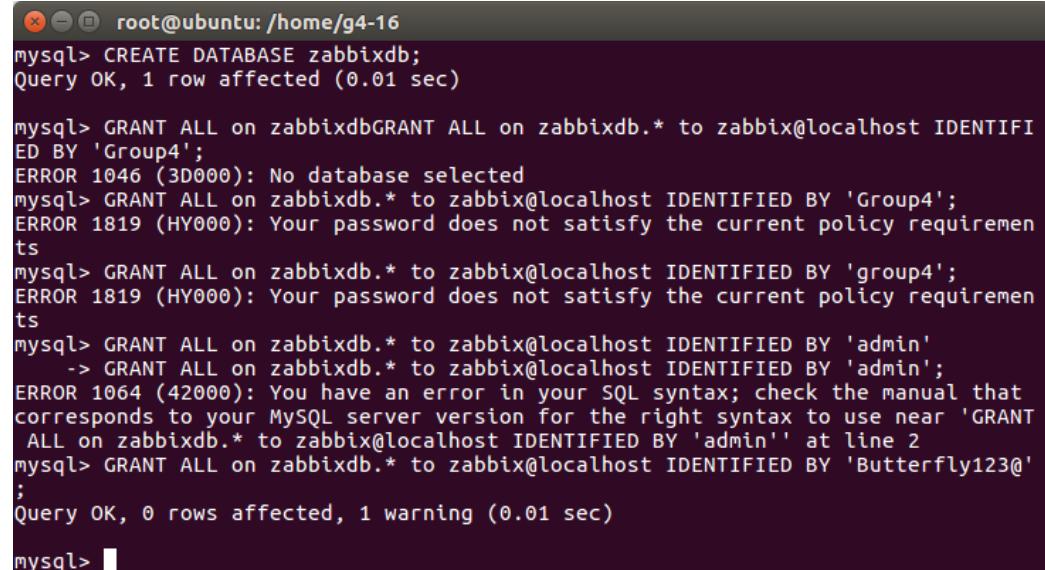
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> 
```

Figure 117: Creating new MySQL database

Step 8 : CREATE DATABASE zabbixdb;. Then create a user that the Zabbix server will give it access to the new database and set the password for the user: Then apply these new permissions. That takes care of the user and the database. Exit out of the database console.



```
root@ubuntu:/home/g4-16
mysql> CREATE DATABASE zabbixdb;
Query OK, 1 row affected (0.01 sec)

mysql> GRANT ALL on zabbixdb.* to zabbix@localhost IDENTIFIED BY 'Group4';
ERROR 1046 (3D000): No database selected
mysql> GRANT ALL on zabbixdb.* to zabbix@localhost IDENTIFIED BY 'Group4';
ERROR 1819 (HY000): Your password does not satisfy the current policy requirements
mysql> GRANT ALL on zabbixdb.* to zabbix@localhost IDENTIFIED BY 'group4';
ERROR 1819 (HY000): Your password does not satisfy the current policy requirements
mysql> GRANT ALL on zabbixdb.* to zabbix@localhost IDENTIFIED BY 'admin'
-> GRANT ALL on zabbixdb.* to zabbix@localhost IDENTIFIED BY 'admin';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'GRANT ALL on zabbixdb.* to zabbix@localhost IDENTIFIED BY 'admin'' at line 2
mysql> GRANT ALL on zabbixdb.* to zabbix@localhost IDENTIFIED BY 'Butterfly123@'
;
Query OK, 0 rows affected, 1 warning (0.01 sec)

mysql>
```

Figure 118: Creating database zabbixdb

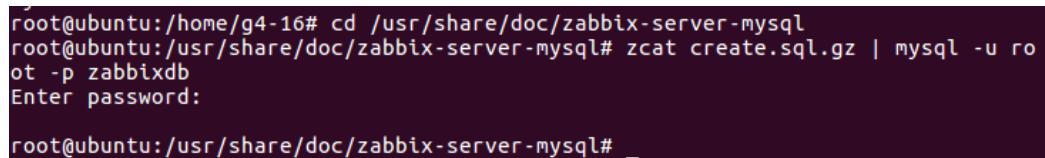


```
mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)

mysql>
```

Figure 119: Continuing creating database zabbixdb

Step 9 : Next we have to import the initial schema and data. The Zabbix installation provided us with a file that sets this up for us. Run the following command to set up the schema and import the data into the zabbixdatabase. We'll use zcat since the data in the file is compressed.



```
root@ubuntu:/home/g4-16# cd /usr/share/doc/zabbix-server-mysql
root@ubuntu:/usr/share/doc/zabbix-server-mysql# zcat create.sql.gz | mysql -u root -p zabbixdb
Enter password:

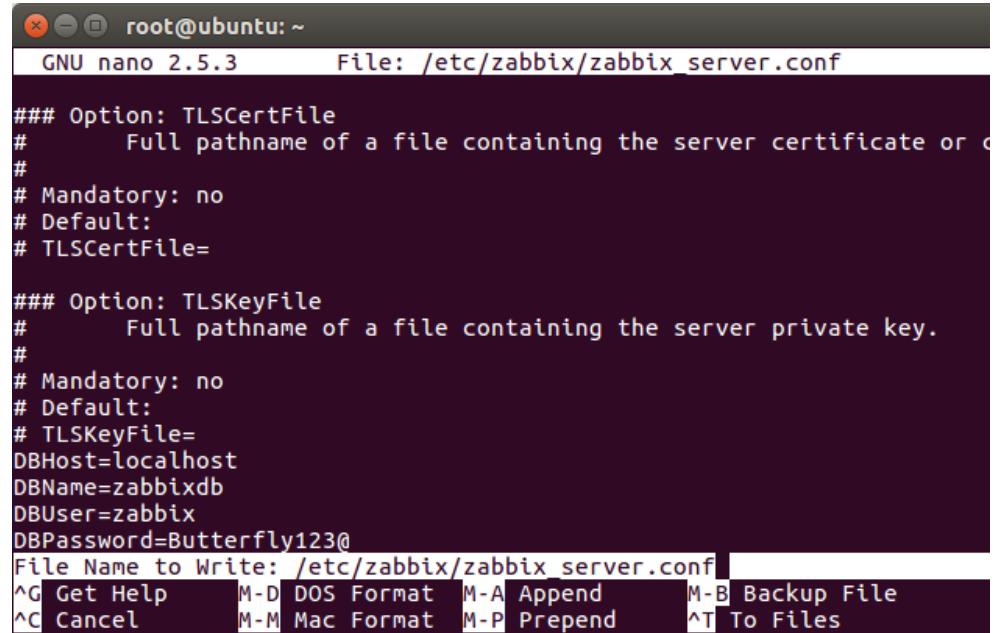
root@ubuntu:/usr/share/doc/zabbix-server-mysql#
```

Figure 120: Importing the initial schema and data

Step 10 : In order for the Zabbix server to use this database, you need to set the database password in the Zabbix server configuration file. Open the configuration file in your editor by running the following command:

```
#sudo nano /etc/zabbix/zabbix-server.conf
```

Step 11 : Change the following lines:



```
root@ubuntu: ~
GNU nano 2.5.3      File: /etc/zabbix/zabbix_server.conf

### Option: TLSCertFile
#       Full pathname of a file containing the server certificate or c
#
# Mandatory: no
# Default:
# TLSCertFile=

### Option: TLSKeyFile
#       Full pathname of a file containing the server private key.
#
# Mandatory: no
# Default:
# TLSKeyFile=
DBHost=localhost
DBName=zabbixdb
DBUser=zabbix
DBPassword=Butterfly123@

File Name to Write: /etc/zabbix/zabbix_server.conf
^G Get Help      M-D DOS Format  M-A Append      M-B Backup File
^C Cancel        M-M Mac Format   M-P Prepend    ^T To Files
```

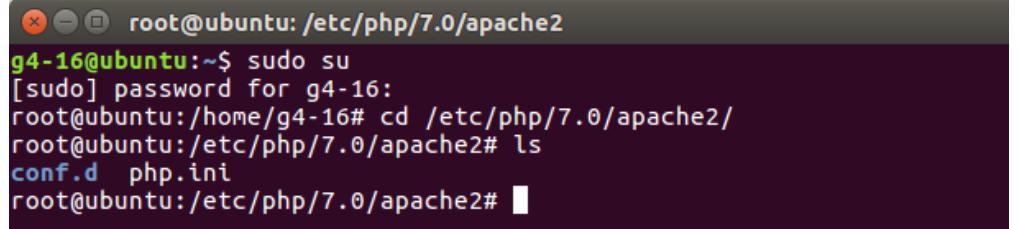
Figure 121: Configuring zabbix-server

Step 12 : Finally, start Apache server and Zabbix server and enable them to start on boot time:

```
root@ubuntu:~# service apache2 restart
root@ubuntu:~# service zabbix-server restart
root@ubuntu:~#
```

Figure 122: Start Apache server

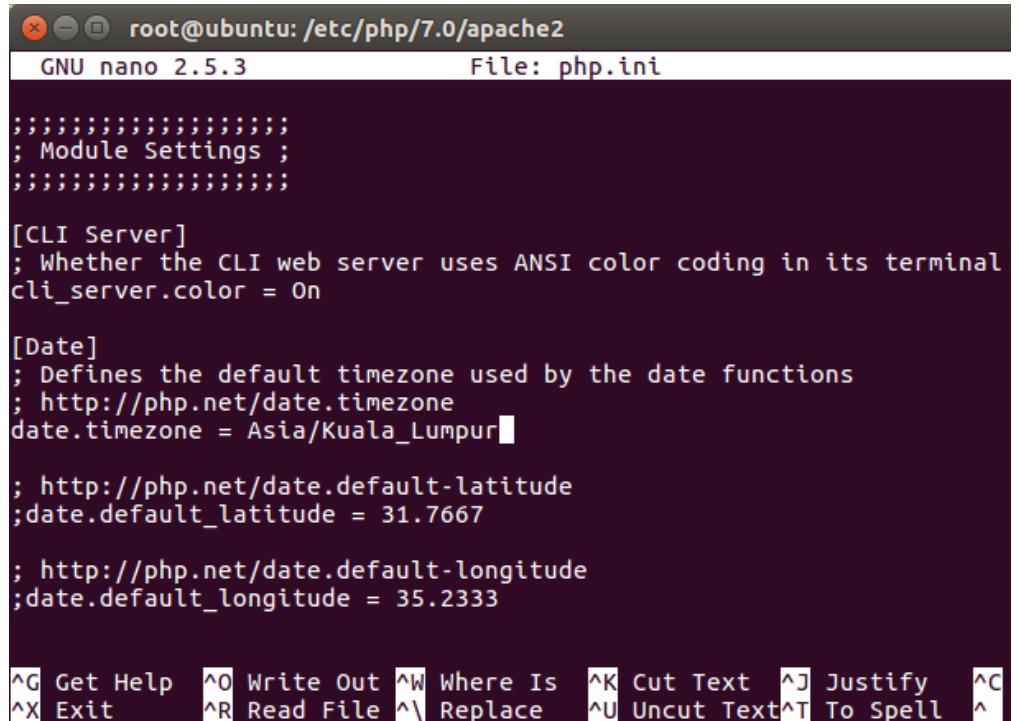
Step 13 The Zabbix installation process created an Apache configuration file that contains these settings. It is located in the directory /etc/php and is loaded automatically by Apache. We need to make a small change to this file, so open it up.



```
root@ubuntu:/etc/php/7.0/apache2
g4-16@ubuntu:~$ sudo su
[sudo] password for g4-16:
root@ubuntu:/home/g4-16# cd /etc/php/7.0/apache2/
root@ubuntu:/etc/php/7.0/apache2# ls
conf.d  php.ini
root@ubuntu:/etc/php/7.0/apache2#
```

Figure 123: Zabbix installation process created

Step 14 : Replace the following line as per your Time zone.



```
root@ubuntu:/etc/php/7.0/apache2
GNU nano 2.5.3          File: php.ini

;;;;;;
; Module Settings ;
;;;;;;

[CLI Server]
; Whether the CLI web server uses ANSI color coding in its terminal
cli_server.color = On

[Date]
; Defines the default timezone used by the date functions
; http://php.net/date.timezone
date.timezone = Asia/Kuala_Lumpur

; http://php.net/date.default-latitude
;date.default_latitude = 31.7667

; http://php.net/date.default-longitude
;date.default_longitude = 35.2333

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

Figure 124: Replacing time zone

Step 15 : Then install the PHP modules Zabbix needs:

```
root@ubuntu:/etc/php/7.0/apache2# apt-get install php7.0-xml
Reading package lists... Done
Building dependency tree
Reading state information... Done
php7.0-xml is already the newest version (7.0.32-2+ubuntu16.04.1+deb.sury.org+1)
.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Figure 125: Install PHP modules that Zabbix needs

```
root@ubuntu:~# apt-get install php7.0-bcmath
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  php7.0-bcmath
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 15.7 kB of archives.
After this operation, 65.5 kB of additional disk space will be used.
Get:1 http://ppa.launchpad.net/ondrej/php/ubuntu xenial/main amd64 php7.0-bcmath
  amd64 7.0.32-2+ubuntu16.04.1+deb.sury.org+1 [15.7 kB]
Fetched 15.7 kB in 0s (21.1 kB/s)
Selecting previously unselected package php7.0-bcmath.
(Reading database ... 252482 files and directories currently installed.)
Preparing to unpack .../php7.0-bcmath_7.0.32-2+ubuntu16.04.1+deb.sury.org+1_amd6
4.deb ...
Unpacking php7.0-bcmath (7.0.32-2+ubuntu16.04.1+deb.sury.org+1) ...
Processing triggers for libapache2-mod-php7.0 (7.0.32-2+ubuntu16.04.1+deb.sury.o
rg+1) ...
Setting up php7.0-bcmath (7.0.32-2+ubuntu16.04.1+deb.sury.org+1) ...

Creating config file /etc/php/7.0/mods-available/bcmath.ini with new version
Processing triggers for libapache2-mod-php7.0 (7.0.32-2+ubuntu16.04.1+deb.sury.o
rg+1) ...

root@ubuntu:~# apt-get install php7.0-mbstring
Reading package lists... Done
Building dependency tree
Reading state information... Done
php7.0-mbstring is already the newest version (7.0.32-2+ubuntu16.04.1+deb.sury.o
rg+1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@ubuntu:~#
```

Figure 126: Continuing to install

Step 16 : Your Zabbix server is now set up and connected to the database. It's time to access the Zabbix web installation wizard. Start Zabbix Server Web Installer. Then, click next step button.

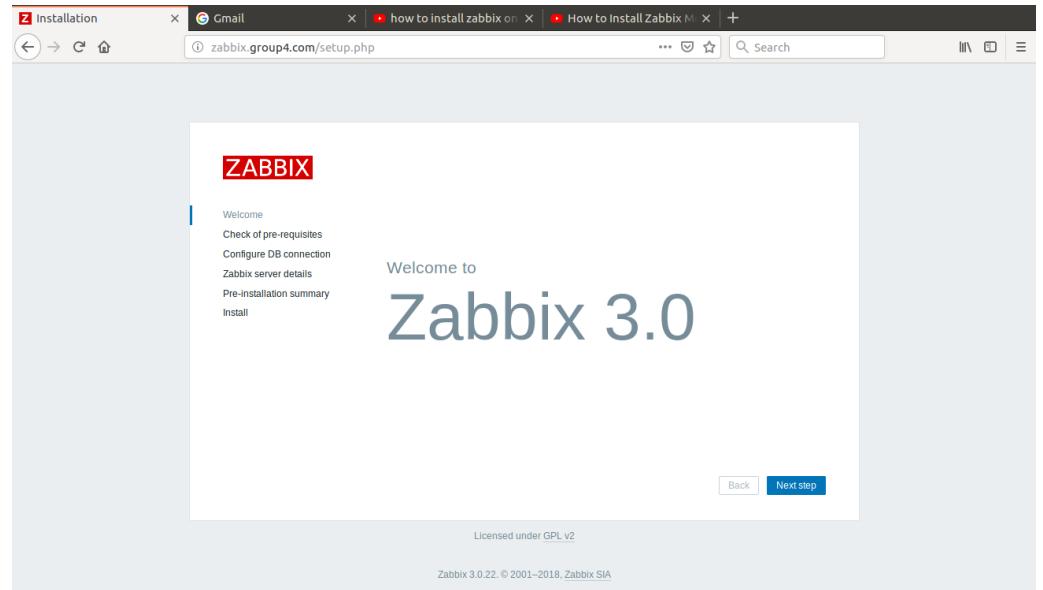


Figure 127: Zabbix Server Web Installer

Step 17 : Make sure all the values are OK. Once you have done. Click on the **Next step** button. You should see the Zabbix database configuration screen:

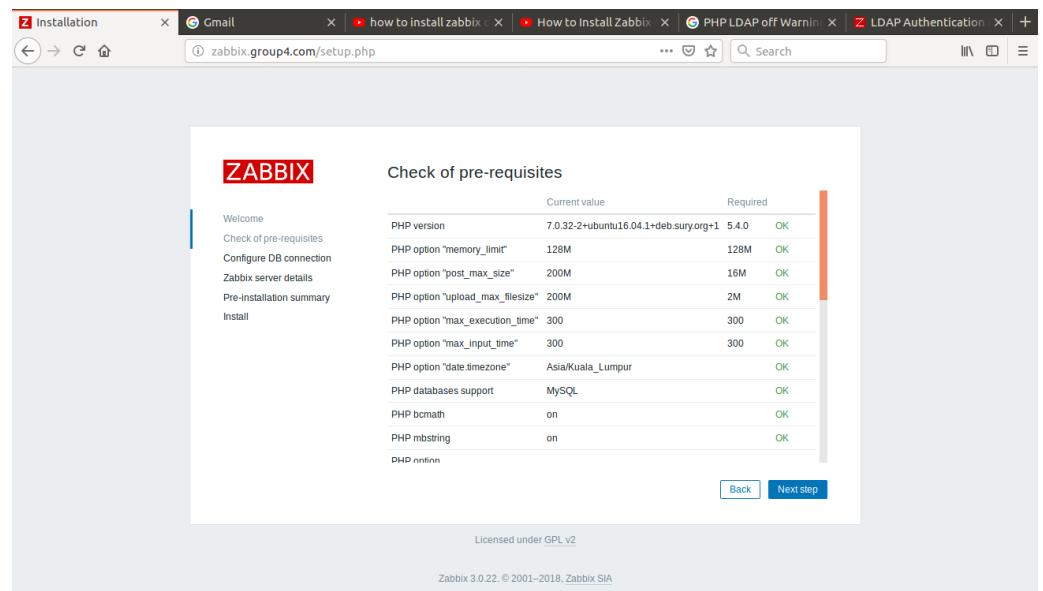


Figure 128: Zabbix database configuration screen

Step 18 : Here, update all the details like, Database name, Database username and the password then, click on the **Next step** button. You should see the following screen:

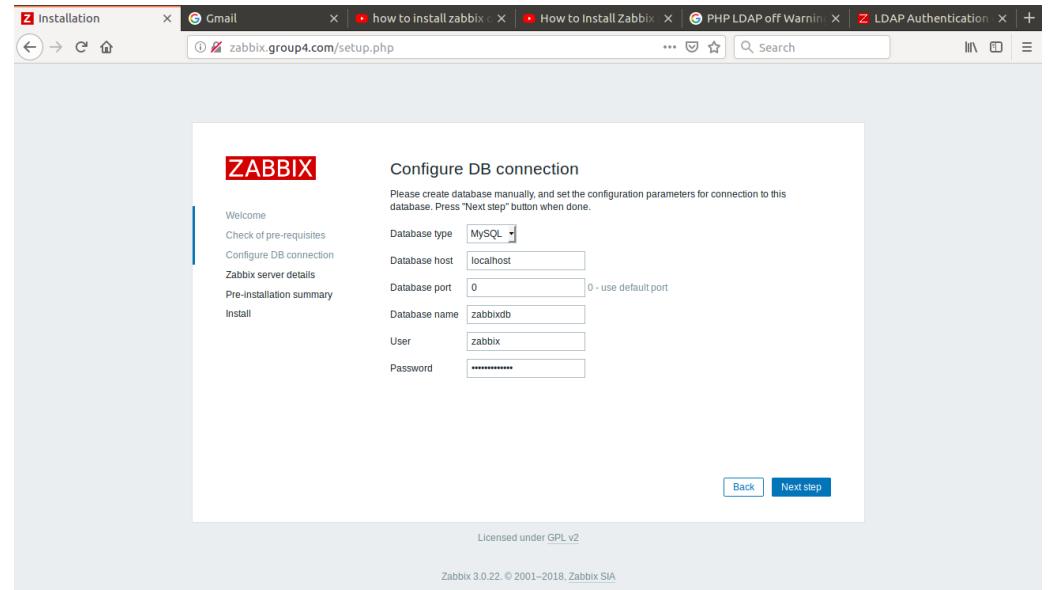


Figure 129: Configuration Zabbix DB connection

Step 19 : Here, provide hostname or IP address and port number of the zabbix server and click on the **Next step**. You should see the following page.

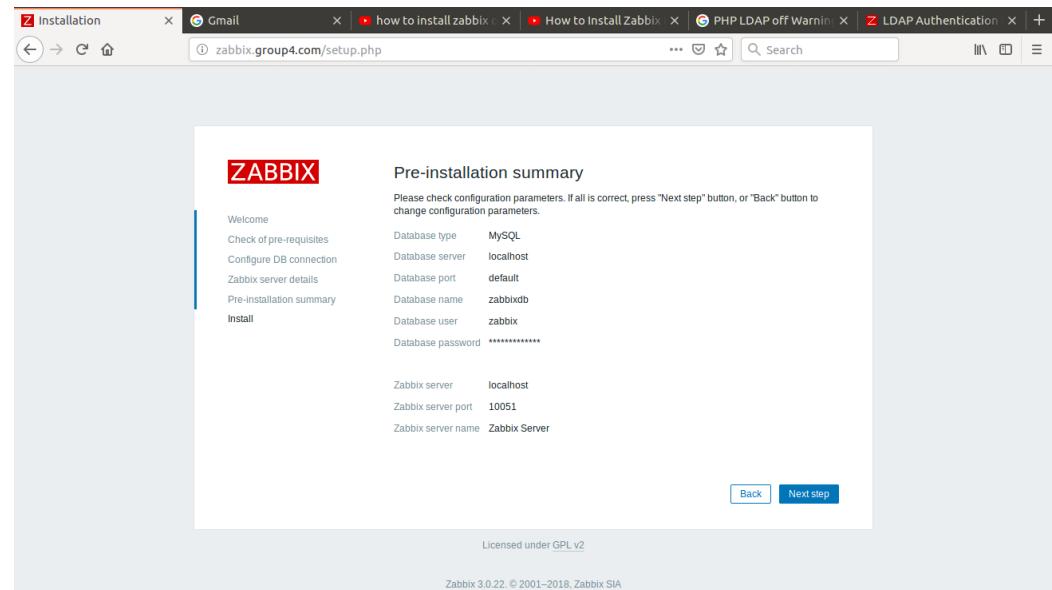


Figure 130: Summary of Pre-Installation

Step 20 : Verify the pre-installation summary then, click on the **Next step** button to start the installation. Once the installation is finished, you should see the following page:

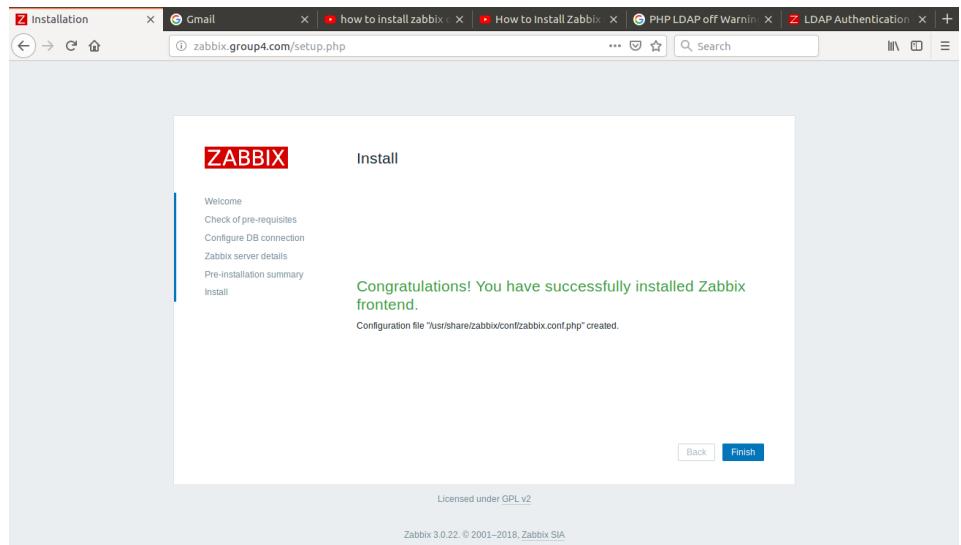


Figure 131: Pre-Installation summary to verify

Install Zabbix Agent on Ubuntu

Step 1 : Login with root. Then, just like on the Zabbix server, run the following commands to install the repository configuration package:

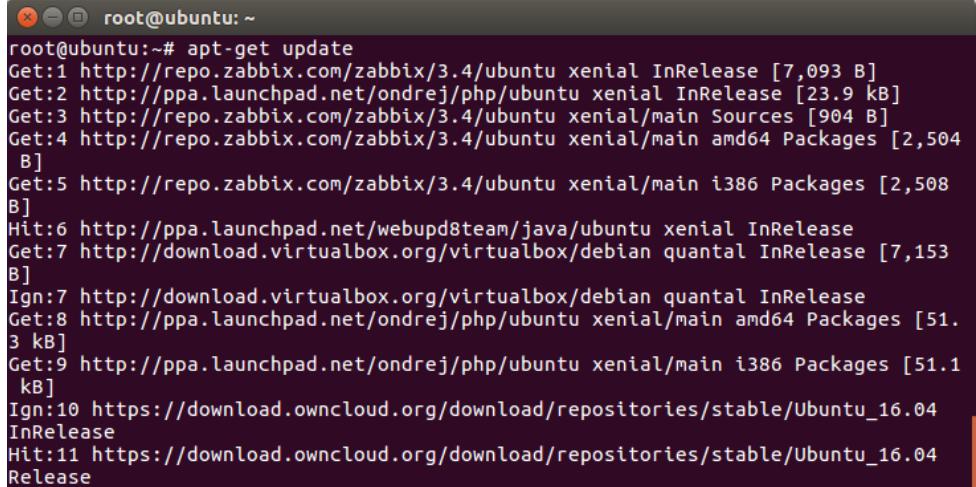
```
root@ubuntu:/etc/php/7.0/apache2# cd
root@ubuntu:~# wget http://repo.zabbix.com/zabbix/3.4/ubuntu/pool/main/z/zabbix-release/zabbix-release_3.4-1+xenial_all.deb
--2018-10-26 16:16:47-- http://repo.zabbix.com/zabbix/3.4/ubuntu/pool/main/z/zabbix-release/zabbix-release_3.4-1+xenial_all.deb
Resolving repo.zabbix.com (repo.zabbix.com)... 162.243.159.138
Connecting to repo.zabbix.com (repo.zabbix.com)|162.243.159.138|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3884 (3.8K) [application/octet-stream]
Saving to: 'zabbix-release_3.4-1+xenial_all.deb'

zabbix-release_3.4- 100%[=====] 3.79K --KB/s in 0s
2018-10-26 16:16:48 (162 MB/s) - 'zabbix-release_3.4-1+xenial_all.deb' saved [3884/3884]

root@ubuntu:~#
```

Figure 132: Installation of repository configuration package

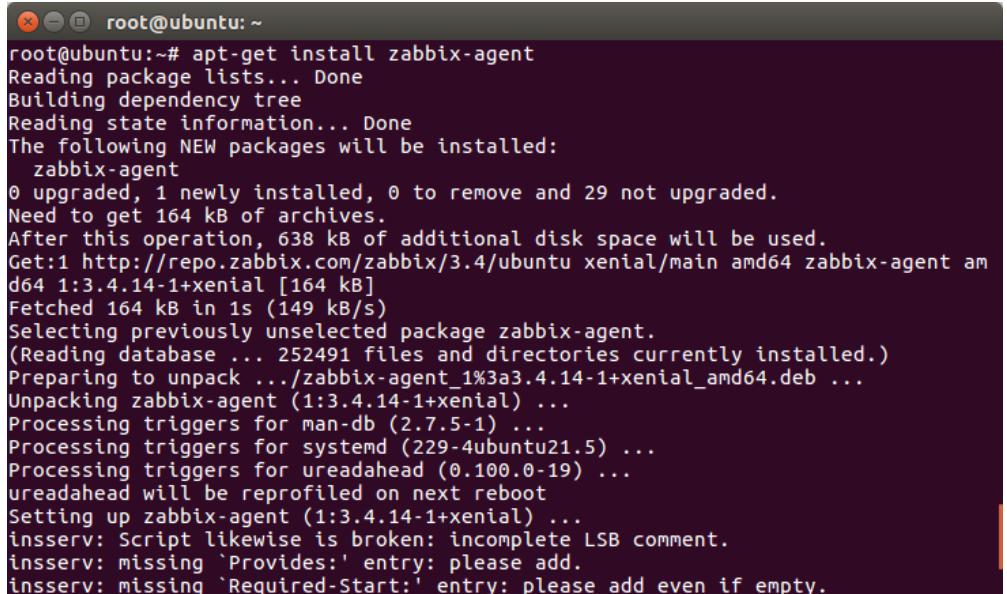
Step 2 Next, update the package index:



```
root@ubuntu:~# apt-get update
Get:1 http://repo.zabbix.com/zabbix/3.4/ubuntu xenial InRelease [7,093 B]
Get:2 http://ppa.launchpad.net/ondrej/php/ubuntu xenial InRelease [23.9 kB]
Get:3 http://repo.zabbix.com/zabbix/3.4/ubuntu xenial/main Sources [904 B]
Get:4 http://repo.zabbix.com/zabbix/3.4/ubuntu xenial/main amd64 Packages [2,504 B]
Get:5 http://repo.zabbix.com/zabbix/3.4/ubuntu xenial/main i386 Packages [2,508 B]
Hit:6 http://ppa.launchpad.net/webupd8team/java/ubuntu xenial InRelease
Get:7 http://download.virtualbox.org/virtualbox/debian quantal InRelease [7,153 B]
Ign:7 http://download.virtualbox.org/virtualbox/debian quantal InRelease
Get:8 http://ppa.launchpad.net/ondrej/php/ubuntu xenial/main amd64 Packages [51.3 kB]
Get:9 http://ppa.launchpad.net/ondrej/php/ubuntu xenial/main i386 Packages [51.1 kB]
Ign:10 https://download.owncloud.org/download/repositories/stable/Ubuntu_16.04 InRelease
Hit:11 https://download.owncloud.org/download/repositories/stable/Ubuntu_16.04 Release
```

Figure 133: Updating package index

Step 3 : Then install the Zabbix agent:



```
root@ubuntu:~# apt-get install zabbix-agent
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  zabbix-agent
0 upgraded, 1 newly installed, 0 to remove and 29 not upgraded.
Need to get 164 kB of archives.
After this operation, 638 kB of additional disk space will be used.
Get:1 http://repo.zabbix.com/zabbix/3.4/ubuntu xenial/main amd64 zabbix-agent amd64 1:3.4.14-1+xenial [164 kB]
Fetched 164 kB in 1s (149 kB/s)
Selecting previously unselected package zabbix-agent.
(Reading database ... 252491 files and directories currently installed.)
Preparing to unpack .../zabbix-agent_1%3a3.4.14-1+xenial_amd64.deb ...
Unpacking zabbix-agent (1:3.4.14-1+xenial) ...
Processing triggers for man-db (2.7.5-1) ...
Processing triggers for systemd (229-4ubuntu21.5) ...
Processing triggers for ureadahead (0.100.0-19) ...
ureadahead will be reprofiled on next reboot
Setting up zabbix-agent (1:3.4.14-1+xenial) ...
insserv: Script likewise is broken: incomplete LSB comment.
insserv: missing `Provides:' entry: please add.
insserv: missing `Required-Start:' entry: please add even if empty.
```

Figure 134: Zabbix agent installation

Step 4 : After installation of Zabbix agent. Edit Zabbix agent configuration file /etc/zabbix/zabbix_agentd.conf and update Zabbix server IP.

```

root@ubuntu: ~
GNU nano 2.5.3      File: /etc/zabbix/zabbix_agentd.conf      Modified
#       Example: Server=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.domain
#
# Mandatory: yes, if StartAgents is not explicitly set to 0
# Default:
# Server=
Server=192.168.20.4

### Option: ListenPort
#       Agent will listen on this port for connections from the server.
#
# Mandatory: no
# Range: 1024-32767
# Default:
# ListenPort=10050

### Option: ListenIP
#       List of comma delimited IP addresses that the agent should listen on.
#       First IP address is sent to Zabbix server if connecting to it to retrieve
^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 135: Zabbix agent configuration file

Step 5 : After adding Zabbix server IP in the configuration file to start agent service using command ‘service zabbix-agent start’.

```

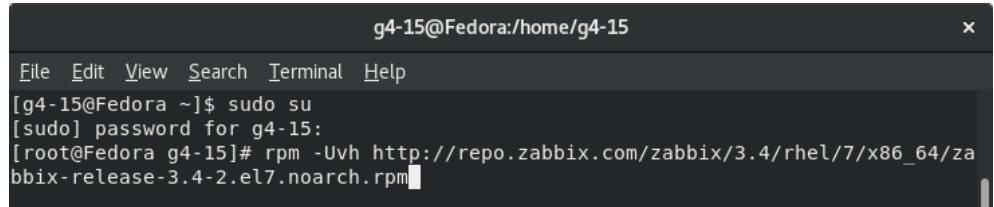
root@ubuntu: ~
Fetched 164 kB in 1s (149 kB/s)
Selecting previously unselected package zabbix-agent.
(Reading database ... 252491 files and directories currently installed.)
Preparing to unpack .../zabbix-agent_1%3a3.4.14-1+xenial_amd64.deb ...
Unpacking zabbix-agent (1:3.4.14-1+xenial) ...
Processing triggers for man-db (2.7.5-1) ...
Processing triggers for systemd (229-4ubuntu21.5) ...
Processing triggers for ureadahead (0.100.0-19) ...
ureadahead will be reprofiled on next reboot
Setting up zabbix-agent (1:3.4.14-1+xenial) ...
insserv: Script likewise is broken: incomplete LSB comment.
insserv: missing 'Provides:' entry: please add.
insserv: missing 'Required-Start:' entry: please add even if empty.
insserv: missing 'Required-Stop:' entry: please add even if empty.
insserv: missing 'Default-Start:' entry: please add even if empty.
insserv: missing 'Default-Stop:' entry: please add even if empty.
insserv: Default-Start undefined, assuming empty start runlevel(s) for script 'likewise'
insserv: Default-Stop undefined, assuming empty stop runlevel(s) for script 'likewise'
Processing triggers for systemd (229-4ubuntu21.5) ...
Processing triggers for ureadahead (0.100.0-19) ...
root@ubuntu:~# nano /etc/zabbix/zabbix_agentd.conf
root@ubuntu:~# service zabbix-agent start

```

Figure 136: Start agent service

Install Zabbix Agent on Fedora

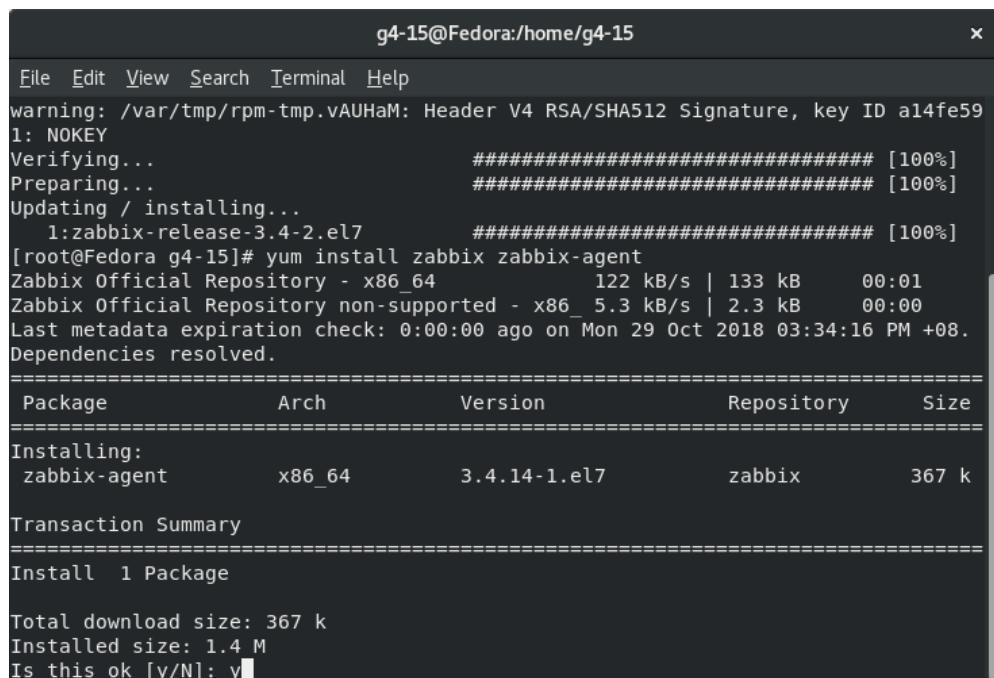
Step 1 : Login with root. Then, just like on the Zabbix server, run the following commands to install the repository configuration package:



```
g4-15@Fedora:/home/g4-15
File Edit View Search Terminal Help
[g4-15@Fedora ~]$ sudo su
[sudo] password for g4-15:
[root@Fedora g4-15]# rpm -Uvh http://repo.zabbix.com/zabbix/3.4/rhel/7/x86_64/zabbix-release-3.4-2.el7.noarch.rpm
```

Figure 137: Installing package on Fedora

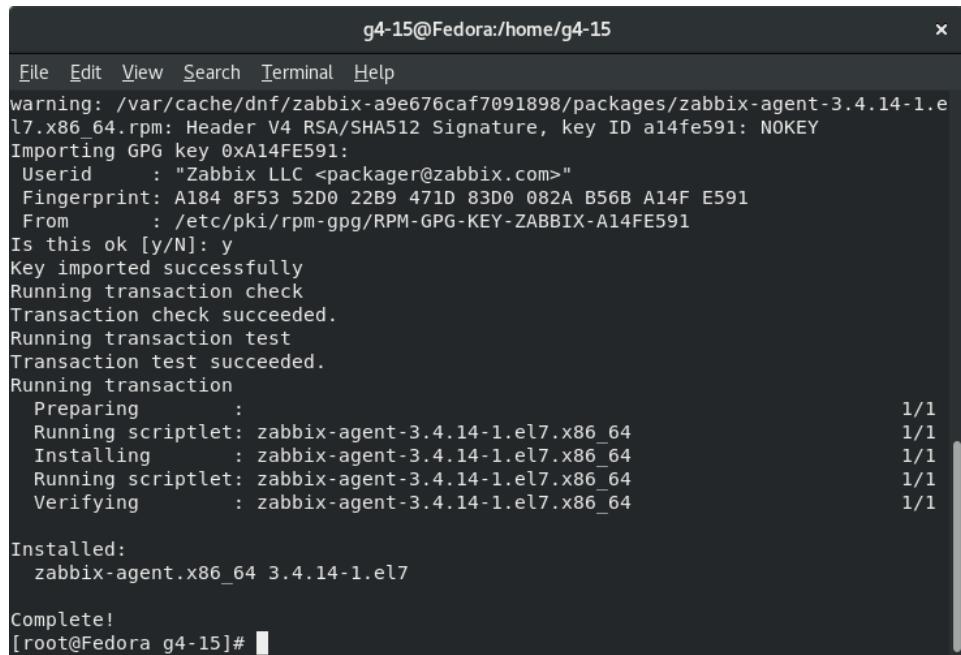
Step 2 : Then install the Zabbix agent:



```
g4-15@Fedora:/home/g4-15
File Edit View Search Terminal Help
warning: /var/tmp/rpm-tmp.vAUHaM: Header V4 RSA/SHA512 Signature, key ID a14fe59
1: NOKEY
Verifying... ###### [100%]
Preparing... ###### [100%]
Updating / installing...
1:zabbix-release-3.4-2.el7 ###### [100%]
[root@Fedora g4-15]# yum install zabbix zabbix-agent
Zabbix Official Repository - x86_64           122 kB/s | 133 kB   00:01
Zabbix Official Repository non-supported - x86_5.3 kB/s | 2.3 kB   00:00
Last metadata expiration check: 0:00:00 ago on Mon 29 Oct 2018 03:34:16 PM +08.
Dependencies resolved.
=====
Package          Arch      Version       Repository      Size
=====
Installing:
zabbix-agent    x86_64    3.4.14-1.el7  zabbix        367 k
Transaction Summary
=====
Install 1 Package

Total download size: 367 k
Installed size: 1.4 M
Is this ok [y/N]: y
```

Figure 138: Installing Zabbix agent in Fedora



```

g4-15@Fedora:/home/g4-15
File Edit View Search Terminal Help
warning: /var/cache/dnf/zabbix-a9e676caf7091898/packages/zabbix-agent-3.4.14-1.el7.x86_64.rpm: Header V4 RSA/SHA512 Signature, key ID a14fe591: NOKEY
Importing GPG key 0xA14FE591:
  Userid      : "Zabbix LLC <packager@zabbix.com>"
  Fingerprint: A184 8F53 52D0 22B9 471D 83D0 082A B56B A14F E591
  From        : /etc/pki/rpm-gpg/RPM-GPG-KEY-ZABBIX-A14FE591
Is this ok [y/N]: y
Key imported successfully
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing           : 1/1
  Running scriptlet: zabbix-agent-3.4.14-1.el7.x86_64          1/1
  Installing         : zabbix-agent-3.4.14-1.el7.x86_64          1/1
  Running scriptlet: zabbix-agent-3.4.14-1.el7.x86_64          1/1
  Verifying          : zabbix-agent-3.4.14-1.el7.x86_64          1/1

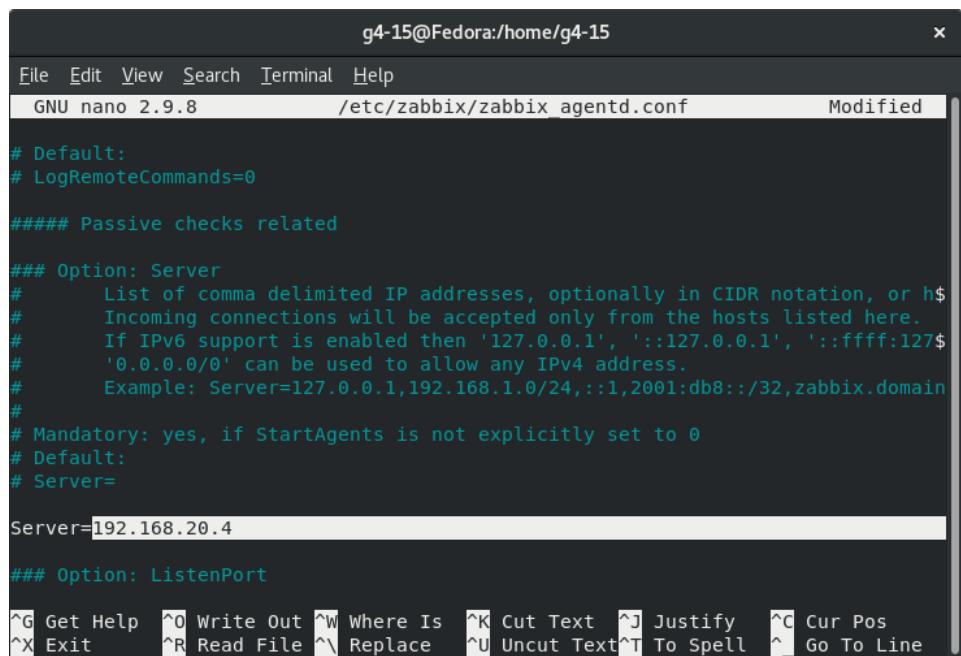
Installed:
  zabbix-agent.x86_64 3.4.14-1.el7

Complete!
[root@Fedora g4-15]#

```

Figure 139: Continuing installing Zabbix agent in Fedora

Step 3 : After installation of Zabbix agent. Edit Zabbix agent configuration file /etc/zabbix/zabbix_agentd.conf and update Zabbix server IP.



```

g4-15@Fedora:/home/g4-15
File Edit View Search Terminal Help
GNU nano 2.9.8          /etc/zabbix/zabbix_agentd.conf      Modified
# Default:
# LogRemoteCommands=0

##### Passive checks related

### Option: Server
#      List of comma delimited IP addresses, optionally in CIDR notation, or h$#
#      Incoming connections will be accepted only from the hosts listed here.
#      If IPv6 support is enabled then '127.0.0.1', '::127.0.0.1', '::ffff:127$#
#      '0.0.0.0/0' can be used to allow any IPv4 address.
#      Example: Server=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.domain
#
# Mandatory: yes, if StartAgents is not explicitly set to 0
# Default:
# Server=

Server=192.168.20.4

### Option: ListenPort

^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 140: Zabbix agent configuration file editting

```

g4-15@Fedora:/home/g4-15
File Edit View Search Terminal Help
GNU nano 2.9.8      /etc/zabbix/zabbix_agentd.conf      Modified
#
#      If this parameter is not specified, active checks are disabled.
#      Example: ServerActive=127.0.0.1:20051,zabbix.domain,[::1]:30051,::1,[12$#
#
# Mandatory: no
# Default:
# ServerActive=
#
ServerActive=192.168.20.4
#
### Option: Hostname
#      Unique, case sensitive hostname.
#      Required for active checks and must match hostname as configured on the$#
#      Value is acquired from HostnameItem if undefined.
#
# Mandatory: no
# Default:
# Hostname=
#
Hostname=Zabbix server
^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 141: Continuing editting Zabbix agent

Step 4 : Enter Zabbix server at the Hostname.

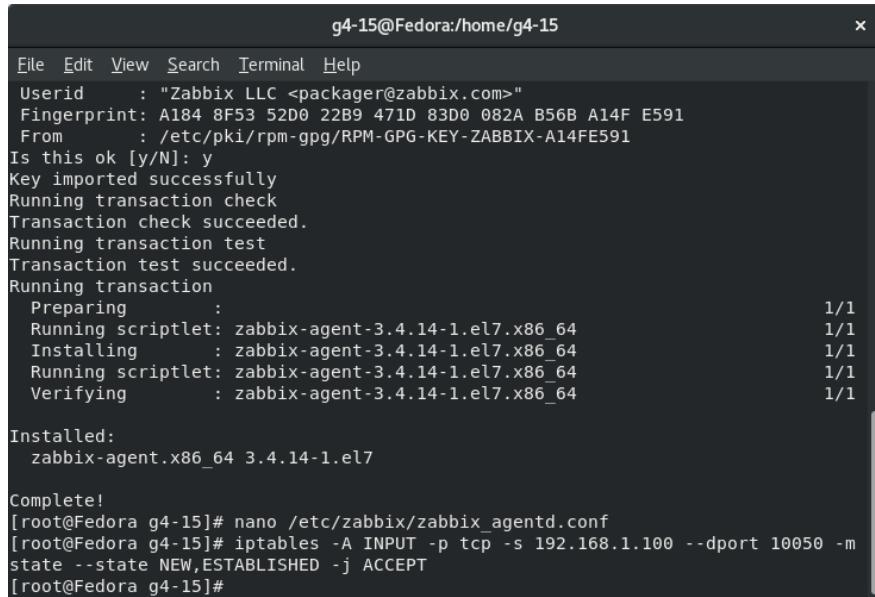
```

g4-15@Fedora:/home/g4-15
File Edit View Search Terminal Help
GNU nano 2.9.8      /etc/zabbix/zabbix_agentd.conf      Modified
#
#      Unique, case sensitive hostname.
#      Required for active checks and must match hostname as configured on the$#
#      Value is acquired from HostnameItem if undefined.
#
# Mandatory: no
# Default:
# Hostname=
#
Hostname=Zabbix server
#
### Option: HostnameItem
#      Item used for generating Hostname if it is undefined. Ignored if Hostna$#
#      Does not support UserParameters or aliases.
#
# Mandatory: no
# Default:
# HostnameItem=system.hostname
#
### Option: HostMetadata
^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 142: Entering Zabbix Server

Step 5 : Zabbix agent uses 10050/tcp port. You are required to open this port to allow Zabbix server with the agent. Execute command to open port in iptables firewall where 192.168.1.100 is IP of Zabbix server.



```

g4-15@Fedora:/home/g4-15
File Edit View Search Terminal Help
Userid      : "Zabbix LLC <packager@zabbix.com>"
Fingerprint: A184 8F53 52D0 22B9 471D 83D0 082A B56B A14F E591
From        : /etc/pki/rpm-gpg/RPM-GPG-KEY-ZABBIX-A14FE591
Is this ok [y/N]: y
Key imported successfully
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing      :
Running scriptlet: zabbix-agent-3.4.14-1.el7.x86_64          1/1
Installing    : zabbix-agent-3.4.14-1.el7.x86_64          1/1
Running scriptlet: zabbix-agent-3.4.14-1.el7.x86_64          1/1
Verifying     : zabbix-agent-3.4.14-1.el7.x86_64          1/1

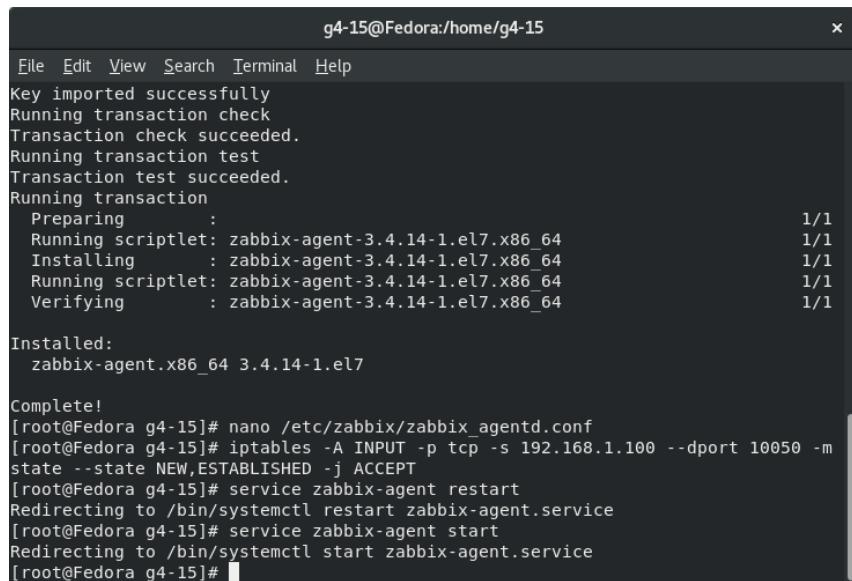
Installed:
zabbix-agent.x86_64 3.4.14-1.el7

Complete!
[root@Fedora g4-15]# nano /etc/zabbix/zabbix_agentd.conf
[root@Fedora g4-15]# iptables -A INPUT -p tcp -s 192.168.1.100 --dport 10050 -m state --state NEW,ESTABLISHED -j ACCEPT
[root@Fedora g4-15]#

```

Figure 143: Opening port to allow Zabbix server with agent

Step 6 : After adding Zabbix server IP to the configuration file, now restart agent service to reload the new settings, using the following command.



```

g4-15@Fedora:/home/g4-15
File Edit View Search Terminal Help
Key imported successfully
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing      :
Running scriptlet: zabbix-agent-3.4.14-1.el7.x86_64          1/1
Installing    : zabbix-agent-3.4.14-1.el7.x86_64          1/1
Running scriptlet: zabbix-agent-3.4.14-1.el7.x86_64          1/1
Verifying     : zabbix-agent-3.4.14-1.el7.x86_64          1/1

Installed:
zabbix-agent.x86_64 3.4.14-1.el7

Complete!
[root@Fedora g4-15]# nano /etc/zabbix/zabbix_agentd.conf
[root@Fedora g4-15]# iptables -A INPUT -p tcp -s 192.168.1.100 --dport 10050 -m state --state NEW,ESTABLISHED -j ACCEPT
[root@Fedora g4-15]# service zabbix-agent restart
Redirecting to /bin/systemctl restart zabbix-agent.service
[root@Fedora g4-15]# service zabbix-agent start
Redirecting to /bin/systemctl start zabbix-agent.service
[root@Fedora g4-15]#

```

Figure 144: Restarting agent service to reload new setting

Install Zabbix Agent on Windows Server

Step 1 : Download latest windows zabbix agent source code from [zabbix official site](https://www.zabbix.com/download_agents) or use below link to download zabbix agent 3.0.0.

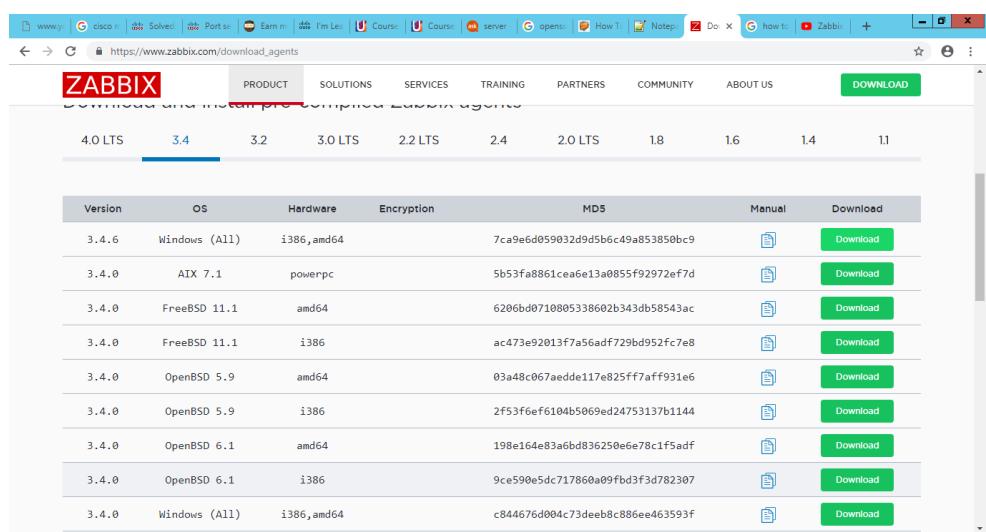


Figure 145: Downloading latest windows zabbix agent

Step 2 : Now make copy of sample configuration file **c:\zabbix_agentd.win.conf** to create zabbix agent configuration file **c:\zabbix_agentd.conf**.

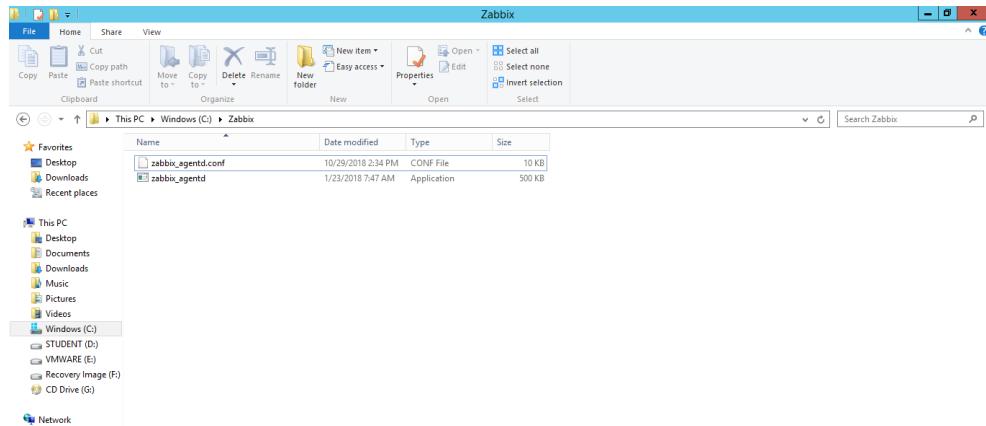


Figure 146: Making copy of sample configuration file

Step 3 : Now edit configuration and update following values.

```

C:\Zabbix\zabbix_agentd.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
change.log zabbix_agentd.conf

70 # Default:
71 # LogRemoteCommands=0
72
73 ##### Passive checks related
74
75 ### Option: Server
76 # List of comma delimited IP addresses, optionally in CIDR notation, or hostnames of Zabbix servers.
77 # Incoming connections will be accepted only from the hosts listed here.
78 # If IPv6 support is enabled then '127.0.0.1', '::127.0.0.1', '::ffff:127.0.0.1' are treated equally and '::/0' will allow all.
79 # '0.0.0.0/0' can be used to allow any IPv4 address.
80 # Example: Server=127.0.0.1,192.168.1.0/24,:1,2001:db8::/32,zabbix.domain
81 #
82 # Mandatory: no
83 # Default:
84 # Server=
85
86 Server=192.168.20.4
87
88 ### Option: ListenPort
89 # Agent will listen on this port for connections from the server.
90 #
91 # Mandatory: no
92 # Range: 1024-32767
93 # Default:
94 # ListenPort=10050
95
96 ### Option: ListenIP
97 # List of comma delimited IP addresses that the agent should listen on.
98 # First IP address is sent to Zabbix server if connecting to it to retrieve list of active checks.
99 #
100 # Mandatory: no
101 # Default:
102 # ListenIP=0.0.0.0
103

Normal text file length:9,899 lines:356 Ln:86 Col:8 Sel:12|1 Unix (LF) UTF-8 INS ...

C:\Zabbix\zabbix_agentd.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
change.log zabbix_agentd.conf

120 # If this parameter is not specified, active checks are disabled.
121 # Example: ServerActive=127.0.0.1:20051,zabbix.domain,[::1]:30051,::1,[12fc::1]
122 #
123 # Mandatory: no
124 # Default:
125 # ServerActive=
126
127 ServerActive=192.168.20.4
128
129 ### Option: Hostname
130 # Unique, case sensitive hostname.
131 # Required for active checks and must match hostname as configured on the server.
132 # Value is acquired from HostnameItem if undefined.
133 #
134 # Mandatory: no
135 # Default:
136 # Hostname=
137
138 Hostname=Windows host
139
140 ### Option: HostnameItem
141 # Item used for generating Hostname if it is undefined. Ignored if Hostname is defined.
142 # Does not support UserParameters or aliases.
143 #
144 # Mandatory: no
145 # Default:
146 # HostnameItem=system.hostname
147
148 ### Option: HostMetadata
149 # Optional parameter that defines host metadata.
150 # Host metadata is used at host auto-registration process.
151 # An agent will issue an error and not start if the value is over limit of 255 characters.
152 # If not defined, value will be acquired from HostMetadataItem.
153 #

Normal text file length:9,899 lines:356 Ln:127 Col:14 Sel:12|1 Unix (LF) UTF-8 INS ...

```

Figure 147: Edit configuration files and update the values

Step 4 Let's install zabbix agent as windows server by executing following command from command line.

```

Administrator: C:\Windows\system32\cmd.exe
C:\Zabbix>zabbix_agentd.exe -c zabbix_agentd.conf --install
zabbix_agentd.exe [6248]: service [Zabbix Agent] installed successfully
zabbix_agentd.exe [6248]: event source [Zabbix Agent] installed successfully
C:\Zabbix>zabbix_agentd.exe -s
zabbix_agentd.exe [8040]: service [Zabbix Agent] started successfully
C:\Zabbix>services.msc
C:\Zabbix>_

```

Figure 148: Installation of Zabbix ad Windows server

Step 5 : Open run windows >> type “services.msc” >> press enter.

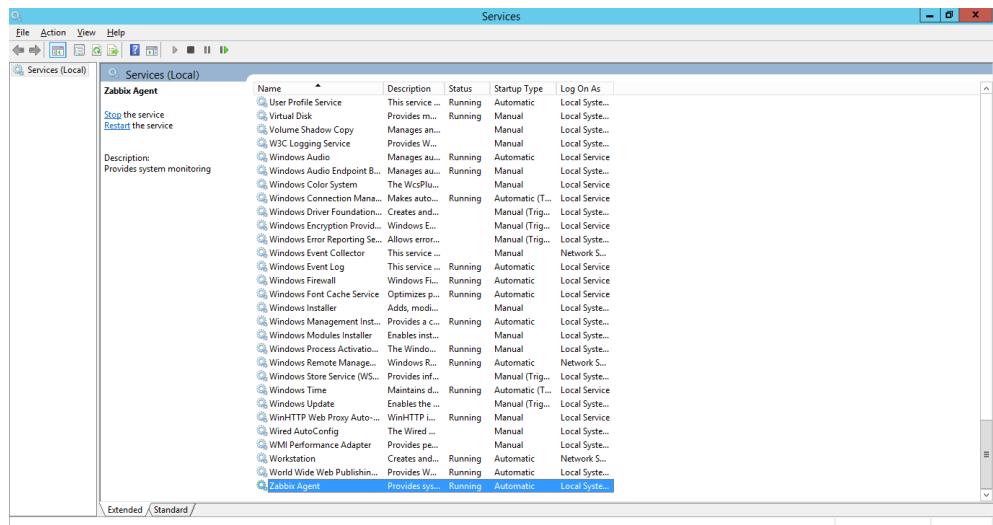


Figure 149: Services.msc window

Step 6 : To make sure that the zabbix agent can connect to the Zabbix Server open **Control Panel** -> **System and Security** -> **Windows Firewall** and hit on **Allow an app through Windows Firewall**.

Next, click on **Allow another app** button and a new window should open. Use the Browse button to navigate to the path of the Zabbix agent executable file, and then hit on Add button.

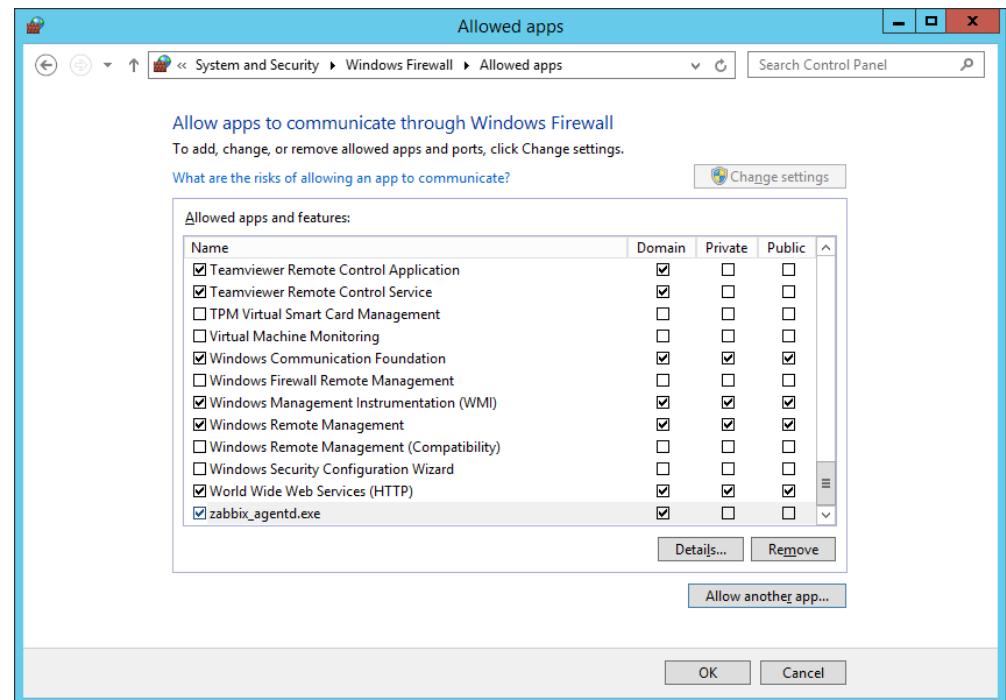


Figure 150: Allowing apps to communicate through Windows firewall

Step 7 : Open the browser and navigate it to ‘<http://zabbix.group4.com/?admin>’. The login screen would appear and enter the default username and password which is **admin** and **zabbix** respectively.

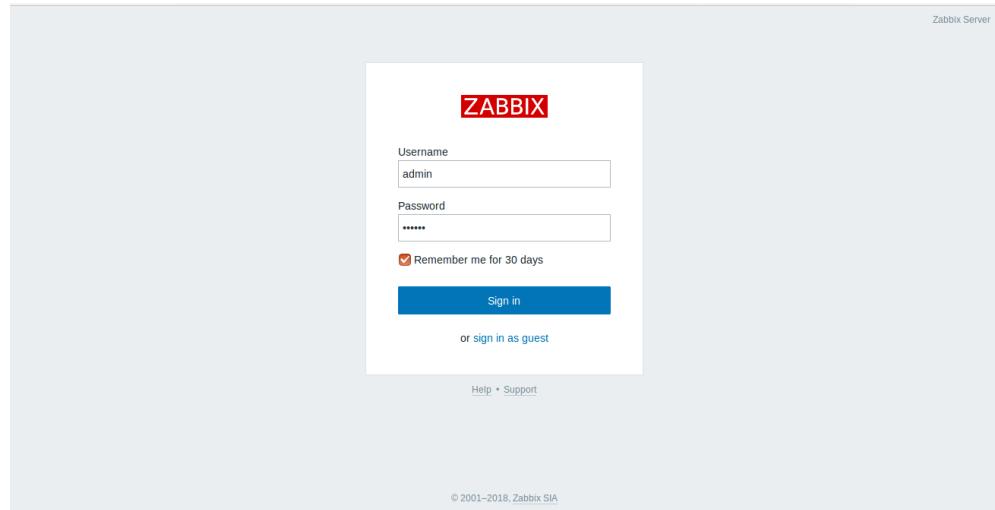


Figure 151: Login screen of Zabbix

Figure 152: Zabbix Dashboard

5.3.12 Server Virtualization

Step 1 : Install Hyper-V in server manager in the Windows Server.

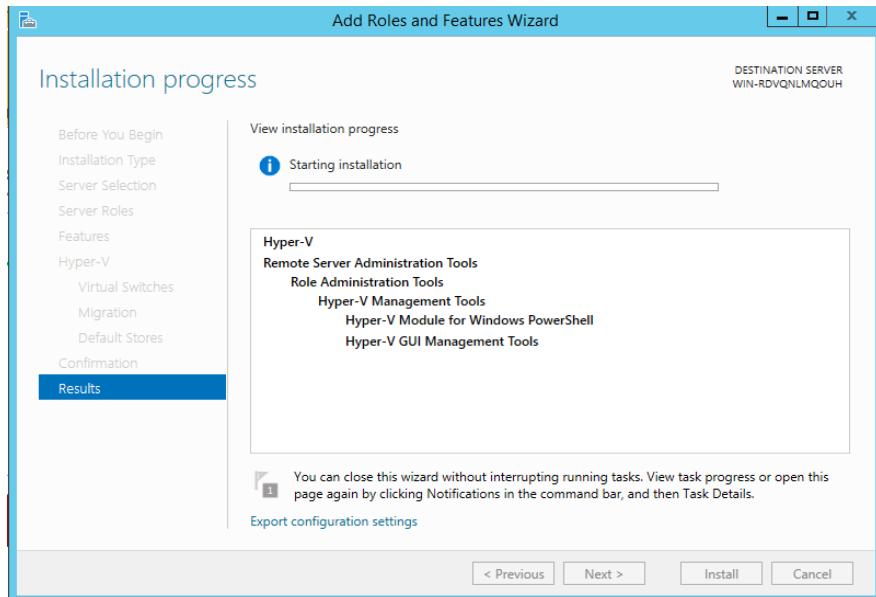


Figure 153: Installation of Hyper-V

Step 2 : Open the Hyper-V manager. Install the virtual Windows Server in the Hyper-V by added the real ISO of Windows Server.

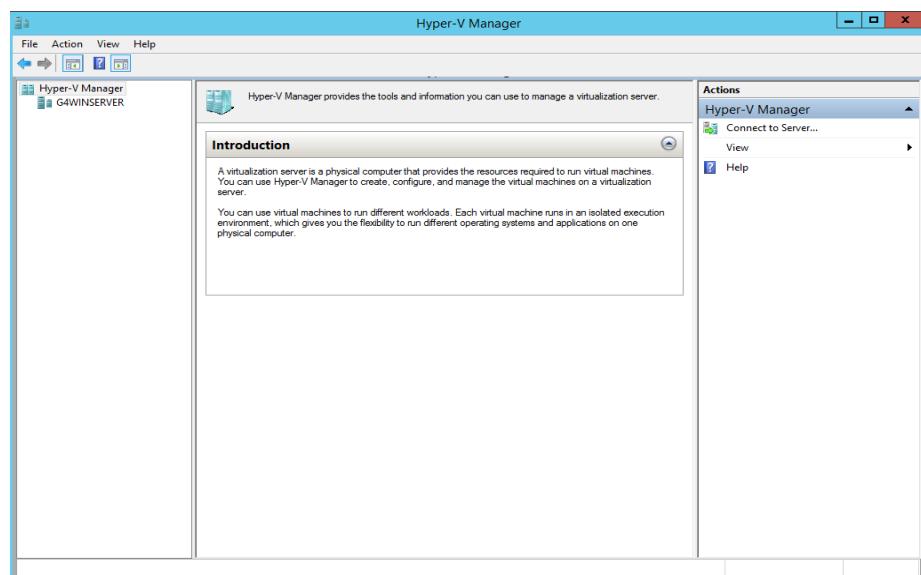


Figure 154: Installation of virtual windows server in Hyper-V

Step 3 The virtual machine of Windows Server has been installed and can be running.

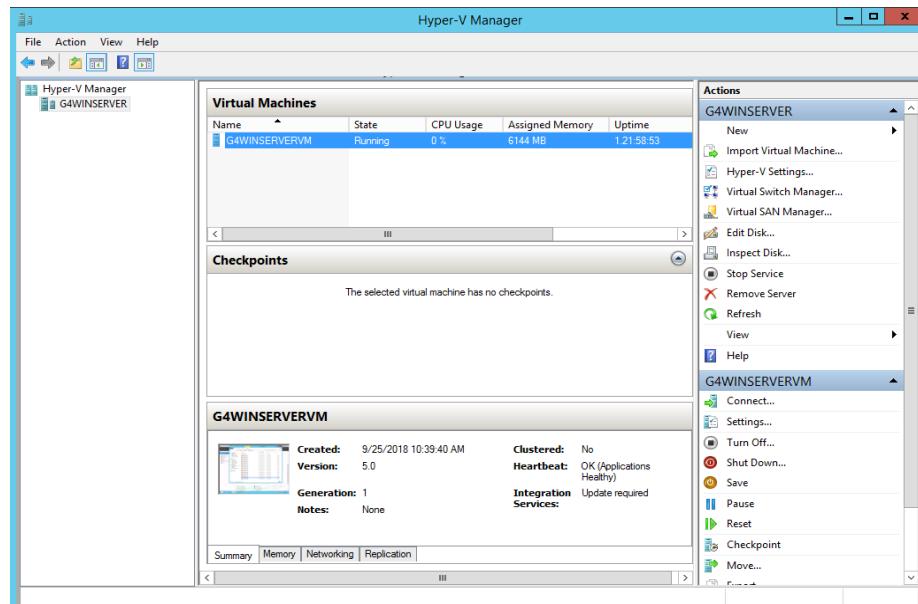


Figure 155: Results of Window Server

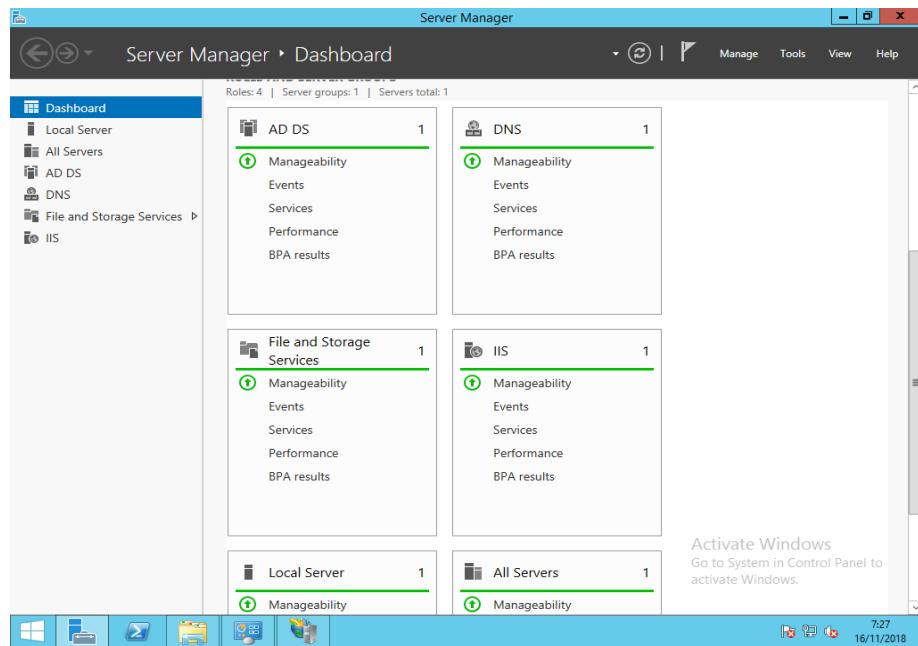


Figure 156: Server manager dashboard

Step 4 : 1 minimum application need to be installed in the virtual Windows Server and the application that has been installed is Web, SSL. DNS and IIS need to be installed in the server manager before that services need to use as well.

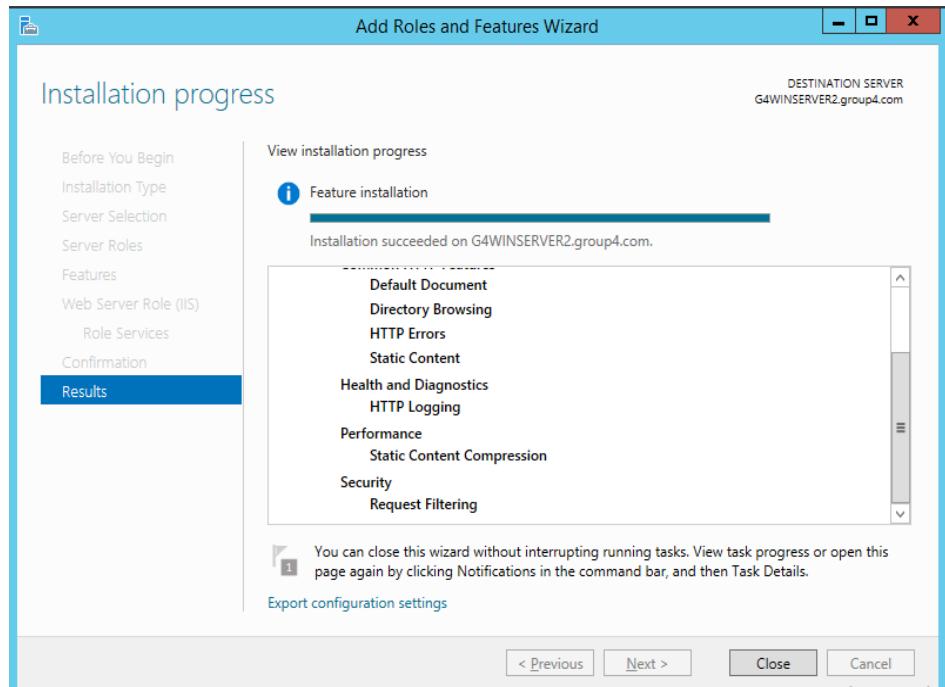


Figure 157: Installation progress in virtual Windows server

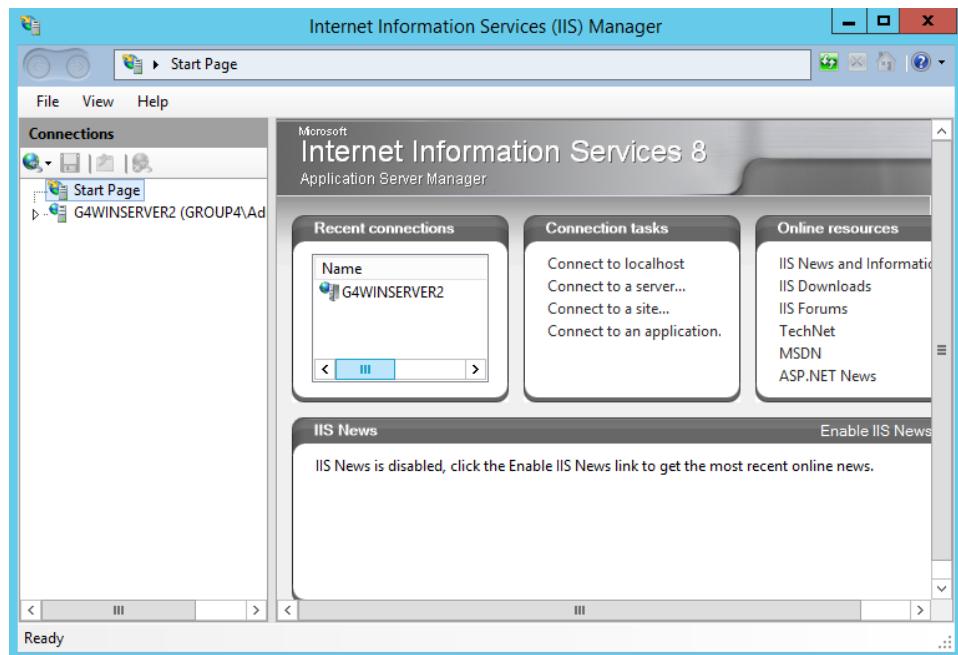


Figure 158: Start page of IIS Manager

Web Installation

Step 1 : Adding New site. Go to IIS and create a new site. Fill all the required details.

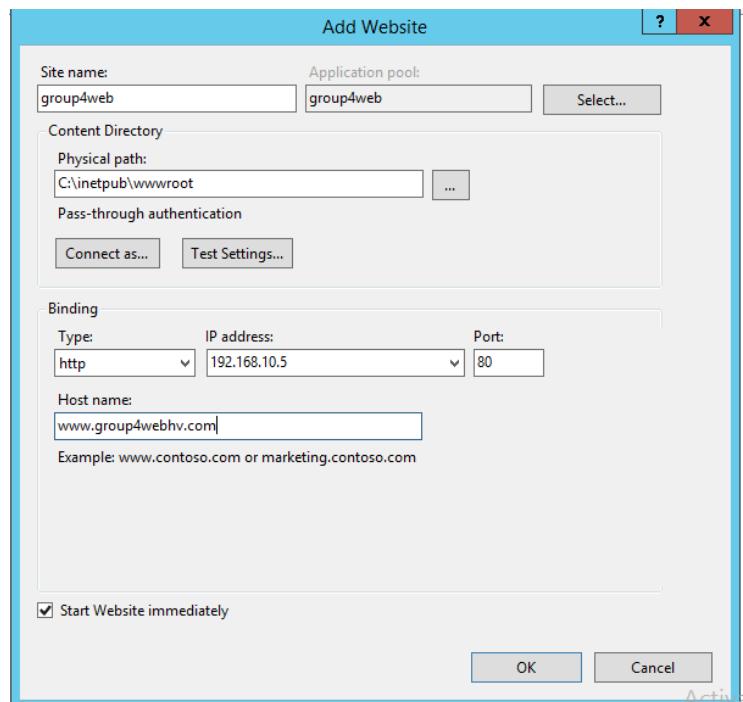


Figure 159: Creating new site in IIS

Step 2 : In Default Document set the document that want to display on the website. Add a new file document html to set a default document web.

The screenshot shows the 'Default Document' configuration page. It includes a header with a globe icon and the title 'Default Document'. Below this is a note: 'Use this feature to specify the default file(s) to return when a client does not request a specific file. Set default documents in order of priority.' A table lists files with their entry types:

Name	Entry Type
iisstart.htm	Local
Default.htm	Local
Default.asp	Local
index.htm	Local
index.html	Local

An 'Actions' sidebar on the right contains links: 'Add...', 'Disable', 'Revert To Parent', and 'Help'.

Figure 1660: Adding new file document

Step 3 : Website has been added in IIS Manager.

The screenshot shows the 'Sites' list in the IIS Manager. The left pane displays a tree view of 'Connections' with nodes for 'Start Page', 'G4WINSERVER2 (GROUP4)\Ad', 'Application Pools', and 'Sites'. Under 'Sites', there are two entries: 'Default Web Site' (ID 1) and 'group4web' (ID 2). The main pane shows a table of sites with columns: Name, ID, Status, Binding, and Path. The table data is as follows:

Name	ID	Status	Binding	Path
Default Web Site	1	Started (ht...)	*:80 (http)	%SystemDrive%\inetpub\wwwroot
group4web	2	Started (ht...)	www.group4webhv.com on 192.1...	C:\inetpub\wwwroot\group4web

An 'Actions' sidebar on the right contains links: 'Add Website...', 'Set Website Defaults...', and 'Help'.

Figure 161: Website that have been added in IIS Manager

Step 4 : Adding a new zone at DNS Manager. Give a name to a new Zone and click Next to continue until Finish for successfully complete for new zone.

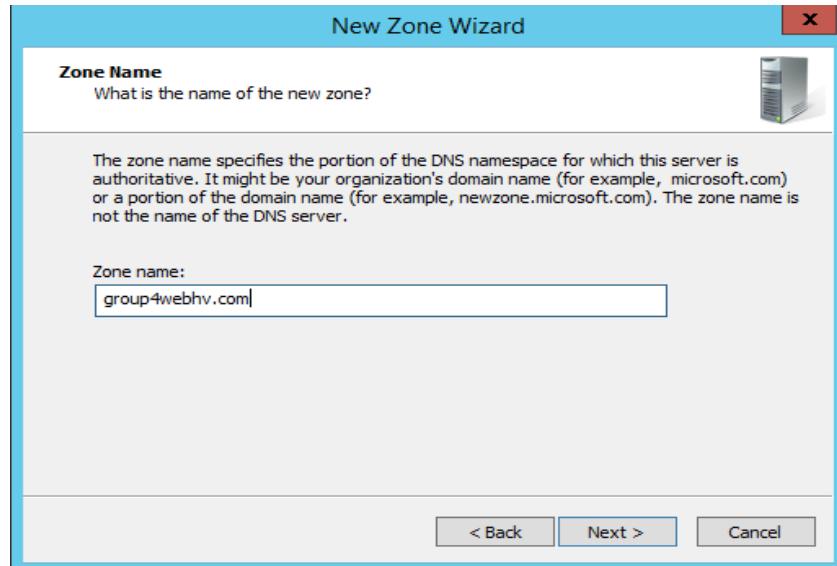


Figure 162: Adding new zone at DNS Manager

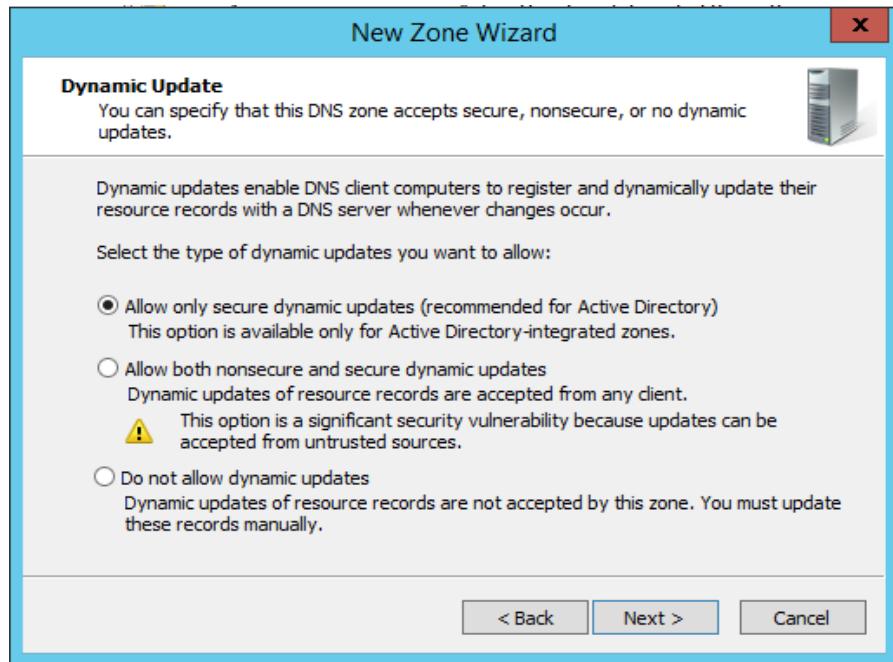


Figure 163: Dynamic update

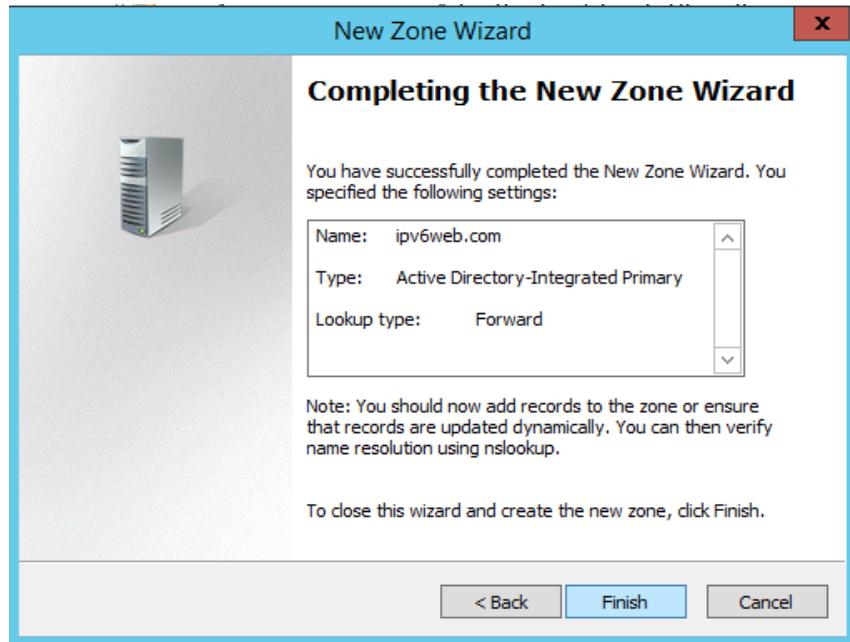


Figure 164: New Zone Wizard completed

Step 5 : After finish adding a new zone, add a new host for domain www.group4webhv.com. Right click and choose for a New Host (A or AAAA).

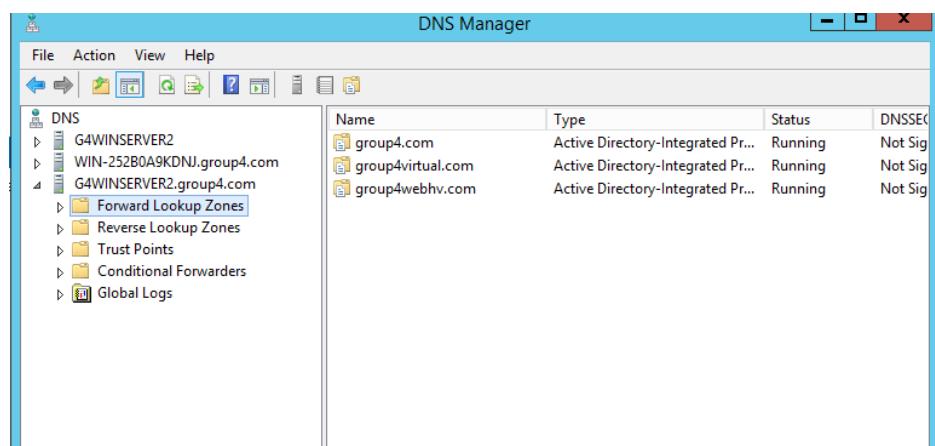


Figure 165: DNS Manager to choose for new host

Step 6 : Add a New Host and IP Address.

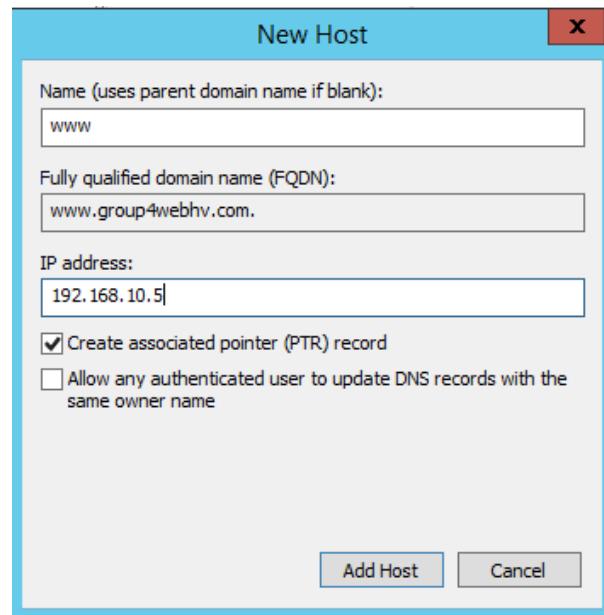


Figure 166: Adding new host and IP Address

SSL Installation

Step 1 : Go to IIS Manager. Choose Server Certificate.

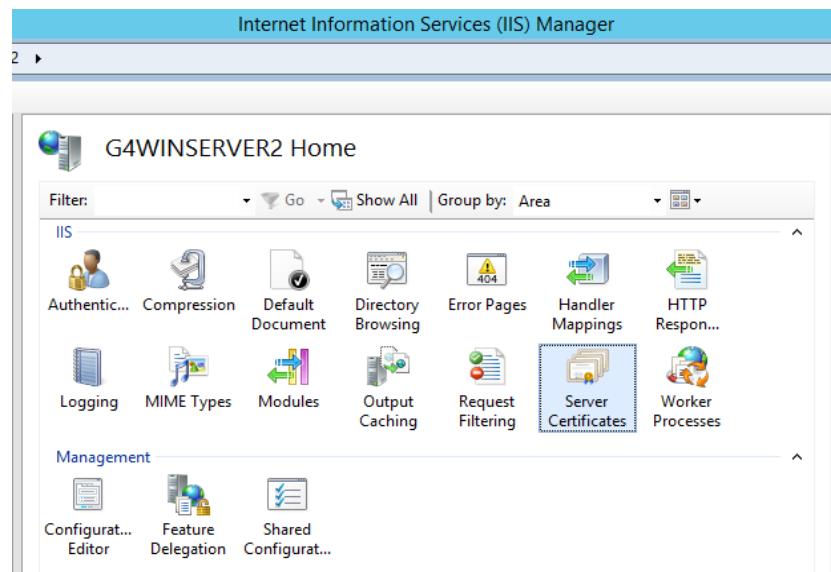


Figure 167: Certificate chosen in IIS Manager

Step 2 : At the Actions panel (right click mouse), choose to create Self-Signed Certificate.

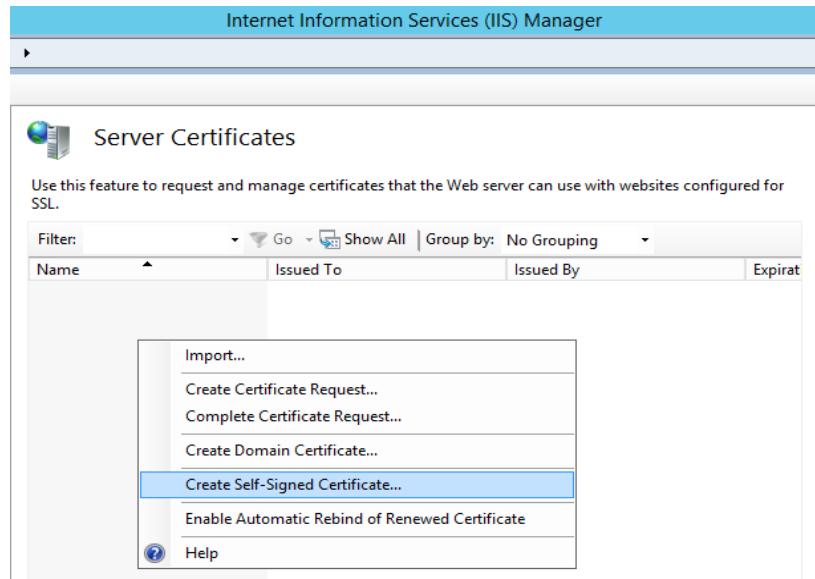


Figure 168: Server Certificates in IIS Manager

Step 3 : Add the name of SSL for the certificate and click OK button.

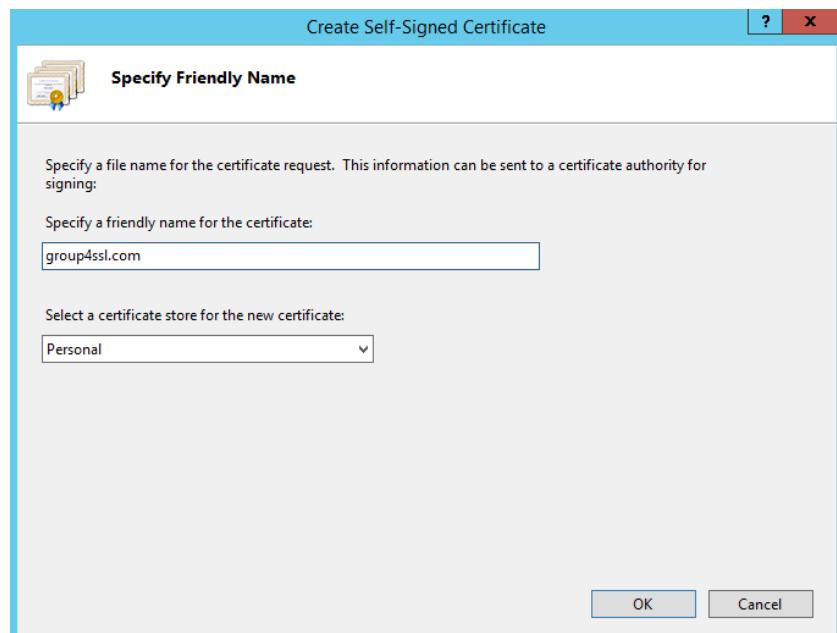


Figure 169: Adding SSL Name

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

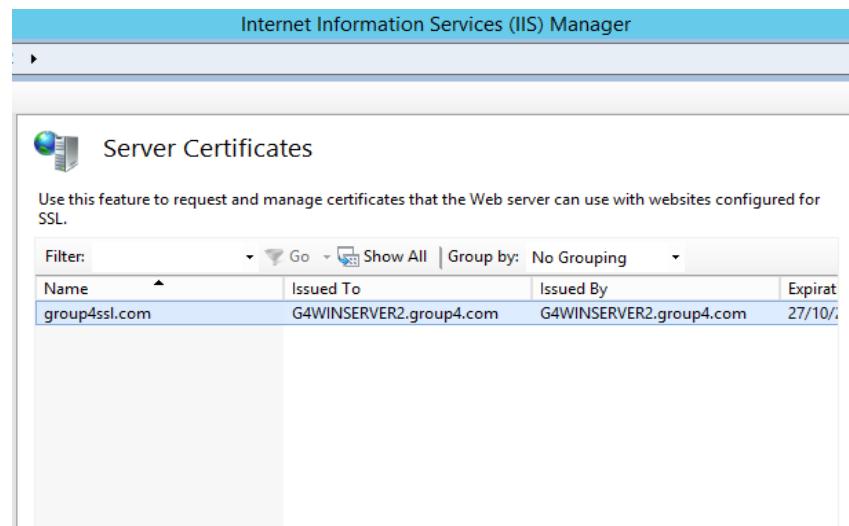


Figure 170: Result of certificate that has been created

Step 5 : Add Website and choose type of https for SSL. Choose the URL of SSL Certificate that already created before.

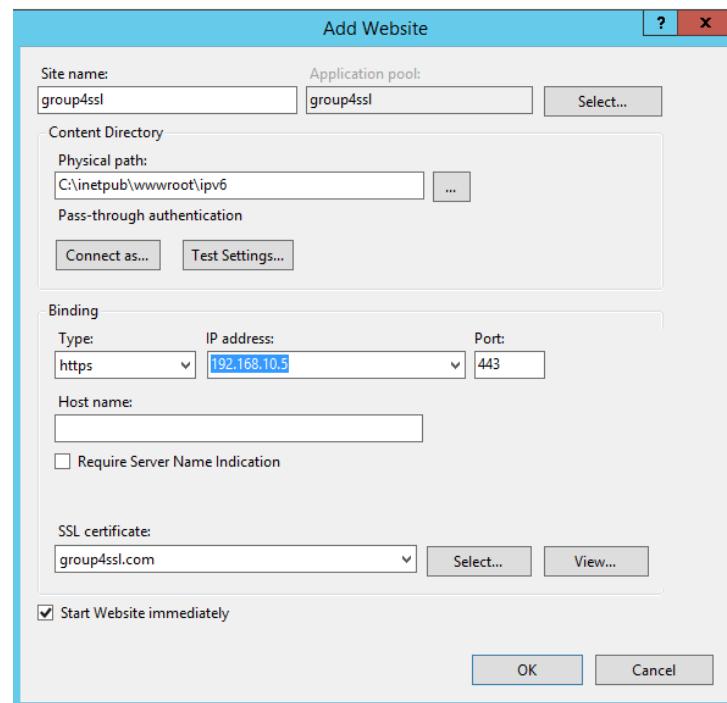


Figure 171: Website Addition

Step 6 : In Default Document set the document that want to display on the website. Add a new file document html to set a default document web.

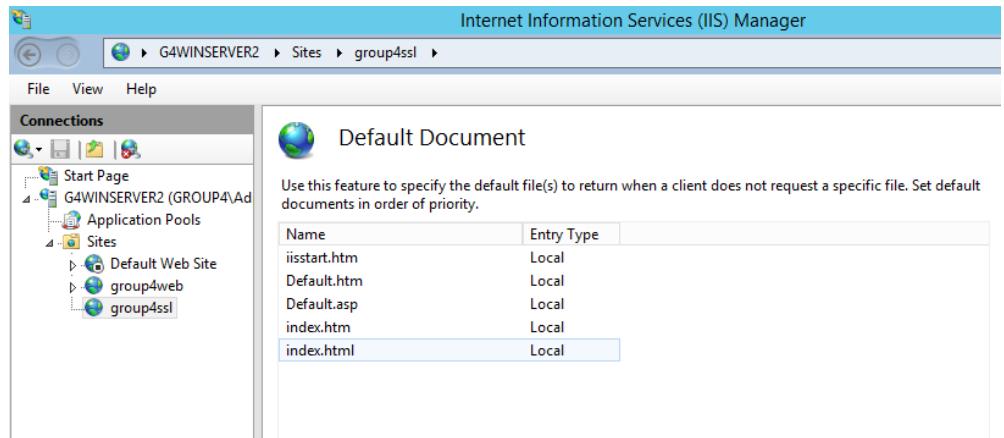


Figure 172: Default Document in IIS Manager

5.3.13 AAA (Authentication, Authorization and Accounting) using Radius

Step 1 : Firstly, to install Radius Server, open Server Manager > Add Role and Features Wizard.

Step 2 : When the window dialogue has opened, on Server Role, select the Network Policy and Access Services. Then, click Next.

Step 3 : After that, tick Network Policy Server, Routing and Remote Access Services and then click Next.

Step 4 : Click through the confirmation screen and click Install.

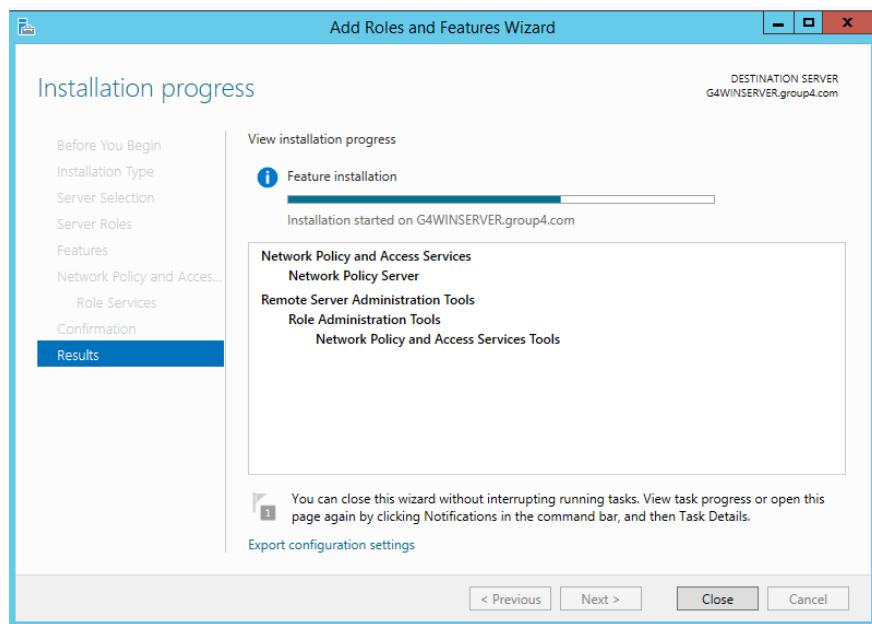


Figure 173: Installation progress of NPS, Routing and Remote Access

Step 5 Wait until the installation is successful and click Close after the installation finished to make it complete.

Step 6 : Insert group name and description and change group scope to global.

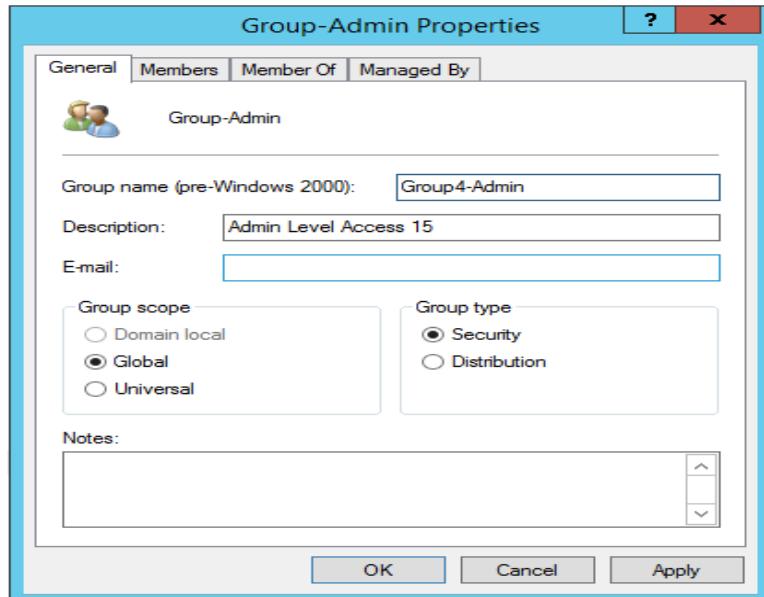


Figure 174: Admin Properties

Step 7 : Now the NPS is already installed. Go to Start> Administrative Tools> Network Policy Server to configure.

Step 8 : In NPS, click on Radius client and Service, the tree under the folder opens. Right Click on Radius Client to add new Radius client.

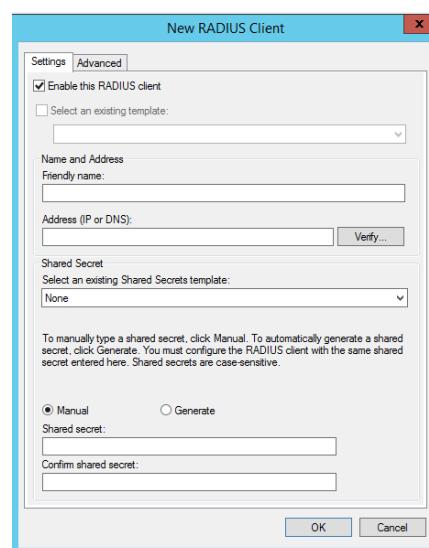


Figure 175: Adding new RADIUS client

Step 9 : Configure the new RADIUS client, enter the friendly name and IP address of the client and set the shared secret then press OK.

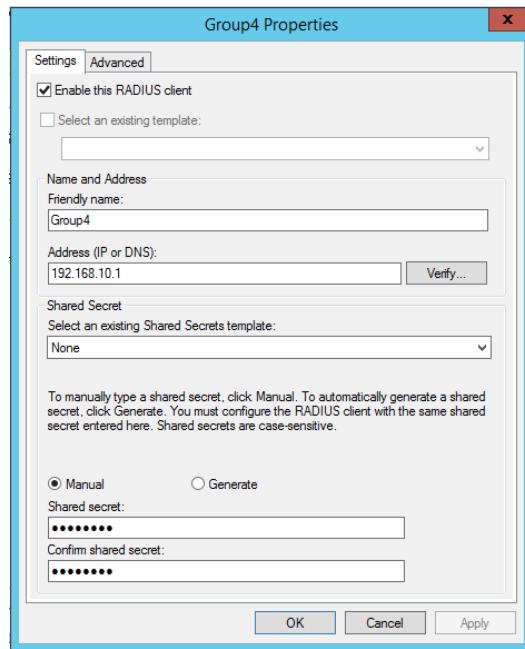


Figure 176: Group4 Properties

Step 10 : Change the vendor name to cisco.

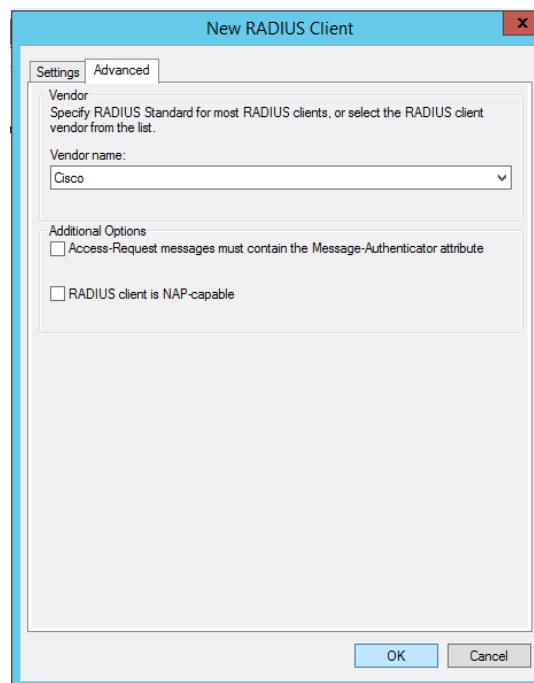


Figure 177: Vendor name of new RADIUS client

Step 11 : Set policy name as “Group4-POLICY” and choose network access server type as “Unspecified”, then click Next.

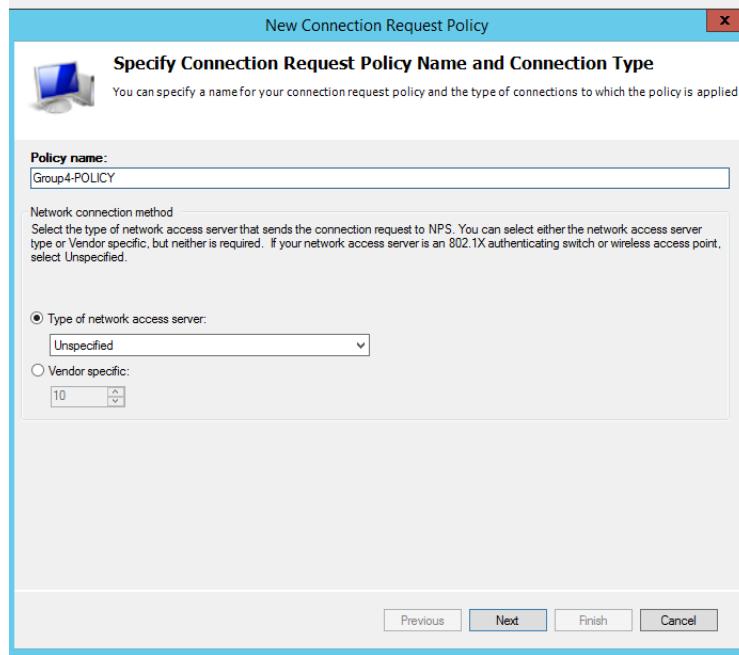


Figure 178: Specify connection request policy

Step 12 : After that, select Client IPv4 Address and click Add.

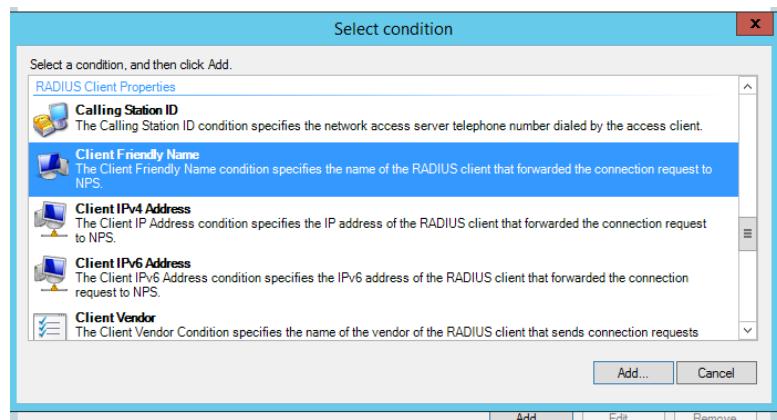


Figure 179: Condition Selection

Step 13 : Configure the setting for the network policy, click Next.

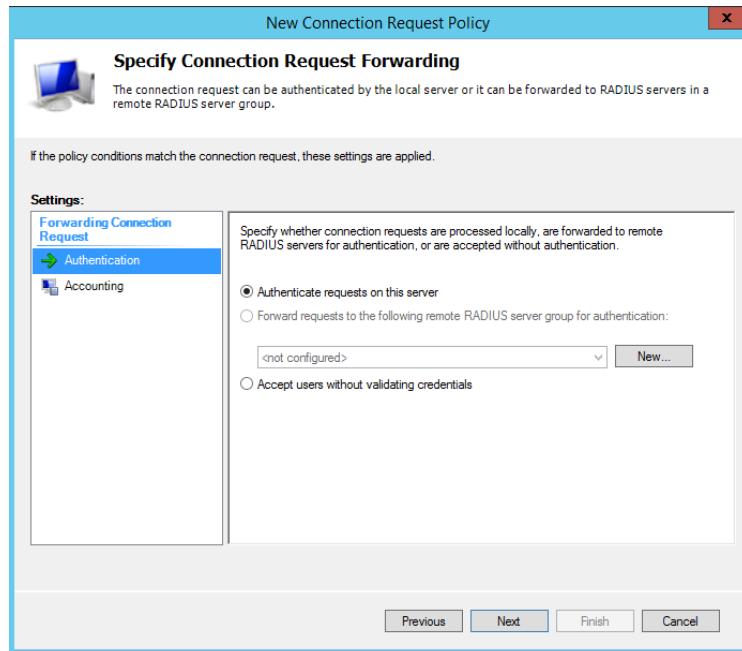


Figure 180: Specify connection request forwarding

Step 14 : The policy has already installed and to check the setting back, double click the policy name.

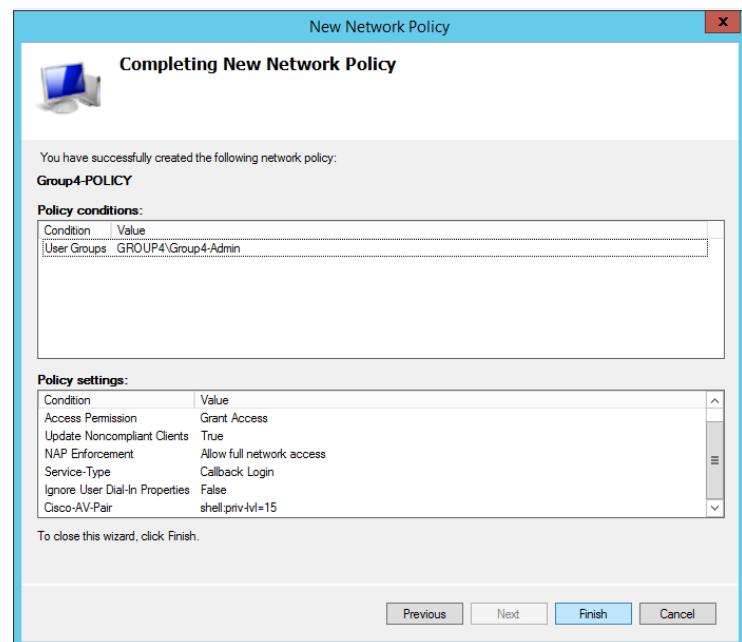


Figure 181: Network Policy

Step 15 : Then, open PuTTY terminal and get into Router.

Step 16 : Configure AAA using command as shown below.

```
G4Router>
G4Router>en
Password:
G4Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
G4Router(config)#aaa new-model
G4Router(config)#aaa authentication login default group radius local-case
G4Router(config)#aaa authentication login vty group radius local-case
G4Router(config)#aaa authentication enable default
G4Router(config)#aaa authentication enable default enable
G4Router(config)#aaa authorization exec default group radius local if
G4Router(config)##$zation exec default group radius local if-authenticated
G4Router(config)#aaa accounting system default ?
    none      No accounting.
    start-stop Record start and stop without waiting
    stop-only  Record stop when service terminates.
    vrf       VPN Routing/Forwarding parameters

G4Router(config)#aaa accounting system default start-stop ?
    broadcast  Use Broadcast for Accounting
    group     Use Server-group

G4Router(config)#aaa accounting system default start-stop group ?
    WORD      Server-group name
    radius    Use list of all Radius hosts.
    tacacs+   Use list of all Tacacs+ hosts.

G4Router(config)#aaa accounting system default start-stop group radius ?
    group    Use Server-group
    <cr>

G4Router(config)#aaa accounting system default start-stop group radius
G4Router(config)##$2.168.10.4 auth-port 1645 acct-port 1646 key AdminGroup4
G4Router(config)##$2.168.10.4 auth-port 1812 acct-port 1813 key AdminGroup4
G4Router(config)#ip radius ?
    source-interface Specify interface for source address in RADIUS packets

G4Router(config)#ip radius source
G4Router(config)#ip radius source-interface f
G4Router(config)#ip radius source-interface fastEthernet 0/1.10
G4Router(config)#
*Oct 31 13:15:24.479: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
*Oct 31 13:15:28.039: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
```

Figure 182: Command AAA at router

5.3.14 Wireless User Authentication using Radius Server

Step 1 : Firstly, go to Google and enter IP Address of your Access Point (AP) to open Linksys.

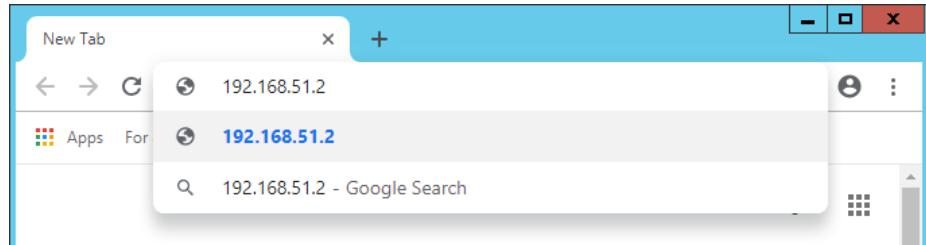


Figure 183: IP Address of the AP

Step 2 : Set IP Address and password for Access Point. Select Connectivity > Internet Settings > Choose Static IP for Connection Type.

Step 3 : Fill all the requirements to set IP for Access Point (AP) and Click OK.

Step 4 : After that select Wireless > Wireless > Enter shared key for both networks. Select security mode for the wireless which is WPA2/WPA Mixed Enterprise and enter the IP Address and Port Number of the Radius Server.

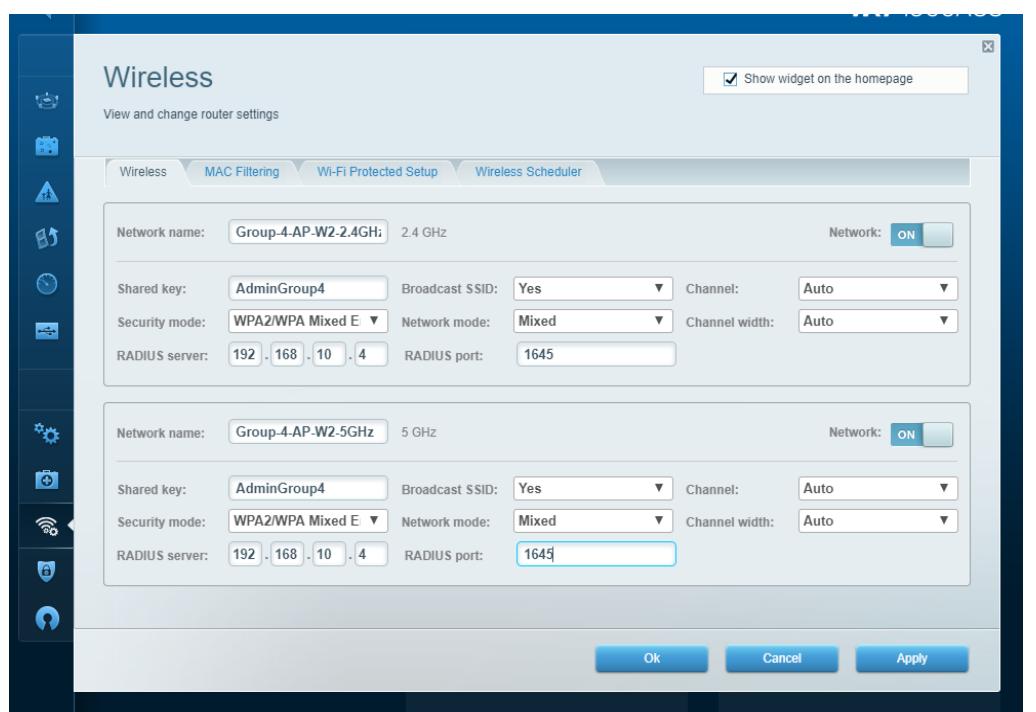


Figure 184: Wireless configuration inside the Linksys

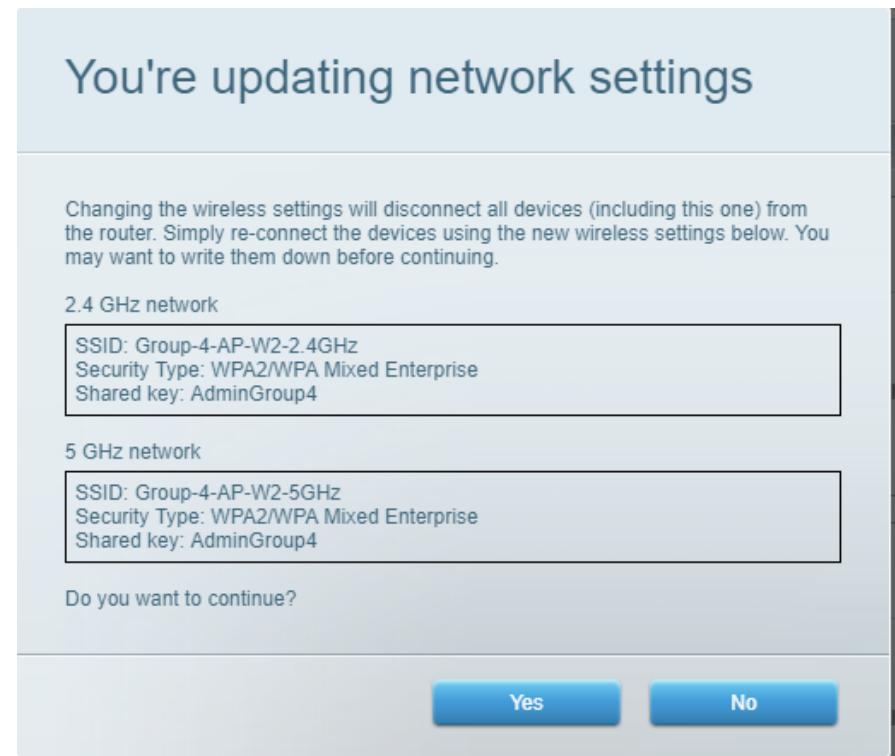


Figure 185: Confirmation to continue updating network setting

Step 5 : Open Server Manager and Windows Server. Click on the Tools bar on upper right of the windows and click on Active Directory Users and Computers. Then, click on the Users in the left pane of the window before creating New Object – Group or User.

Step 6 : Click on this symbol to create New Object – Group.



Figure 186: Symbol to create new group

Step 7 : Then, fill in the Group Name (group4wifi). Then, click OK.

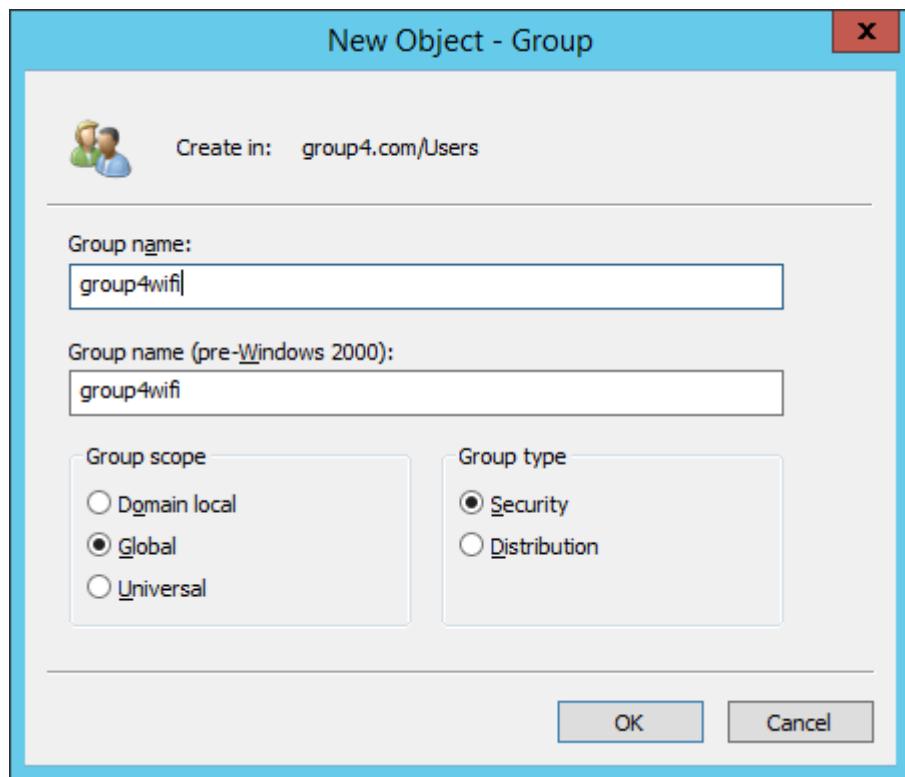


Figure 187: Creating new object – Group

Step 8 : Click on this symbol to create New Object – User.



Figure 188: Symbol to create new object – User

Step 9 : Then, fill in the first name and user logon name for all your group members. Then, click Next.

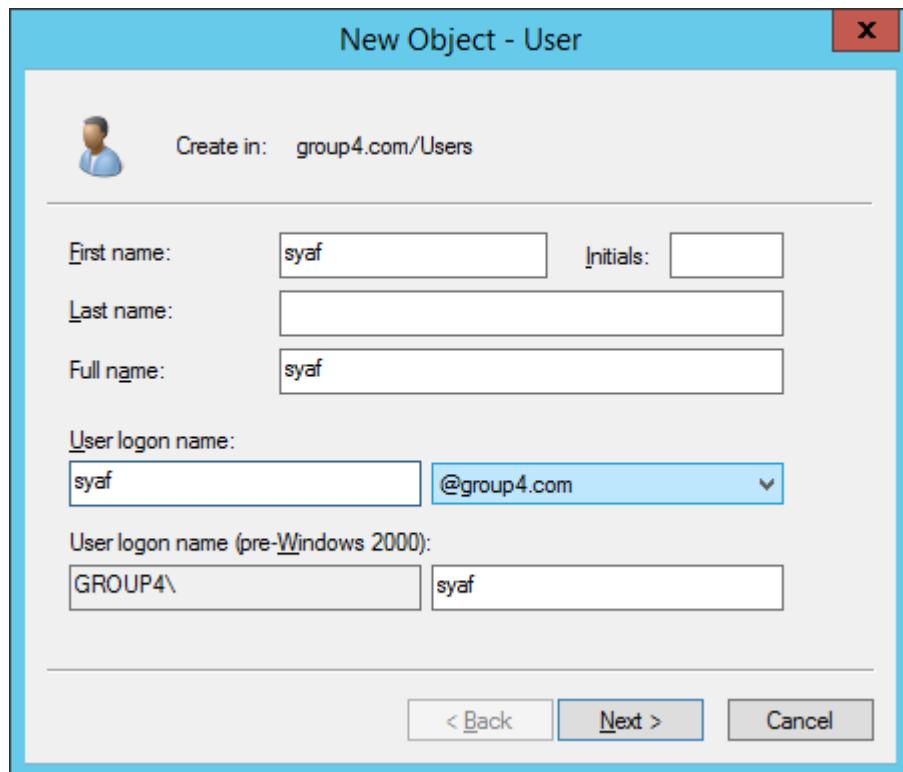


Figure 189: Creating new user

Step 10 It will request you to set the password and confirm the password.

Click on Password never expires before clicking Next. Then, click Finish.

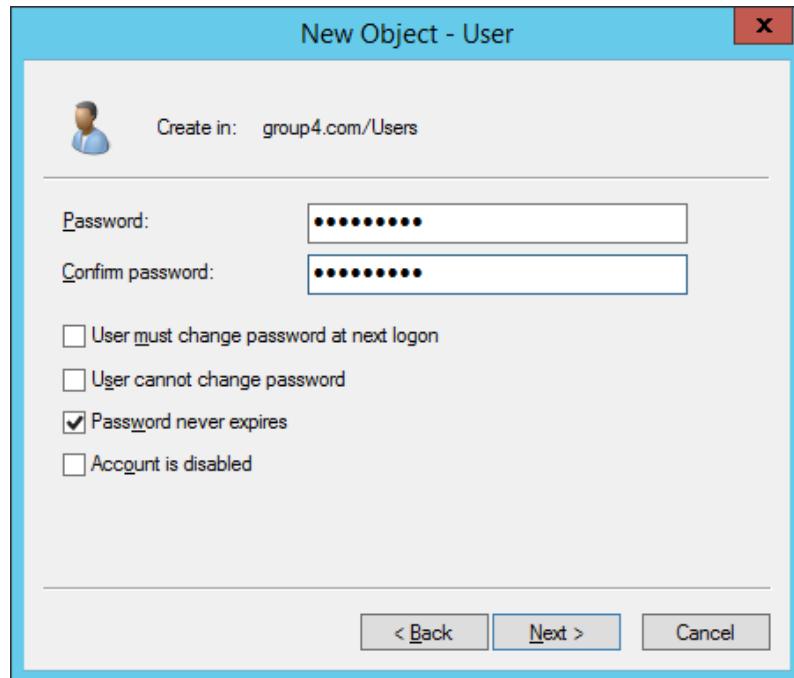


Figure 190: Creating password to the user

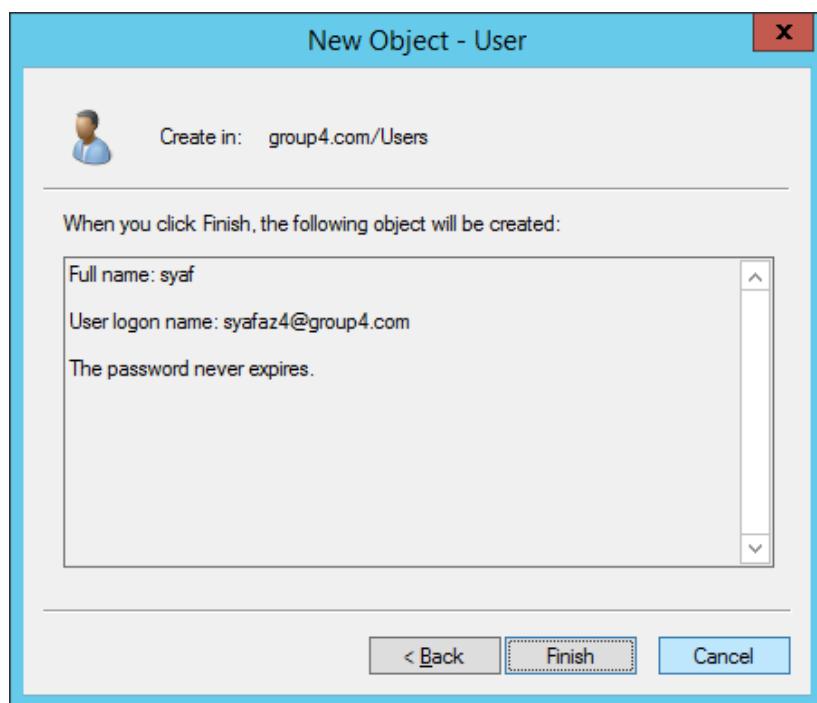


Figure 191: Confirmation of User

Step 11 : To check the members of group4wifi, right click on group4wifi and select Properties.

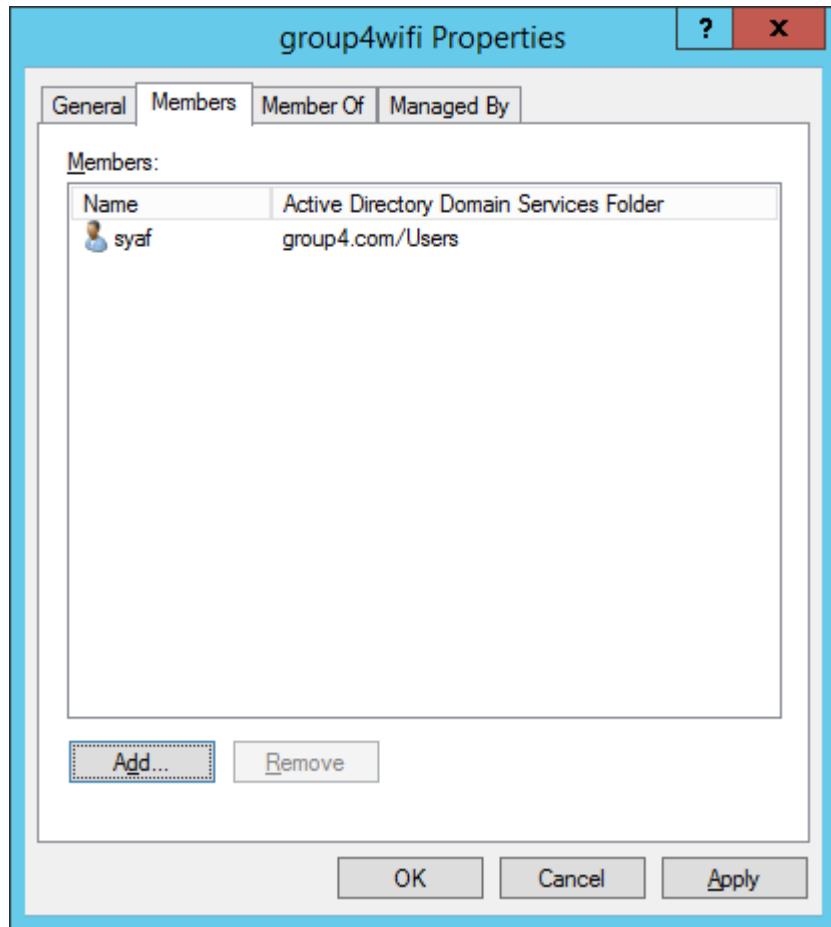


Figure 192: Members of group4wifi

Step 12 : After success creating user, go to Server Manager and click on Add Roles and Features Wizard, click on Next.

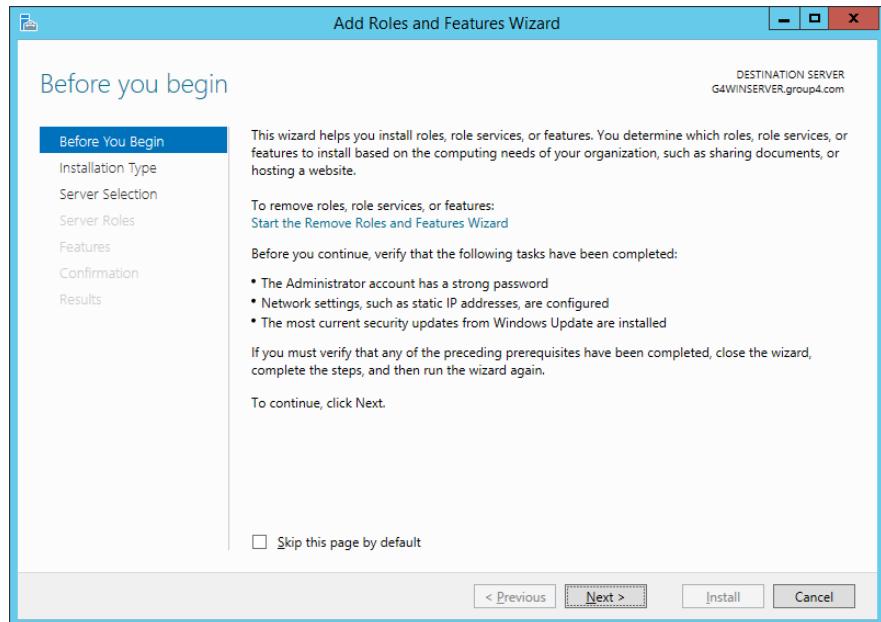


Figure 193: Add Roles and Features Wizard

Step 13 : For Installation Type, select Role-based or feature-based installation and then, click Next.

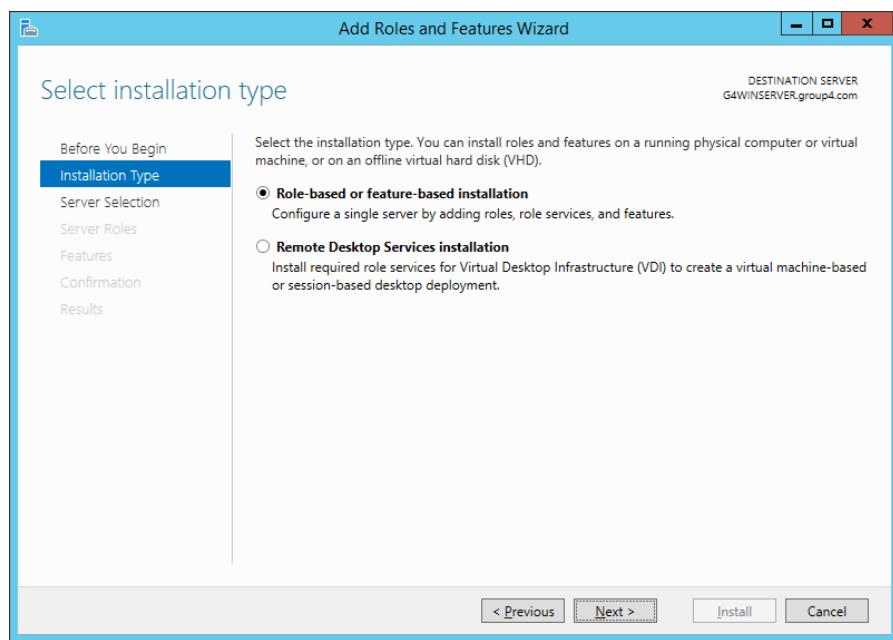


Figure 194: Select installation type

Step 14 : For Server Selection, click on Select a server from the server pool.

Then, click Next.

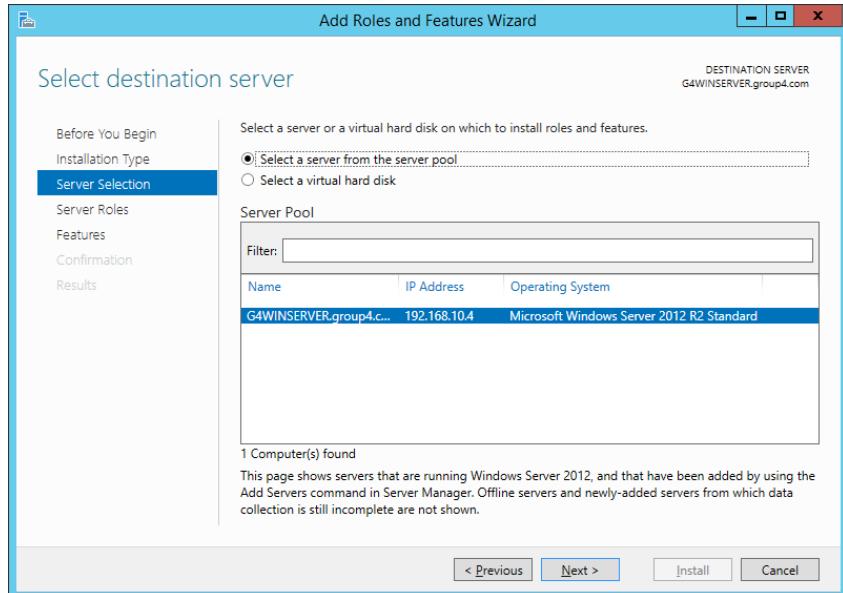


Figure 195: Select destination server

Step 15 : This window will pop up, select [Tools] Certification Authority Management Tools and click Add Features.

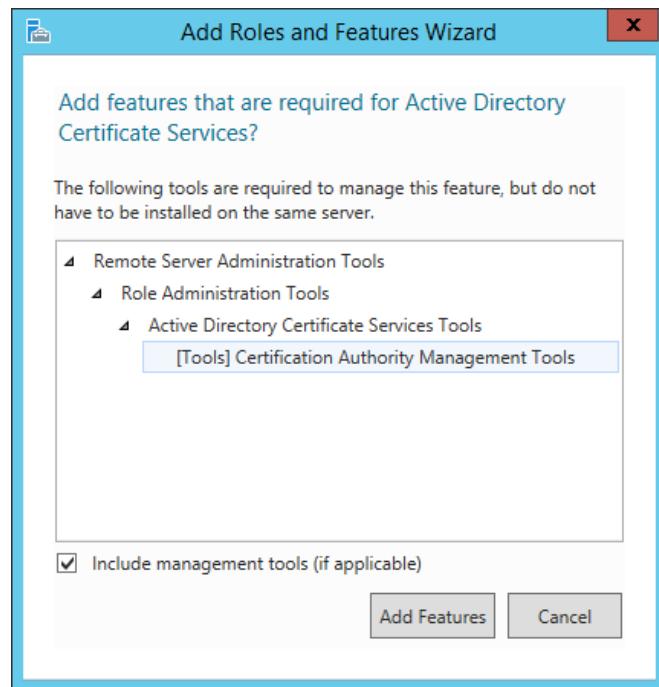


Figure 196: Adding features for AD CS

Step 16 : For Server Roles, make sure to make tick at Active Directory Certificate Service, DHCP Server and Network Policy and Access Services. Then click Next > Next for Features.

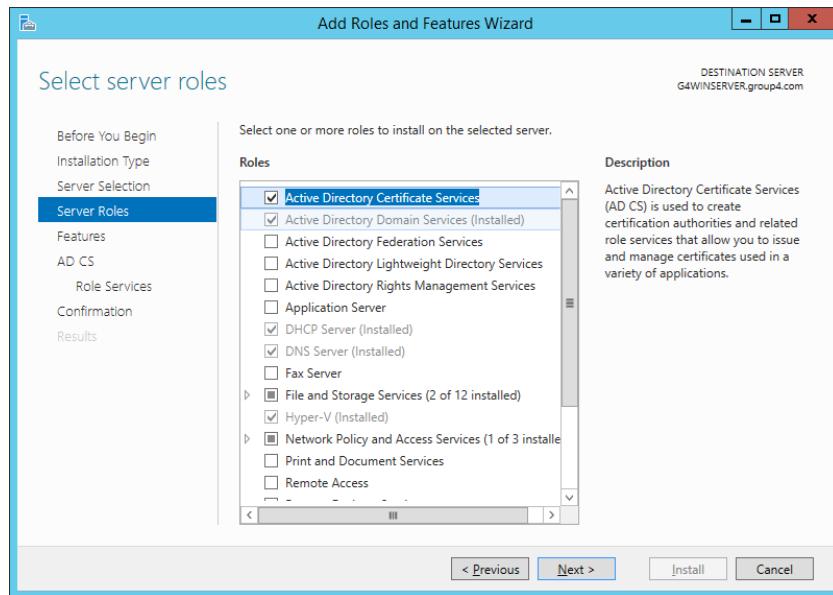


Figure 197: Selecting Server Roles

Step 17 : For AD CS, firstly, click Next and it will bring you to Role Services. On Role Services, tick on Certification Authority and click Next. After that, for Confirmation, click Install. Close it after the installation of the features success.

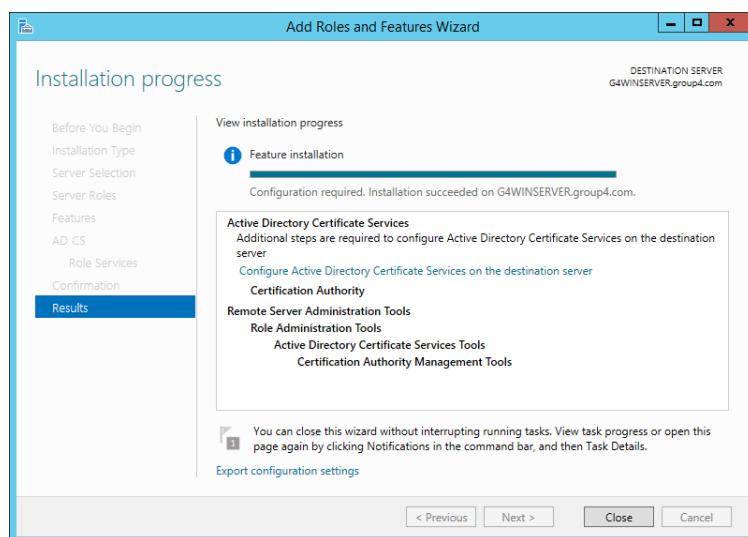


Figure 198: Installation progress of the additional features

Step 18 : Then, go to AD CS Configuration to configure the role services.

Click on Next.

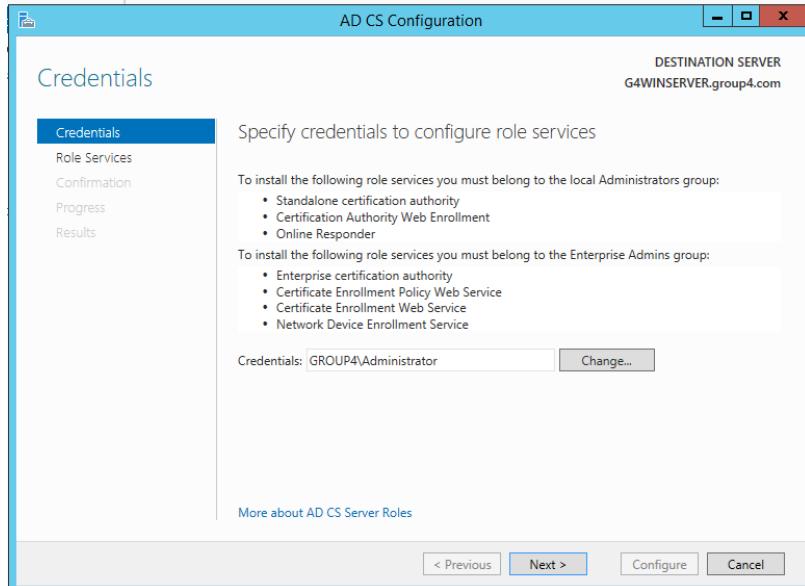


Figure 199: Role services configuration

Step 19 : For Roles Service, make sure to tick on Certification Authority.

Then, click Next.

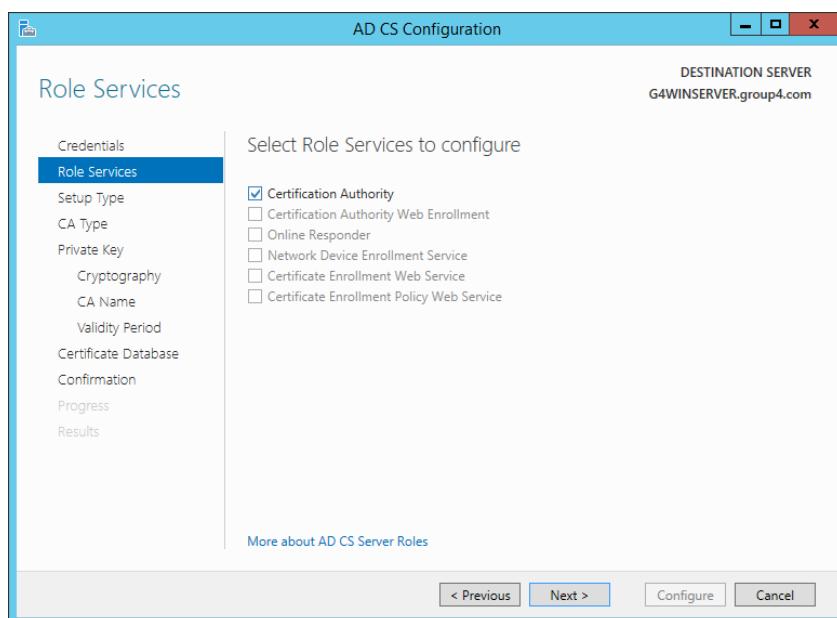


Figure 200: Role service selection for AD CS configuration

Step 20 : For Setup Type, choose Enterprise CA and click Next.

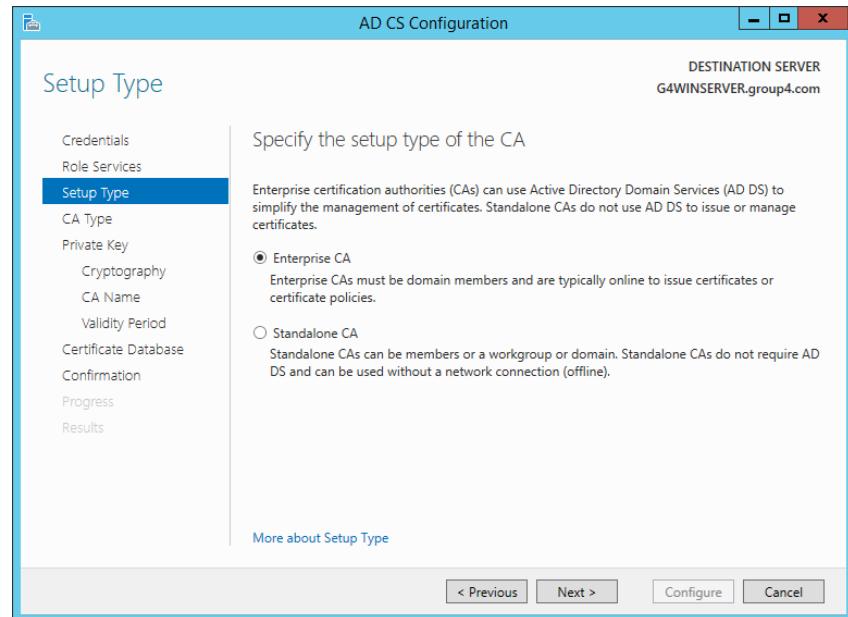


Figure 201: Setup type of CA

Step 21 : For CA Type, specify the type of CA to Root CA. Then, click Next.

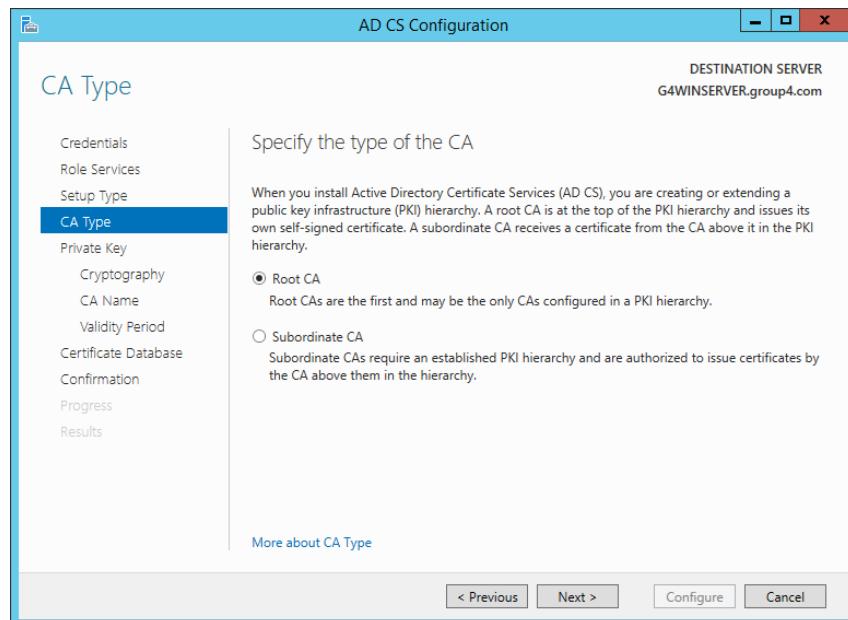


Figure 202: CA type specification

Step 22 : For Private Key, choose Create a new private key and click Next.

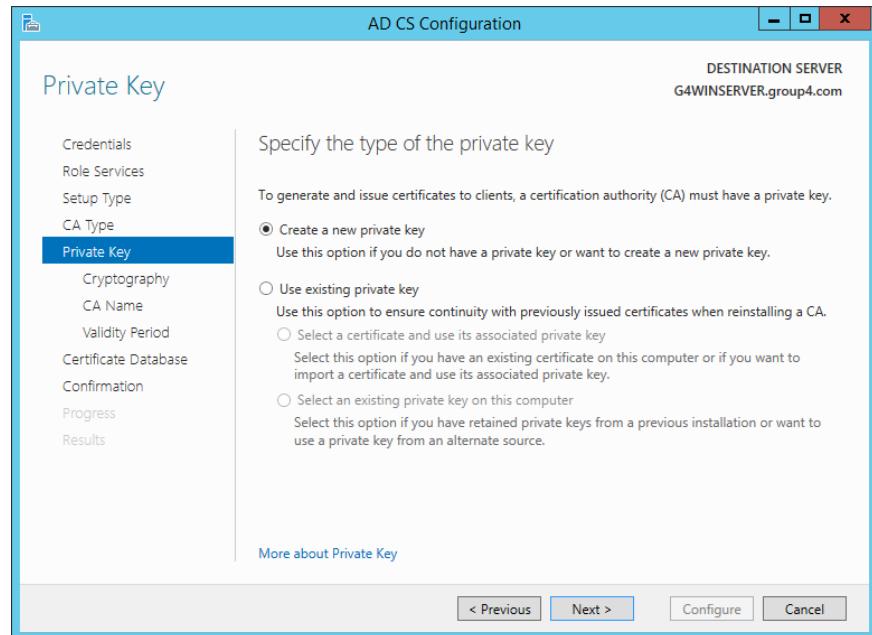


Figure 203: Choosing the private key

Step 23 : For Cryptography, make sure the key length is 2048 and the hash algorithm is SHA1. Then, click Next.

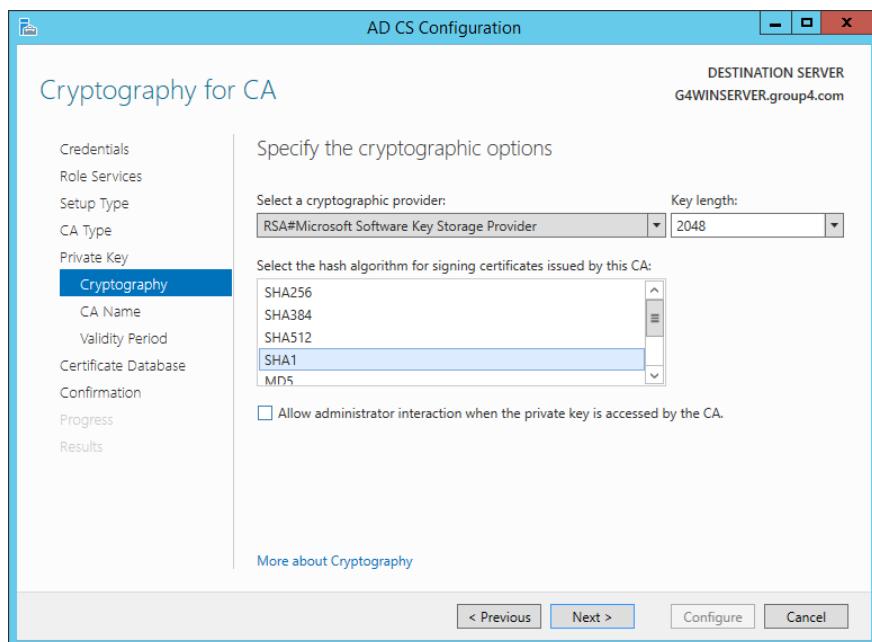


Figure 204: Selecting cryptography for CA

Step 24 : Checking the name of the CA and click Next.

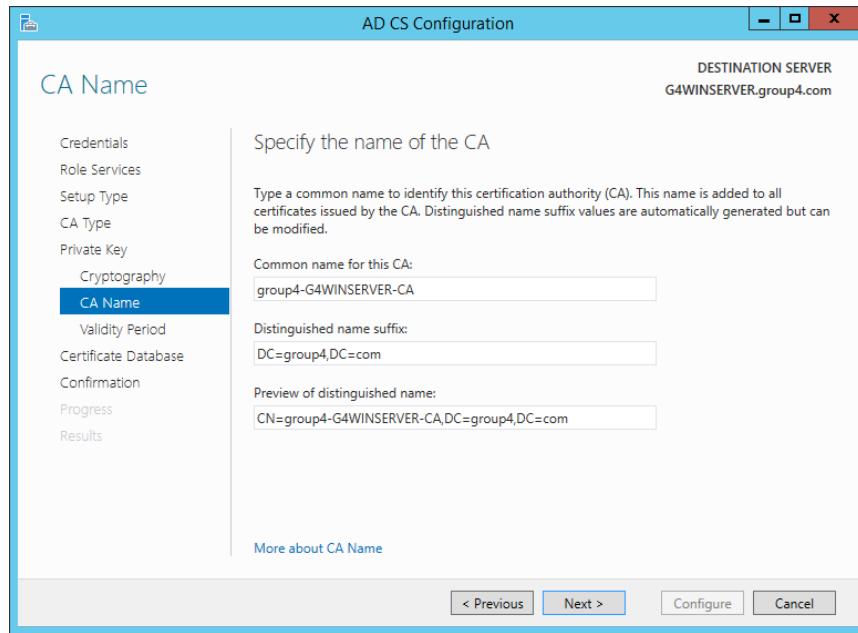


Figure 175: Specify CA name

Step 25 : Then, specify the validity period. In our case, we choose 5 Years.

After that, click Next.

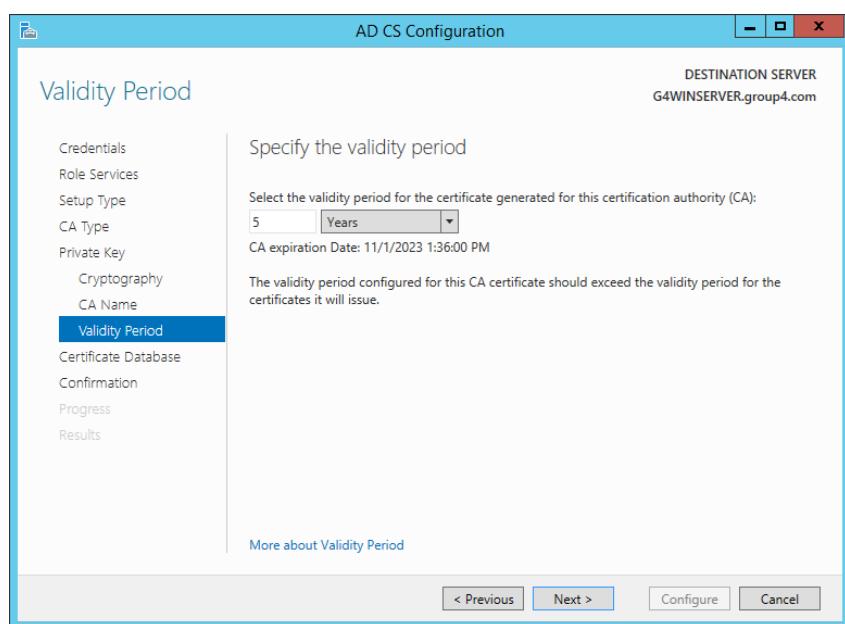


Figure 206: Specify validity period

Step 26 : For Certificate database, specify the database locations and click Next.

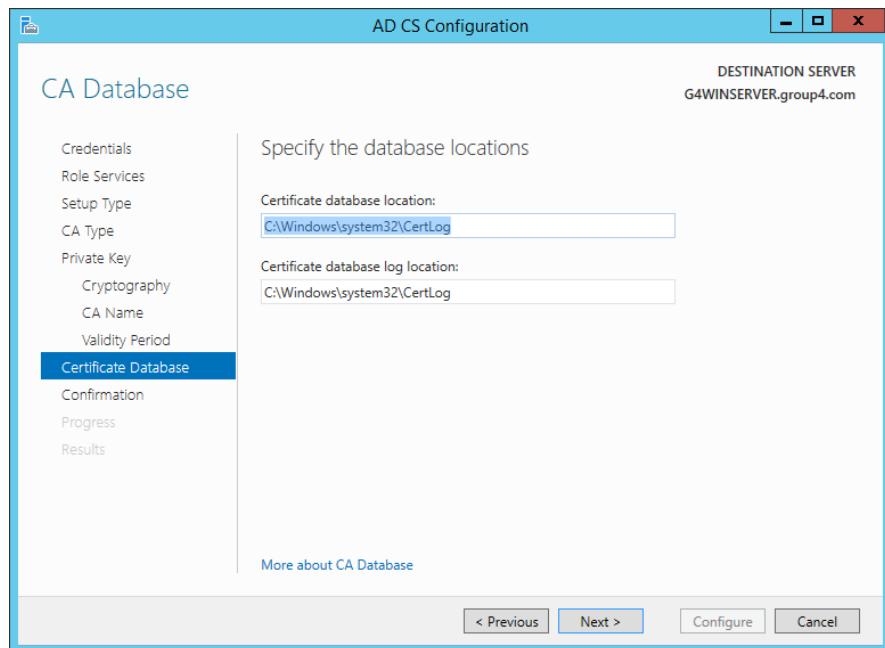


Figure 207: Specify database location

Step 27 : After looking for the confirmation, click on Configure. Click close after the configuration succeeded.

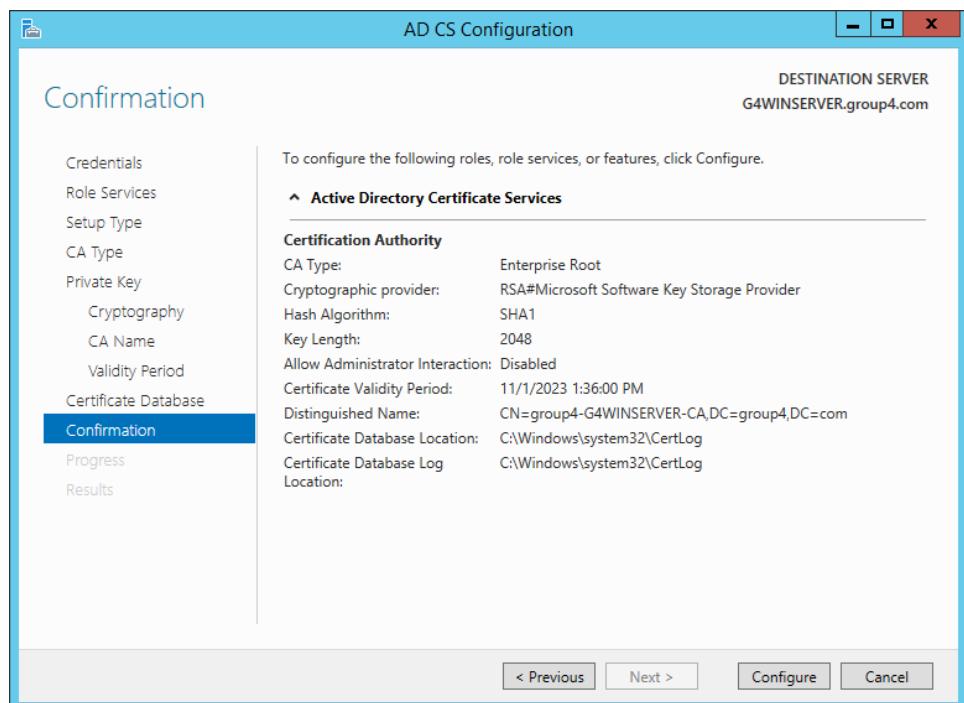


Figure 208: Confirmation of AD CS configuration

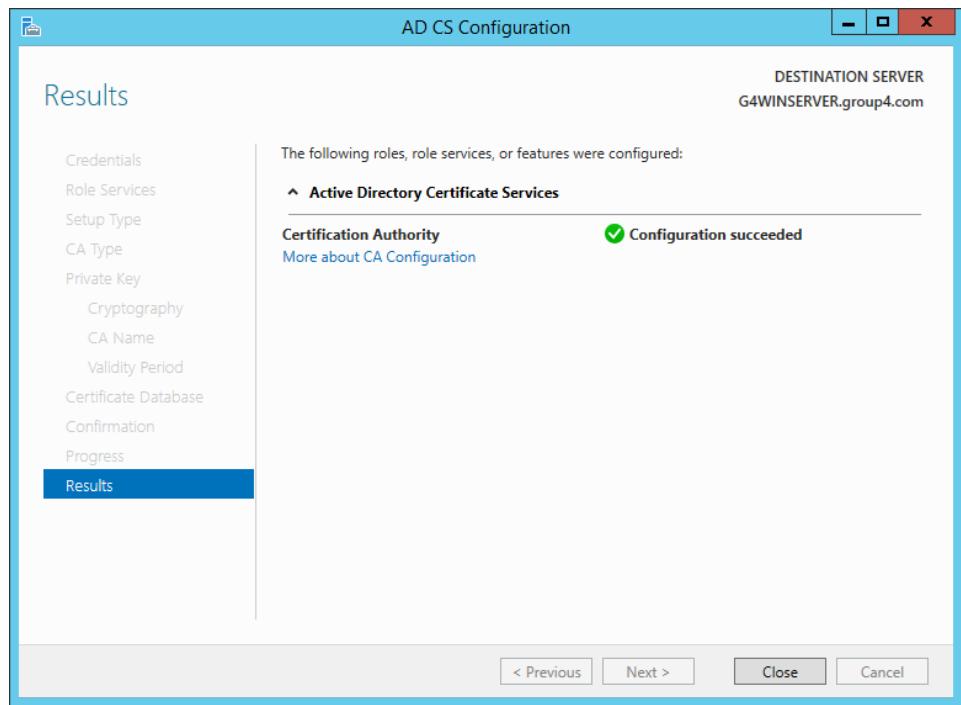


Figure 209: Results of AD CS Configuration

Step 28 : Then, click Windows (at keyboard) +R, search for mmc, and click enter. Then, the console root will show up. Then, right click on certificates and click on Add or Remove Snap-ins. After that, choose Certificates and Add it, then click OK.

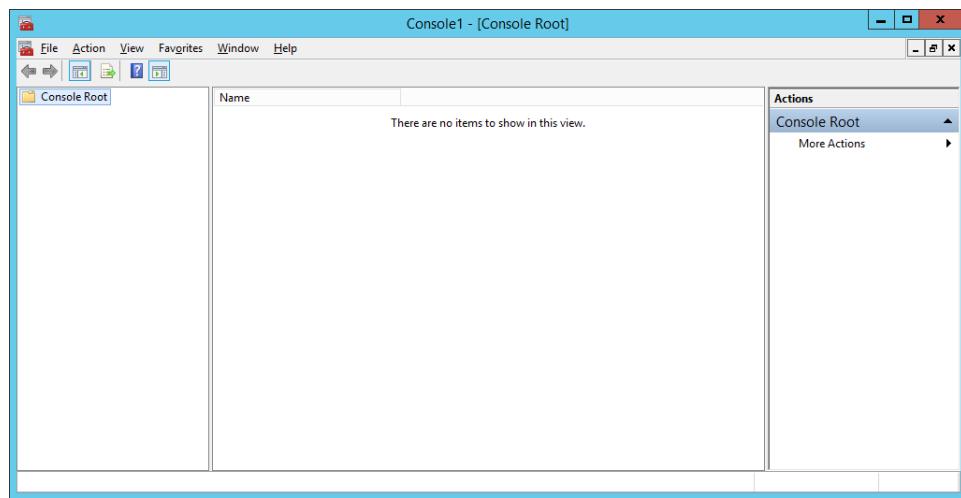


Figure 210: Console root page

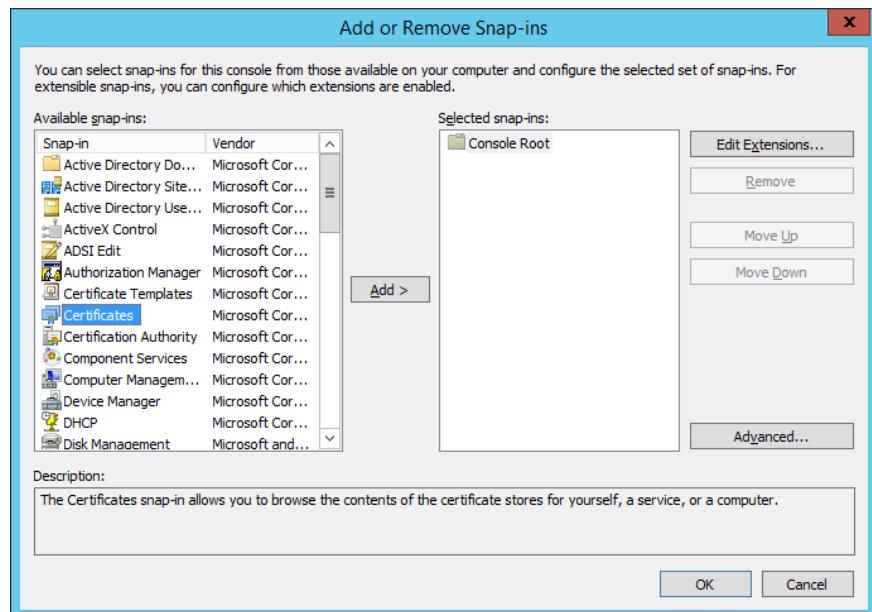


Figure 211: Adding or Remove snap-ins

Step 29 : For Certificates snap-in, click on Computer account. Then, click Next.

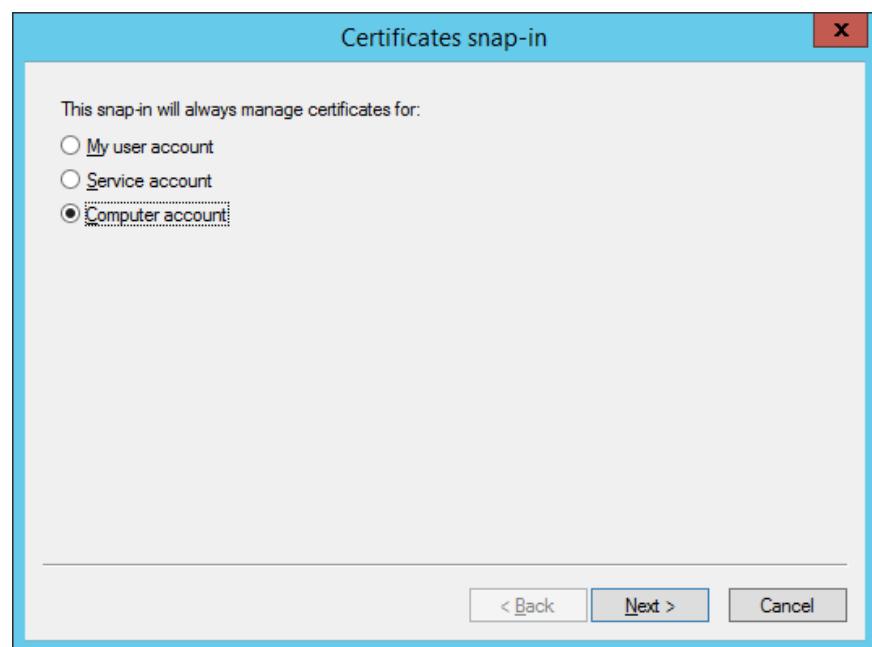


Figure 212: Choosing certificates snap in

Step 30 : Then, select the computer to manage this snap-in. (In our case, we choose Local computer). Click Finish.

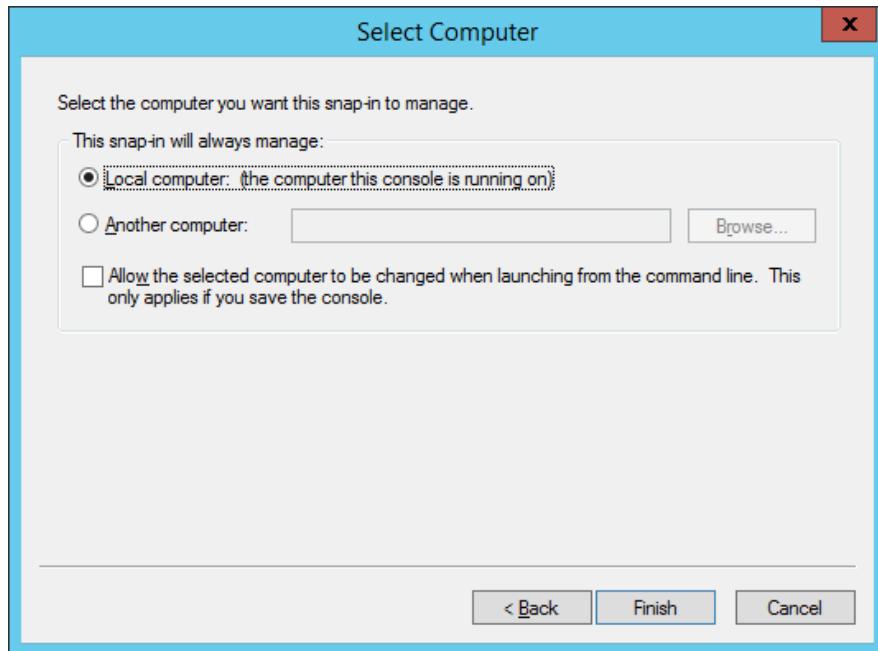


Figure 213: Select the computer to manage snap-in

Step 31 : Then, open mmc again, and load again the file. After that, right click on the certificate and choose All Tasks > Request New Certificate. Before begin the certificate enrolment, make sure that the computer is connected to the network and you have credentials that can be used to verify your right to obtain the certificate. After making sure of the following, click Next.

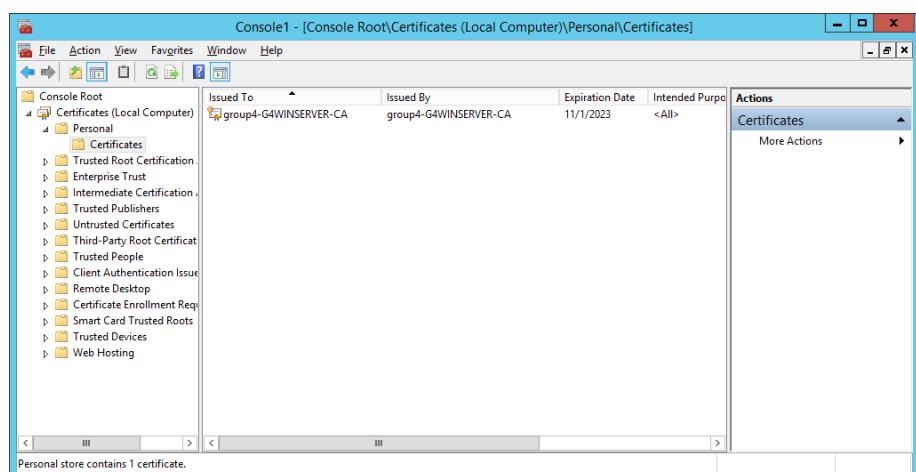


Figure 214: Loading the certificate into console

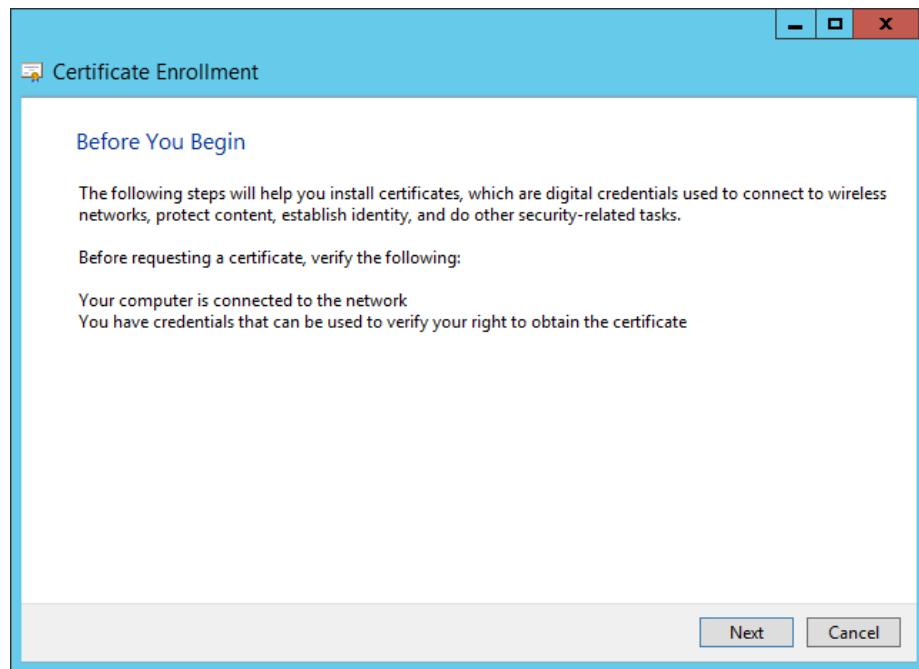


Figure 215: Beginning of certificate enrollment

Step 32 : The select certificate enrolment Policy and click Next.

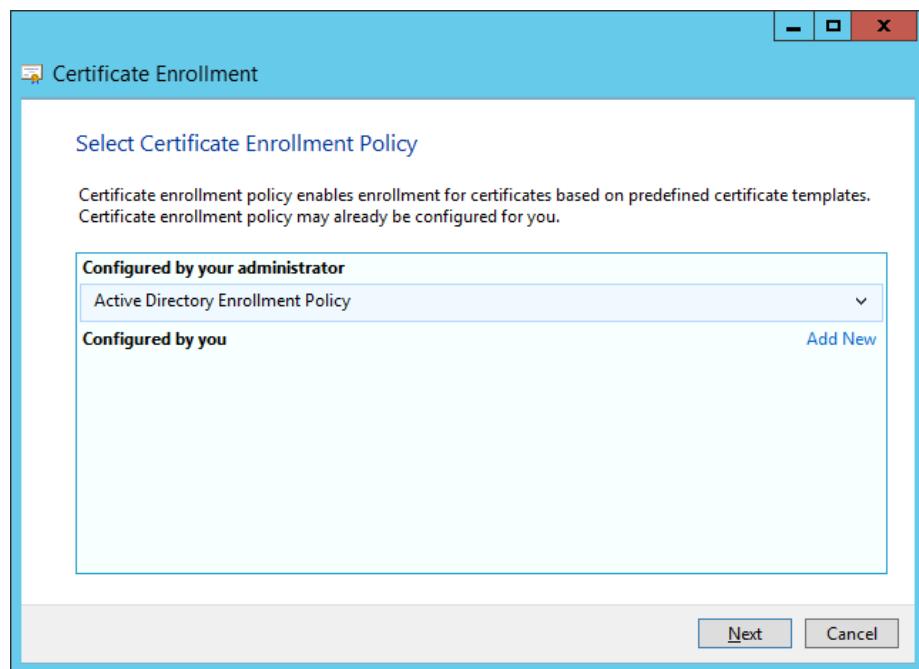


Figure 18: Selecting certificate enrollment policy

Step 33 : For Request Certificates, tick on Domain Controller and then, click Enroll. After that, the enrollment will be installed and then, click Finish.

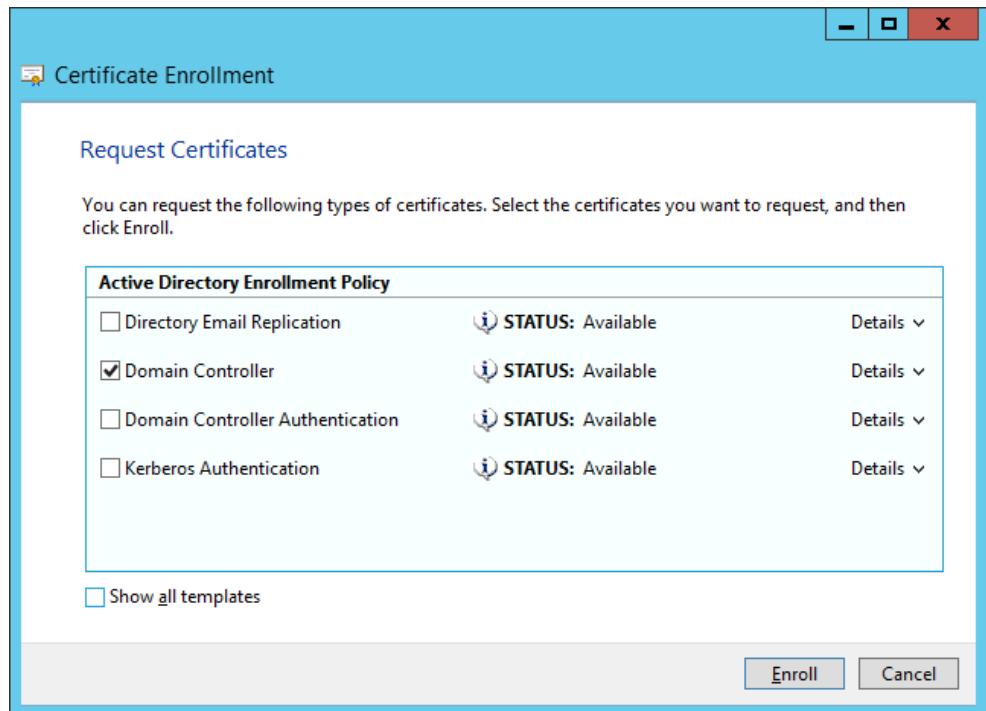


Figure 197: Requesting certificates

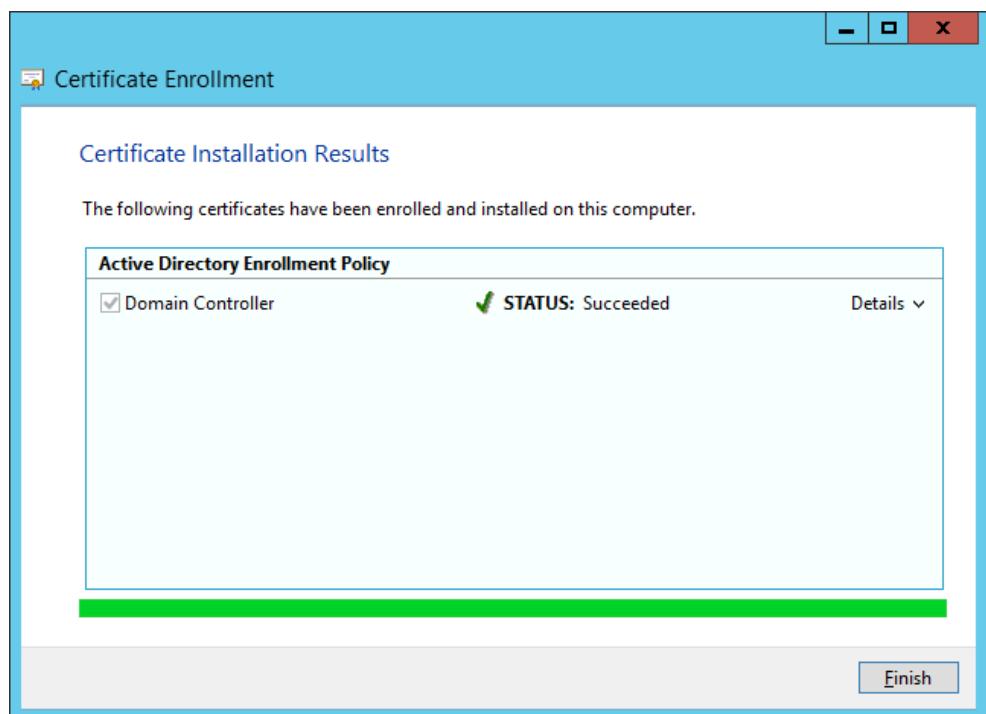


Figure 218: Installation of certificate

Step 34 : Go to Network Policy Server, select a configuration scenario (RADIUS server for 802.1X Wireless or Wired Connections). Then, click on Configure 802.1X.

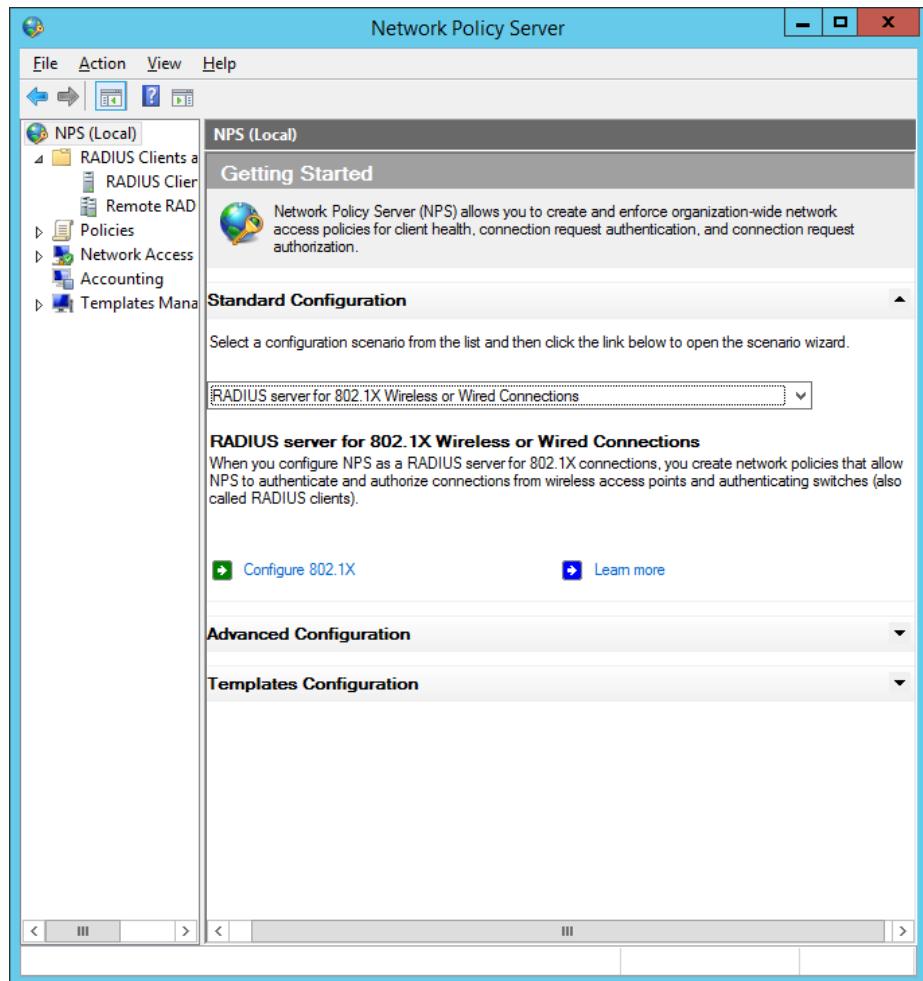


Figure 219: Network Policy Server page

Step 35 : Then, select Secure Wireless Connection for 802.1X Connections

Type and click Next > Next.

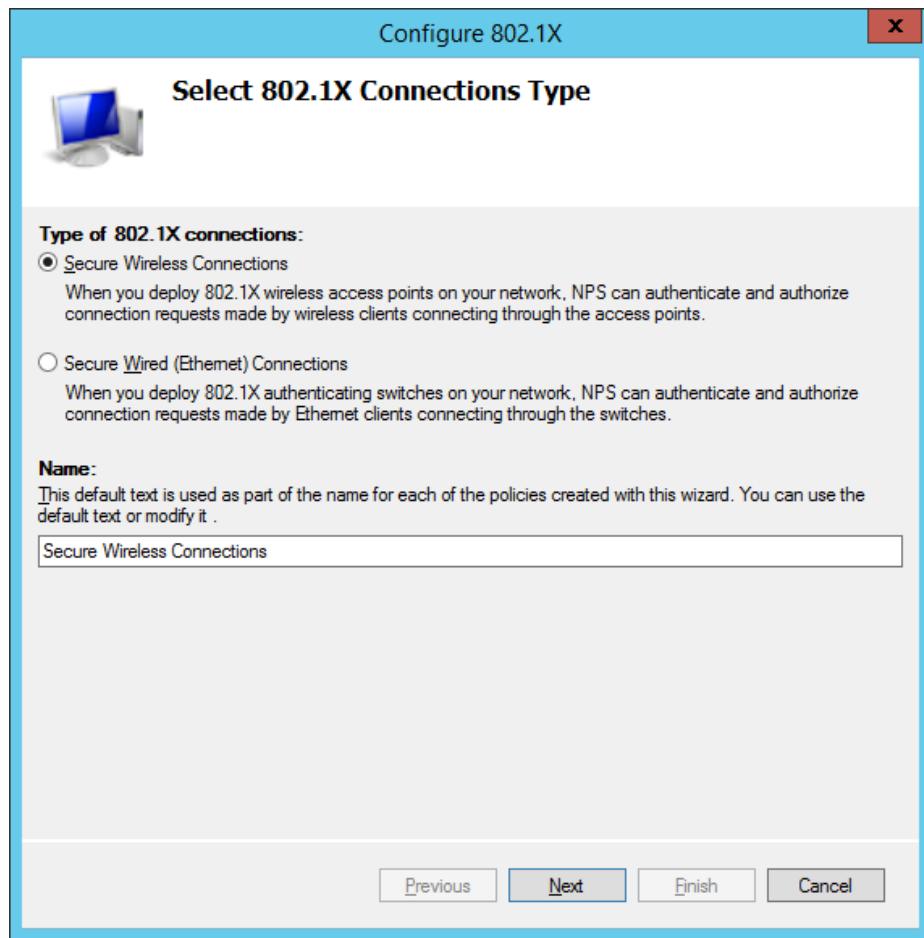


Figure 220: Select 802.1X connections type

Step 36 : Then, setting up New RADIUS Client. Set the Friendly name and the Address of the Access Point. Fill in the shared secret and click OK.

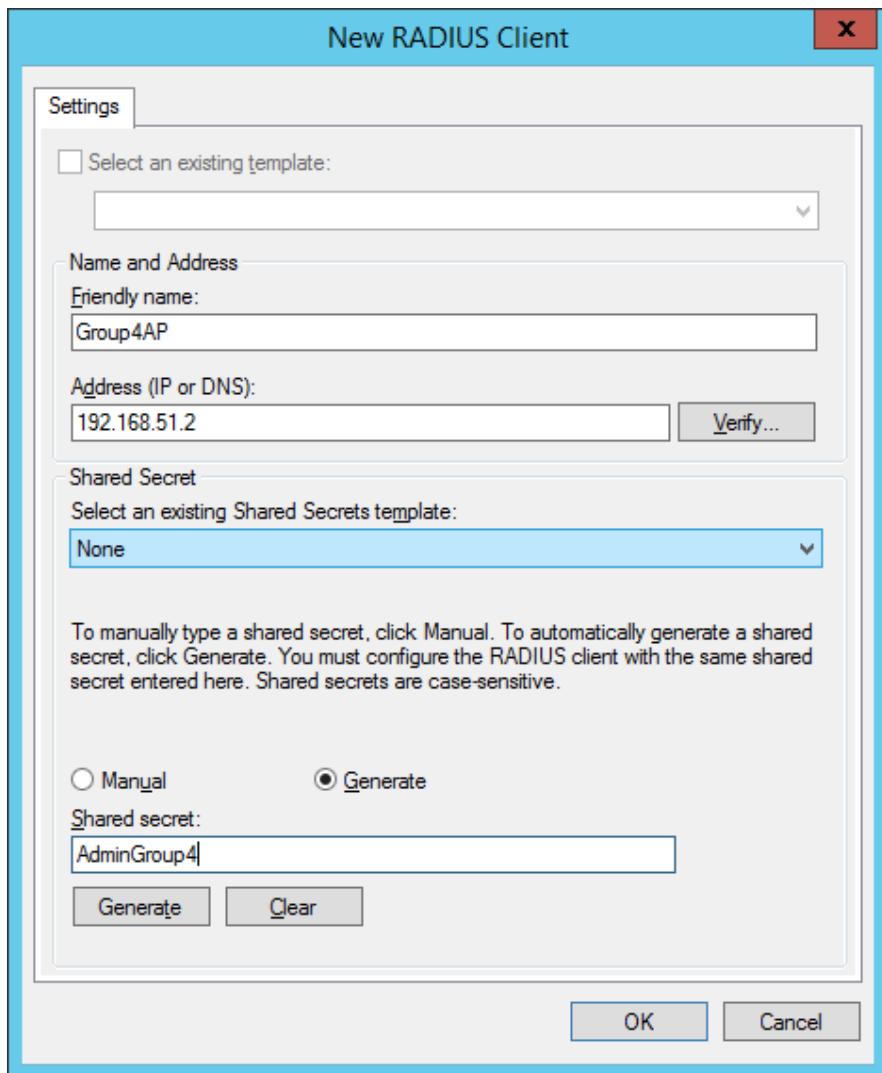


Figure 221: Setting up new RADIUS client

Step 37 : Make sure, to add the RADIUS client. After adding the RADIUS client, click Next.

Step 38 : During configuration of an authentication method, select the EAP type for this policy. Choose “Microsoft: Protected EAP (PEAP)”. Then, click Next.

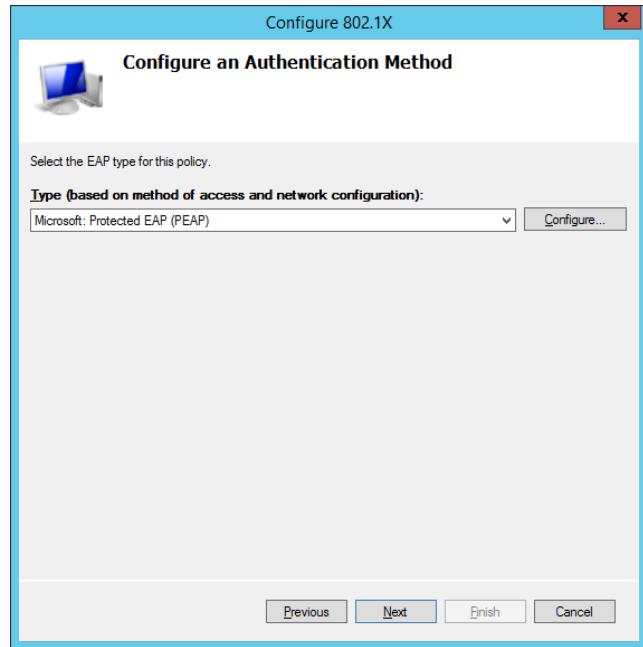


Figure 222: Select the EAP type for the policy

Step 39 : Then, specify the user groups for the group that have been created and add it (group4wifi). After that, click Next > Next.

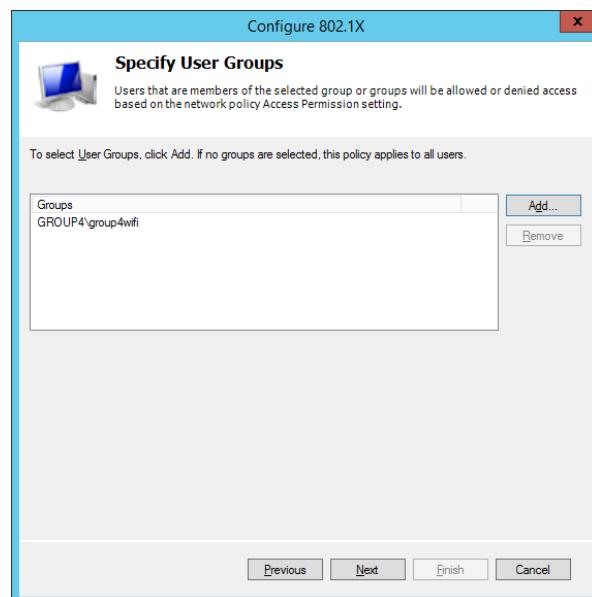


Figure 223: Specify user group

Step 40 : Upon completing configuration of 802.1X, it will tell you that you have successfully created policies and configured the RADIUS clients. Then, click Finish.

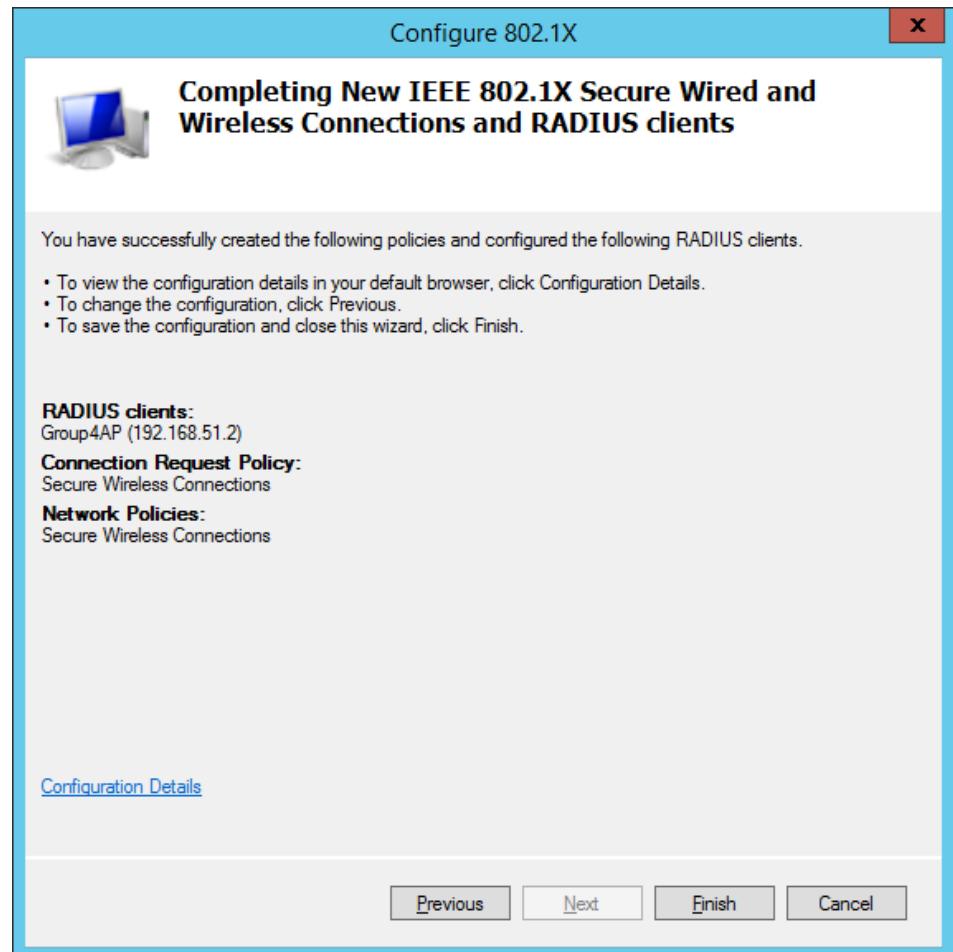


Figure 224: Completing the RADIUS client

Step 41 Then, go back to the console, right click the certificate that specific for Wireless Radius and click All Tasks > Export.

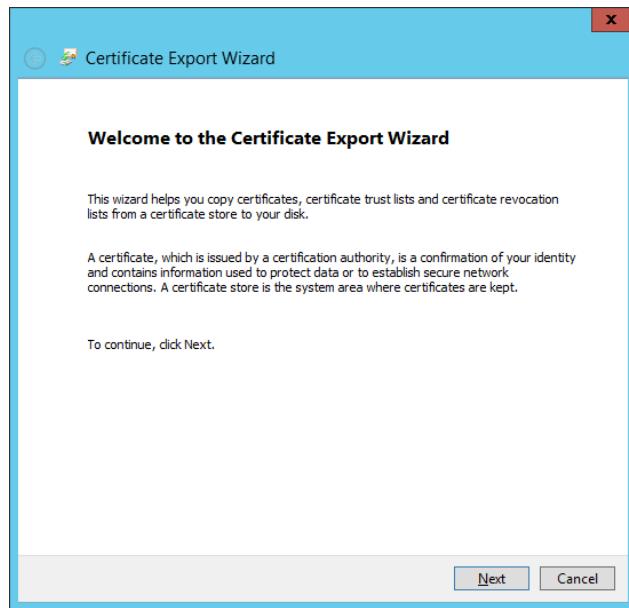


Figure 225: Certificate Export Wizard

Step 42 : In certificate export private key, choose No, do not export private key and click Next.

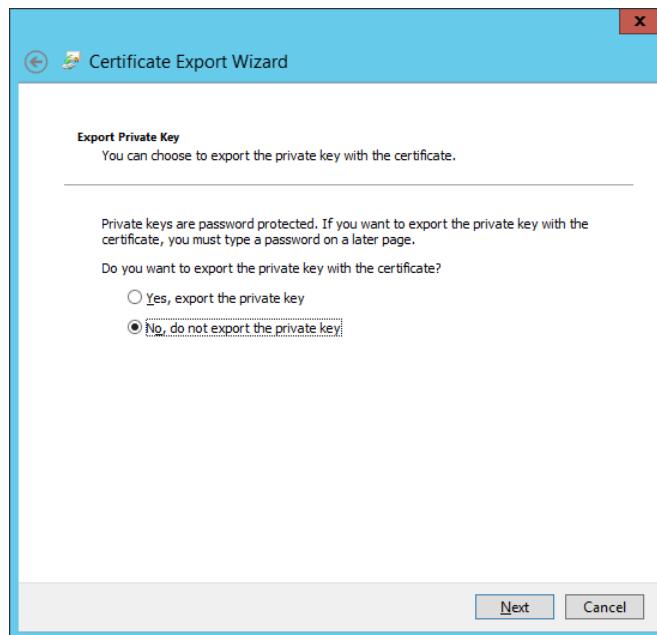


Figure 226: Choose whether to export the private key or not

Step 43 : In export file format, select DER encoded binary X.509 (.CER) and click Next. Then, specify the name of the file that wanted to export and click Next.

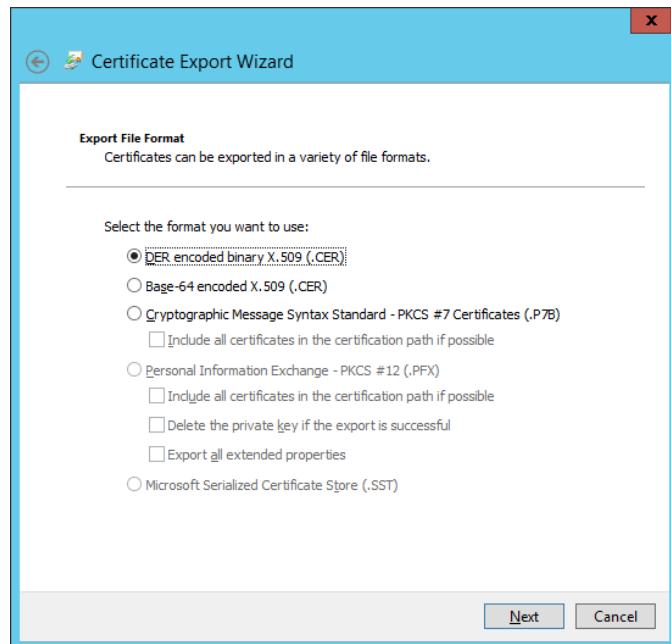


Figure 227: Selecting export file format

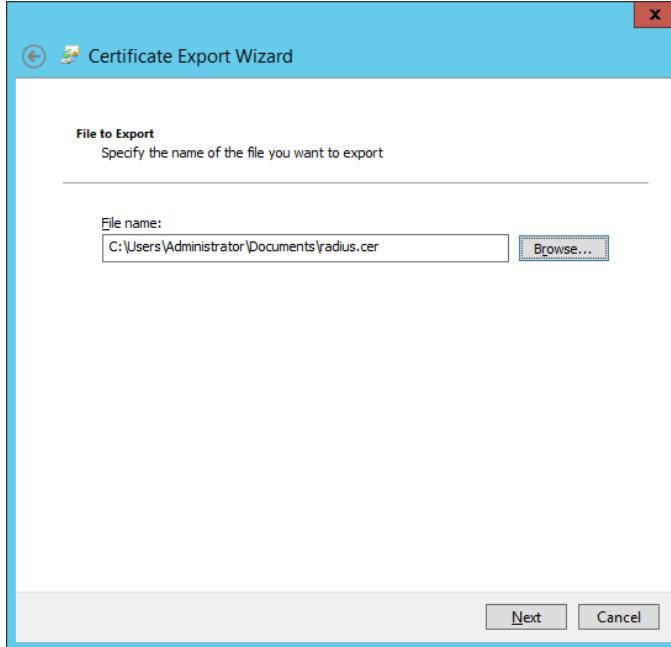


Figure 228: Specify the name of the file that wanted to be exported

Step 44 : Upon completing the certificate export wizard, it will tell all the settings that have been succeed. Then, click on Finish.



Figure 229: Completing the certificate export wizard

5.3.15 Access Control List (ACL)

Step 1 : Configure ACL (Access Control List) at Router.

```
G4Router(config)#access-list 104 permit tcp any 200.200.202.7 0.0.0.15 eq 443
G4Router(config)#access-list 104 deny tcp any 200.200.202.7 0.0.0.15 eq 22
G4Router(config)#access-list 104 deny tcp any 200.200.202.7 0.0.0.15 eq 80
G4Router(config)#access-list 104 deny tcp any host 200.200.202.6 eq 445
G4Router(config)#access-list 104 permit ip any any
G4Router(config)#int f0/1
G4Router(config-if)#ip access-group 104 in
```

Figure 230: Configuring ACL at Router

Step 2 : Show ACL configuration.

```
access-list 104 permit tcp any 200.200.202.0 0.0.0.15 eq 443
access-list 104 deny    tcp any 200.200.202.0 0.0.0.15 eq 22
access-list 104 deny    tcp any 200.200.202.0 0.0.0.15 eq www
access-list 104 deny    tcp any host 200.200.202.6 eq 445
access-list 104 permit ip any any
```

Figure 231: Showing ACL configuration

5.3.16 Secured FTP

Step 1 : Firstly, open Terminal in Fedora

Step 2 : Then, update all package to prevent from error during the installation of vsftpd using command “`dnf -y update`”

Figure 232: Updating all package before installation

Step 3 : Next, install vsftpd service in Fedora using command “`dnf -y install vsftpd`”.

```
Activities Terminal Thu 10:31
g4-15@kifly:/home/g4-15

File Edit View Search Terminal Help
[root@kifly g4-15]# dnf -y install vsftpd
Last metadata expiration check: 0:05:53 ago on Thu 04 Oct 2018 10:25:29 AM +08.
Dependencies resolved.
=====
Transaction Summary
=====
install 1 Package

Total download size: 178 k
Installed size: 354 k
Downloading Packages:
vsftpd-3.0.3-28.fc28.x86_64.rpm                                     953 kB/s | 178 kB   00:00
Total                                         100 kB/s | 178 kB   00:01

Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing                                           :
  Installing  : vsftpd-3.0.3-28.fc28.x86_64                               1/1
  Running scriptlet: vsftpd-3.0.3-28.fc28.x86_64                           1/1
  Verifying    : vsftpd-3.0.3-28.fc28.x86_64                               1/1

Installed:
  vsftpd.x86_64 3.0.3-28.fc28

Complete!
[root@kifly g4-15]#
```

Figure 233: Installing vsftpd service

Step 4 Get in vsftpd configuration and allow anonymous download using command “*nano/etc/vsftpd/vsftpd.conf*”

```

Activities Terminal Thu 10:42
g4-15@kifly:/home/g4-15
File Edit View Search Terminal Help /etc/vsftpd/vsftpd.conf Modified
GNU nano 2.9.8
# users to NOT chroot().
# (Warning! chroot'ing can be very dangerous. If using chroot, make sure that
# the user does not have write access to the top level directory within the
# chroot)
chroot_local_user=YES
chroot_list_enable=YES
# (default follows)
chroot_list_file=/etc/vsftpd/chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
ls_recurse_enable=YES
#
# When "listen" directive is enabled, vsftpd runs in standalone mode and
# listens on IPv4 sockets. This directive cannot be used in conjunction
# with the "listen_ipv6" directive.
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
# addresses) then you must run two copies of vsftpd with two configuration
# files.
# Make sure, that one of the listen options is commented !!
listen_ipv6=YES
pam_service_name=vsftpd
userlist_enable=YES
File Name to Write: /etc/vsftpd/vsftpd.conf
^D Get Help M-D DOS Format M-A Append M-B Backup File
^C Cancel M-M Mac Format M-P Prepend T To Files
Page 4 of 4 | 0 words, 0 characters | Default Style | English (USA) | | | | | 100%

```

Figure 234: Get in vsftpd configuration

Step 5 : Then, restart and enable service vsftpd with creation of system link in user file.

```

Activities Terminal Thu 10:43
g4-15@kifly:/home/g4-15
File Edit View Search Terminal Help
[root@kifly g4-15]# sudo nano /etc/vsftpd/vsftpd.conf
[root@kifly g4-15]# systemctl restart vsftpd
[root@kifly g4-15]# systemctl enable vsftpd
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /usr/lib/systemd/system/vsftpd.service.
[root@kifly g4-15]#

```

Figure 235: Restarting and enabling service

Step 6 : Then, port 21 is needed to be add for the purpose to secure ftp into firewall to prevent from that port blocked.

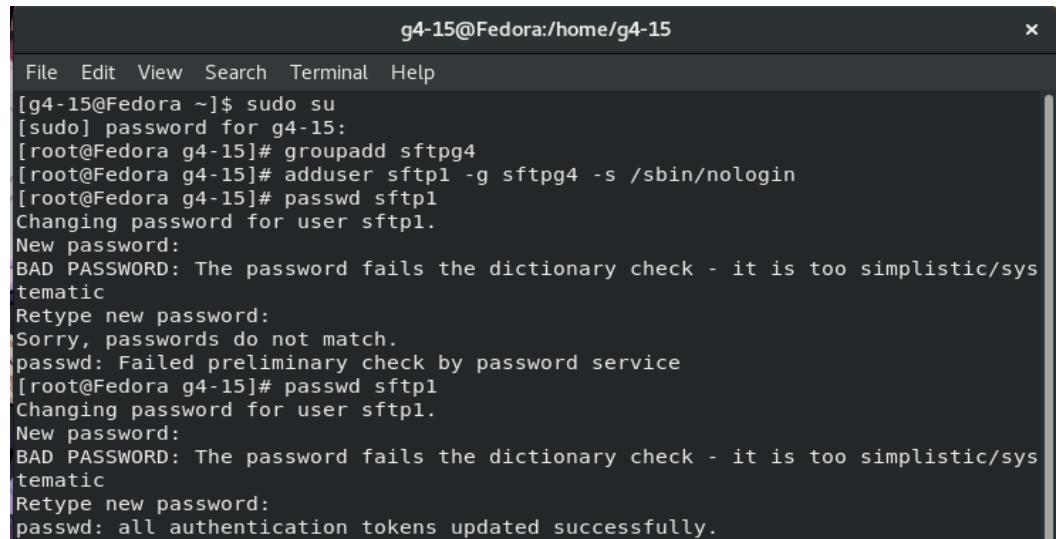
```

Activities Terminal Thu 10:49
g4-15@kifly:/home/g4-15
File Edit View Search Terminal Help
[root@kifly g4-15]# sudo nano /etc/vsftpd/vsftpd.conf
[root@kifly g4-15]# systemctl restart vsftpd
[root@kifly g4-15]# systemctl enable vsftpd
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /usr/lib/systemd/system/vsftpd.service.
[root@kifly g4-15]# firewall-cmd --permanent --add-port=21/tcp
success
[root@kifly g4-15]# firewall-cmd --reload
success
[root@kifly g4-15]#

```

Figure 236: Adding port 21 to secure ftp

Step 7 : Next, create group and user that can only access into secure ftp.



```
g4-15@Fedora:/home/g4-15
File Edit View Search Terminal Help
[g4-15@Fedora ~]$ sudo su
[sudo] password for g4-15:
[root@Fedora g4-15]# groupadd sftpg4
[root@Fedora g4-15]# adduser sftp1 -g sftpg4 -s /sbin/nologin
[root@Fedora g4-15]# passwd sftp1
Changing password for user sftp1.
New password:
BAD PASSWORD: The password fails the dictionary check - it is too simplistic/systematic
Retype new password:
Sorry, passwords do not match.
passwd: Failed preliminary check by password service
[root@Fedora g4-15]# passwd sftp1
Changing password for user sftp1.
New password:
BAD PASSWORD: The password fails the dictionary check - it is too simplistic/systematic
Retype new password:
passwd: all authentication tokens updated successfully.
```

Figure 237: Create group and user

Step 8 : Make directory at home folder which is only for secure ftp sharing the file.

```
[root@Fedora g4-15]# mkdir /home/sharefiles/
```

Figure 238: Making directory

Step 9 : Change the mode of secure ftp so that only the one who get permission can access the secure ftp share folder.

```
[root@Fedora g4-15]# chmod g+r /home/sharefiles/
[root@Fedora g4-15]# mkdir -p /home/sharefiles/files/
[root@Fedora g4-15]# chmod g+rwx /home/sharefiles/files/
[root@Fedora g4-15]# chgrp -R sftpg4 /home/sharefiles/
```

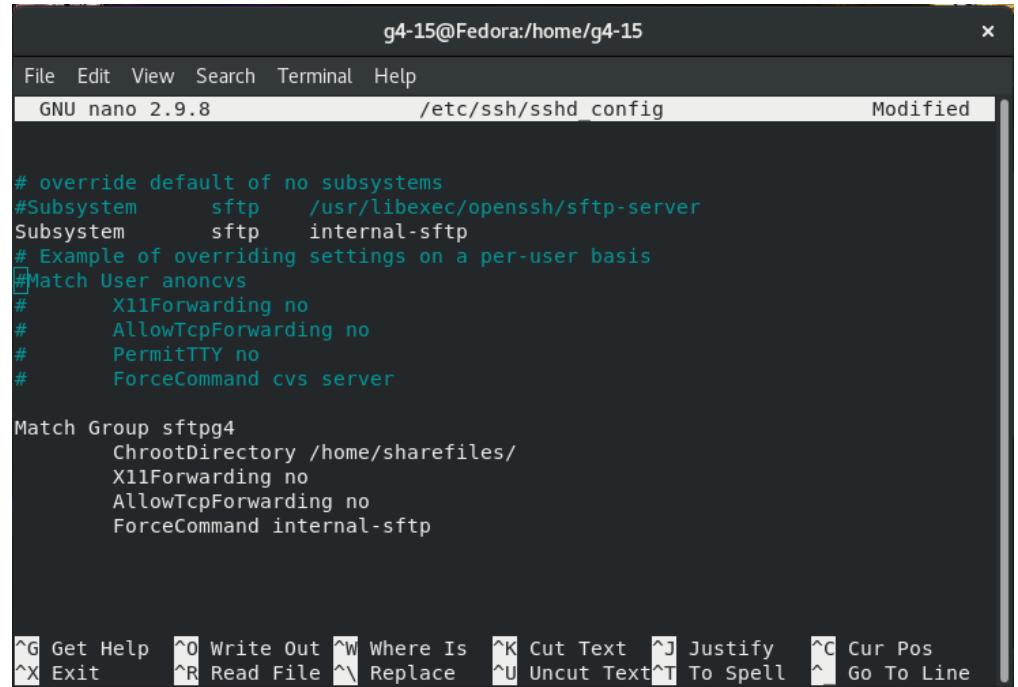
Figure 239: Changing the mode of secure ftp

Step 10 : Then, go into SSH file to split the secure ftp access and SSH access using this command.

```
[root@Fedora g4-15]# nano /etc/ssh/sshd_config
[root@Fedora g4-15]#
```

Figure 240: Get into sshd config

Step 11 : Insert comment at subsystem sftp that shared the permission with SSH and new subsystem of the internal sftp only. After that, include specific group for secure ftp with point the file that get permission to access.



```
# override default of no subsystems
#Subsystem      sftp      /usr/libexec/openssh/sftp-server
Subsystem      sftp      internal-sftp
# Example of overriding settings on a per-user basis
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server

Match Group sftpg4
    ChrootDirectory /home/sharefiles/
    X11Forwarding no
    AllowTcpForwarding no
    ForceCommand internal-sftp
```

Figure 20: Inserting comment at subsystem sftp

Step 12 : Restart the SSH service before using secure ftp.

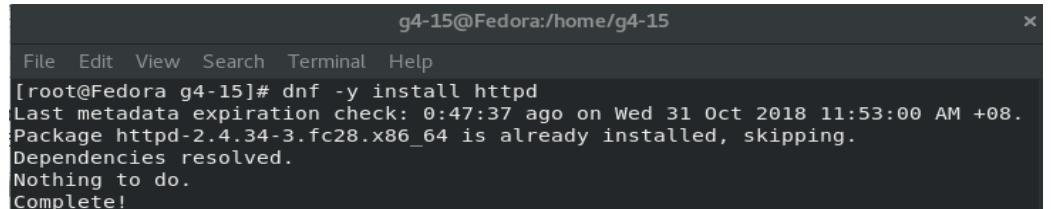
```
[root@Fedora g4-15]# systemctl restart sshd
[root@Fedora g4-15]#
```

Figure 242: Restarting SSH service

5.3.17 Web, SSL & Virtual Hosting

5.3.17.1 Web

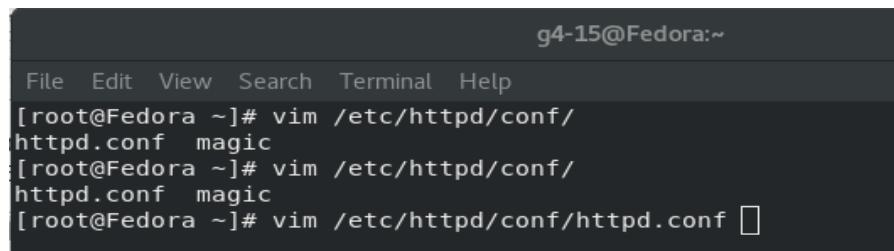
Step 1 : Install http service packet using command “*dnf -y install httpd*”.



```
g4-15@Fedora:/home/g4-15
File Edit View Search Terminal Help
[root@Fedora g4-15]# dnf -y install httpd
Last metadata expiration check: 0:47:37 ago on Wed 31 Oct 2018 11:53:00 AM +08.
Package httpd-2.4.34-3.fc28.x86_64 is already installed, skipping.
Dependencies resolved.
Nothing to do.
Complete!
```

Figure 243: Installing http service packet

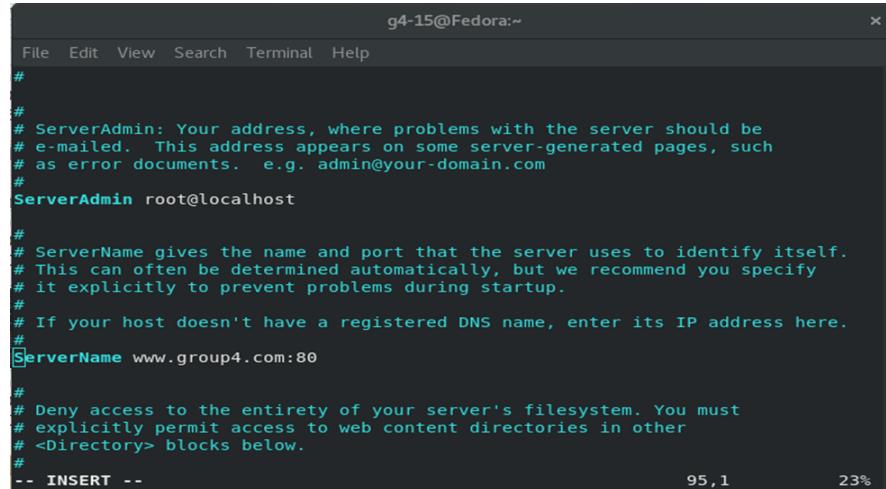
Step 2 : Then, open the configuration file of httpd and edit the configuration by using command below.



```
g4-15@Fedora:~
File Edit View Search Terminal Help
[root@Fedora ~]# vim /etc/httpd/conf/
httpd.conf  magic
[root@Fedora ~]# vim /etc/httpd/conf/
httpd.conf  magic
[root@Fedora ~]# vim /etc/httpd/conf/httpd.conf □
```

Figure 244: Edit the configuration file of httpd

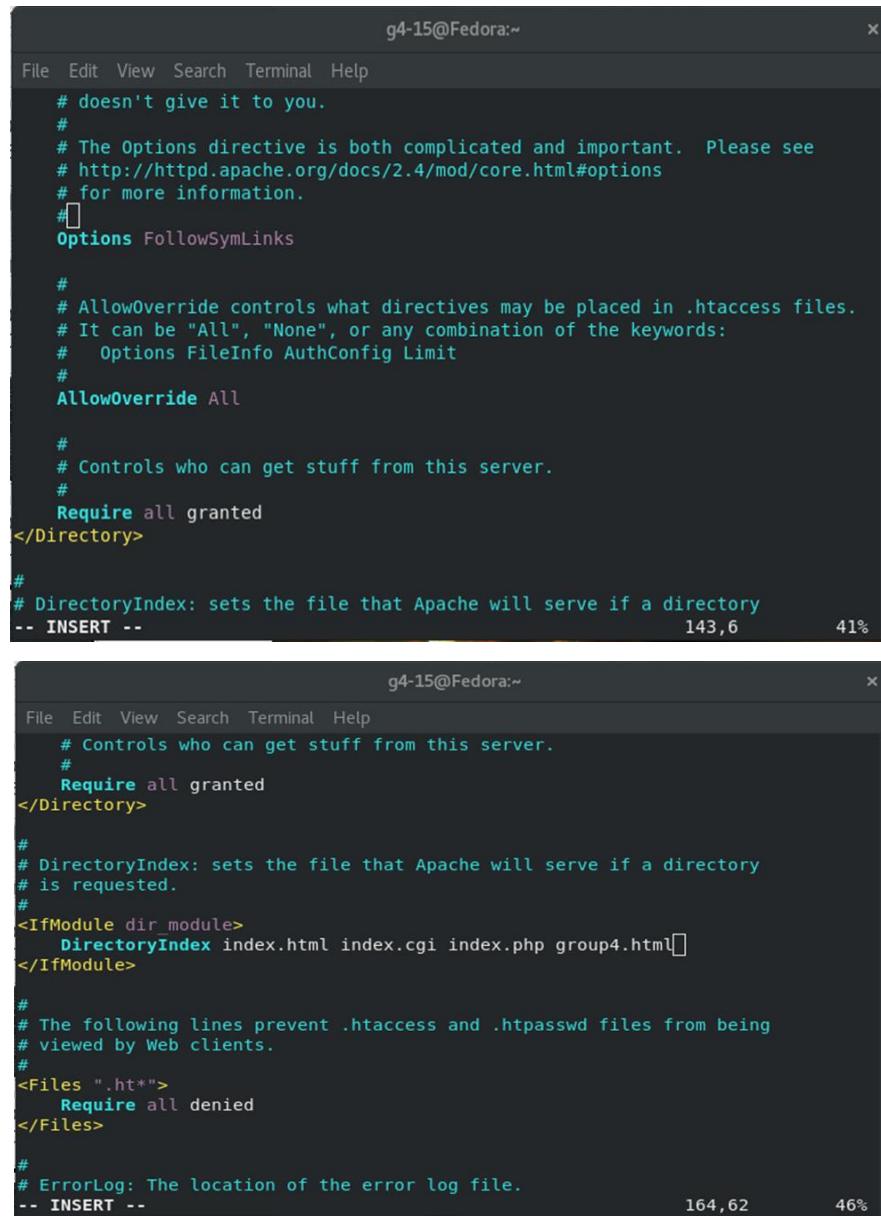
Step 3 : Configure httpd file. Change the correct web name at ServerName section.



```
g4-15@Fedora:~
File Edit View Search Terminal Help
#
#
# ServerAdmin: Your address, where problems with the server should be
# e-mailed. This address appears on some server-generated pages, such
# as error documents. e.g. admin@your-domain.com
#
ServerAdmin root@localhost
#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
ServerName www.group4.com:80
#
# Deny access to the entirety of your server's filesystem. You must
# explicitly permit access to web content directories in other
# <Directory> blocks below.
#
-- INSERT --          95,1          23%
```

Figure 245: Configure the httpd

Step 4 : Change the status AllowOverride to All.



The image shows two screenshots of a terminal window titled "g4-15@Fedora:~". Both screenshots display the Apache configuration file (httpd.conf) in a code editor. The configuration includes directives like "FollowSymLinks", "AllowOverride All", and "Require all granted". The bottom screenshot shows the addition of the "DirectoryIndex" directive within an "IfModule" block. The status bar at the bottom right of both windows indicates the file size (143,6 or 164,62) and the current line number (41% or 46%).

```
# doesn't give it to you.
#
# The Options directive is both complicated and important. Please see
# http://httpd.apache.org/docs/2.4/mod/core.html#options
# for more information.
# Options FollowSymLinks

#
# AllowOverride controls what directives may be placed in .htaccess files.
# It can be "All", "None", or any combination of the keywords:
#   Options FileInfo AuthConfig Limit
#
AllowOverride All

#
# Controls who can get stuff from this server.
#
Require all granted
</Directory>

#
# DirectoryIndex: sets the file that Apache will serve if a directory
-- INSERT --
```



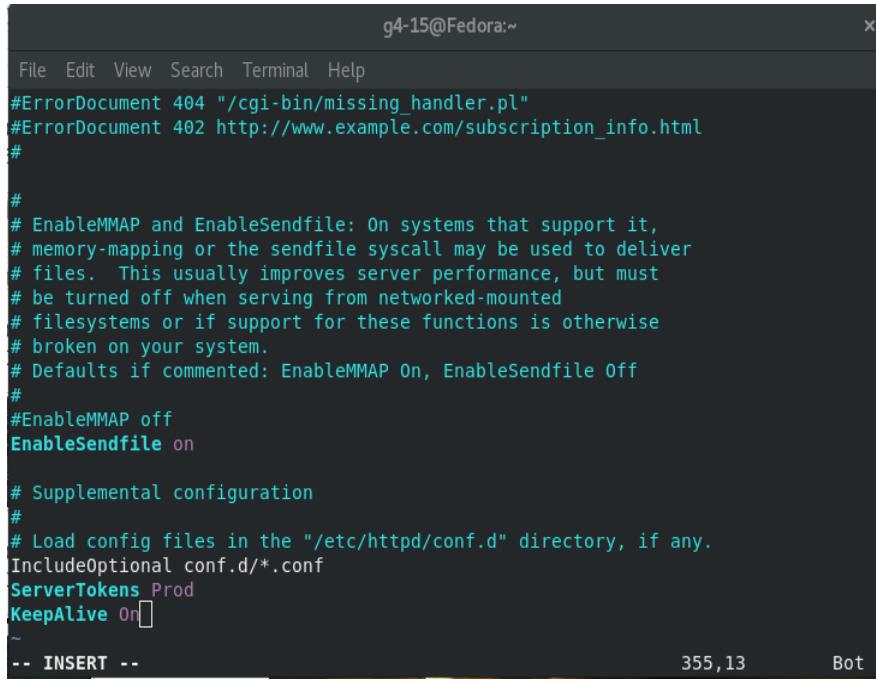
```
# Controls who can get stuff from this server.
#
# Require all granted
</Directory>

#
# DirectoryIndex: sets the file that Apache will serve if a directory
# is requested.
#
<IfModule dir_module>
    DirectoryIndex index.html index.cgi index.php group4.html
</IfModule>

#
# The following lines prevent .htaccess and .htpasswd files from being
# viewed by Web clients.
#
<Files ".ht*">
    Require all denied
</Files>

#
# ErrorLog: The location of the error log file.
-- INSERT --
```

Figure 246: Changing the status



The screenshot shows a terminal window titled "g4-15@Fedora:~". The window contains the configuration file for the Apache HTTP Server (httpd). The configuration includes various directives such as ErrorDocument, EnableMMAP, EnableSendfile, and ServerTokens. A cursor is visible at the end of the "KeepAlive On" directive. The status bar at the bottom right shows "355,13" and "Bot".

```
#ErrorDocument 404 "/cgi-bin/missing_handler.pl"
#ErrorDocument 402 http://www.example.com/subscription_info.html
#
#
# EnableMMAP and EnableSendfile: On systems that support it,
# memory-mapping or the sendfile syscall may be used to deliver
# files. This usually improves server performance, but must
# be turned off when serving from networked-mounted
# filesystems or if support for these functions is otherwise
# broken on your system.
# Defaults if commented: EnableMMAP On, EnableSendfile Off
#
#EnableMMAP off
EnableSendfile on

# Supplemental configuration
#
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf
ServerTokens Prod
KeepAlive On
~
-- INSERT --
```

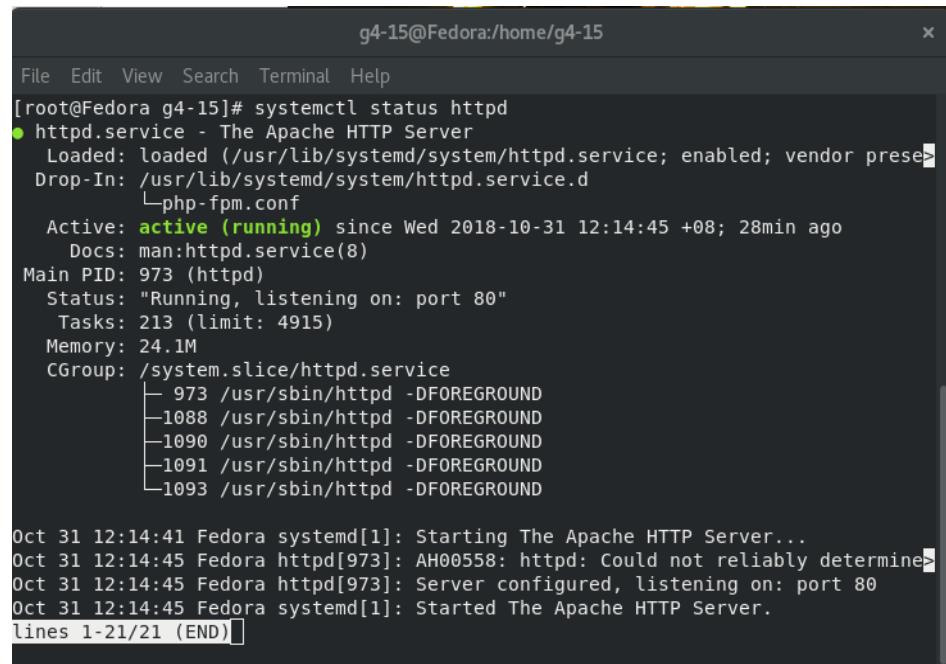
Figure 247: Configuration file of httpd

Step 5 : Restart HTTP service and allow firewall to access the web.

```
[root@Fedora g4-15]# firewall-cmd --permanent --add-port=80/tcp
Warning: ALREADY_ENABLED: 80:tcp
success
[root@Fedora g4-15]# firewall-cmd --permanent --add-port=443/tcp
success
[root@Fedora g4-15]# firewall-cmd --reload
success
[root@Fedora g4-15]# systemctl start httpd
[root@Fedora g4-15]# systemctl enable httpd
[root@Fedora g4-15]#
```

Figure 248: Restart http service and allow the firewall

Step 6 : Check the status of httpd service by using command as stated below.



```
g4-15@Fedora:/home/g4-15
File Edit View Search Terminal Help
[root@Fedora g4-15]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor presen>
   Drop-In: /usr/lib/systemd/system/httpd.service.d
             └─php-fpm.conf
   Active: active (running) since Wed 2018-10-31 12:14:45 +08; 28min ago
     Docs: man:httpd.service(8)
   Main PID: 973 (httpd)
      Status: "Running, listening on: port 80"
        Tasks: 213 (limit: 4915)
       Memory: 24.1M
      CGroup: /system.slice/httpd.service
              ├─ 973 /usr/sbin/httpd -DFOREGROUND
              ├─1088 /usr/sbin/httpd -DFOREGROUND
              ├─1090 /usr/sbin/httpd -DFOREGROUND
              ├─1091 /usr/sbin/httpd -DFOREGROUND
              ├─1093 /usr/sbin/httpd -DFOREGROUND

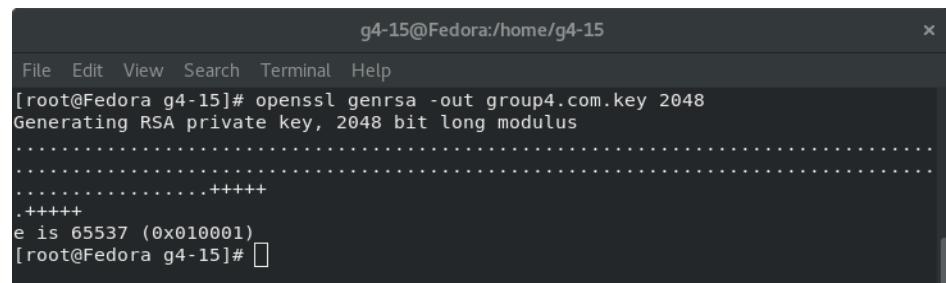
Oct 31 12:14:41 Fedora systemd[1]: Starting The Apache HTTP Server...
Oct 31 12:14:45 Fedora httpd[973]: AH00558: httpd: Could not reliably determine the parent PID of this process.
Oct 31 12:14:45 Fedora httpd[973]: Server configured, listening on: port 80
Oct 31 12:14:45 Fedora systemd[1]: Started The Apache HTTP Server.
lines 1-21/21 (END)
```

Figure 249: Status of httpd

5.3.17.2 Secure Socket Layer (SSL)

Step 1 : Firstly, open the Terminal in Fedora.

Step 2 : Then, go to certification folder and create key for web server.



```
g4-15@Fedora:/home/g4-15
File Edit View Search Terminal Help
[root@Fedora g4-15]# openssl genrsa -out group4.com.key 2048
Generating RSA private key, 2048 bit long modulus
.....+....+
e is 65537 (0x010001)
[root@Fedora g4-15]#
```

Figure 250: Creating key for web server in certification folder

Step 3 : Then, create csr for your group. Fill all the blank and follow the instruction.

The screenshot shows a terminal window titled 'g4-15@Fedora:/home/g4-15'. The user runs the command 'openssl req -new -key group4.com.key -out group4.com.csr -sha512'. The terminal then prompts for various certificate details:

- Country Name (2 letter code) [XX]:MY
- State or Province Name (full name) []:Kuala Lumpur
- Locality Name (eg, city) [Default City]:
- Organization Name (eg, company) [Default Company Ltd]:group4.com
- Organizational Unit Name (eg, section) []:OU
- Common Name (eg, your name or your server's hostname) []:group4.com
- Email Address []:mail.gropu4.com

After entering the details, the terminal asks for extra attributes:

- Please enter the following 'extra' attributes
- to be sent with your certificate request

The user enters a challenge password and an optional company name, both followed by an empty square bracket. The command concludes with '[root@Fedora g4-15]#'.
[root@Fedora g4-15]# openssl req -new -key group4.com.key -out group4.com.csr -sha512
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [XX]:MY
State or Province Name (full name) []:Kuala Lumpur
Locality Name (eg, city) [Default City]:
Organization Name (eg, company) [Default Company Ltd]:group4.com
Organizational Unit Name (eg, section) []:OU
Common Name (eg, your name or your server's hostname) []:group4.com
Email Address []:mail.gropu4.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:g4123456
An optional company name []:
[root@Fedora g4-15]#

Figure 251: Creating csr for the group

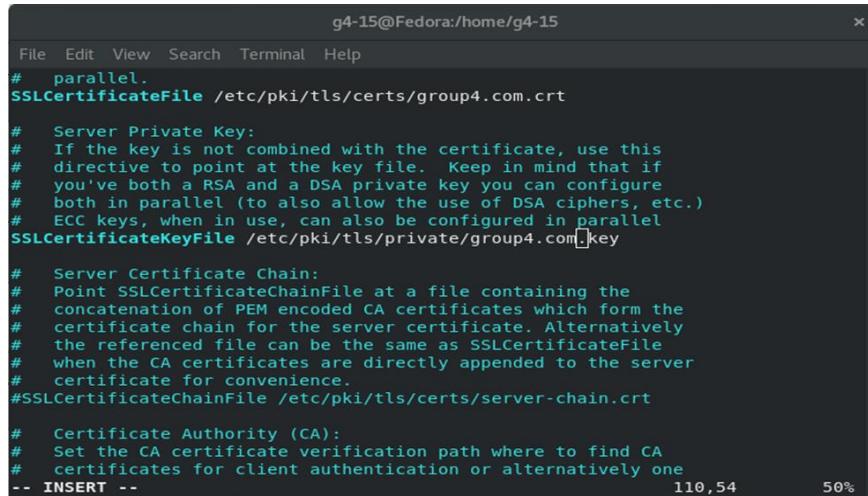
Step 4 : Set all the implementation that have been done at previous picture.

The screenshot shows a terminal window titled 'g4-15@Fedora:/home/g4-15'. The user runs the command 'openssl x509 -req -days 365 -in group4.com.csr -signkey group4.com.key -out group4.com.crt -sha512'. The terminal displays the certificate details and the generation of the private key:

Signature ok
subject=C = MY, ST = Kuala Lumpur, L = Default City, O = group4.com, OU = OU, CN = group4.com, emailAddress = mail.gropu4.com
Getting Private key
[root@Fedora g4-15]#

Figure 252: Setting all the implementation

Step 5 : Make the SSL certificate at correct location to apply group4.com key and group4.com crt.



```

g4-15@Fedora:/home/g4-15
File Edit View Search Terminal Help
# parallel.
SSLCertificateFile /etc/pki/tls/certs/group4.com.crt

# Server Private Key:
# If the key is not combined with the certificate, use this
# directive to point at the key file. Keep in mind that if
# you've both a RSA and a DSA private key you can configure
# both in parallel (to also allow the use of DSA ciphers, etc.)
# ECC keys, when in use, can also be configured in parallel
SSLCertificateKeyFile /etc/pki/tls/private/group4.com.key

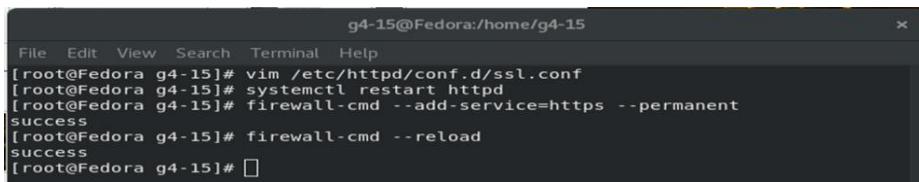
# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM encoded CA certificates which form the
# certificate chain for the server certificate. Alternatively
# the referenced file can be the same as SSLCertificateFile
# when the CA certificates are directly appended to the server
# certificate for convenience.
#SSLCertificateChainFile /etc/pki/tls/certs/server-chain.crt

# Certificate Authority (CA):
# Set the CA certificate verification path where to find CA
# certificates for client authentication or alternatively one
-- INSERT --                                         110,54      50%

```

Figure 253: Making SSL certificate at correct location

Step 6 : Reload the SSL to accessing the web using command “systemctl restart httpd”.



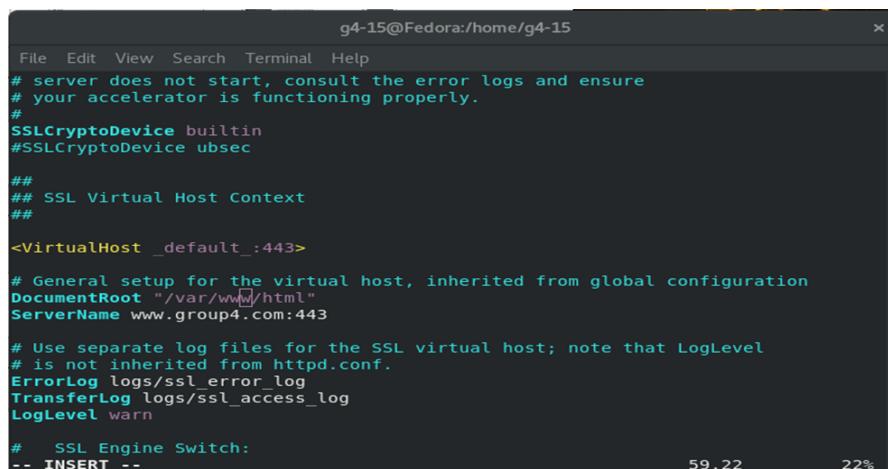
```

g4-15@Fedora:/home/g4-15
File Edit View Search Terminal Help
[root@Fedora g4-15]# vim /etc/httpd/conf.d/ssl.conf
[root@Fedora g4-15]# systemctl restart httpd
[root@Fedora g4-15]# firewall-cmd --add-service=https --permanent
success
[root@Fedora g4-15]# firewall-cmd --reload
success
[root@Fedora g4-15]#

```

Figure 254: Reloading the SSL

Step 7 : Set all the SSL Protocols as shown.



```

g4-15@Fedora:/home/g4-15
File Edit View Search Terminal Help
# server does not start, consult the error logs and ensure
# your accelerator is functioning properly.
#
SSLCryptoDevice builtin
#SSLCryptoDevice ubsec

##
## SSL Virtual Host Context
##

<VirtualHost _default_:443>
# General setup for the virtual host, inherited from global configuration
DocumentRoot "/var/www/html"
ServerName www.group4.com:443

# Use separate log files for the SSL virtual host; note that LogLevel
# is not inherited from httpd.conf.
ErrorLog logs/ssl_error_log
TransferLog logs/ssl_access_log
LogLevel warn

# SSL Engine Switch:
-- INSERT --

```

Figure 255: Setting the SSL protocols

5.3.17.3 Virtual Hosting

Step 1 : Open Server Manager at Windows Server and open DNS.

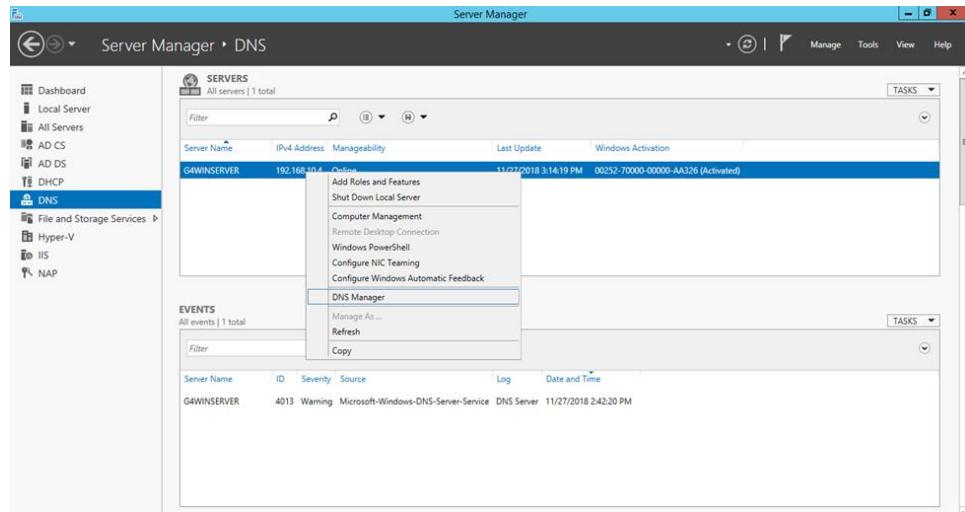


Figure 256: Server Manager and click on DNS

Step 2 : Then, open the DNS Manager.

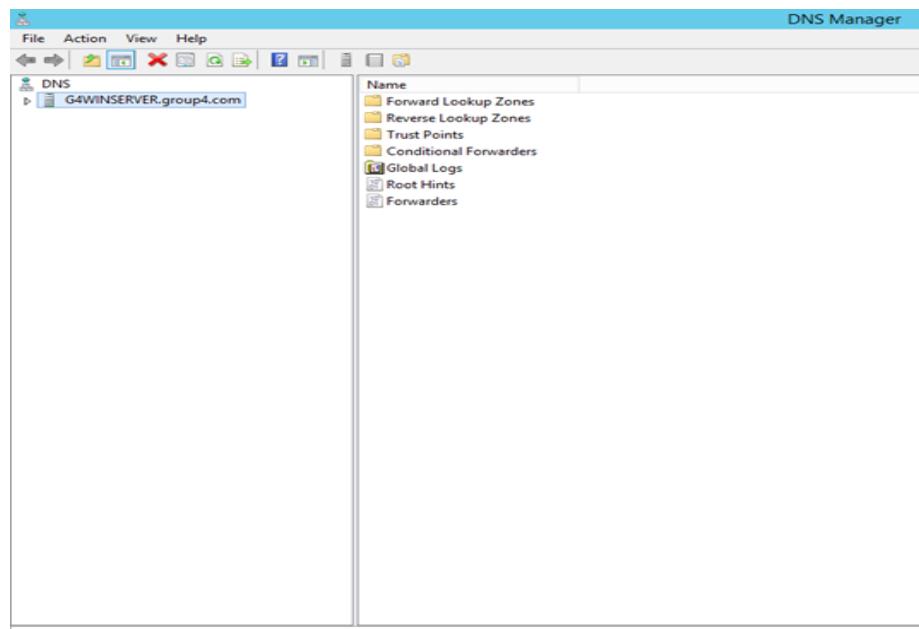


Figure 257: DNS Manager

Step 3 Right click at the folder Forward Lookup Zone.

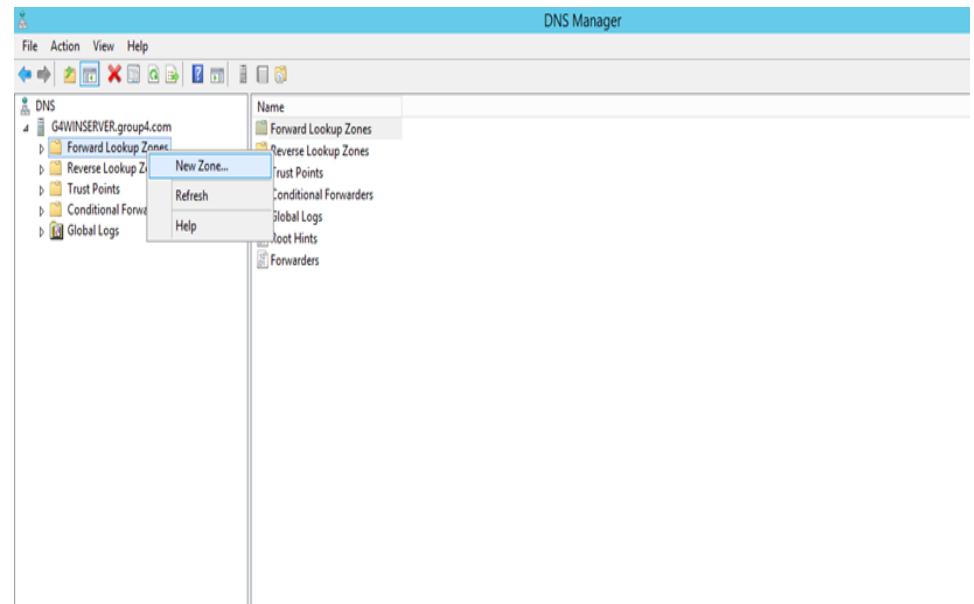


Figure 258: Forward Lookup zone

Step 4 : Then, it will display the New Zone Wizard and click Next.



Figure 259: New Zone Wizard page

Step 5 : Select the Zone type that need to be created. Then, click Next



Figure 260: Selecting the zone type

Step 6 : Insert new zone name for virtual host and click Next.

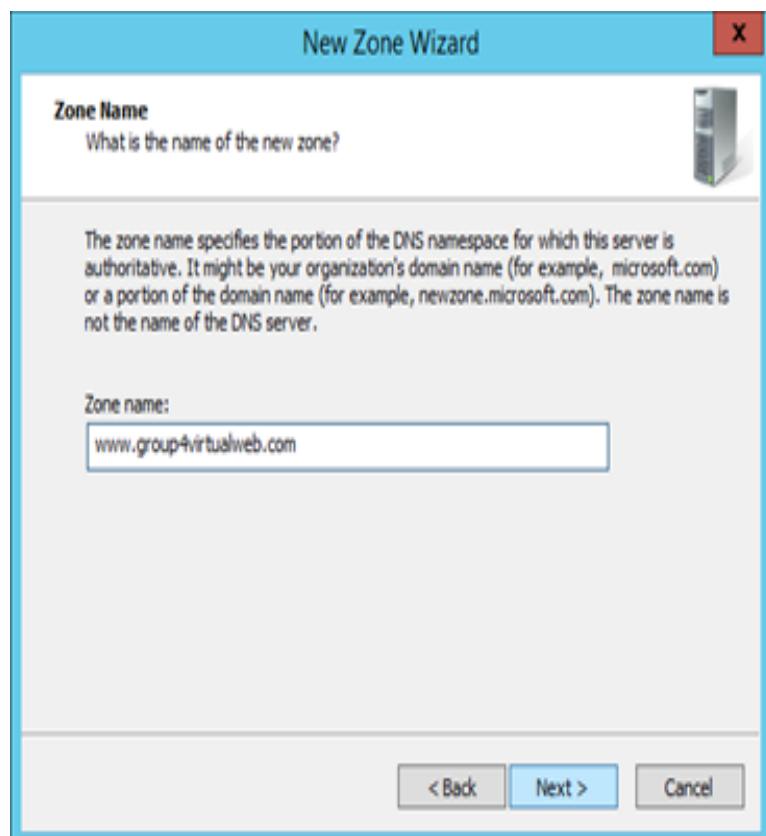


Figure 261: Insert new zone name for virtual host

Step 7 : Select Dynamic Update that is preferable and click Next button.



Figure 262: Selecting dynamic update

Step 8 : Upon completing the New Zone, it will display the result and then, click Finish.



Figure 263: Completing new zone wizard

Step 9 : Create New Host in the New Zone that has been created.

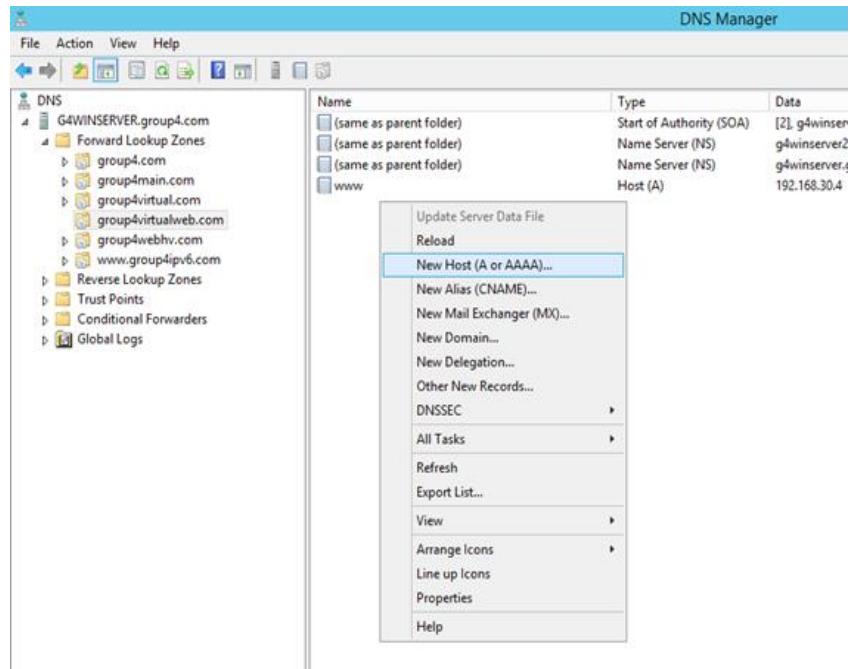


Figure 264: Create new Host in the new zone

Step 10 : Insert the name and IP Address for the New Host to point the other destination of the virtual Host.

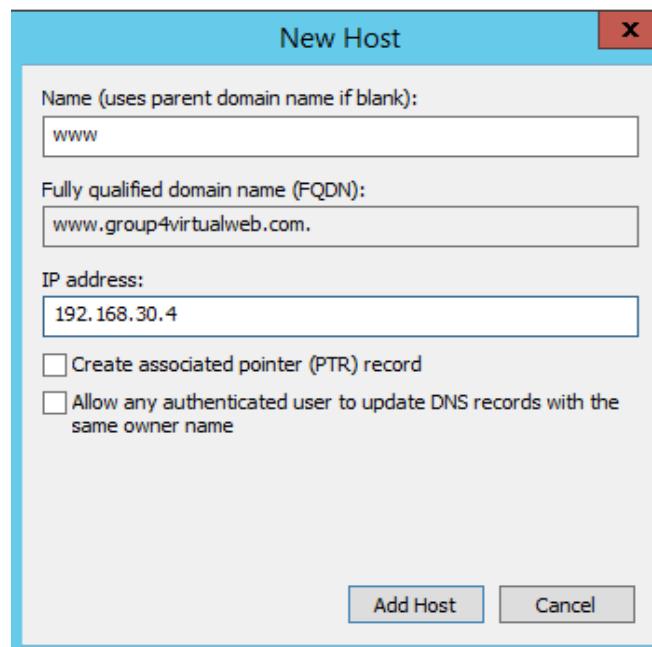
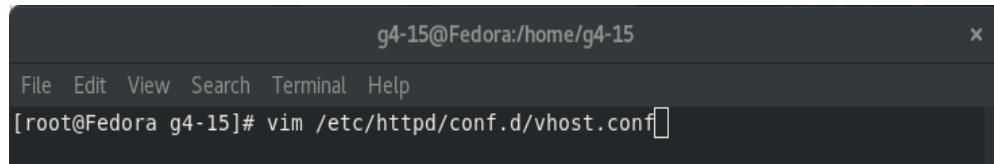


Figure 265: Inserting the name and IP Address for new host

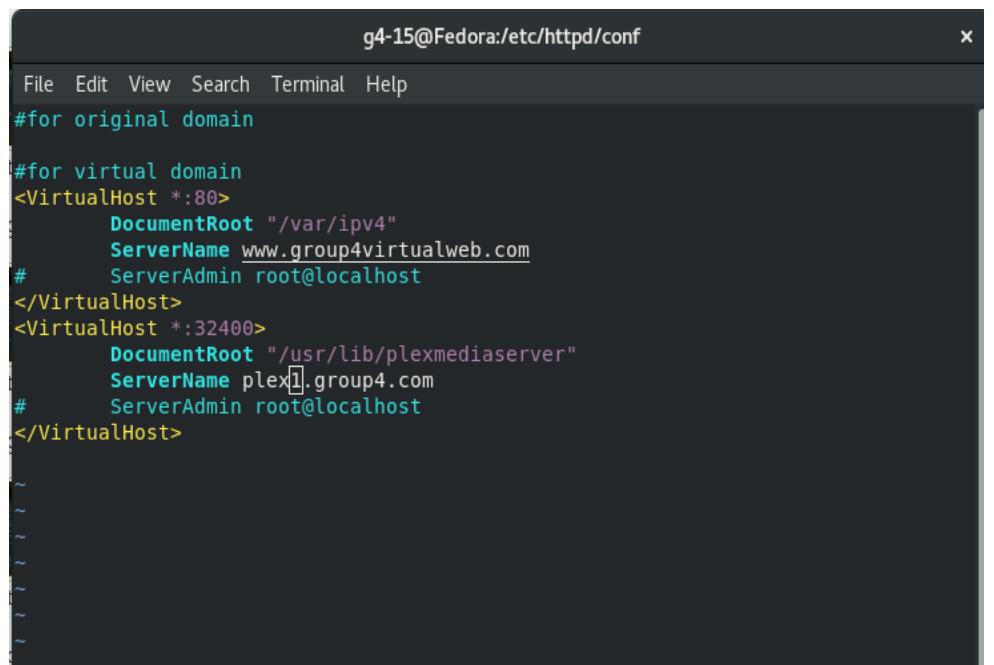
Step 11 : Next, open back Terminal in Fedora and edit the configuration file using command “vhost.conf” to configure the Virtual Hosting configuration file.



```
g4-15@Fedora:/home/g4-15
File Edit View Search Terminal Help
[root@Fedora g4-15]# vim /etc/httpd/conf.d/vhost.conf
```

Figure 266: Open Terminal in Fedora and edit the configuration file

Step 12 : Check all the port and path directory making sure that they are in right directory.



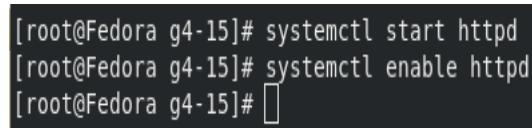
```
g4-15@Fedora:/etc/httpd/conf
File Edit View Search Terminal Help
#for original domain

#for virtual domain
<VirtualHost *:80>
    DocumentRoot "/var/ipv4"
    ServerName www.group4virtualweb.com
#        ServerAdmin root@localhost
</VirtualHost>
<VirtualHost *:32400>
    DocumentRoot "/usr/lib/plexmediaserver"
    ServerName plex[1].group4.com
#        ServerAdmin root@localhost
</VirtualHost>

~
~
~
~
~
~
```

Figure 267: Checking all port and path directory

Step 13 : Restart the httpd service to get the service start.



```
[root@Fedora g4-15]# systemctl start httpd
[root@Fedora g4-15]# systemctl enable httpd
[root@Fedora g4-15]#
```

Figure 268: Restart the httpd service

5.3.18 Linux Email Server

Step 1 : Install Postfix by running the following command. Then, ‘choose Internet Site’ and click OK. Next enter the system mail name as ‘group4.com’.

```
root@ubuntu:/var/www# sudo apt-get install postfix -y
```

Figure 269: Install the postfix using this command

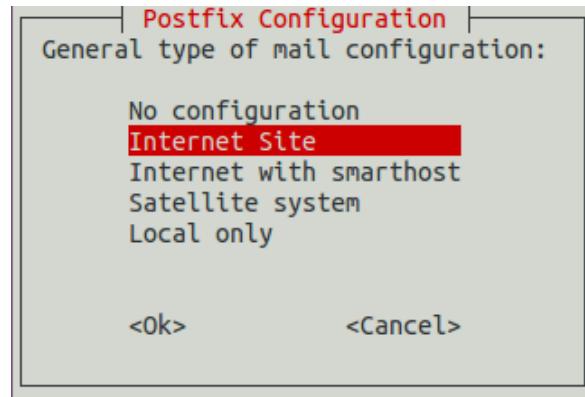


Figure 270: Postfix configuration

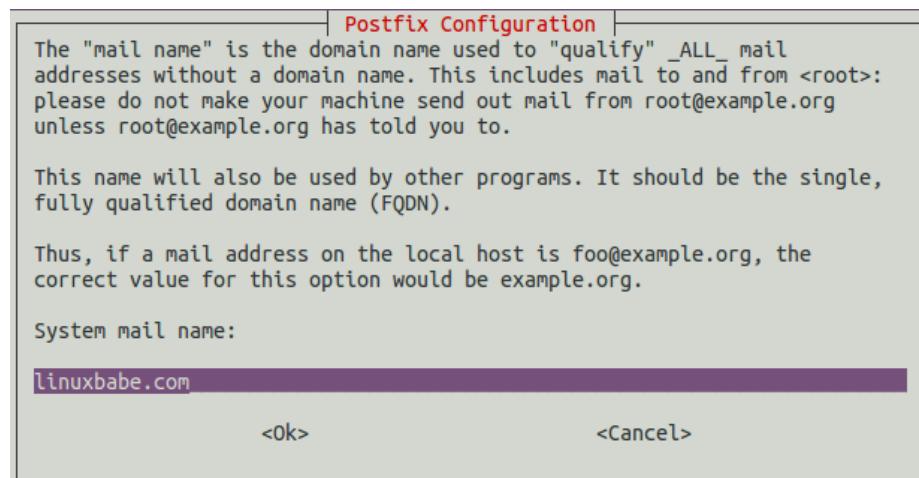


Figure 271: Postfix configuration

Installing and Configuring Dovecot IMAP Server

Step 1 : Enter the following command to install Dovecot core package and the IMAP daemon package on Ubuntu server.

```
root@ubuntu:/var/www# sudo apt install dovecot-core dovecot-imapd
```

Figure 272: Installing Dovecot core package

Step 2 : Check Dovecot version.

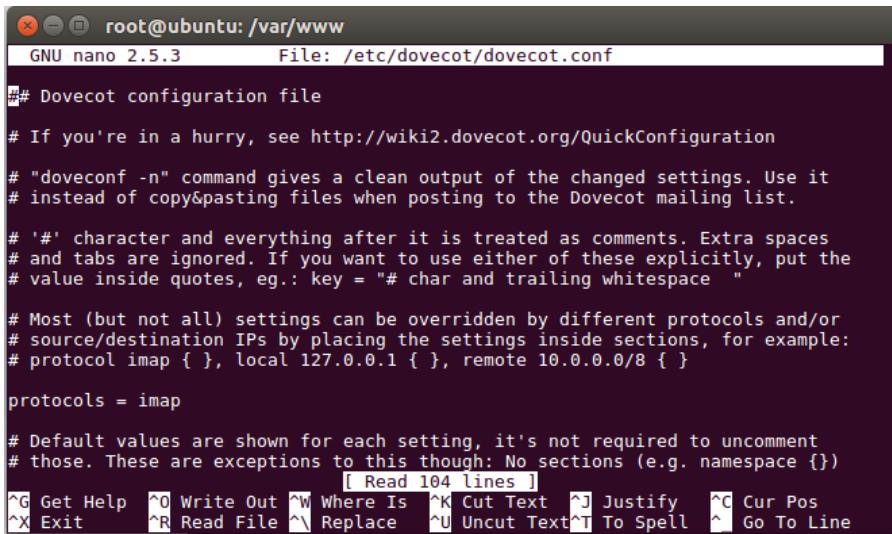
```
root@ubuntu:/var/www# sudo dovecot --version
2.2.22 (fe789d2)
root@ubuntu:/var/www#
```

Figure 273: Checking Dovecot package

Step 3 : Start configuring Dovecot by edit main config file. Run the following command and add the following line to enable IMAP protocol.

```
root@ubuntu:/var/www
g4-16@ubuntu:~$ sudo su
[sudo] password for g4-16:
root@ubuntu:/home/g4-16# vim /etc/apache2/sites-available/rainloop.conf
root@ubuntu:/home/g4-16# cd /var/www/
root@ubuntu:/var/www# a2enmod rewrite
Module rewrite already enabled
root@ubuntu:/var/www# sudo apt install dovecot-core dovecot-imapd
Reading package lists... Done
Building dependency tree
Reading state information... Done
dovecot-core is already the newest version (1:2.2.22-1ubuntu2).
dovecot-imapd is already the newest version (1:2.2.22-1ubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 46 not upgraded.
root@ubuntu:/var/www# sudo dovecot --version
2.2.22 (fe789d2)
root@ubuntu:/var/www# sudo nano /etc/dovecot/dovecot.conf
root@ubuntu:/var/www#
```

Figure 274: Edit main config file



```

root@ubuntu:/var/www
GNU nano 2.5.3      File: /etc/dovecot/dovecot.conf

# Dovecot configuration file
# If you're in a hurry, see http://wiki2.dovecot.org/QuickConfiguration
# "doveconf -n" command gives a clean output of the changed settings. Use it
# instead of copy&pasting files when posting to the Dovecot mailing list.
# '#' character and everything after it is treated as comments. Extra spaces
# and tabs are ignored. If you want to use either of these explicitly, put the
# value inside quotes, eg.: key = "# char and trailing whitespace "
# Most (but not all) settings can be overridden by different protocols and/or
# source/destination IPs by placing the settings inside sections, for example:
# protocol imap { }, local 127.0.0.1 { }, remote 10.0.0.0/8 { }

protocols = imap

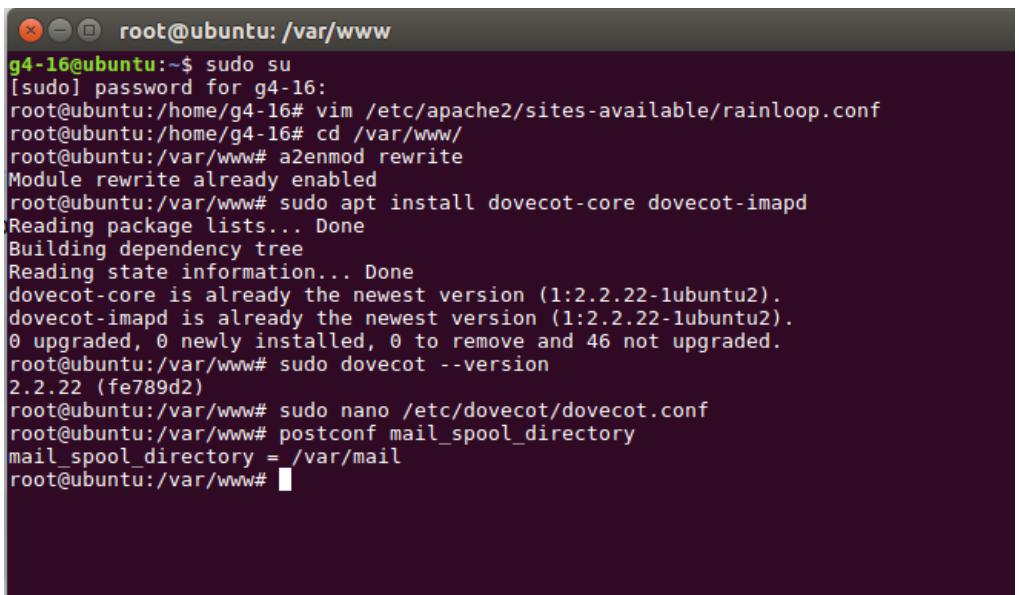
# Default values are shown for each setting, it's not required to uncomment
# those. These are exceptions to this though: No sections (e.g. namespace {})

[ Read 104 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit  ^R Read File  ^X Replace  ^U Uncut Text  ^T To Spell  ^L Go To Line

```

Figure 275: Edit main config file

Step 4 : Run the following command to find the email spool directory.



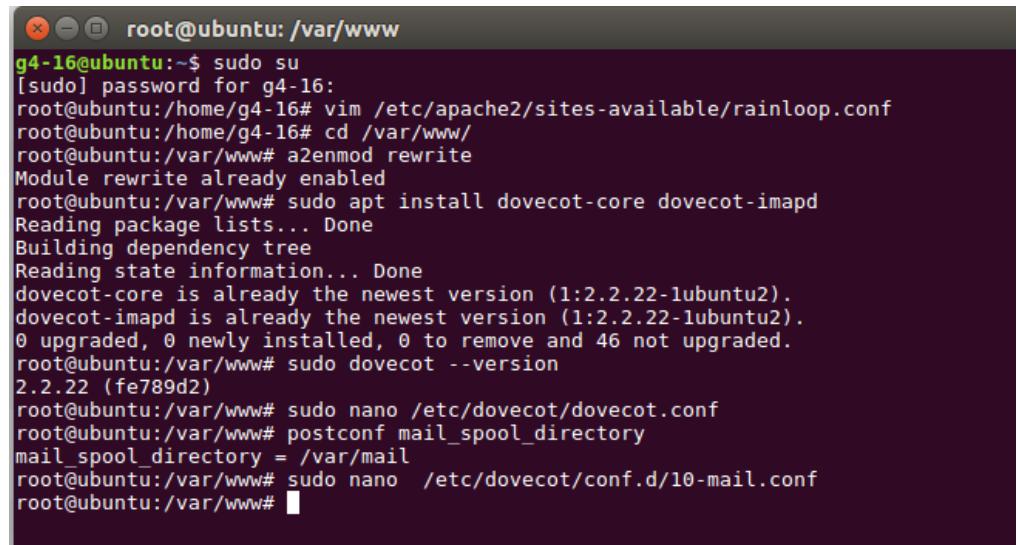
```

g4-16@ubuntu:~$ sudo su
[sudo] password for g4-16:
root@ubuntu:/home/g4-16# vim /etc/apache2/sites-available/rainloop.conf
root@ubuntu:/home/g4-16# cd /var/www/
root@ubuntu:/var/www# a2enmod rewrite
Module rewrite already enabled
root@ubuntu:/var/www# sudo apt install dovecot-core dovecot-imapd
Reading package lists... Done
Building dependency tree
Reading state information... Done
dovecot-core is already the newest version (1:2.2.22-1ubuntu2).
dovecot-imapd is already the newest version (1:2.2.22-1ubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 46 not upgraded.
root@ubuntu:/var/www# sudo dovecot --version
2.2.22 (fe789d2)
root@ubuntu:/var/www# sudo nano /etc/dovecot/dovecot.conf
root@ubuntu:/var/www# postconf mail_spool_directory
mail_spool_directory = /var/mail
root@ubuntu:/var/www#

```

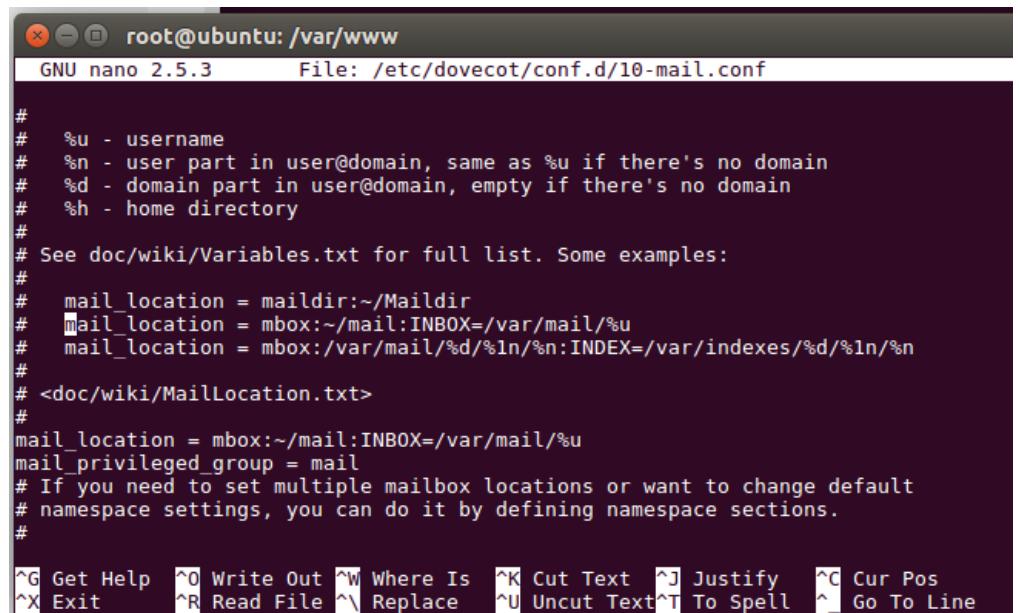
Figure 276: Find email spool directory

Step 5 : Start configuring authentication mechanism by configure mailbox by running the following command and add the following line.



```
root@ubuntu:~$ sudo su
[sudo] password for g4-16:
root@ubuntu:/home/g4-16# vim /etc/apache2/sites-available/rainloop.conf
root@ubuntu:/home/g4-16# cd /var/www/
root@ubuntu:/var/www# a2enmod rewrite
Module rewrite already enabled
root@ubuntu:/var/www# sudo apt install dovecot-core dovecot-imapd
Reading package lists... Done
Building dependency tree
Reading state information... Done
dovecot-core is already the newest version (1:2.2.22-1ubuntu2).
dovecot-imapd is already the newest version (1:2.2.22-1ubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 46 not upgraded.
root@ubuntu:/var/www# sudo dovecot --version
2.2.22 (fe789d2)
root@ubuntu:/var/www# sudo nano /etc/dovecot/dovecot.conf
root@ubuntu:/var/www# postconf mail_spool_directory
mail_spool_directory = /var/mail
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/10-mail.conf
root@ubuntu:/var/www#
```

Figure 277: Configuring authentication mechanism

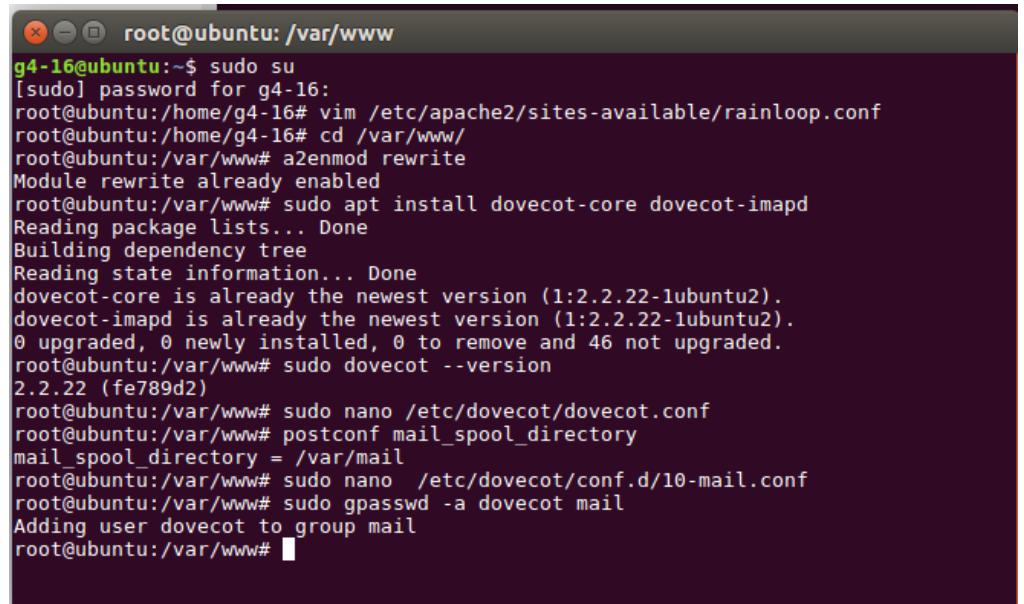


```
GNU nano 2.5.3      File: /etc/dovecot/conf.d/10-mail.conf

#
# %u - username
# %n - user part in user@domain, same as %u if there's no domain
# %d - domain part in user@domain, empty if there's no domain
# %h - home directory
#
# See doc/wiki/Variables.txt for full list. Some examples:
#
# mail_location = mailldir:~/Maildir
# mail_location = mbox:~/mail:INBOX=/var/mail/%u
# mail_location = mbox:/var/mail/%d/%n:INDEX=/var/indexes/%d/%n/%n
#
# <doc/wiki/MailLocation.txt>
#
mail_location = mbox:~/mail:INBOX=/var/mail/%u
mail_privileged_group = mail
# If you need to set multiple mailbox locations or want to change default
# namespace settings, you can do it by defining namespace sections.
#
```

Figure 278: Configuring authentication mechanism

Step 6 : After that, add dovecot to the mail group so that Dovecot can read the INBOX.



```
root@ubuntu:~$ sudo su
[sudo] password for g4-16:
root@ubuntu:/home/g4-16# vim /etc/apache2/sites-available/rainloop.conf
root@ubuntu:/home/g4-16# cd /var/www/
root@ubuntu:/var/www# a2enmod rewrite
Module rewrite already enabled
root@ubuntu:/var/www# sudo apt install dovecot-core dovecot-imapd
Reading package lists... Done
Building dependency tree
Reading state information... Done
dovecot-core is already the newest version (1:2.2.22-1ubuntu2).
dovecot-imapd is already the newest version (1:2.2.22-1ubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 46 not upgraded.
root@ubuntu:/var/www# sudo dovecot --version
2.2.22 (fe789d2)
root@ubuntu:/var/www# sudo nano /etc/dovecot/dovecot.conf
root@ubuntu:/var/www# postconf mail_spool_directory
mail_spool_directory = /var/mail
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/10-mail.conf
root@ubuntu:/var/www# sudo gpasswd -a dovecot mail
Adding user dovecot to group mail
root@ubuntu:/var/www#
```

Figure 279: Adding dovecot to mail group

Step 7 : Edit the authentication config file and add the following line.

The image shows two terminal windows side-by-side. The top window is a root shell on an Ubuntu system, displaying a series of commands used to install Dovecot and its components, enable rewrite rules for Apache, and configure Dovecot's main and auth files. The bottom window is a nano editor showing the /etc/dovecot/conf.d/10-auth.conf file, which contains various configuration options for Dovecot's authentication processes, including disabling plaintext authentication by default.

```
g4-16@ubuntu:~$ sudo su
[sudo] password for g4-16:
root@ubuntu:/home/g4-16# vim /etc/apache2/sites-available/rainloop.conf
root@ubuntu:/home/g4-16# cd /var/www/
root@ubuntu:/var/www# a2enmod rewrite
Module rewrite already enabled
root@ubuntu:/var/www# sudo apt install dovecot-core dovecot-imapd
Reading package lists... Done
Building dependency tree
Reading state information... Done
dovecot-core is already the newest version (1:2.2.22-1ubuntu2).
dovecot-imapd is already the newest version (1:2.2.22-1ubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 46 not upgraded.
root@ubuntu:/var/www# sudo dovecot --version
2.2.22 (fe789d2)
root@ubuntu:/var/www# sudo nano /etc/dovecot/dovecot.conf
root@ubuntu:/var/www# postconf mail_spool_directory
mail_spool_directory = /var/mail
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/10-mail.conf
root@ubuntu:/var/www# sudo gpasswd -a dovecot mail
Adding user dovecot to group mail
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/10-auth.conf
root@ubuntu:/var/www#
```

```
GNU nano 2.5.3      File: /etc/dovecot/conf.d/10-auth.conf

## 
## Authentication processes
## 

# Disable LOGIN command and all other plaintext authentications unless
# SSL/TLS is used (LOGINDISABLED capability). Note that if the remote IP
# matches the local IP (ie. you're connecting from the same computer), the
# connection is considered secure and plaintext authentication is allowed.
# See also ssl=required setting.
disable_plaintext_auth = yes
auth_username_format = %
# Authentication cache size (e.g. 10M). 0 means it's disabled. Note that
# bsdauth, PAM and vpopmail require cache_key to be set for caching to be used.
#auth_cache_size = 0
# Time to live for cached data. After TTL expires the cached record is no
# longer used, *except* if the main database lookup returns internal failure.
# We also try to handle password changes automatically: If user's previous
# authentication was successful, but this one wasn't, the cache isn't used.
# For now this works only with plaintext authentication.

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

Figure 280: Edit the authentication file

```

root@ubuntu:/var/www
GNU nano 2.5.3          File: /etc/dovecot/conf.d/10-auth.conf

#auth_ssl_require_client_cert = no

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

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

#
# Password database is used to verify user's password (and nothing more).
# You can have multiple passdbs and userdbs. This is useful if you want to
# allow both system users (/etc/passwd) and virtual users to login without
# duplicating the system users into virtual database.
#
# <doc/wiki/PasswordDatabase.txt>
#

^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 281: Edit the authentication file

Step 8 : Next, edit SSL/TLS config file and change **ssl = no** to **ssl = required**.

Then specify the location of your SSL/TLS cert and private key. Don't leave out < character. It's necessary.

```

root@ubuntu:~#
[sudo] password for g4-16:
root@ubuntu:/home/g4-16# vim /etc/apache2/sites-available/rainloop.conf
root@ubuntu:/home/g4-16# cd /var/www/
root@ubuntu:/var/www# a2enmod rewrite
Module rewrite already enabled
root@ubuntu:/var/www# sudo apt install dovecot-core dovecot-imapd
Reading package lists... Done
Building dependency tree
Reading state information... Done
dovecot-core is already the newest version (1:2.2.22-1ubuntu2).
dovecot-imapd is already the newest version (1:2.2.22-1ubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 46 not upgraded.
root@ubuntu:/var/www# sudo dovecot --version
2.2.22 (fe789d2)
root@ubuntu:/var/www# sudo nano /etc/dovecot/dovecot.conf
root@ubuntu:/var/www# postconf mail_spool_directory
mail_spool_directory = /var/mail
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/10-mail.conf
root@ubuntu:/var/www# sudo gpasswd -a dovecot mail
Adding user dovecot to group mail
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/10-auth.conf
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/10-auth.conf
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/10-ssl.conf
root@ubuntu:/var/www#

```

Figure 282: Edit SSL/TLS config

```
root@ubuntu:/var/www
GNU nano 2.5.3          File: /etc/dovecot/conf.d/10-ssl.conf

## 
## SSL settings
## 

# SSL/TLS support: yes, no, required. <doc/wiki/SSL.txt>
ssl = required

# PEM encoded X.509 SSL/TLS certificate and private key. They're opened before
# dropping root privileges, so keep the key file unreadable by anyone but
# root. Included doc/mkcert.sh can be used to easily generate self-signed
# certificate, just make sure to update the domains in dovecot-openssl.cnf
ssl_cert = </etc/ssl/certs/g4.pem
ssl_key = </etc/ssl/private/g4.key

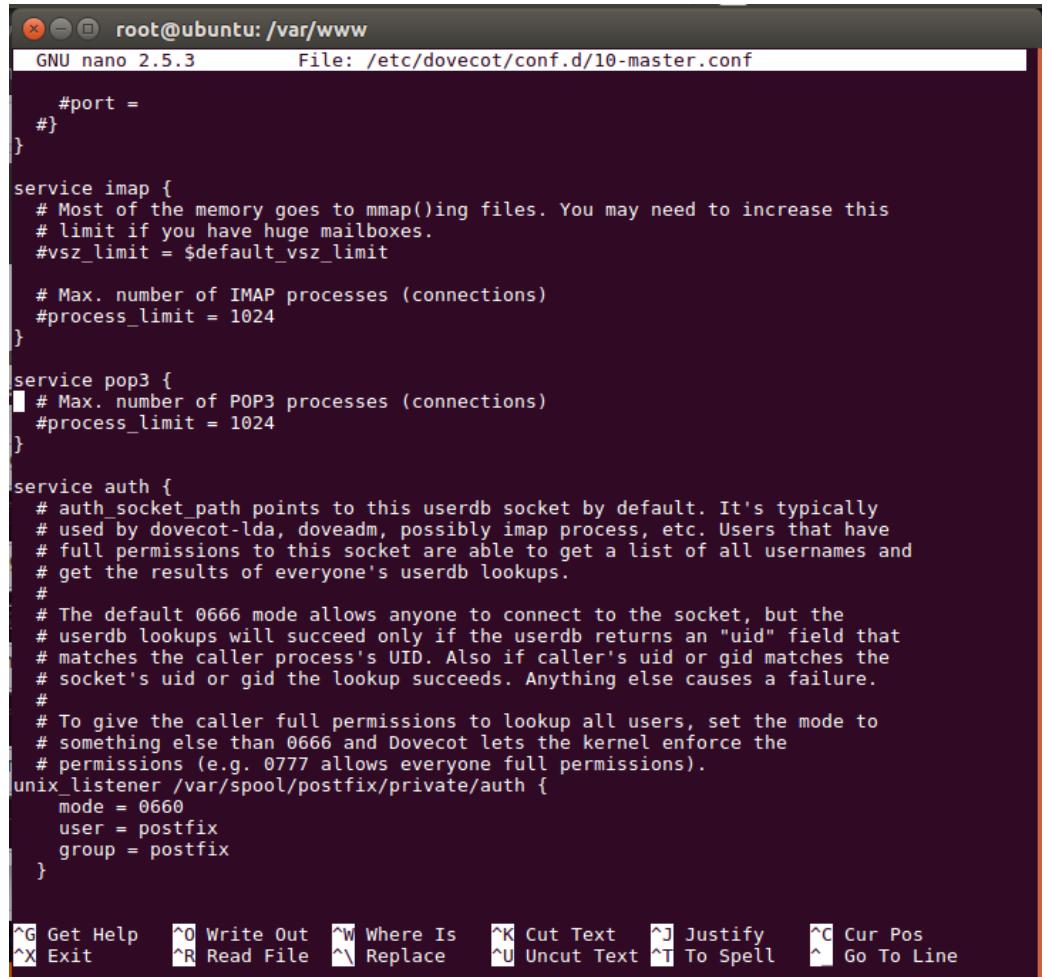
# If key file is password protected, give the password here. Alternatively
# give it when starting dovecot with -p parameter. Since this file is often
# world-readable, you may want to place this setting instead to a different
# root owned 0600 file by using ssl_key_password = <path>.
#ssl_key_password =
                                         [ Read 62 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File   ^\ Replace   ^U Uncut Text ^T To Spell  ^L Go To Line
```

Figure 283: Continuing editing SSL/TLS file

Step 9 : Edit the following file. Then change service auth section to the following so that Postfix can find the Dovecot authentication server.

```
g4-16@ubuntu:~$ sudo su
[sudo] password for g4-16:
root@ubuntu:/home/g4-16# vim /etc/apache2/sites-available/rainloop.conf
root@ubuntu:/home/g4-16# cd /var/www/
root@ubuntu:/var/www# a2enmod rewrite
Module rewrite already enabled
root@ubuntu:/var/www# sudo apt install dovecot-core dovecot-imapd
Reading package lists... Done
Building dependency tree
Reading state information... Done
dovecot-core is already the newest version (1:2.2.22-1ubuntu2).
dovecot-imapd is already the newest version (1:2.2.22-1ubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 46 not upgraded.
root@ubuntu:/var/www# sudo dovecot --version
2.2.22 (fe789d2)
root@ubuntu:/var/www# sudo nano /etc/dovecot/dovecot.conf
root@ubuntu:/var/www# postconf mail_spool_directory
mail_spool_directory = /var/mail
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/10-mail.conf
root@ubuntu:/var/www# sudo gpasswd -a dovecot mail
Adding user dovecot to group mail
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/10-auth.conf
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/10-auth.conf
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/10-ssl.conf
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/10-ssl.conf
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/10-master.conf
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/15-mailboxes.conf
root@ubuntu:/var/www#
```

Figure 284: Edit the file so that Postfix can find dovecot authentication server



The screenshot shows a terminal window titled "root@ubuntu: /var/www". The window displays the contents of the file "/etc/dovecot/conf.d/10-master.conf" using the nano editor. The configuration file contains several sections for services like imap, pop3, and auth, with various parameters and comments. At the bottom of the screen, a series of keyboard shortcuts are listed.

```
root@ubuntu: /var/www
GNU nano 2.5.3          File: /etc/dovecot/conf.d/10-master.conf

    #port =
#}

service imap {
    # Most of the memory goes to mmap()ing files. You may need to increase this
    # limit if you have huge mailboxes.
    #vsz_limit = $default_vsz_limit

    # Max. number of IMAP processes (connections)
    #process_limit = 1024
}

service pop3 {
    # Max. number of POP3 processes (connections)
    #process_limit = 1024
}

service auth {
    # auth_socket_path points to this userdb socket by default. It's typically
    # used by dovecot-lda, dovecadm, possibly imap process, etc. Users that have
    # full permissions to this socket are able to get a list of all usernames and
    # get the results of everyone's userdb lookups.
    #
    # The default 0666 mode allows anyone to connect to the socket, but the
    # userdb lookups will succeed only if the userdb returns an "uid" field that
    # matches the caller process's UID. Also if caller's uid or gid matches the
    # socket's uid or gid the lookup succeeds. Anything else causes a failure.
    #
    # To give the caller full permissions to lookup all users, set the mode to
    # something else than 0666 and Dovecot lets the kernel enforce the
    # permissions (e.g. 0777 allows everyone full permissions).
    unix_listener /var/spool/postfix/private/auth {
        mode = 0660
        user = postfix
        group = postfix
    }

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

Figure 285: Continuation of editing file

Step 10 : Edit the below config file. Then, at auto create a folder, simply add the following line in the mailbox section.

```
root@ubuntu:~$ sudo su
[sudo] password for g4-16:
root@ubuntu:/home/g4-16# vim /etc/apache2/sites-available/rainloop.conf
root@ubuntu:/home/g4-16# cd /var/www/
root@ubuntu:/var/www# a2enmod rewrite
Module rewrite already enabled
root@ubuntu:/var/www# sudo apt install dovecot-core dovecot-imapd
Reading package lists... Done
Building dependency tree
Reading state information... Done
dovecot-core is already the newest version (1:2.2.22-1ubuntu2).
dovecot-imapd is already the newest version (1:2.2.22-1ubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 46 not upgraded.
root@ubuntu:/var/www# sudo dovecot --version
2.2.22 (fe789d2)
root@ubuntu:/var/www# sudo nano /etc/dovecot/dovecot.conf
root@ubuntu:/var/www# postconf mail_spool_directory
mail_spool_directory = /var/mail
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/10-mail.conf
root@ubuntu:/var/www# sudo gpasswd -a dovecot mail
Adding user dovecot to group mail
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/10-auth.conf
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/10-auth.conf
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/10-ssl.conf
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/10-ssl.conf
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/10-master.conf
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/15-mailboxes.conf
root@ubuntu:/var/www# 
```



```
root@ubuntu:~$ nano /etc/dovecot/conf.d/15-mailboxes.conf
GNU nano 2.5.3           File: /etc/dovecot/conf.d/15-mailboxes.conf

#   value.

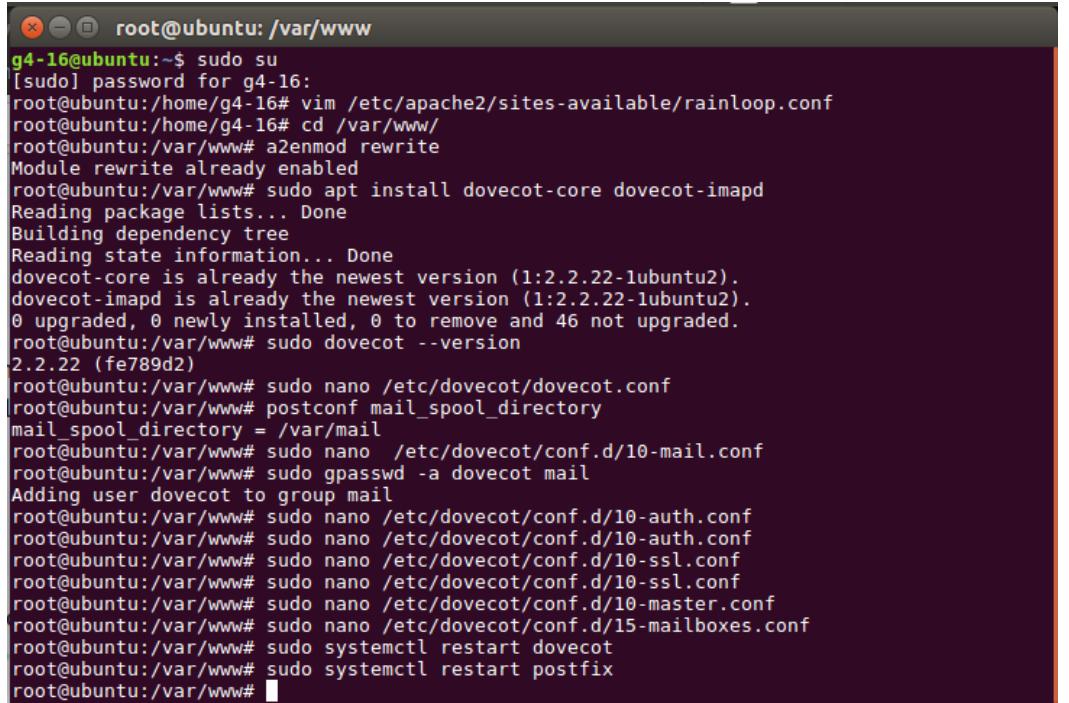
# NOTE: Assumes "namespace inbox" has been defined in 10-mail.conf.
namespace inbox {
    # These mailboxes are widely used and could perhaps be created automatically:
    mailbox Drafts {
        special_use = \Drafts
    }
    mailbox Junk {
        special_use = \Junk
    }
    mailbox Trash {
        auto = create
        special_use = \Trash
    }

    # For \Sent mailboxes there are two widely used names. We'll mark both of
    # them as \Sent. User typically deletes one of them if duplicates are created.
    mailbox Sent {
        special_use = \Sent
    }
    mailbox "Sent Messages" {
        special_use = \Sent
    }
}

^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 ^I To Spell  ^L Go To Line
```

Figure 286: Edit and auto create a folder

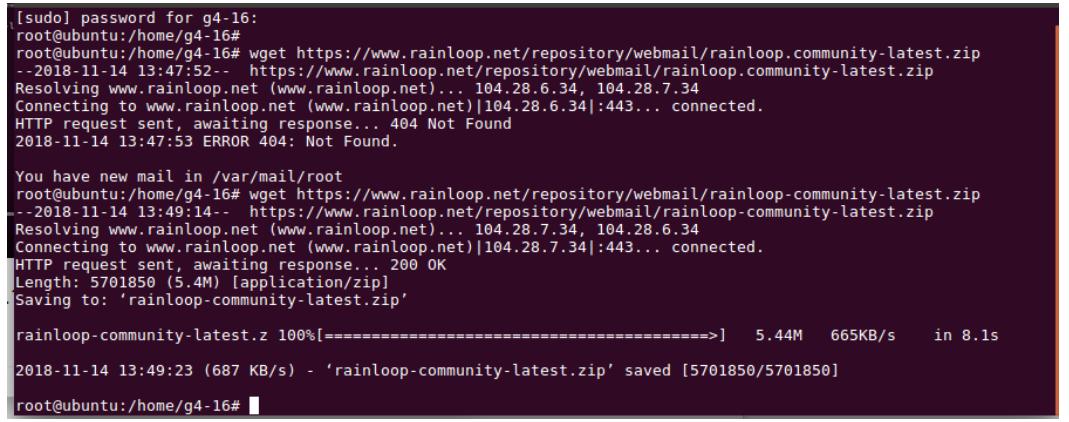
Step 11 : Restart Dovecot and restart Postfix.



```
root@ubuntu:~$ sudo su
[sudo] password for g4-16:
root@ubuntu:/home/g4-16# vim /etc/apache2/sites-available/rainloop.conf
root@ubuntu:/home/g4-16# cd /var/www/
root@ubuntu:/var/www# a2enmod rewrite
Module rewrite already enabled
root@ubuntu:/var/www# sudo apt install dovecot-core dovecot-imapd
Reading package lists... Done
Building dependency tree
Reading state information... Done
dovecot-core is already the newest version (1:2.2.22-1ubuntu2).
dovecot-imapd is already the newest version (1:2.2.22-1ubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 46 not upgraded.
root@ubuntu:/var/www# sudo dovecot --version
2.2.22 (fe789d2)
root@ubuntu:/var/www# sudo nano /etc/dovecot/dovecot.conf
root@ubuntu:/var/www# postconf mail_spool_directory
mail_spool_directory = /var/mail
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/10-mail.conf
root@ubuntu:/var/www# sudo gpasswd -a dovecot mail
Adding user dovecot to group mail
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/10-auth.conf
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/10-auth.conf
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/10-ssl.conf
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/10-ssl.conf
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/10-master.conf
root@ubuntu:/var/www# sudo nano /etc/dovecot/conf.d/15-mailboxes.conf
root@ubuntu:/var/www# sudo systemctl restart dovecot
root@ubuntu:/var/www# sudo systemctl restart postfix
root@ubuntu:/var/www#
```

Figure 287: Restarting Dovecot and restart Postfix

Step 12 : Install Rainloop web mail application package using following url.



```
[sudo] password for g4-16:
root@ubuntu:/home/g4-16# wget https://www.rainloop.net/repository/webmail/rainloop.community-latest.zip
--2018-11-14 13:47:52-- https://www.rainloop.net/repository/webmail/rainloop.community-latest.zip
Resolving www.rainloop.net (www.rainloop.net)... 104.28.6.34, 104.28.7.34
Connecting to www.rainloop.net (www.rainloop.net)|104.28.6.34|:443... connected.
HTTP request sent, awaiting response... 404 Not Found
2018-11-14 13:47:53 ERROR 404: Not Found.

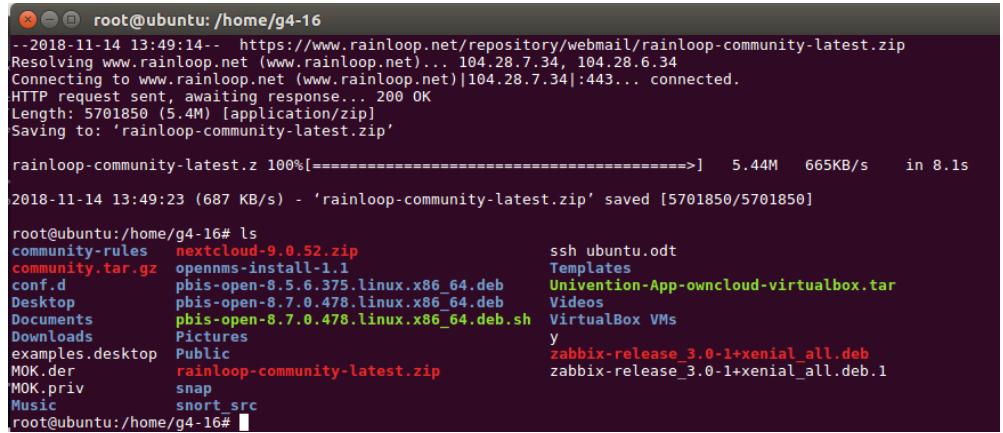
You have new mail in /var/mail/root
root@ubuntu:/home/g4-16# wget https://www.rainloop.net/repository/webmail/rainloop-community-latest.zip
--2018-11-14 13:49:14-- https://www.rainloop.net/repository/webmail/rainloop-community-latest.zip
Resolving www.rainloop.net (www.rainloop.net)... 104.28.7.34, 104.28.6.34
Connecting to www.rainloop.net (www.rainloop.net)|104.28.7.34|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5701850 (5.4M) [application/zip]
Saving to: 'rainloop-community-latest.zip'

rainloop-community-latest.zip 100%[=====] 5.44M 665KB/s in 8.1s
2018-11-14 13:49:23 (687 KB/s) - 'rainloop-community-latest.zip' saved [5701850/5701850]

root@ubuntu:/home/g4-16#
```

Figure 288: Installing Rainloop

Step 13 To see the rainloop successfully install.



```
root@ubuntu:/home/g4-16
--2018-11-14 13:49:14-- https://www.rainloop.net/repository/webmail/rainloop-community-latest.zip
Resolving www.rainloop.net (www.rainloop.net)... 104.28.7.34, 104.28.6.34
Connecting to www.rainloop.net (www.rainloop.net)|104.28.7.34|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5701850 (5.4M) [application/zip]
Saving to: 'rainloop-community-latest.zip'

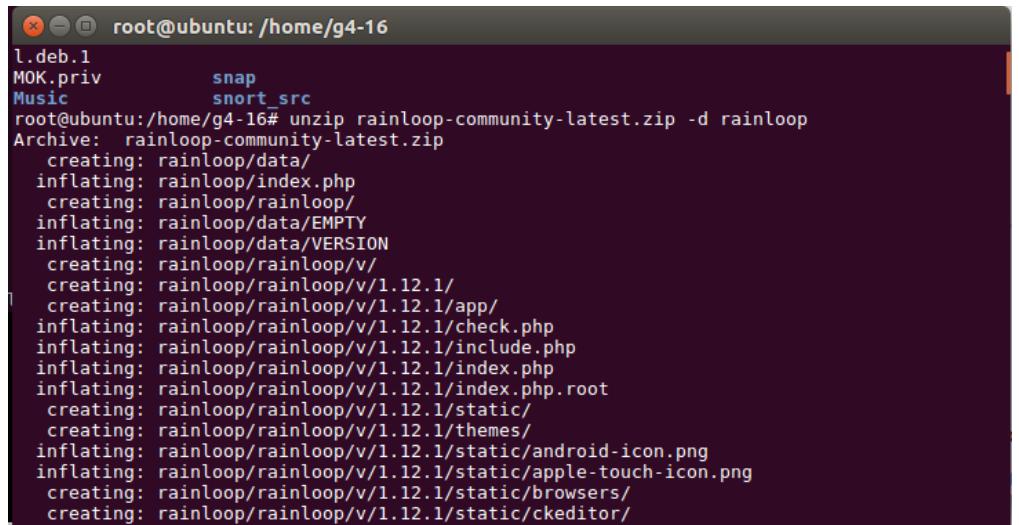
rainloop-community-latest.zip 100%[=====] 5.44M 665KB/s in 8.1s

2018-11-14 13:49:23 (687 KB/s) - 'rainloop-community-latest.zip' saved [5701850/5701850]

root@ubuntu:/home/g4-16# ls
community-rules    nextcloud-9.0.52.zip          ssh ubuntu.odt
community.tar.gz   opennms-install-1.1           Templates
conf.d              pbis-open-8.5.6.375.linux.x86_64.deb  Univention-App-owncloud-virtualbox.tar
Desktop             pbis-open-8.7.0.478.linux.x86_64.deb  Videos
Documents           pbis-open-8.7.0.478.linux.x86_64.deb.sh VirtualBox VMs
Downloads           Pictures
examples.desktop    Public
MOK.der             rainloop-community-latest.zip  zabbix-release_3.0-1+xenial_all.deb
MOK.priv            snap
Music               snort_src
root@ubuntu:/home/g4-16#
```

Figure 289: See the rainloop installation status

Step 14 : Unzip Rainloop using following command.



```
root@ubuntu:/home/g4-16
l.deb.1
MOK.priv      snap
Music         snort_src
root@ubuntu:/home/g4-16# unzip rainloop-community-latest.zip -d rainloop
Archive: rainloop-community-latest.zip
  creating: rainloop/data/
  inflating: rainloop/index.php
  creating: rainloop/rainloop/
  inflating: rainloop/data/EMPTY
  inflating: rainloop/data/VERSION
  creating: rainloop/rainloop/v/
  creating: rainloop/rainloop/v/1.12.1/
  creating: rainloop/rainloop/v/1.12.1/app/
  inflating: rainloop/rainloop/v/1.12.1/check.php
  inflating: rainloop/rainloop/v/1.12.1/include.php
  inflating: rainloop/rainloop/v/1.12.1/index.php
  inflating: rainloop/rainloop/v/1.12.1/index.php.root
  creating: rainloop/rainloop/v/1.12.1/static/
  creating: rainloop/rainloop/v/1.12.1/themes/
  inflating: rainloop/rainloop/v/1.12.1/static/android-icon.png
  inflating: rainloop/rainloop/v/1.12.1/static/apple-touch-icon.png
  creating: rainloop/rainloop/v/1.12.1/static/browsers/
  creating: rainloop/rainloop/v/1.12.1/static/ckeditor/
```

Figure 290: Unzip Rainloop

```

root@ubuntu:/home/g4-16
/iicons/file.png
  inflating: rainloop/rainloop/v/1.12.1/app/libraries/SabreForRainLoop/DAV/Browser/assets
/iicons/parent.png
  inflating: rainloop/rainloop/v/1.12.1/app/libraries/SabreForRainLoop/DAV/Browser/assets
/iicons/principal.png
root@ubuntu:/home/g4-16#
root@ubuntu:/home/g4-16# ls
community-rules          Pictures
community.tar.gz          Public
conf.d                     rainloop
Desktop                   rainloop-community-latest.zip
Documents                 snap
Downloads                 snort_src
examples.desktop           ssh ubuntu.odt
MOK.der                   Templates
MOK.priv                  Univention-App-owncloud-virtualbox.tar
Music                     Videos
nextcloud-9.0.52.zip      VirtualBox VMs
opennms-install-1.1        y
pbis-open-8.5.6.375.linux.x86_64.deb zabbix-release_3.0-1+xenial_all.deb
pbis-open-8.7.0.478.linux.x86_64.deb zabbix-release_3.0-1+xenial_all.deb.1

```

Figure 291: See the entire file.

Step 15 : Type ls to see the file.

Step 16 : Run the following command.

```

root@ubuntu:/home/g4-16# mv rainloop /var/www/
root@ubuntu:/home/g4-16# cd /var/www/
root@ubuntu:/var/www# ls
html  rainloop

```

```

root@ubuntu:/var/www# chown -R www-data.www-data rainloop
root@ubuntu:/var/www# chmod -R 775 rainloop

```

Figure 292: Changing mode of the rainloop

Step 17 : Create new file and insert the following command.

```

root@ubuntu:/home/g4-16# cd /var/www/
root@ubuntu:/var/www# vim /etc/apache2/sites-available/rainloop.conf

```

```

root@ubuntu:/home/g4-16
VirtualHost *:80>
ServerName mail.group4.com
DocumentRoot "/var/www/rainloop/"
ServerAdmin mail.group4.com

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

<Directory /var/www/rainloop/>
AllowOverride All
Order deny,allow
allow from all
Require all granted
</Directory>
</VirtualHost>

```

~
~
~
~
~
~
~
"/etc/apache2/sites-available/rainloop.conf" 16L, 338C

Figure 293: Creating new file

Step 18 : Run the following command and restart apache.

```

root@ubuntu:/var/www# a2ensite rainloop.conf
Site rainloop already enabled

root@ubuntu:/var/www# a2dissite 000-default.conf
Site 000-default disabled.

root@ubuntu:/var/www# a2enmod rewrite
Module rewrite already enabled

root@ubuntu:/var/www# systemctl restart apache2

```

Figure 294: Restart the Apache

Step 19 : Open browser and open following url ‘<http://mail.group4.com/?admin>’. Login as admin and default password is 12345.



Figure 295: Mail page at browser

Step 20 : Next, change the password. Tick ‘Allow 2-step Verification’ and ‘Enforce 2-Step Verification’. Then, update password.

The image consists of two screenshots of the RainLoop Admin Panel interface.

Top Screenshot (Security Page):

- The title bar says "RainLoop — Admin Panel".
- The left sidebar menu includes: General, Domains, Login, Branding, Contacts, Security (which is selected), Integrations, Plugins, Packages, and About.
- The main content area is titled "Security". It contains several configuration options:
 - "Allow 2-Step Verification" and "Enforce 2-Step Verification" are checked (indicated by green checkmarks).
 - "Use local proxy for external images" and "Allow OpenPGP" are unchecked (indicated by empty boxes).
 - A link "Show PHP information" is present.
- The "Admin Panel Access Credentials" section contains four input fields:
 - "Current password": (redacted)
 - "New login": admin
 - "New password":
 - "Repeat":
- A "Update Password" button is located at the bottom right of the credentials section.

Bottom Screenshot (About Page):

- The title bar says "RainLoop — Admin Panel".
- The left sidebar menu includes: General, Domains, Login, Branding, Contacts, Security, Integrations, Plugins, Packages, and About (which is selected).
- The main content area is titled "About". It features the RainLoop logo (an envelope icon with arrows) and the text:
 - RainLoop**
 - 1.12.1
 - Simple, modern & fast web-based email client
- Copyright information at the bottom: 2018 © All Rights Reserved. <http://rainloop.net/>

Figure 296: Changing the password

5.3.19 IPv6 Web with IPv6 Tunnelling

Step 1 : Adding New site for IPV6. Go to IIS and create a new site. Fill all the required details.

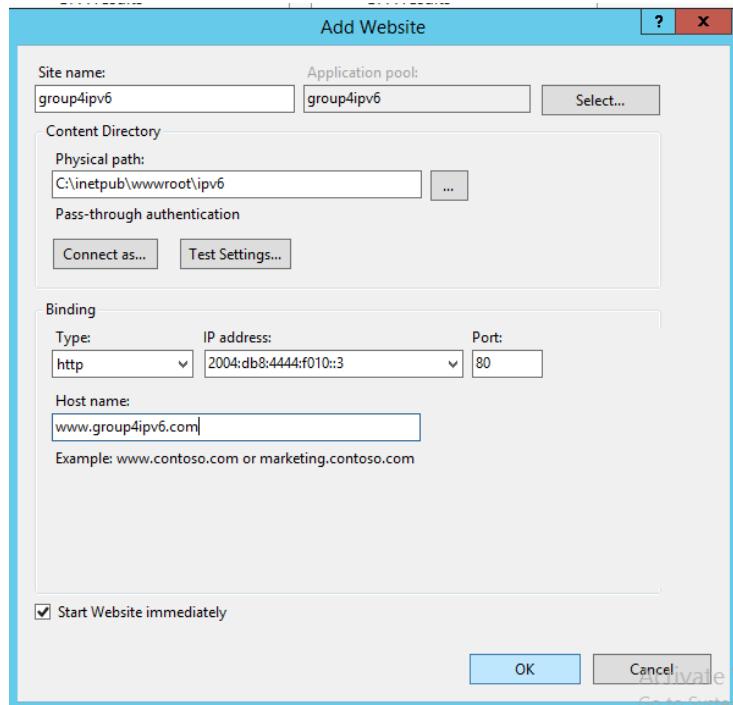


Figure 297: Adding new website

Step 2 : In Default Document set the document that want to display on the website. Add a new file document html to set a default document web.

The screenshot shows the 'Default Document' configuration page. It lists files with their entry types: 'iisstart.htm' (Local), 'Default.htm' (Local), 'Default.asp' (Local), 'index.htm' (Local), and 'index.html' (Local). The 'index.html' row is currently selected. On the right, there's an 'Actions' sidebar with options: 'Add...', 'Disable', 'Revert To Parent', and 'Help'.

Figure 298: Set the document that want to display on website

Step 3 : Adding a new zone at DNS Manager. Give a name to a new Zone and click Next to continue until Finish for successfully complete for new zone.

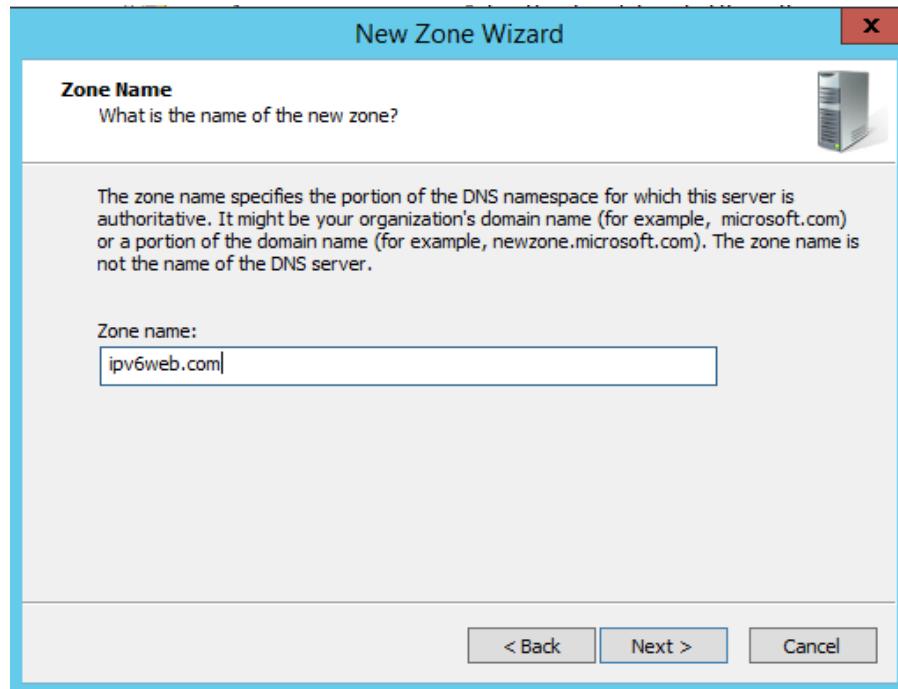


Figure 299: Adding new zone at DNS Manager

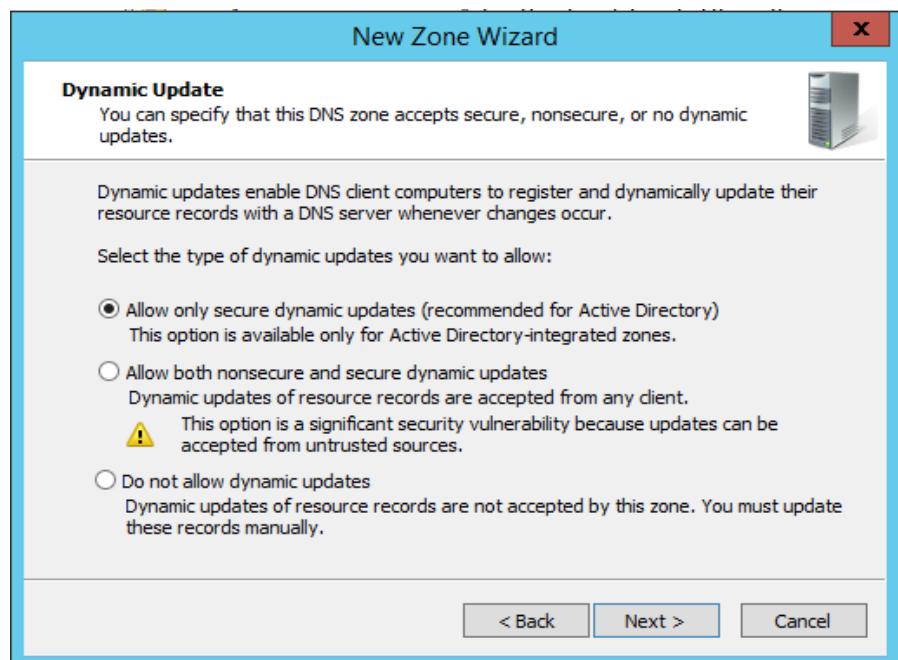


Figure 300: Specify the Dynamic Update

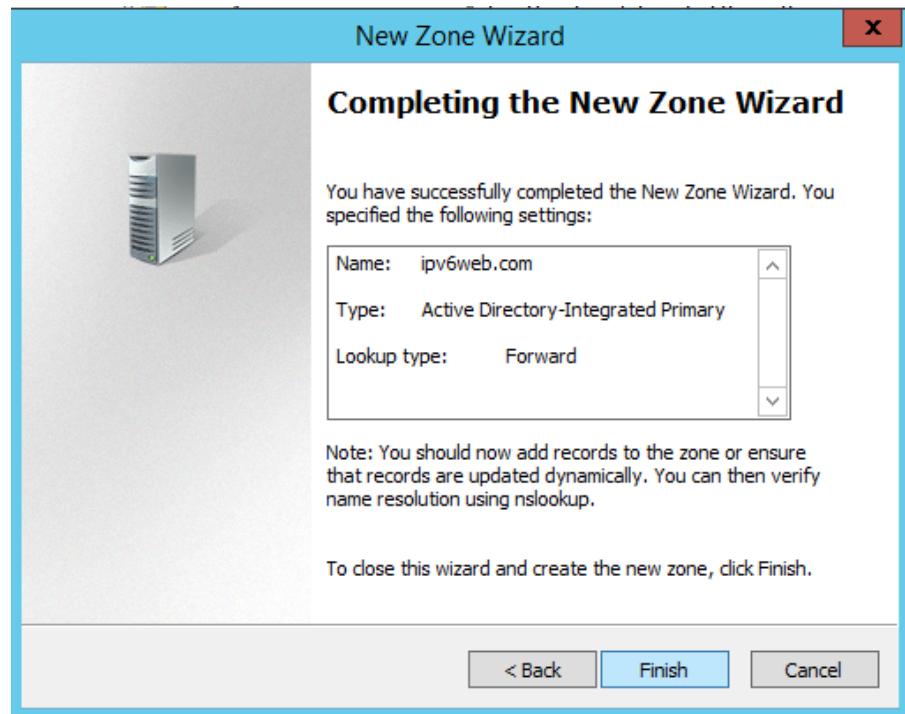


Figure 301: Completing new zone wizard

Step 4 : After finish adding a new zone, add a new host for domain www.group4ipv6.com. Right click and choose for a New Host (A or AAAA).

Name	Type	Status	DNSSEC
group4.com	Active Directory-Integrated Pr...	Running	Not Sig
group4main.com	Active Directory-Integrated Pr...	Running	Not Sig
group4virtual.com	Active Directory-Integrated Pr...	Running	Not Sig
group4virtualweb.com	Active Directory-Integrated Pr...	Running	Not Sig
group4webhv.com	Active Directory-Integrated Pr...	Running	Not Sig
ipv6web.com	Active Directory-Integrated Pr...	Running	Not Sig

Figure 302: Adding new host for the domain

Step 5 : Add a New Host and IP Address.

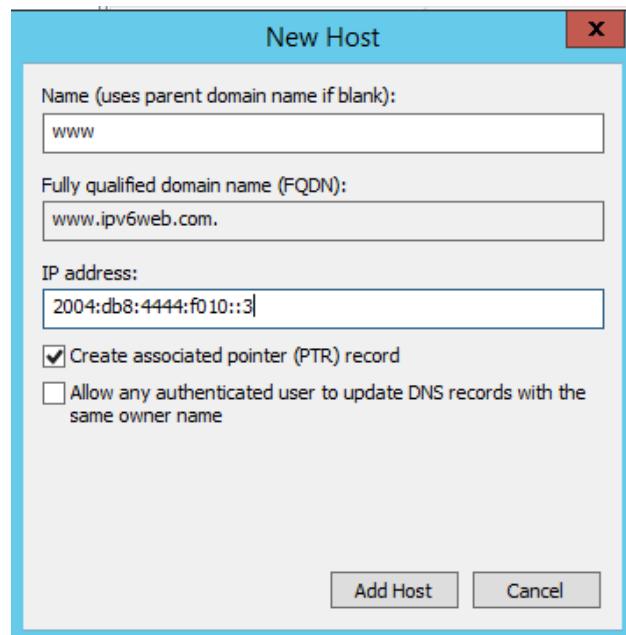


Figure 303: Add new host and IP Address

Step 6 : Check site binding both the ipv6 address and the host name that already set is correct or incorrect if the website can't be access.

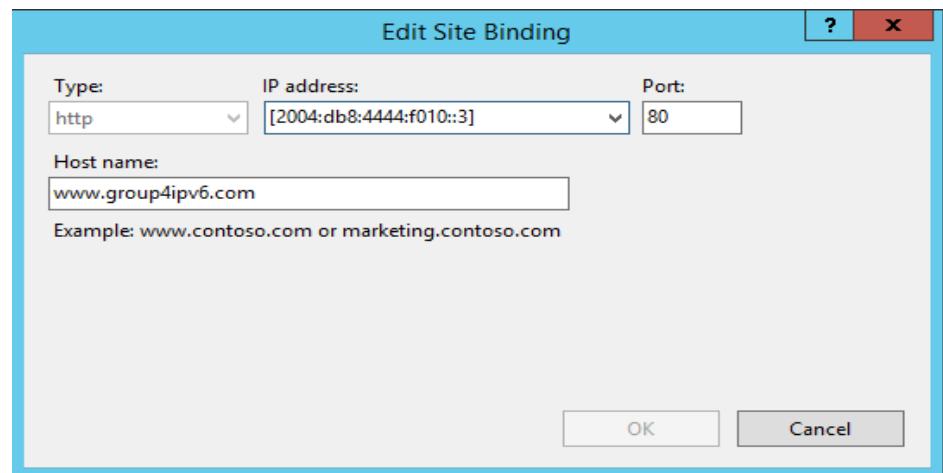


Figure 304: Check the Site Binding

IPv6 Tunneling

Step 1 : On a router, create the tunnel interface, set the ipv6 address and specify its cloud-facing IPV4 interface as the tunnel source. The tunnel destination is 200.200.202.11 which is the neighbor IP address.

```
G4Router(config)#interface Tunnel8
G4Router(config-if)#
*Jan  9 00:10:36.351: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel8, changed state to down
G4Router(config-if)#ipv6 address 2000:FE8E:AAAA:B005::3/48
G4Router(config-if)#ipv6 enable
G4Router(config-if)#tunnel source 200.200.202.7
G4Router(config-if)#tunnel mode ipv6ip
G4Router(config-if)#tunnel destination 200.200.202.11
G4Router(config-if)#
*Jan  9 00:11:29.843: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel8, changed state to up
G4Router(config-if)#exit
```

Figure 305: Create tunnel interface at router

Step 2 : Next, set the ipv6 router OSPF and redistribute as static.

```
G4Router(config-if)#exit
G4Router(config)#ipv6 router ospf 8
G4Router(config-rtr)#router-id 8.8.8.8
G4Router(config-rtr)#redistribute static
G4Router(config-rtr)#
```

Figure 306: Set the IPv6 Router OSPF

Step 3 : After that, insert the ipv6 address of the neighbor into the terminal configuration.

```
G4Router(config-rtr)#ipv6 route 2001:db8:1234:10::/64 tunnel8
G4Router(config)#ipv6 route 2001:db8:1234:20::/64 tunnel8
G4Router(config)#ipv6 route 2001:db8:1234:30::/64 tunnel8
G4Router(config)#
G4Router(config)#ipv6 route 2001:db8:1234:50::/64 tunnel8
G4Router(config)#ipv6 route 2001:db8:1234:100::/64 tunnel8
G4Router(config)#ipv6 route 2000:FE8E:AAAA:B005::/48 tunnel8
G4Router(config)#
G4Router(config)#exit
G4Router#copy
*Jan  9 00:14:31.995: %SYS-5-CONFIG_I: Configured from console by console
% Incomplete command.

G4Router#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

Figure 307: Insert IPv6 address into terminal configuration

Step 4 : Set the OSPF and area of each inter-VLAN that already configure in the terminal.

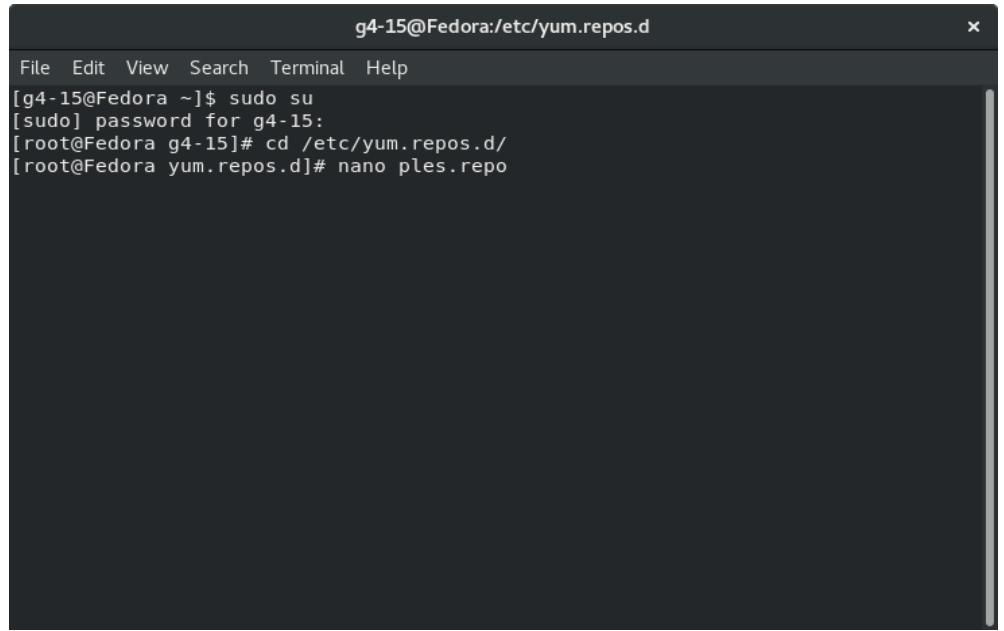
```
G4Router(config)#interface FastEthernet0/0.10
G4Router(config-subif)#ipv6 enable
G4Router(config-subif)#ipv6 ospf 8 area 0
G4Router(config-subif)#
G4Router(config-subif)#exit
G4Router(config)#
G4Router(config)#interface FastEthernet0/0.20
G4Router(config-subif)#ipv6 enable
G4Router(config-subif)#ipv6 ospf 8 area 0
G4Router(config-subif)#
G4Router(config)#interface FastEthernet0/0.30
G4Router(config-subif)#ipv6 enable
G4Router(config-subif)#ipv6 ospf 8 area 0
G4Router(config-subif)#
G4Router(config)#interface FastEthernet0/0.50
G4Router(config-subif)#
G4Router(config-subif)#
G4Router(config-subif)#
G4Router(config-subif)#ipv6 enable
G4Router(config-subif)#
G4Router(config-subif)#
G4Router(config-subif)#
G4Router(config-subif)#ipv6 ospf 8 area 0
G4Router(config-subif)#
G4Router(config)#interface FastEthernet0/0.51
G4Router(config-subif)#ipv6 enable
G4Router(config-subif)#ipv6 ospf 8 area 0
G4Router(config-subif)#
G4Router(config)#
G4Router#
```

Figure 308: Set the OSPF and area of each inter-VLAN

5.3.20 Media Streaming Server

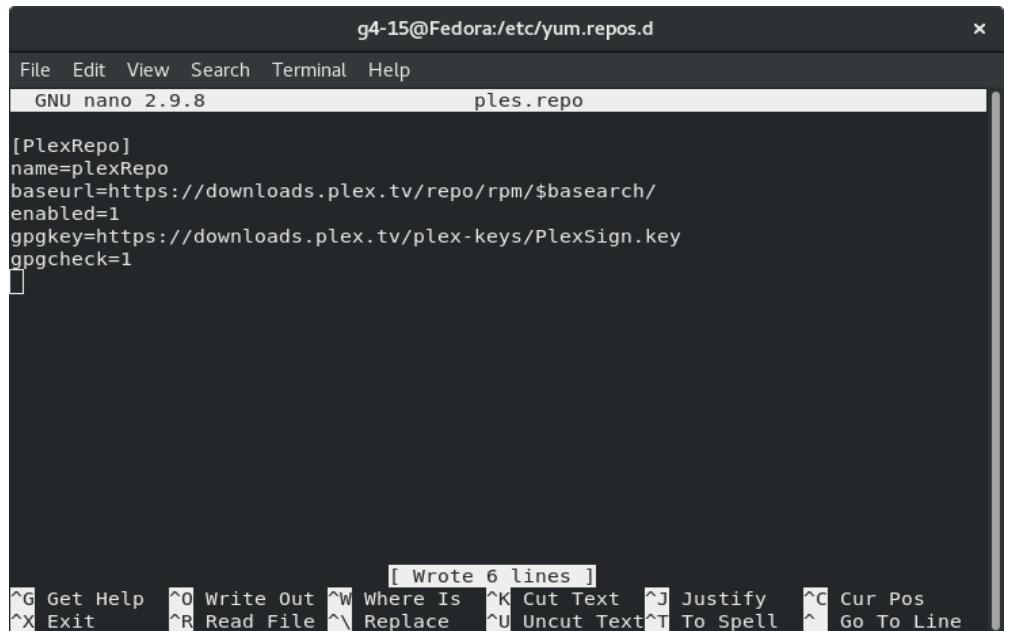
Step 1 : Open the Terminal in Fedora.

Step 2 : Go to the ‘yum.repos.d’ directory and create new repo file ‘plex.repo’ using the nano editor. Then, paste the following Plex repository configuration there.



```
g4-15@Fedora:/etc/yum.repos.d
File Edit View Search Terminal Help
[g4-15@Fedora ~]$ sudo su
[sudo] password for g4-15:
[root@Fedora g4-15]# cd /etc/yum.repos.d/
[root@Fedora yum.repos.d]# nano ples.repo
```

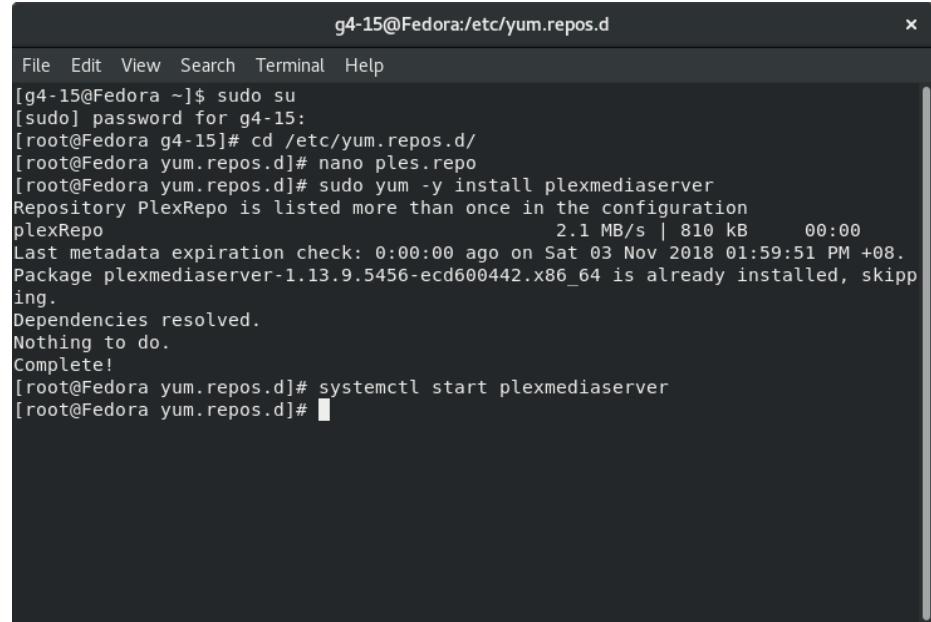
Figure 309: Create new repo file



```
g4-15@Fedora:/etc/yum.repos.d
File Edit View Search Terminal Help
GNU nano 2.9.8          ples.repo
[PlexRepo]
name=plexRepo
baseurl=https://downloads.plex.tv/repo/rpm/$basearch/
enabled=1
gpgkey=https://downloads.plex.tv/plex-keys/PlexSign.key
gpgcheck=1
[ Wrote 6 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit     ^R Read File  ^\ Replace   ^U Uncut Text^T To Spell  ^  Go To Line
```

Figure 310: Downloads the plex

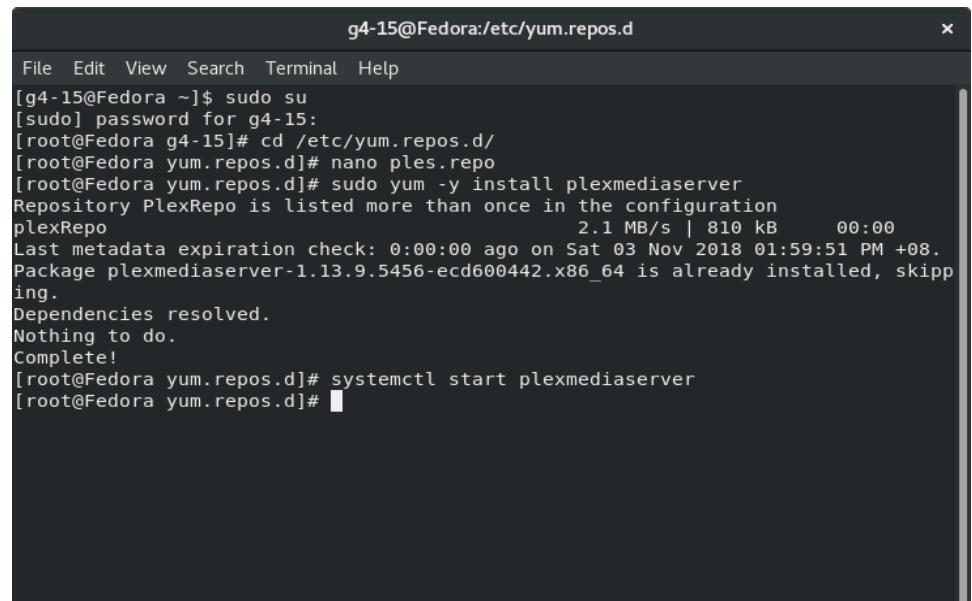
Step 3 : Now, install Plex media server on our Fedora server. Run the yum command below.



```
g4-15@Fedora:/etc/yum.repos.d
File Edit View Search Terminal Help
[g4-15@Fedora ~]$ sudo su
[sudo] password for g4-15:
[root@Fedora g4-15]# cd /etc/yum.repos.d/
[root@Fedora yum.repos.d]# nano ples.repo
[root@Fedora yum.repos.d]# sudo yum -y install plexmediaserver
Repository PlexRepo is listed more than once in the configuration
plexRepo          2.1 MB/s | 810 kB     00:00
Last metadata expiration check: 0:00:00 ago on Sat 03 Nov 2018 01:59:51 PM +08.
Package plexmediaserver-1.13.9.5456-ecd600442.x86_64 is already installed, skipping.
Dependencies resolved.
Nothing to do.
Complete!
[root@Fedora yum.repos.d]# systemctl start plexmediaserver
[root@Fedora yum.repos.d]#
```

Figure 311: Installing plex media server

Step 4 : After the installation is complete, start the plex service and enable it to launch everytime at system boot using the systemctl commands below.



```
g4-15@Fedora:/etc/yum.repos.d
File Edit View Search Terminal Help
[g4-15@Fedora ~]$ sudo su
[sudo] password for g4-15:
[root@Fedora g4-15]# cd /etc/yum.repos.d/
[root@Fedora yum.repos.d]# nano ples.repo
[root@Fedora yum.repos.d]# sudo yum -y install plexmediaserver
Repository PlexRepo is listed more than once in the configuration
plexRepo          2.1 MB/s | 810 kB     00:00
Last metadata expiration check: 0:00:00 ago on Sat 03 Nov 2018 01:59:51 PM +08.
Package plexmediaserver-1.13.9.5456-ecd600442.x86_64 is already installed, skipping.
Dependencies resolved.
Nothing to do.
Complete!
[root@Fedora yum.repos.d]# systemctl start plexmediaserver
[root@Fedora yum.repos.d]#
```

Figure 312: Start plex service

```
g4-15@Fedora:/etc/yum.repos.d
File Edit View Search Terminal Help
[g4-15@Fedora ~]$ sudo su
[sudo] password for g4-15:
[root@Fedora g4-15]# cd /etc/yum.repos.d/
[root@Fedora yum.repos.d]# nano ples.repo
[root@Fedora yum.repos.d]# sudo yum -y install plexmediaserver
Repository PlexRepo is listed more than once in the configuration
plexRepo                                         2.1 MB/s | 810 kB     00:00
Last metadata expiration check: 0:00:00 ago on Sat 03 Nov 2018 01:59:51 PM +08.
Package plexmediaserver-1.13.9.5456-ecd600442.x86_64 is already installed, skipping.
Dependencies resolved.
Nothing to do.
Complete!
[root@Fedora yum.repos.d]# systemctl start plexmediaserver
[root@Fedora yum.repos.d]# systemctl enable plexmediaserver
Synchronizing state of plexmediaserver.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable plexmediaserver
[root@Fedora yum.repos.d]#
```

Figure 313: Start and enable plex media server

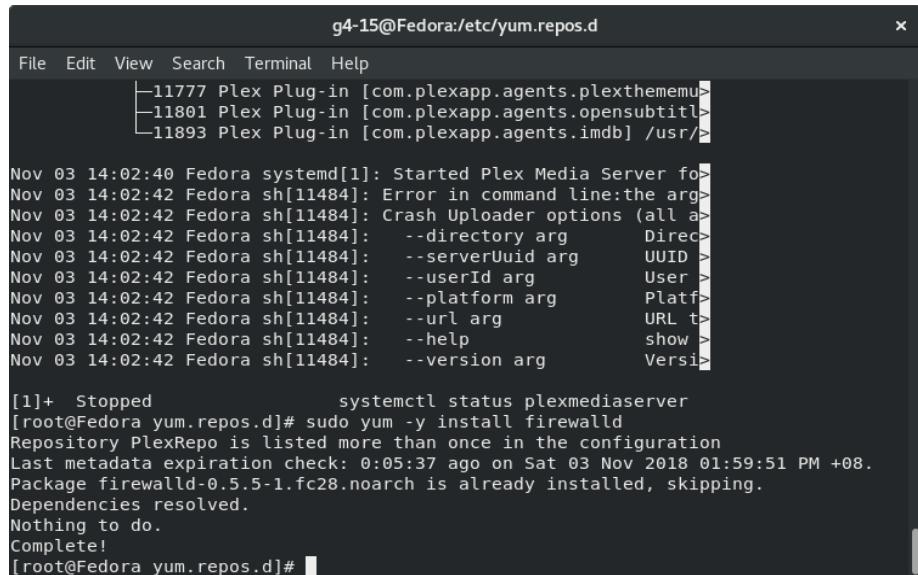
Step 5 : Plex media server has been installed. Check it using the following command. ‘`systemctl status plexmediaserver`’

```
g4-15@Fedora:/etc/yum.repos.d
File Edit View Search Terminal Help
● plexmediaserver.service - Plex Media Server for Linux
   Loaded: loaded (/usr/lib/systemd/system/plexmediaserver.service; enabled; vendor preset: disabled)
   Active: active (running) since Sat 2018-11-03 14:02:40 +08; 1min 50s ago
     Main PID: 11484 (Plex Media Serv)
        Tasks: 128 (limit: 4915)
       Memory: 308.0M
      CGroup: /system.slice/plexmediaserver.service
              └─11484 /usr/lib/plexmediaserver/Plex Media Server
                  ├─11501 Plex Plug-in [com.plexapp.system] /usr/lib/plexmediaserver/Resources/Plug-ins-ecd600442/Framework.bundle/Contents/MacOS/Plex
                  ├─11547 /usr/lib/plexmediaserver/Plex DNLA Server
                  ├─11548 /usr/lib/plexmediaserver/Tuner Service /usr/lib/plexmediaserver/Resources/Tuner/Private /usr/lib/plexmediaserver/Resources/Tuner/Private/Contents/MacOS/Tuner
                  ├─11576 Plex Plug-in [com.plexapp.agents.thetvdb] /usr/lib/plexmediaserver/Resources/Plug-ins-ecd600442/Framework.bundle/Contents/MacOS/TheTVDB
                  ├─11699 Plex Plug-in [com.plexapp.agents.plexmusic] /usr/lib/plexmediaserver/Resources/Plug-ins-ecd600442/Framework.bundle/Contents/MacOS/PlexMusic
                  ├─11771 Plex Plug-in [com.plexapp.agents.themoviedb] /usr/lib/plexmediaserver/Resources/Plug-ins-ecd600442/Framework.bundle/Contents/MacOS/TheMovieDB
                  ├─11777 Plex Plug-in [com.plexapp.agents.plexthememusic] /usr/lib/plexmediaserver/Resources/Plug-ins-ecd600442/Framework.bundle/Contents/MacOS/PlexThemeMusic
                  ├─11801 Plex Plug-in [com.plexapp.agents.opensubtitles] /usr/lib/plexmediaserver/Resources/Plug-ins-ecd600442/Framework.bundle/Contents/MacOS/OpenSubtitles
                  └─11893 Plex Plug-in [com.plexapp.agents.imdb] /usr/lib/plexmediaserver/Resources/Plug-ins-ecd600442/Framework.bundle/Contents/MacOS/IMDb

Nov 03 14:02:40 Fedora systemd[1]: Started Plex Media Server for Linux.
Nov 03 14:02:42 Fedora sh[11484]: Error in command line:the argument for option '--serverUuid' should follow immediately after the e ↵
Nov 03 14:02:42 Fedora sh[11484]: Crash Uploader options (all are required):
Nov 03 14:02:42 Fedora sh[11484]:   --directory arg      Directory to scan for crash reports
Nov 03 14:02:42 Fedora sh[11484]:   --serverUuid arg    UUID of the server that crashed
lines 1-23
```

Figure 314: Check the status of media plex server

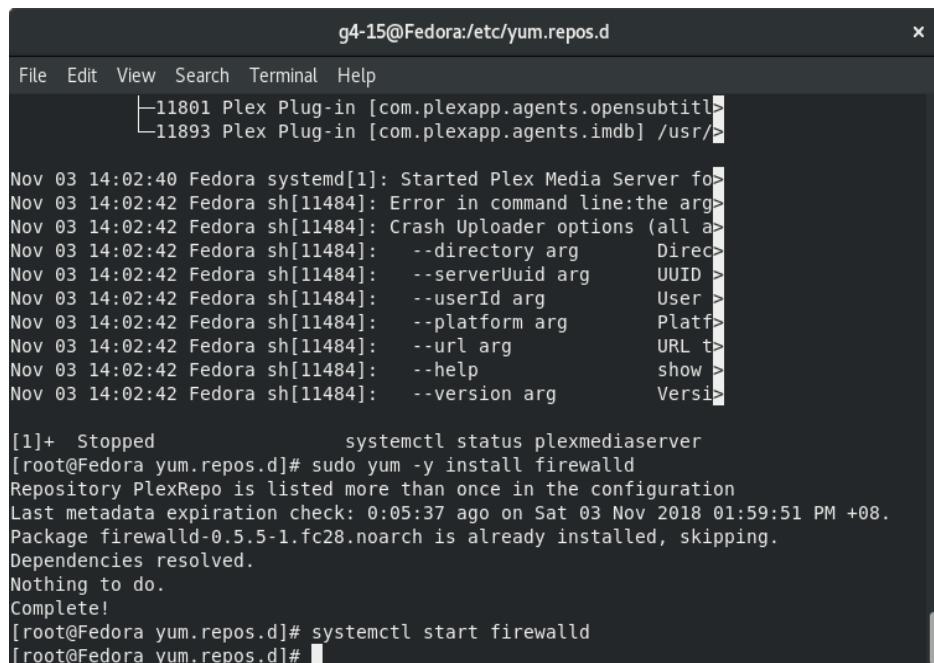
Step 6 : We will enable Firewalld services. Make sure firewalld packages are installed on the system. We can install them using the yum command below.



```
g4-15@Fedora:/etc/yum.repos.d
File Edit View Search Terminal Help
[1]+  Stopped                  systemctl status plexmediaserver
[root@Fedora yum.repos.d]# sudo yum -y install firewalld
Repository PlexRepo is listed more than once in the configuration
Last metadata expiration check: 0:05:37 ago on Sat 03 Nov 2018 01:59:51 PM +08.
Package firewalld-0.5.5-1.fc28.noarch is already installed, skipping.
Dependencies resolved.
Nothing to do.
Complete!
[root@Fedora yum.repos.d]#
```

Figure 21: Enabling Firewall services

Step 7 : Now, start the firewalld service and enable it to launch every time at the system boot.



```
g4-15@Fedora:/etc/yum.repos.d
File Edit View Search Terminal Help
[1]+  Stopped                  systemctl status plexmediaserver
[root@Fedora yum.repos.d]# sudo yum -y install firewalld
Repository PlexRepo is listed more than once in the configuration
Last metadata expiration check: 0:05:37 ago on Sat 03 Nov 2018 01:59:51 PM +08.
Package firewalld-0.5.5-1.fc28.noarch is already installed, skipping.
Dependencies resolved.
Nothing to do.
Complete!
[root@Fedora yum.repos.d]# systemctl start firewalld
[root@Fedora yum.repos.d]#
```

Figure 22: Start firewall service

Step 8 : Next, we need to add new firewalld configuration for our plex installation. Plex media server needs some port in the ‘LISTEN’ state, so we will create new firewalld XML configuration. Go to the ‘/etc/firewalld/service’ directory and create a new service firewalld configuration ‘plex.xml’ using nano. There, paste the following configuration.

```
[root@Fedora yum.repos.d]# cd /etc/firewalld/services/  
[root@Fedora services]# nano plexmediaserver.xml  
[root@Fedora services]#
```

The screenshot shows a terminal window titled 'g4-15@Fedora:/etc/firewalld/services'. The command 'nano plexmediaserver.xml' has been run, opening a nano editor window. The XML configuration for the Plex media server is displayed:

```
<?xml version="1.0" encoding="utf-8"?>  
<service>  
    <short>plexmediaserver</short>  
    <description>Ports required by plexmediaserver</description>  
    <port protocol="tcp" port="32400"></port>  
    <port protocol="udp" port="1900"></port>  
    <port protocol="tcp" port="3005"></port>  
    <port protocol="udp" port="5353"></port>  
    <port protocol="tcp" port="8324"></port>  
    <port protocol="udp" port="32410"></port>  
    <port protocol="udp" port="32412"></port>  
    <port protocol="udp" port="32413"></port>  
    <port protocol="udp" port="32414"></port>  
    <port protocol="tcp" port="32469"></port>  
</service>
```

At the bottom of the nano window, status information is shown: '[Wrote 16 lines]'. Below the status bar are various nano key bindings:

- ^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

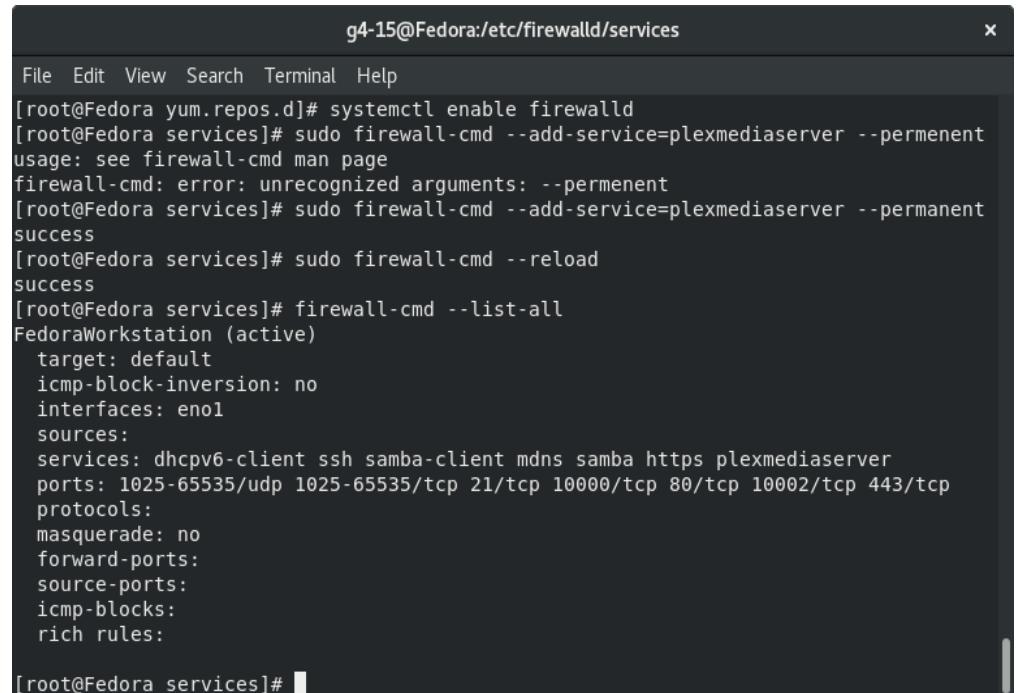
Figure 23: Add new firewall for plex

Step 9 : Now, add the ‘plexmediaserver’ service to the firewalld services list, then reload the configuration.

```
[root@Fedora services]# sudo firewall-cmd --add-service=plexmediaserver --permanent
usage: see firewall-cmd man page
firewall-cmd: error: unrecognized arguments: --permenent
[root@Fedora services]# sudo firewall-cmd --add-service=plexmediaserver --permanent
success
[root@Fedora services]# sudo firewall-cmd --reload
success
[root@Fedora services]#
```

Figure 24: Add plex media server to firewalld service

Step 10 : The plexmediaserver service has been added to firewalld. Check it using the firewalld command below.



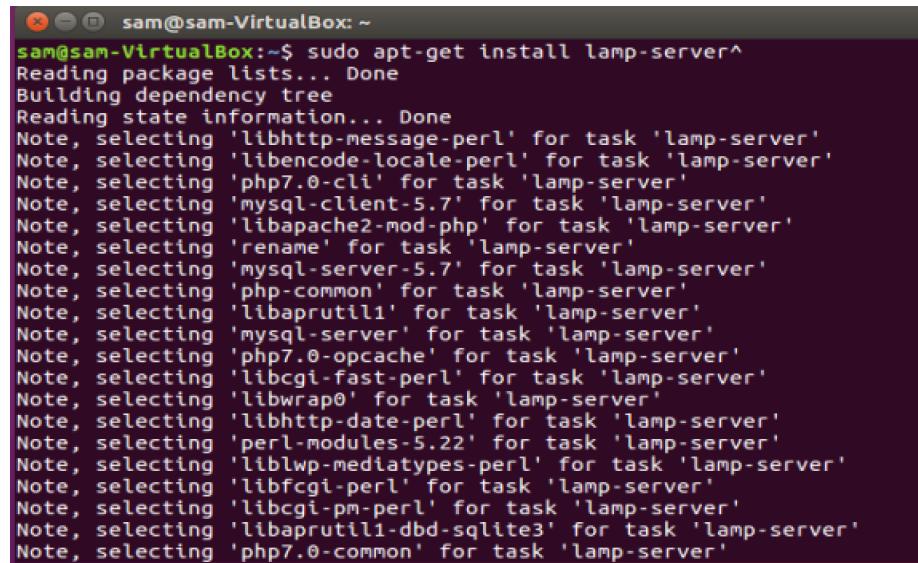
```
g4-15@Fedora:/etc/firewalld/services
File Edit View Search Terminal Help
[root@Fedora yum.repos.d]# systemctl enable firewalld
[root@Fedora services]# sudo firewall-cmd --add-service=plexmediaserver --permanent
usage: see firewall-cmd man page
firewall-cmd: error: unrecognized arguments: --permenent
[root@Fedora services]# sudo firewall-cmd --add-service=plexmediaserver --permanent
success
[root@Fedora services]# sudo firewall-cmd --reload
success
[root@Fedora services]# firewall-cmd --list-all
FedoraWorkstation (active)
  target: default
  icmp-block-inversion: no
  interfaces: en0
  sources:
    services: dhcpcv6-client ssh samba-client mdns samba https plexmediaserver
    ports: 1025-65535/udp 1025-65535/tcp 21/tcp 10000/tcp 80/tcp 10002/tcp 443/tcp
    protocols:
    masquerade: no
    forward-ports:
    source-ports:
    icmp-blocks:
    rich rules:

[root@Fedora services]#
```

Figure 319: Check the status

5.3.21 Cloud Server

Step 1 : Install lamp server.



```
 sam@sam-VirtualBox: ~
sam@sam-VirtualBox:~$ sudo 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'
Note, selecting 'php7.0-cli' for task 'lamp-server'
Note, selecting 'mysql-client-5.7' for task 'lamp-server'
Note, selecting 'libapache2-mod-php' for task 'lamp-server'
Note, selecting 'rename' for task 'lamp-server'
Note, selecting 'mysql-server-5.7' for task 'lamp-server'
Note, selecting 'php-common' for task 'lamp-server'
Note, selecting 'libaprutil1' for task 'lamp-server'
Note, selecting 'mysql-server' for task 'lamp-server'
Note, selecting 'php7.0-opcache' for task 'lamp-server'
Note, selecting 'libcgi-fast-perl' for task 'lamp-server'
Note, selecting 'libwrap0' for task 'lamp-server'
Note, selecting 'libhttp-date-perl' for task 'lamp-server'
Note, selecting 'perl-modules-5.22' for task 'lamp-server'
Note, selecting 'liblwp-mediatypes-perl' for task 'lamp-server'
Note, selecting 'libfcgi-perl' for task 'lamp-server'
Note, selecting 'libcgi-pm-perl' for task 'lamp-server'
Note, selecting 'libaprutil1-dbd-sqlite3' for task 'lamp-server'
Note, selecting 'php7.0-common' for task 'lamp-server'
```

Figure 320: Installing Lamp Server

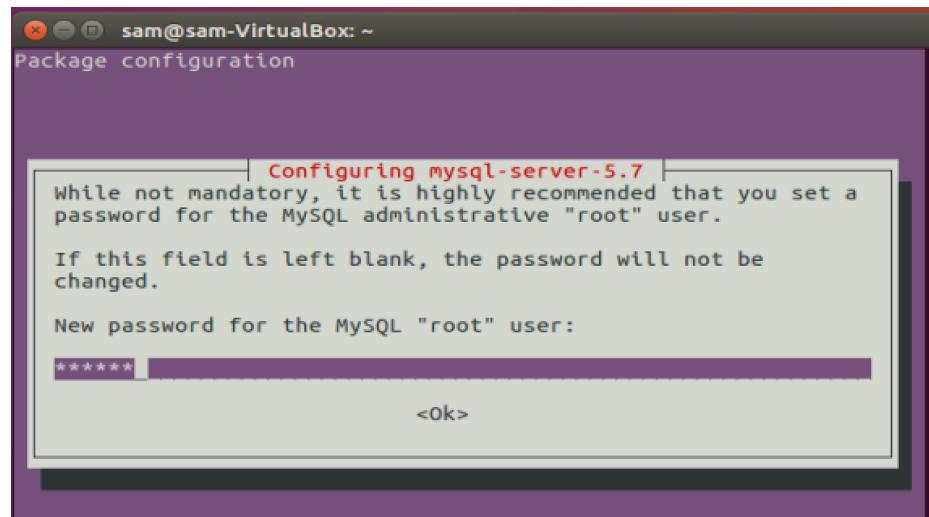
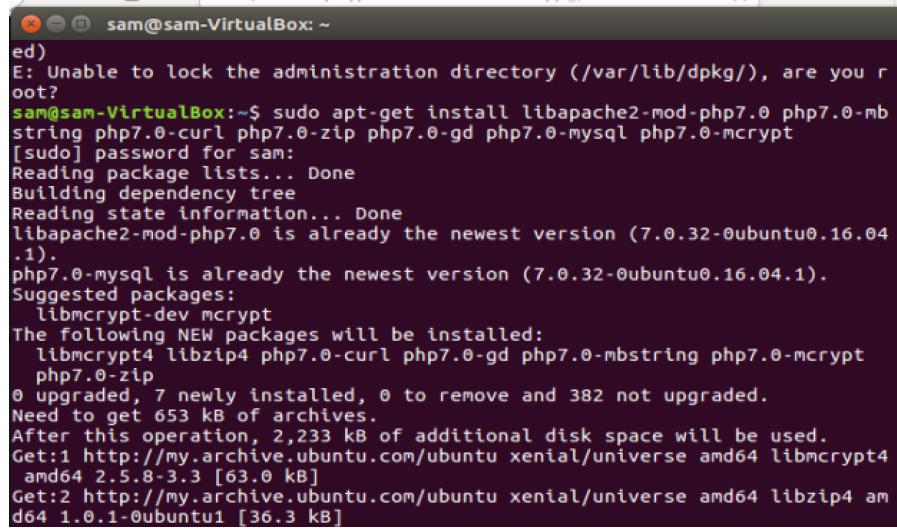


Figure 25: Configuring root password for MySQL

Step 2 : Configure root password for MySQL.

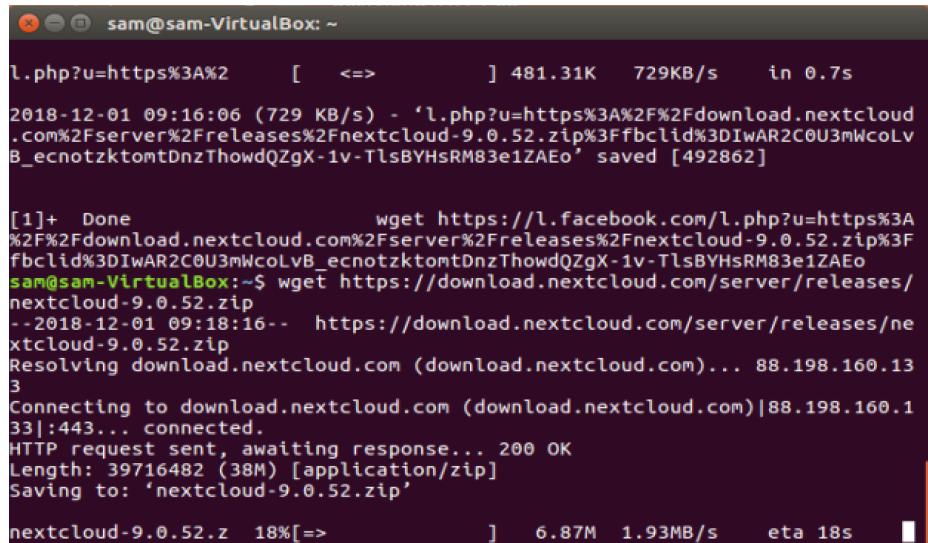
Step 3 : Install related dependencies.



```
ed)
E: Unable to lock the administration directory (/var/lib/dpkg/), are you root?
[sudo] password for sam:
Reading package lists... Done
Building dependency tree
Reading state information... Done
libapache2-mod-php7.0 is already the newest version (7.0.32-0ubuntu0.16.04.1).
php7.0-mysql is already the newest version (7.0.32-0ubuntu0.16.04.1).
Suggested packages:
  libmcrypt-dev mcrypt
The following NEW packages will be installed:
  libmcrypt4 libzip4 php7.0-curl php7.0-gd php7.0-mbstring php7.0-mcrypt
  php7.0-zip
0 upgraded, 7 newly installed, 0 to remove and 382 not upgraded.
Need to get 653 kB of archives.
After this operation, 2,233 kB of additional disk space will be used.
Get:1 http://my.archive.ubuntu.com/ubuntu xenial/universe amd64 libmcrypt4
  amd64 2.5.8-3.3 [63.0 kB]
Get:2 http://my.archive.ubuntu.com/ubuntu xenial/universe amd64 libzip4 am
d64 1.0.1-0ubuntu1 [36.3 kB]
```

Figure 322: Install related dependencies

Step 4 : Download Nextcloud zip files.



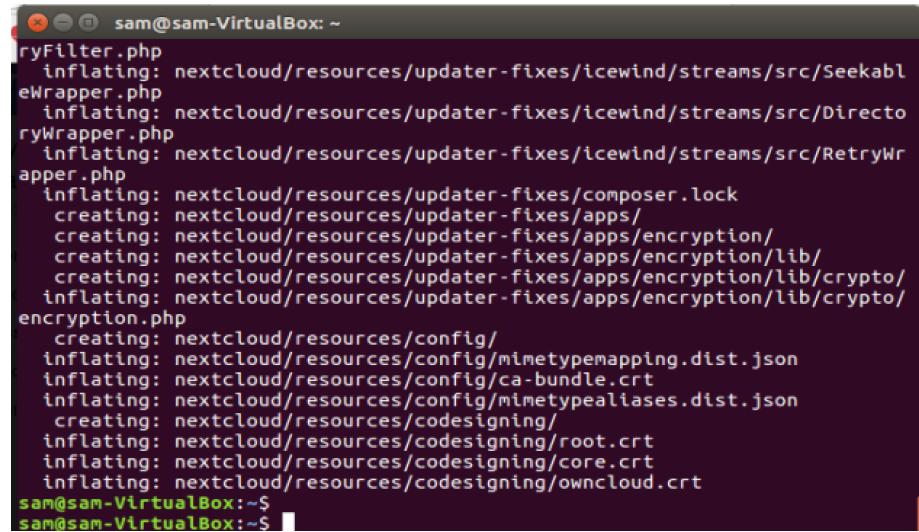
```
l.php?u=https%3A%2F%2Fdownload.nextcloud.com%2Fserver%2Freleases%2Fnextcloud-9.0.52.zip%3Ffbclid%3DIwAR2C0U3mWcoLvB_ecnotzktomtDnzThowdQZgX-1v-TlsBYHsRM83e1ZAEo' saved [492862]

[1]+  Done                      wget https://l.facebook.com/l.php?u=https%3A%2F%2Fdownload.nextcloud.com%2Fserver%2Freleases%2Fnextcloud-9.0.52.zip%3Ffbclid%3DIwAR2C0U3mWcoLvB_ecnotzktomtDnzThowdQZgX-1v-TlsBYHsRM83e1ZAEo
sam@sam-VirtualBox:~$ wget https://download.nextcloud.com/server/releases/nextcloud-9.0.52.zip
--2018-12-01 09:18:16--  https://download.nextcloud.com/server/releases/nextcloud-9.0.52.zip
Resolving download.nextcloud.com (download.nextcloud.com)... 88.198.160.13
Connecting to download.nextcloud.com (download.nextcloud.com)|88.198.160.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 39716482 (38M) [application/zip]
Saving to: 'nextcloud-9.0.52.zip'

nextcloud-9.0.52.z 18%[=>          ]  6.87M  1.93MB/s  eta 18s
```

Figure 26: Download Nextcloud zip files

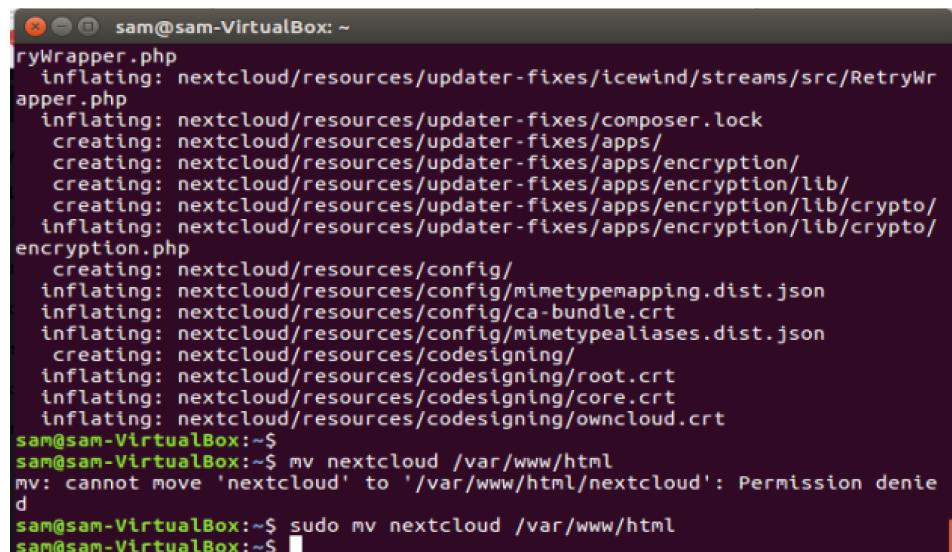
Step 5 : Extract Nextcloud.zip.



```
tryFilter.php
    inflating: nextcloud/resources/updater-fixes/icewindstreams/src/SeekableWrapper.php
    inflating: nextcloud/resources/updater-fixes/icewindstreams/src/DirectoryWrapper.php
    inflating: nextcloud/resources/updater-fixes/icewindstreams/src/RetryWrapper.php
    inflating: nextcloud/resources/updater-fixes/composer.lock
    creating: nextcloud/resources/updater-fixes/apps/
    creating: nextcloud/resources/updater-fixes/apps/encryption/
    creating: nextcloud/resources/updater-fixes/apps/encryption/lib/
    creating: nextcloud/resources/updater-fixes/apps/encryption/lib/crypto/
    inflating: nextcloud/resources/updater-fixes/apps/encryption/lib/crypto/
    creating: nextcloud/resources/config/
    inflating: nextcloud/resources/config/mimetypemapping.dist.json
    inflating: nextcloud/resources/config/ca-bundle.crt
    inflating: nextcloud/resources/config/mimetypealiases.dist.json
    creating: nextcloud/resources/codesigning/
    inflating: nextcloud/resources/codesigning/root.crt
    inflating: nextcloud/resources/codesigning/core.crt
    inflating: nextcloud/resources/codesigning/owncloud.crt
sam@sam-VirtualBox:~$
```

Figure 27: Extract Nextcloud.zip

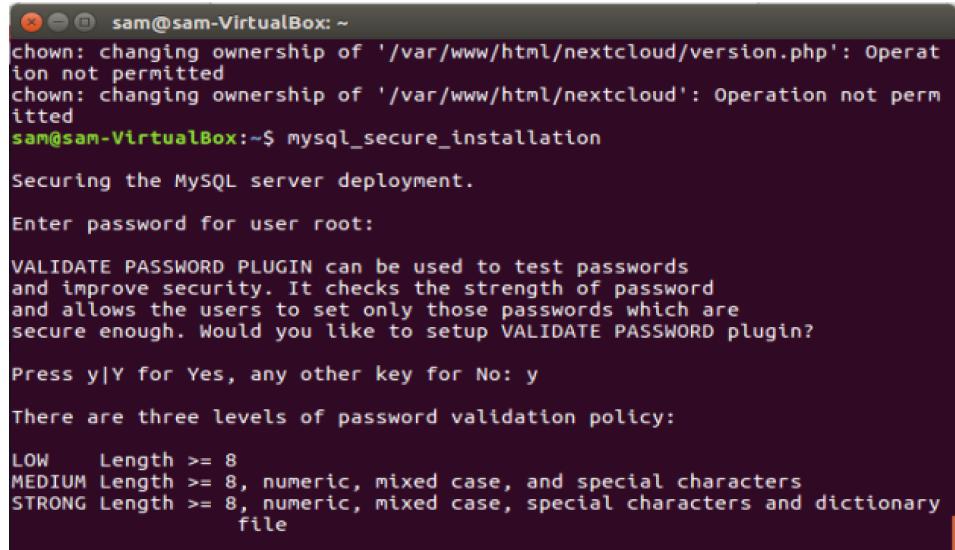
Step 6 : Move the extracted files to /var/www/html.



```
tryWrapper.php
    inflating: nextcloud/resources/updater-fixes/icewindstreams/src/RetryWrapper.php
    inflating: nextcloud/resources/updater-fixes/composer.lock
    creating: nextcloud/resources/updater-fixes/apps/
    creating: nextcloud/resources/updater-fixes/apps/encryption/
    creating: nextcloud/resources/updater-fixes/apps/encryption/lib/
    creating: nextcloud/resources/updater-fixes/apps/encryption/lib/crypto/
    inflating: nextcloud/resources/updater-fixes/apps/encryption/lib/crypto/
    creating: nextcloud/resources/config/
    inflating: nextcloud/resources/config/mimetypemapping.dist.json
    inflating: nextcloud/resources/config/ca-bundle.crt
    inflating: nextcloud/resources/config/mimetypealiases.dist.json
    creating: nextcloud/resources/codesigning/
    inflating: nextcloud/resources/codesigning/root.crt
    inflating: nextcloud/resources/codesigning/core.crt
    inflating: nextcloud/resources/codesigning/owncloud.crt
sam@sam-VirtualBox:~$ sam@sam-VirtualBox:~$ mv nextcloud /var/www/html
mv: cannot move 'nextcloud' to '/var/www/html/nextcloud': Permission denied
sam@sam-VirtualBox:~$ sudo mv nextcloud /var/www/html
sam@sam-VirtualBox:~$
```

Figure 28: Move the extracted file

Step 7 : Change ownership and setup MySQL.



```
 sam@sam-VirtualBox: ~
chown: changing ownership of '/var/www/html/nextcloud/version.php': Operation not permitted
chown: changing ownership of '/var/www/html/nextcloud': Operation not permitted
sam@sam-VirtualBox:~$ mysql_secure_installation

Securing the MySQL server deployment.

Enter password for user root:

VALIDATE PASSWORD PLUGIN can be used to test passwords
and improve security. It checks the strength of password
and allows the users to set only those passwords which are
secure enough. Would you like to setup VALIDATE PASSWORD plugin?

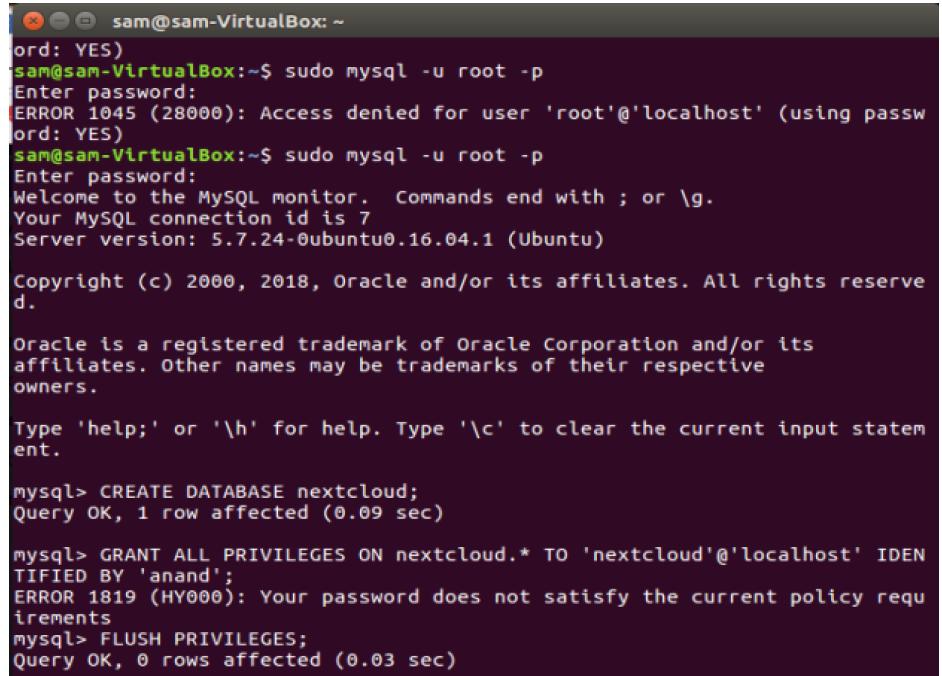
Press y|Y for Yes, any other key for No: y

There are three levels of password validation policy:

LOW    Length >= 8
MEDIUM Length >= 8, numeric, mixed case, and special characters
STRONG Length >= 8, numeric, mixed case, special characters and dictionary
file
```

Figure 29: Change the ownership and setup MySQL

Step 8 : Create database Nextcloud and admin user.



```
 sam@sam-VirtualBox: ~
ord: YES)
sam@sam-VirtualBox:~$ sudo mysql -u root -p
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)
sam@sam-VirtualBox:~$ sudo mysql -u root -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 7
Server version: 5.7.24-0ubuntu0.16.04.1 (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.

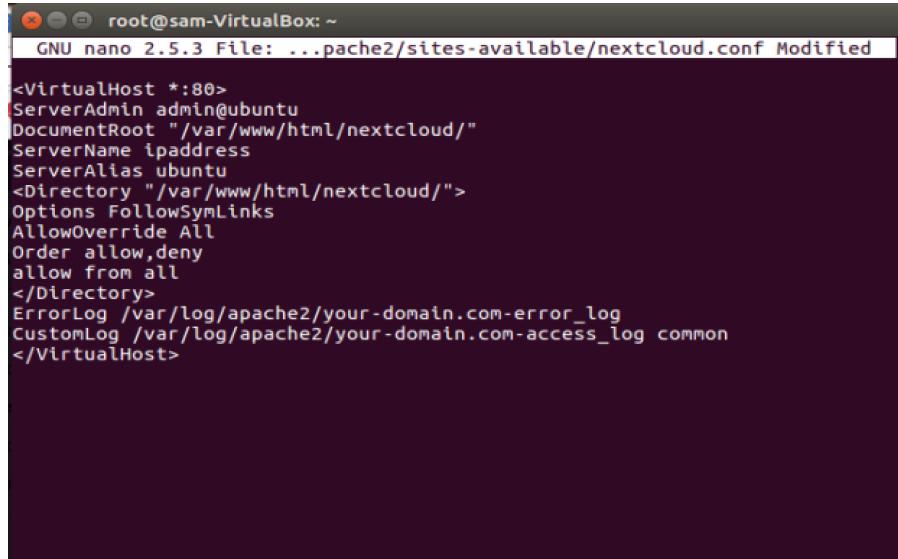
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> CREATE DATABASE nextcloud;
Query OK, 1 row affected (0.09 sec)

mysql> GRANT ALL PRIVILEGES ON nextcloud.* TO 'nextcloud'@'localhost' IDENTIFIED BY 'anand';
ERROR 1819 (HY000): Your password does not satisfy the current policy requirements
mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.03 sec)
```

Figure 30: Create database Nextcloud and admin user

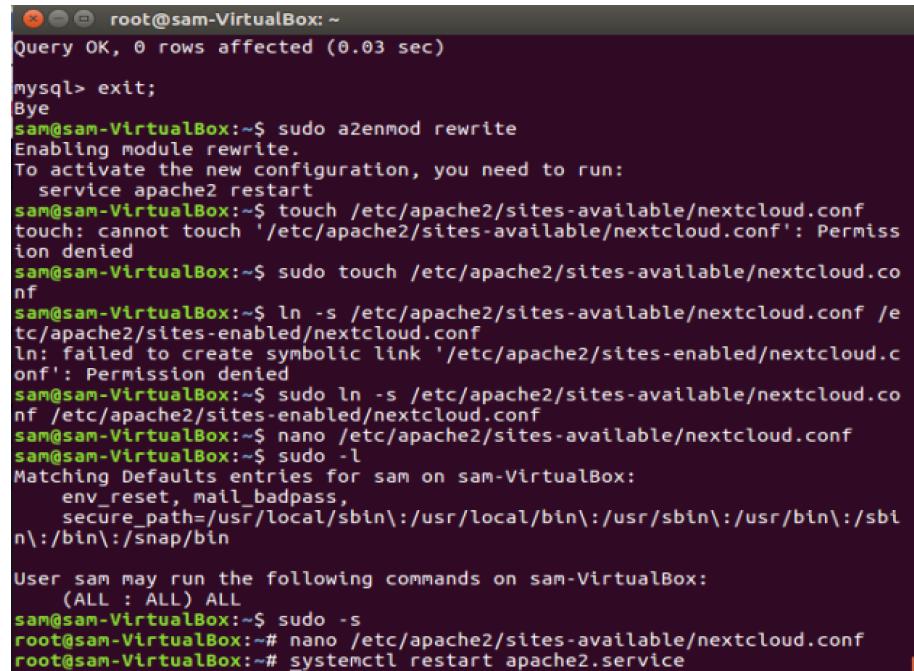
Step 9 Setup Nextcloud configuration file.



The screenshot shows a terminal window titled "root@sam-VirtualBox: ~". It displays the contents of the Apache2 configuration file for Nextcloud, specifically the "/etc/apache2/sites-available/nextcloud.conf" file. The configuration includes a VirtualHost block for port 80, specifying the ServerAdmin, DocumentRoot, ServerName, and ServerAlias. It also defines a Directory block for the Nextcloud directory, setting options like FollowSymLinks, AllowOverride, Order, and Allow/Deny. Log paths for ErrorLog and CustomLog are also specified. The file ends with a closing </VirtualHost> tag.

Figure 31: Setup Nextcloud configuration file

Step 10 : Enable module rewrite & restart apache2 to complete the installation.



The screenshot shows a terminal window titled "root@sam-VirtualBox: ~". It starts with a MySQL command: "Query OK, 0 rows affected (0.03 sec)". Then, the user exits MySQL with "exit;". The next series of commands are run as root: "sudo a2enmod rewrite", "touch /etc/apache2/sites-available/nextcloud.conf", "ln -s /etc/apache2/sites-available/nextcloud.conf /etc/apache2/sites-enabled/nextcloud.conf", "sudo ln -s /etc/apache2/sites-enabled/nextcloud.conf", "nano /etc/apache2/sites-available/nextcloud.conf", "sudo -l", "User sam may run the following commands on sam-VirtualBox: (ALL : ALL)", "sudo -s", "nano /etc/apache2/sites-available/nextcloud.conf", and finally "systemctl restart apache2.service". The terminal uses color coding for different command types and output levels.

Figure 32: Enable module rewrite and restart apache2

5.3.22 Remote Login using SSH

Configuration SSH in Router

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

Step 2 : Install SSH using this command below.

```
#conf t
#ip domain-name group4.com
#crypto key generate rsa general-keys modulus 1024
#line vty 0 4
#transport input ssh
#username group4 privilege 15 secret g4123456
#ip ssh version 2
#exit
#wr
```

Figure 33: SSH configuration in router

Configuration SSH in Switch

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

Step 2 : Install SSH using this command below.

```
#conf t
#ip address 192.168.50.50 255.255.255.192
#ip domain-name group4.com
#crypto key generate rsa general-keys modulus 1024
#line vty 0 4
#transport input ssh
#username group4 privilege 15 secret g4123456
#ip ssh version 2
#exit
#wr
```

Figure 34: SSH configuration in switch

Configuration SSH in Ubuntu

Step 1 : Open Terminal in Ubuntu.

Step 2 : Firstly, update package list from the repository before installing the SSH.

Step 3 : Then, install openssh-server package using the command below.

```
g4-16@Ubuntu:~$ sudo apt install -y openssh-server
sudo: unable to resolve host Ubuntu: Connection timed out
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 32 not upgraded.
```

Figure 35: SSH configuration in Ubuntu

Step 4 : SSH service should be started and enabled by default after the installation. To do a confirmation, it can be checked the status using command below.

```
g4-16@Ubuntu:~$ sudo systemctl status ssh
sudo: unable to resolve host Ubuntu: Connection timed out
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor pre
  Active: active (running) since Mon 2018-10-15 10:07:33 EDT; 7h ago
    Process: 2895 ExecReload=/bin/kill -HUP $MAINPID (code=exited, status
   Main PID: 1538 (sshd)
     CGroup: /system.slice/ssh.service
             └─1538 /usr/sbin/sshd -D

Oct 15 10:07:46 Ubuntu systemd[1]: Reloading OpenBSD Secure Shell serve
Oct 15 10:07:46 Ubuntu sshd[1538]: Received SIGHUP; restarting.
Oct 15 10:07:46 Ubuntu systemd[1]: Reloaded OpenBSD Secure Shell server
Oct 15 10:07:46 Ubuntu sshd[1538]: Server listening on 0.0.0.0 port 22.
Oct 15 10:07:46 Ubuntu sshd[1538]: Server listening on :: port 22.
Oct 15 10:07:56 Ubuntu systemd[1]: Reloading OpenBSD Secure Shell serve
Oct 15 10:07:56 Ubuntu sshd[1538]: Received SIGHUP; restarting.
Oct 15 10:07:56 Ubuntu systemd[1]: Reloaded OpenBSD Secure Shell server
Oct 15 10:07:56 Ubuntu sshd[1538]: Server listening on 0.0.0.0 port 22.
Oct 15 10:07:56 Ubuntu sshd[1538]: Server listening on :: port 22.

[2]+  Stopped                  sudo systemctl status ssh
```

Figure 36: Check the status of the SSH

Configuration SSH in Fedora

Step 1 : Open PuTTY Terminal.

Step 2 : Change User to root.

```
[g4-15@kifly ~]$ sudo su  
[sudo] password for g4-15:
```

Figure 37: Change user to root

Step 3 : Install SSH using command as shown below.

```
[root@kifly g4-15]# yum install openssh-server  
Fedora 28 - x86_64 - Updates 1.2 MB/s | 25 MB 00:20  
Last metadata expiration check: 0:00:16 ago on Wed 03 Oct 2018 01:41:33 PM +08.  
Package openssh-server-7.8p1-2.fc28.x86_64 is already installed, skipping.  
Dependencies resolved.  
Nothing to do.  
Complete!
```

Figure 38: SSH command to install

Step 4 : After finished the installation, start the SSH service.

```
[root@kifly g4-15]# /sbin/service sshd start  
Redirecting to /bin/systemctl start sshd.service
```

Figure 39: Start the SSH Service

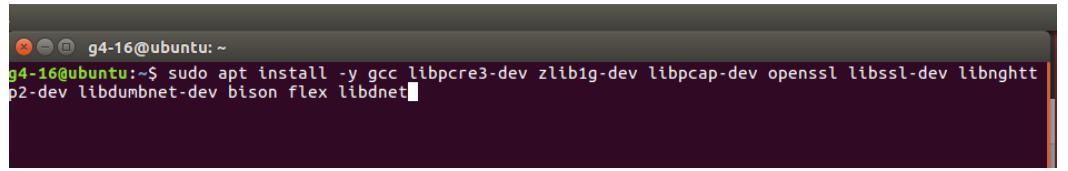
Step 5 : Then, checked the status of SSH service. If the status is active, that's

mean that the SSH is already start.

```
[root@kifly g4-15]# /sbin/service sshd status  
Redirecting to /bin/systemctl status sshd.service  
● sshd.service - OpenSSH server daemon  
  Loaded: loaded (/usr/lib/systemd/system/sshd.service; disabled; vendor prese>  
  Active: active (running) since Wed 2018-10-03 13:43:14 +08; 16s ago  
    Docs: man:sshd(8)  
          man:sshd_config(5)  
  Main PID: 5839 (sshd)  
     Tasks: 1 (limit: 4915)  
   Memory: 2.1M  
  CGroup: /system.slice/sshd.service  
          └─5839 /usr/sbin/sshd -D -oCiphers=aes256-gcm@openssh.com,sha256-p
```

Figure 40: Check the status of SSH service

5.3.23 IDS with Port Mirror

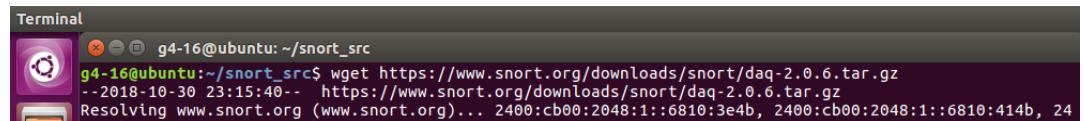


```
g4-16@ubuntu: ~
g4-16@ubuntu:~$ sudo apt install -y gcc libpcre3-dev zlib1g-dev libpcap-dev openssl libssl-dev libnghpp2-dev libdumbnet-dev bison flex libdnet
```

Figure 41: Install the library needs for snort

Step 1 : Install all the library needs for snort.

Step 2 : Install and build the Data Acquisition Library (DAQ). DAQ can be downloaded from <http://www.snort.org/snortdownloads>.



```
Terminal
g4-16@ubuntu: ~
g4-16@ubuntu:~/snort_src$ wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
--2018-10-30 23:15:40-- https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
Resolving www.snort.org (www.snort.org)... 2400:cb00:2048:1::6810:3e4b, 2400:cb00:2048:1::6810:414b, 24
```

Figure 42: Install and build DAQ

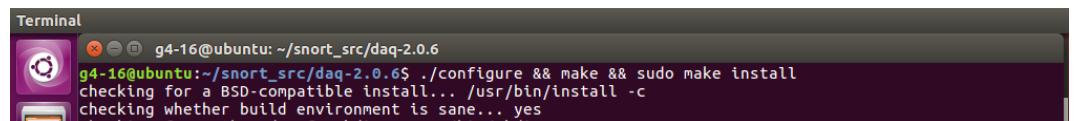
Step 3 : After downloaded it, type command “tar -xvzf daq2.0.6. tar.gz” to extract the file.



```
Terminal
g4-16@ubuntu: ~
g4-16@ubuntu:~/snort_src$ tar -xvzf daq-2.0.6.tar.gz
daq-2.0.6/
```

Figure 43: Extract the file

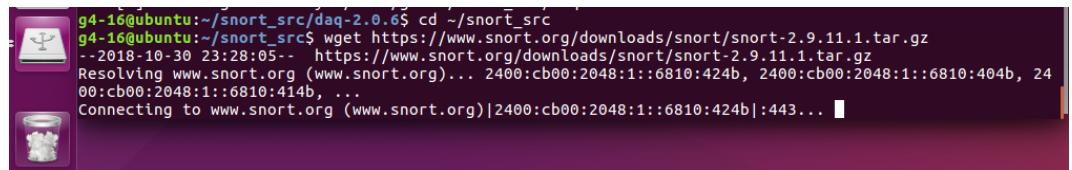
Step 4 : After that, we need to configure, make and install the file. The command is “cd /snort_src/daq2.0.6” and “./configure && make && sudo make install”.



```
Terminal
g4-16@ubuntu: ~
g4-16@ubuntu:~/snort_src/daq-2.0.6$ ./configure && make && sudo make install
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
```

Figure 44: Configure, make and install the file

Step 5 : Next, install the Snort. It can be downloaded from <http://www.snort.org/snortdownloads>. The version downloaded is snort-2.9.12.



```
g4-16@ubuntu:~/snort_src$ cd ~/snort_src
g4-16@ubuntu:~/snort_src$ wget https://www.snort.org/downloads/snort/snort-2.9.11.1.tar.gz
--2018-10-30 23:28:05-- https://www.snort.org/downloads/snort/snort-2.9.11.1.tar.gz
Resolving www.snort.org (www.snort.org)... 2400:cb00:2048:1::6810:424b, 2400:cb00:2048:1::6810:404b, 24
00:cb00:2048:1::6810:414b, ...
Connecting to www.snort.org (www.snort.org)|2400:cb00:2048:1::6810:424b|:443... [
```

Figure 45: Install the Snort

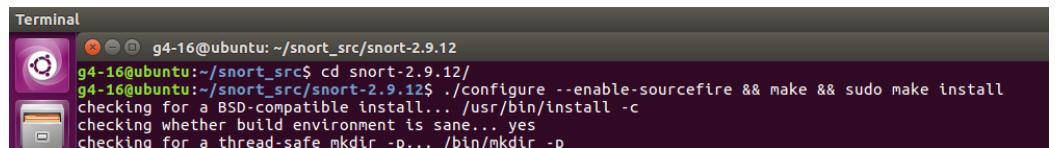
Step 6 : Then, extract the downloaded file by entering this command as shown below.



```
Terminal
g4-16@ubuntu:~/snort_src
g4-16@ubuntu:~/snort_src$ tar -xvzf snort-2.9.12.tar.gz
snort-2.9.12/
snort-2.9.12/depcomp
snort-2.9.12/tools/
```

Figure 46: Extract the downloaded file

Step 7 : After that, repeat the step in DAQ installation which is enter the same command as above.



```
Terminal
g4-16@ubuntu:~/snort_src/snort-2.9.12
g4-16@ubuntu:~/snort_src/snort-2.9.12$ ./configure --enable-sourcefire && make && sudo make install
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
```

Figure 47: Repeat step for DAQ installation

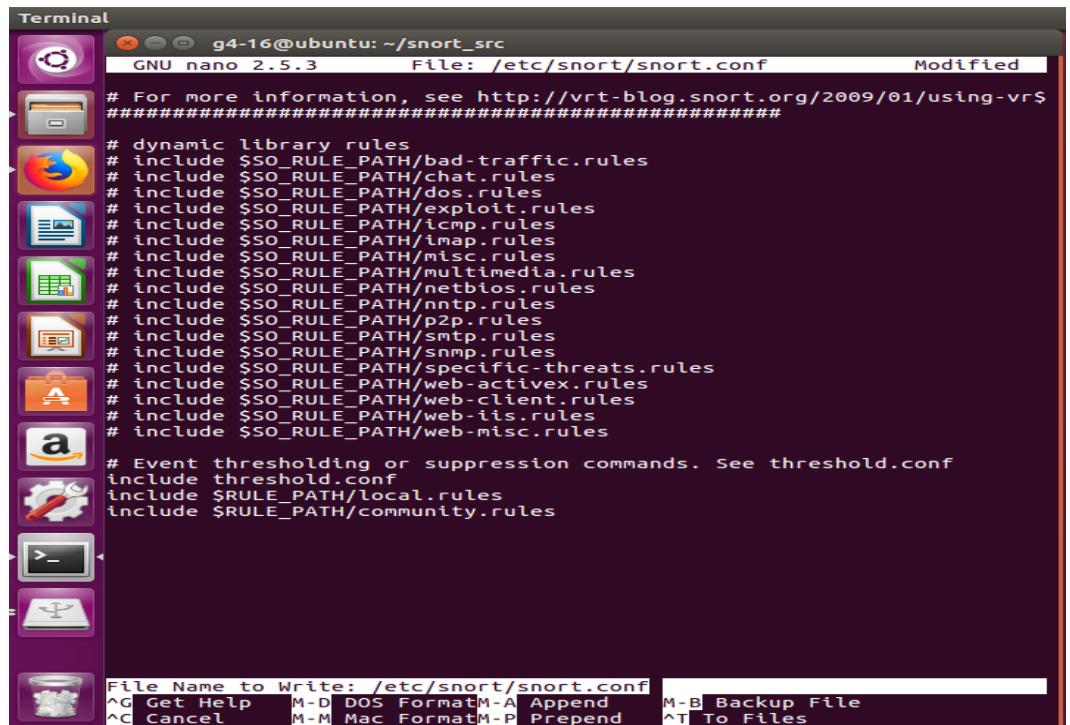
Step 8 : Create a log directory for snort and give snort ownership of it. Verify that snort is installed properly by running “snort -V”



```
o"-*- Snort! <*-
      Version 2.9.9.0 GRE (Build 56)
      By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
      Copyright (C) 2014-2016 Cisco and/or its affiliates. All rights reserved.
      Copyright (C) 1998-2013 Sourcefire, Inc., et al.
      Using libpcap version 1.5.3
      Using PCRE version: 8.31 2012-07-06
      Using ZLIB version: 1.2.8
```

Figure 48: Create a log directory and give ownership to Snort

Step 9 : Now we can download snort rule to further configuration. The rules can be downloaded from <http://www.snort.org/snortrules/> , and the rules version must same as the Snort version installed.



```
Terminal
g4-16@ubuntu: ~/snort_src
GNU nano 2.5.3      File: /etc/snort/snort.conf      Modified
#####
# For more information, see http://vrt-blog.snort.org/2009/01/using-vrs#
#####
# dynamic library rules
# include $SO_RULE_PATH/bad-traffic.rules
# include $SO_RULE_PATH/chat.rules
# include $SO_RULE_PATH/dos.rules
# include $SO_RULE_PATH/exploit.rules
# include $SO_RULE_PATH/icmp.rules
# include $SO_RULE_PATH/imap.rules
# include $SO_RULE_PATH/misc.rules
# include $SO_RULE_PATH/multimedia.rules
# include $SO_RULE_PATH/netbios.rules
# include $SO_RULE_PATH/nntp.rules
# include $SO_RULE_PATH/p2p.rules
# include $SO_RULE_PATH/smtp.rules
# include $SO_RULE_PATH/snmp.rules
# include $SO_RULE_PATH/specific-threats.rules
# include $SO_RULE_PATH/web-activex.rules
# include $SO_RULE_PATH/web-client.rules
# include $SO_RULE_PATH/web-iis.rules
# include $SO_RULE_PATH/web-misc.rules

# Event thresholding or suppression commands. See threshold.conf
include threshold.conf
include $RULE_PATH/local.rules
include $RULE_PATH/community.rules

File Name to Write: /etc/snort/snort.conf
^C Get Help      M-D DOS FormatM-A Append      M-B Backup File
^C Cancel        M-M Mac FormatM-P Prepend      ^T To Files
```

Figure 346: Download snort rule

Step 10 : Then, create a white list rules file and black list rules file using command “touch”.

```
~/Downloads$ sudo touch /etc/snort/rules/white_list.rules
~/Downloads$ sudo touch /etc/snort/rules/black_list.rules
```

Figure 347: Create white list and black list rule

Step 11 : After that, create directory for Dynamic Rules.

```
~/Downloads$ sudo mkdir /usr/local/lib/snort_dynamicrules
```

Figure 348: Create directory for dynamic rule

Step 12 : Change the ownership of /etc/snort and move directory and files from the unpacked snort rules.

```
~$ cd Downloads
~/Downloads$ sudo chown -R snort:snort /etc/snort/*
~/Downloads$ sudo mv /etc/snort/etc/* /etc/snort
~/Downloads$
```

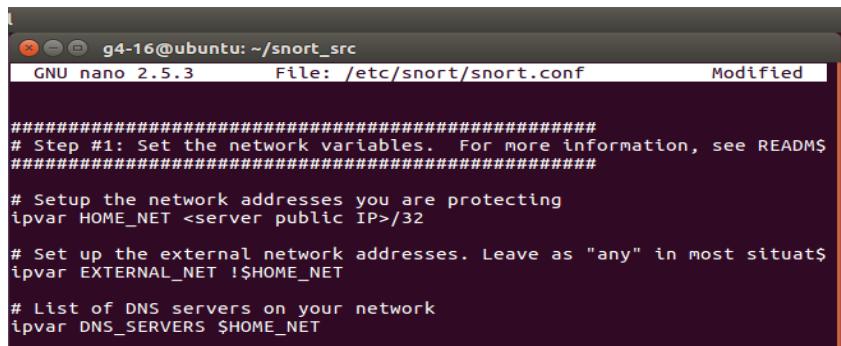
Figure 349: Change the ownership

Step 13 : Now, we can edit the default of the snort configuration.

```
root@...:
~/Downloads$ sudo nano /etc/snort/snort.conf
```

Figure 350: Edit default snort configuration

Step 14 : Scroll down to “ipvar HOME_NET” and change it to the network that we are protecting.



```
g4-16@ubuntu: ~/snort_src
GNU nano 2.5.3           File: /etc/snort/snort.conf          Modified

#####
# Step #1: Set the network variables. For more information, see README
#####

# Setup the network addresses you are protecting
ipvar HOME_NET <server public IP>/32

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

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

Figure 49: Change to network that we are protecting

Step 15 : Next, change the rules path.

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

# If you are using reputation preprocessor set these
var WHITE_LIST_PATH /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules
```

Figure 50: Change the rules path

Installation of IDS (Port Mirror)

Step 1 : Configure port monitor on switch.

```
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#monitor session 1 source interface fa0/22
Switch(config)#monitor session 1 destination interface fa0/5
Switch(config)#exit
Switch#
05:01:44: %SYS-5-CONFIG_I: Configured from console by console
Switch#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
```

Figure 51: Configuring port monitor at switch

Step 2 : Display monitor session interface by using command “show monitor session 1”.

```
Switch#
Switch#show monitor session 1
Session 1
-----
Type          : Local Session
Source Ports  :
    Both      : Fa0/22
Destination Ports : Fa0/5
    Encapsulation : Native
        Ingress: Disabled
```

Figure 52: Display monitor session

5.3.24 IPsec VPN for Remote Employees

Step 1 : Install Softether VPN server manager by selecting on the option and click Next.

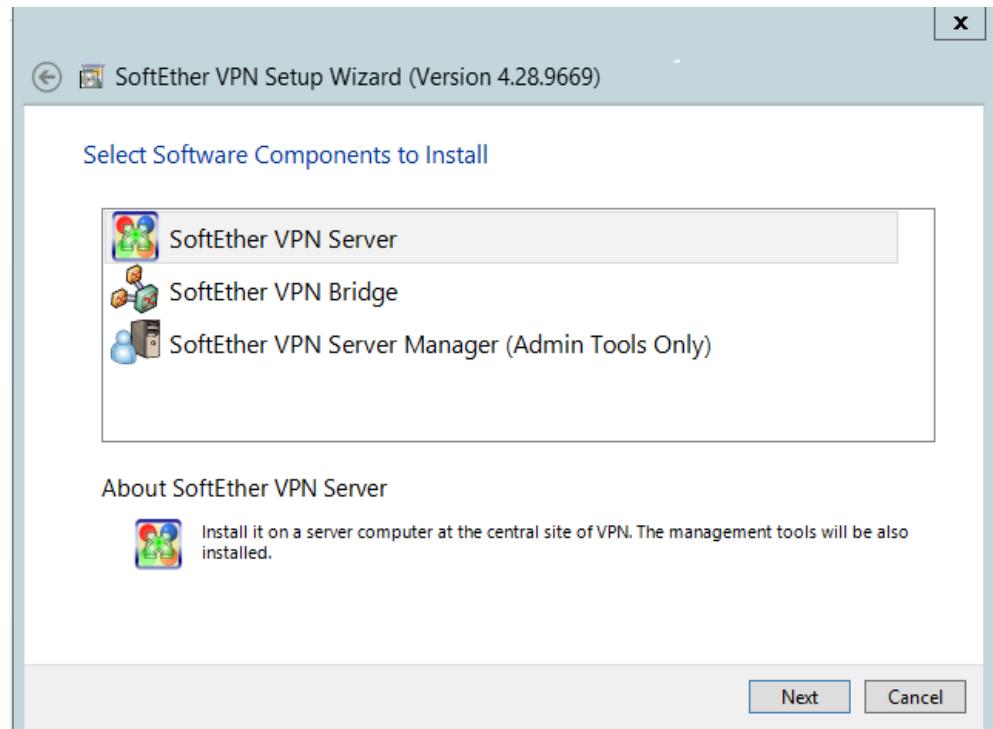


Figure 53: SoftEther Setup Wizard

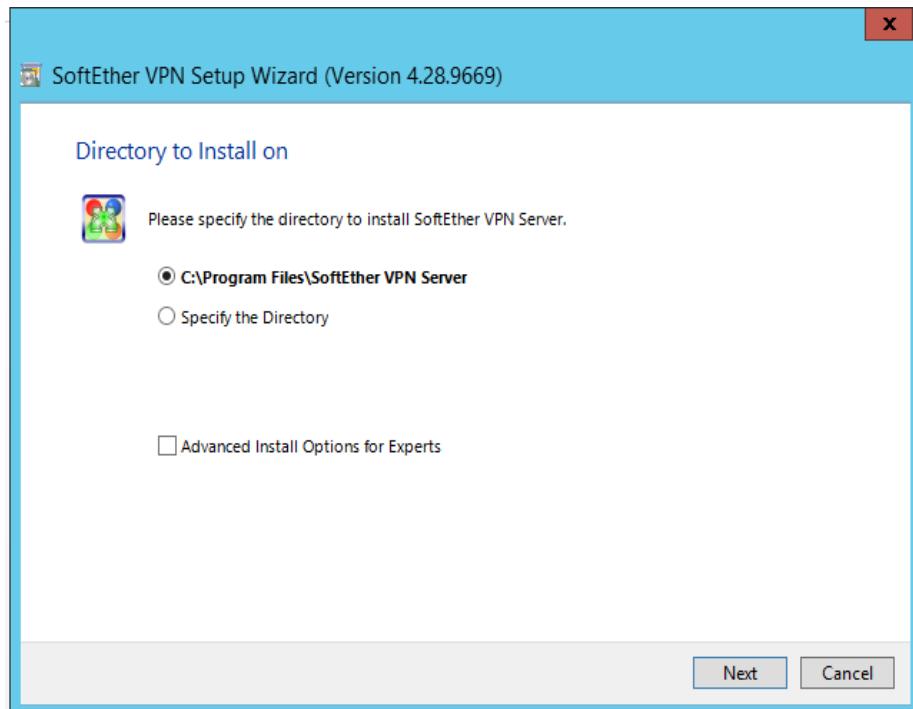


Figure 356: Specify directory to install

Step 2 : Specify the directory to install and click Next.

Step 3 : Click Next.

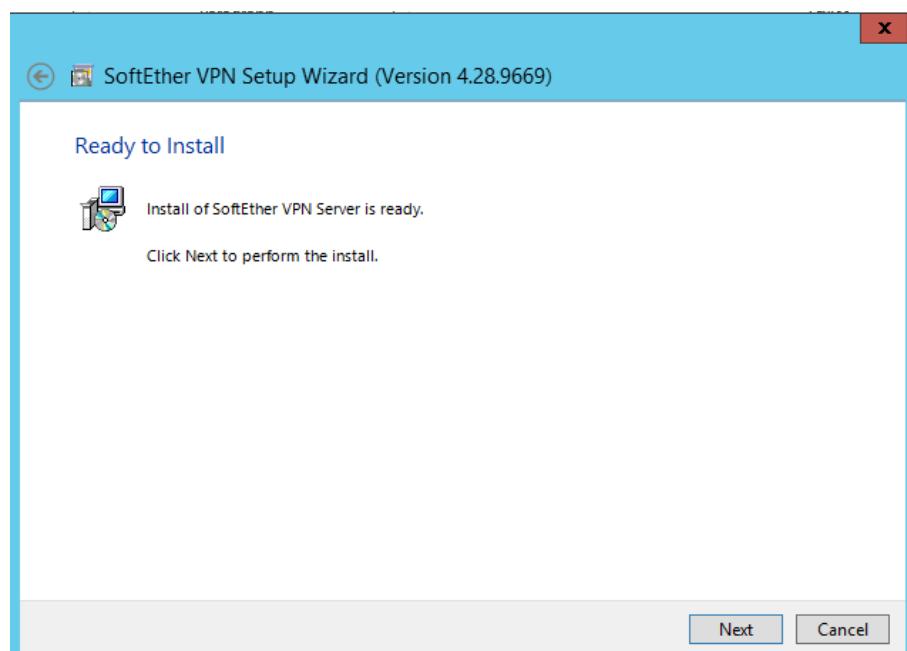


Figure 357: Install SoftEther VPN server

Step 4 : After installation completed, click finish.



Figure 54: Click on Localhost

Step 5 : Click twice on localhost.

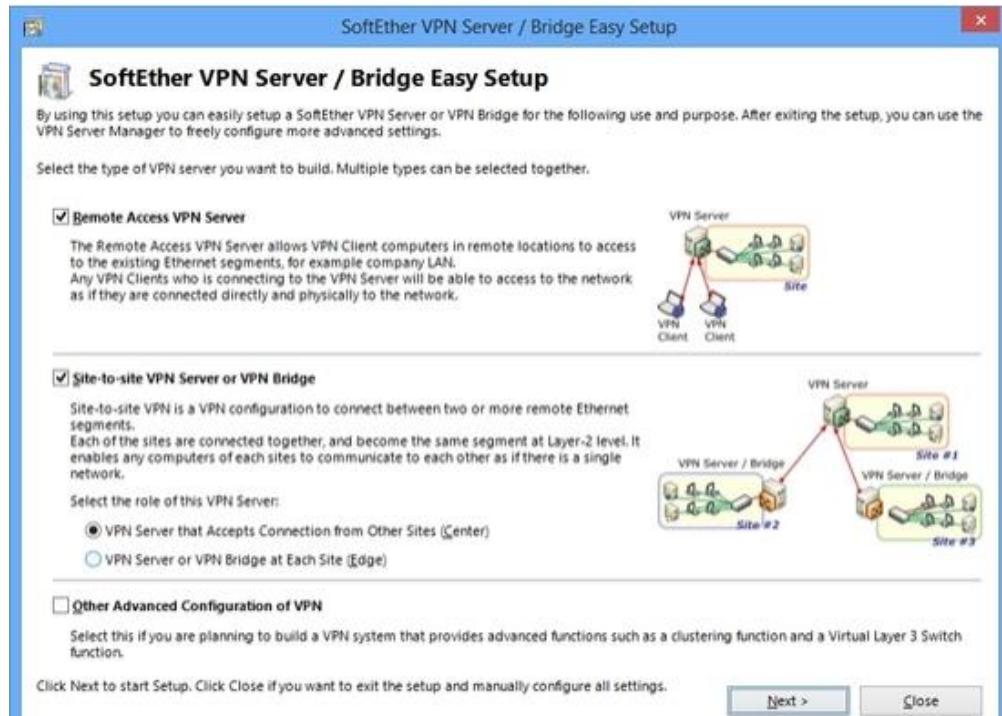


Figure 359: SoftEther VPN server/ Bridge Easy Setup

Step 6 : Click Next.

Step 7 : Create IPsec pre-shared key. When finished, click OK.

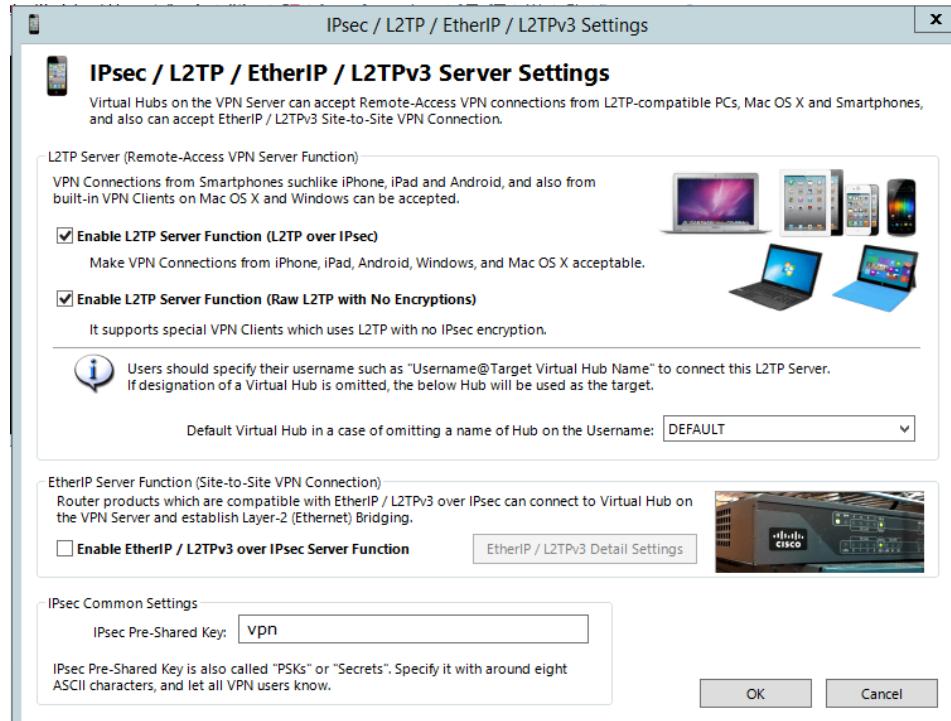


Figure 55: Create IPsec pre-shared key

Step 8 : Before creating user, create a group and full name.

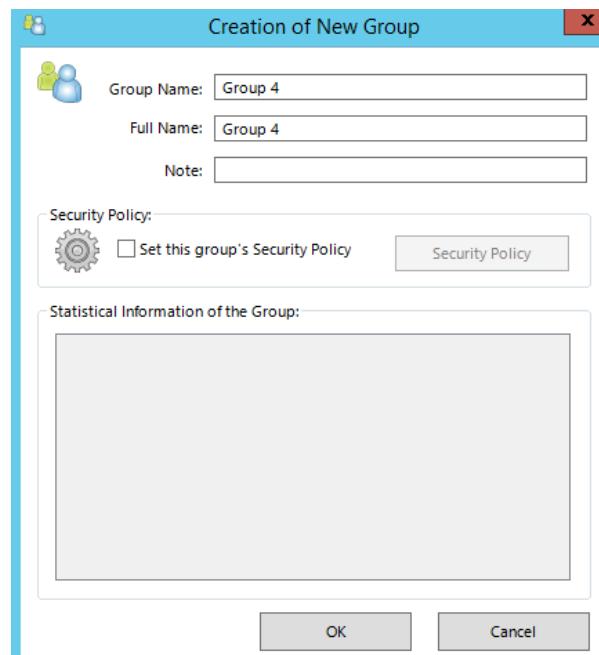


Figure 361: Create a group and full name

Step 9 : Click manage virtual hub.

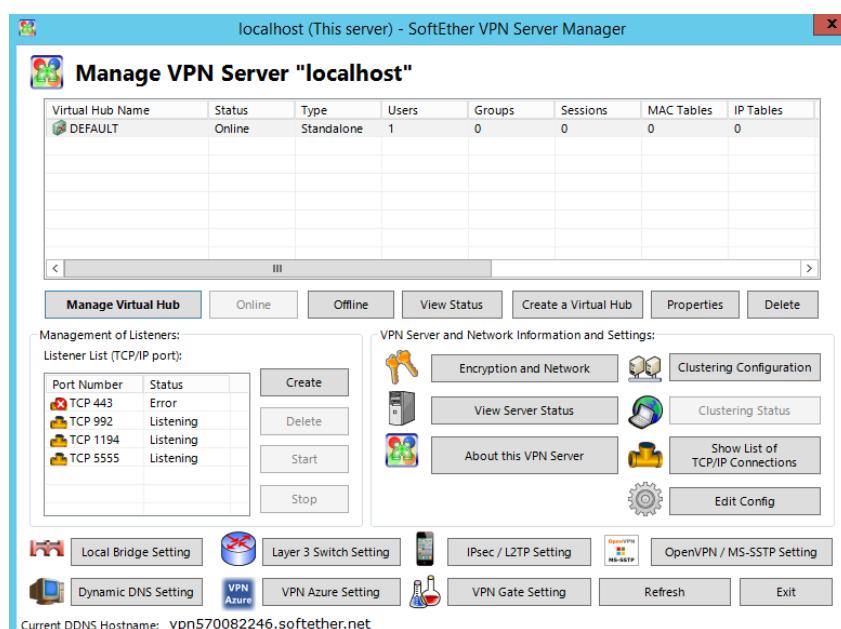


Figure 362: Manage virtual hub

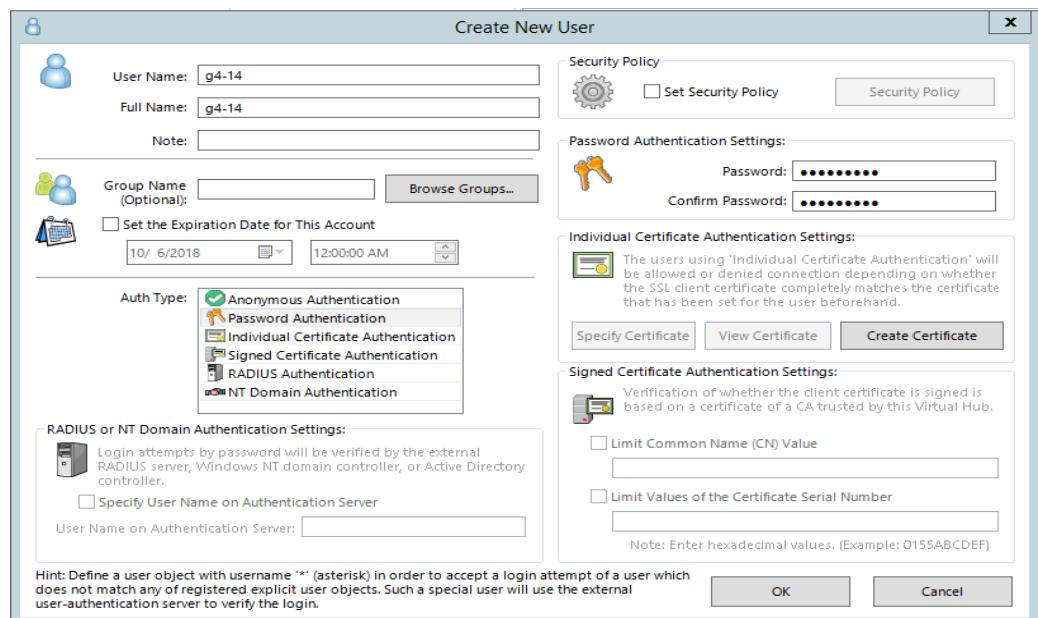


Figure 363: Create User

Step 10 : Create user by clicking manage users and fill in the details.

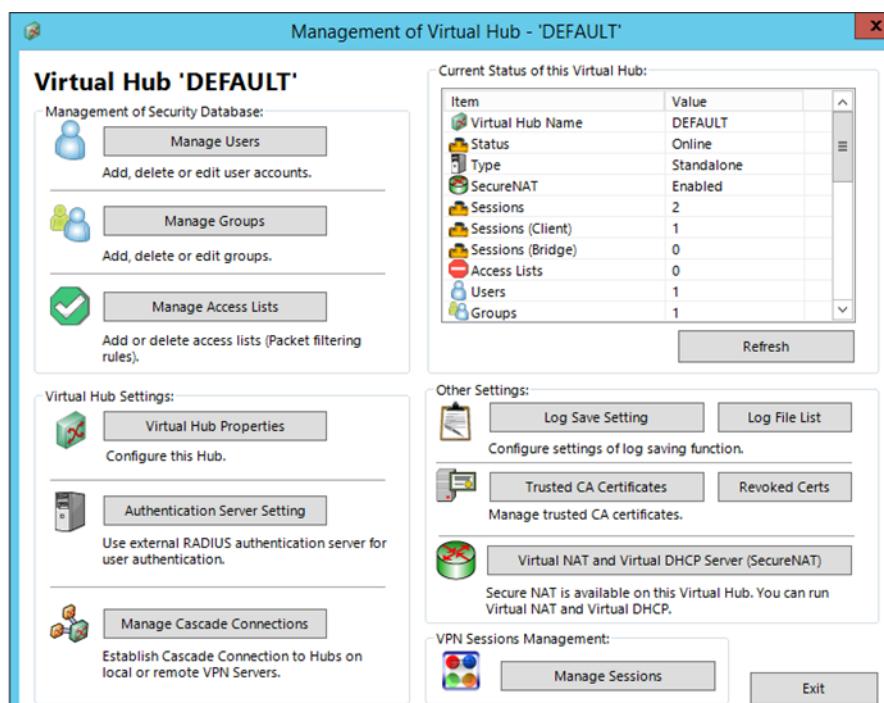


Figure 364: Management of Virtual NAT and DHCP

Step 11 : Click on virtual NAT and virtual DHCP server.

Step 12 : Enable SecureNAT. Click on SecureNAT configuration for specifying IP range.

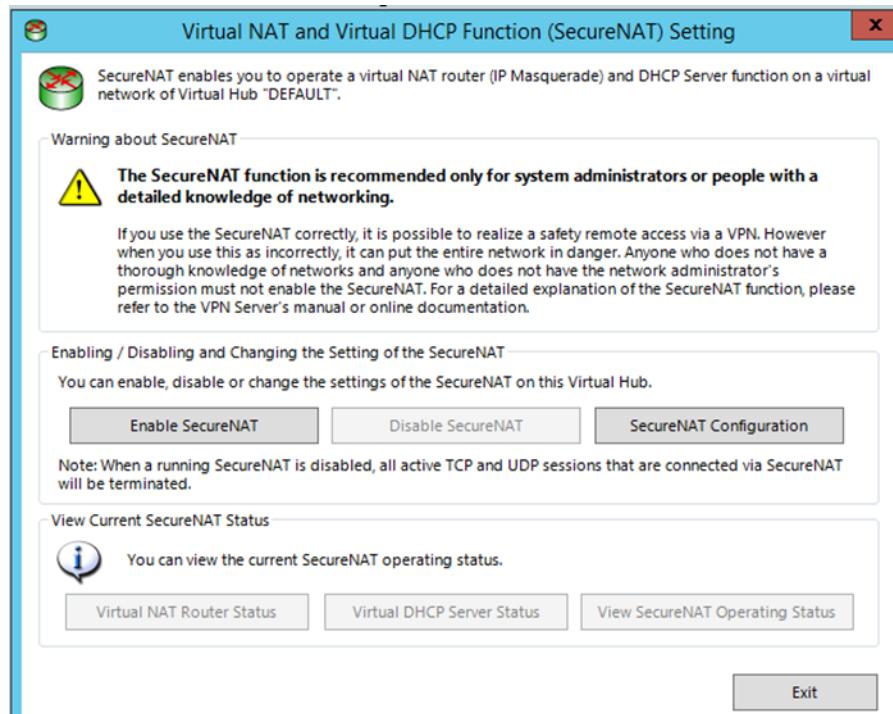


Figure 57: Enabling Secure NAT

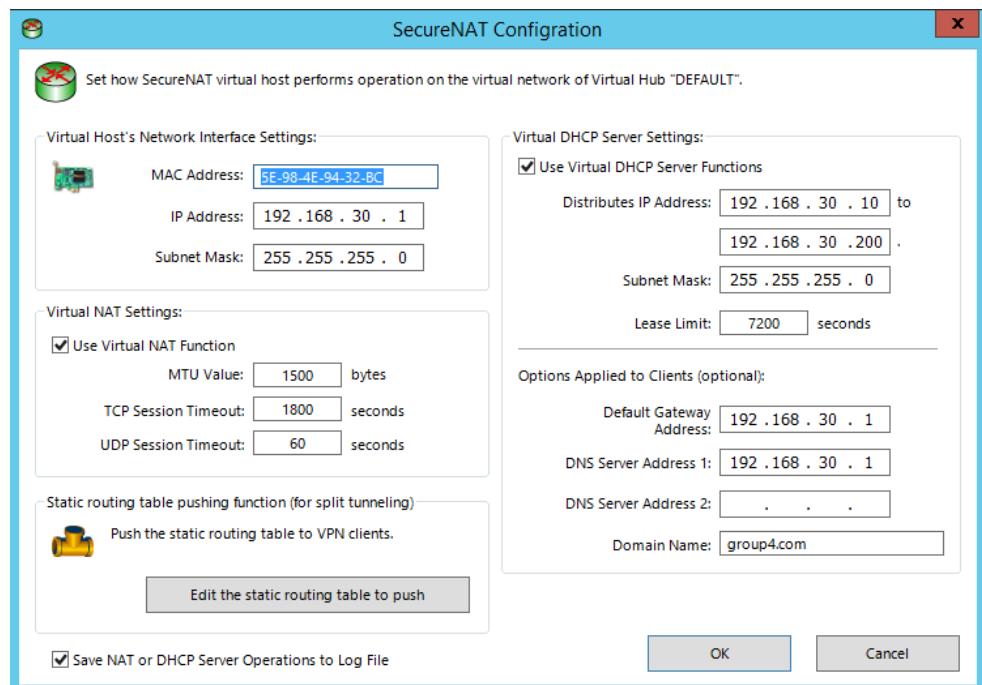


Figure 58: Specify IP Address range

Step 13 : Specify the range of the IP Address.

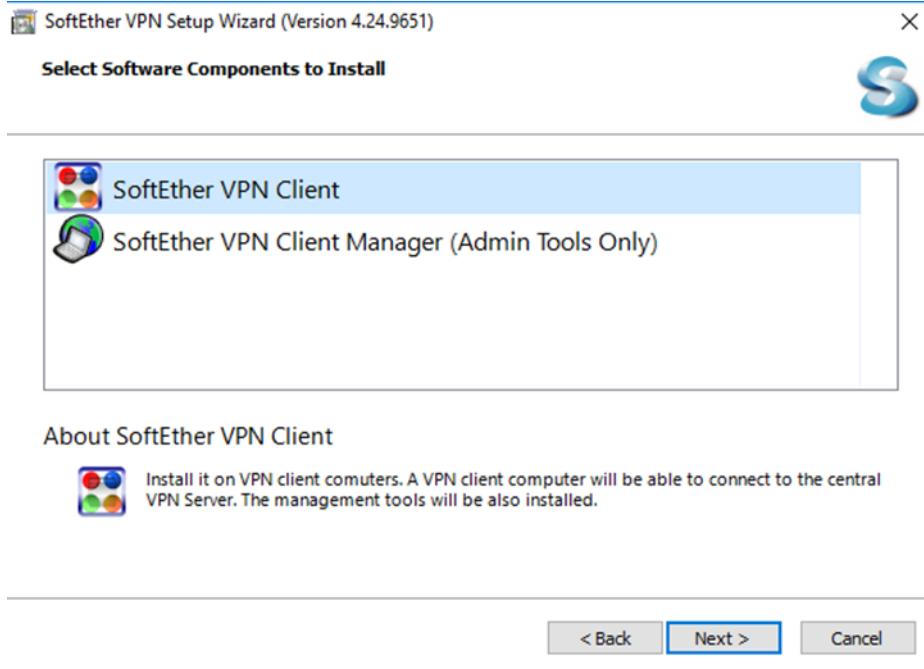


Figure 367: Install SoftEther client on client's PC

Step 14 : Install Softether Client on the client's PC. Select Softether Client.

Step 15 : Wait for installation to finish.

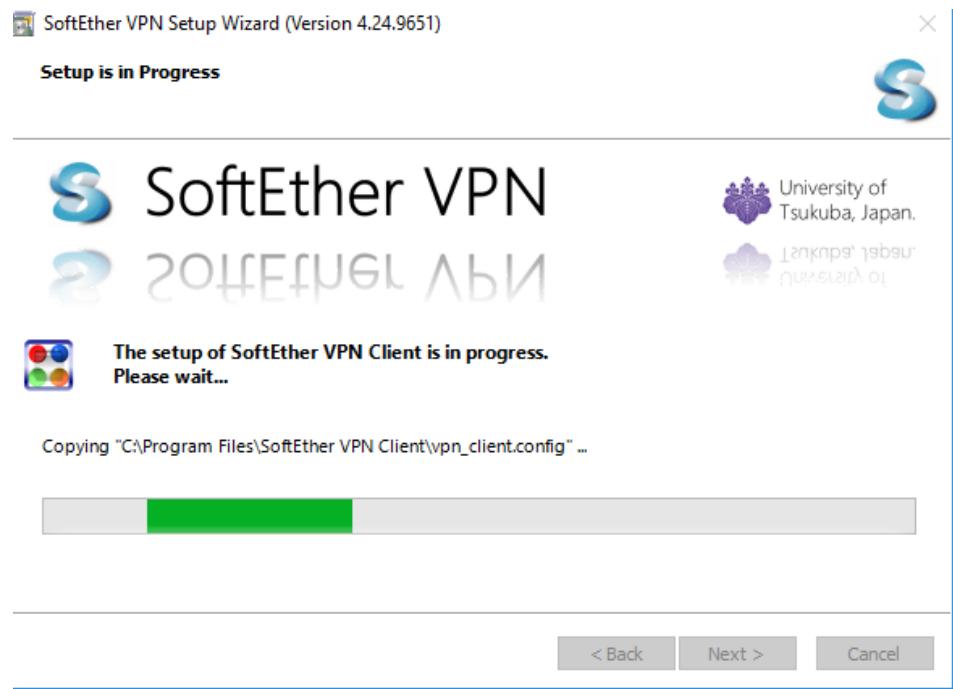


Figure 368: Finish installation

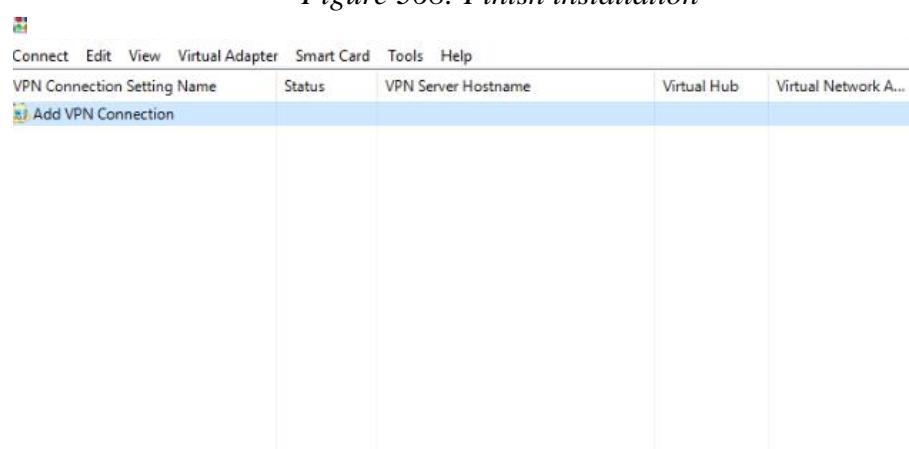


Figure 59: SoftEther VPN Client Manager

Step 16 : Click add VPN connection.

Step 17 : Click OK on option create virtual network adapter.

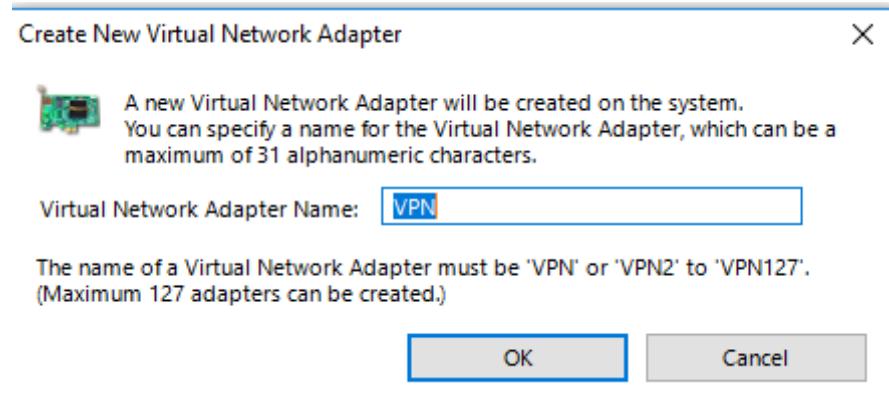


Figure 60: Creating virtual network adapter

Step 18 : Enter server IP in hostname. Enter preferred port number, username and password. Click OK.

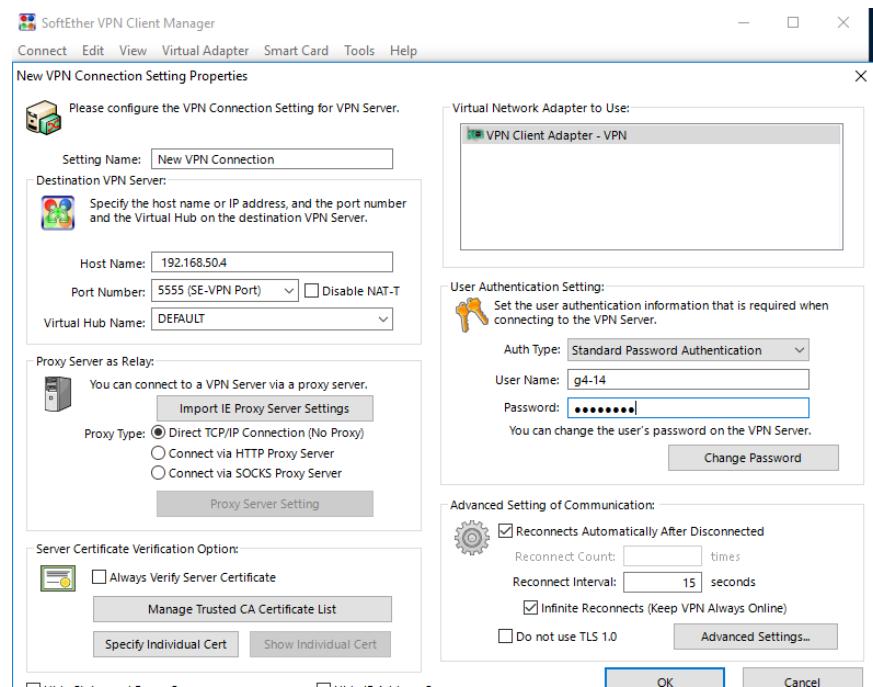


Figure 371: Enter all details in of server IP

Step 19 : Wait until connection is established.

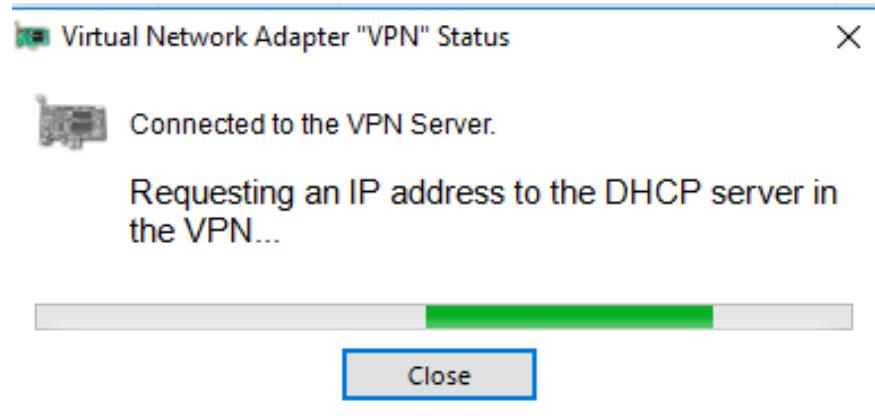


Figure 372: Establishing VPN connection

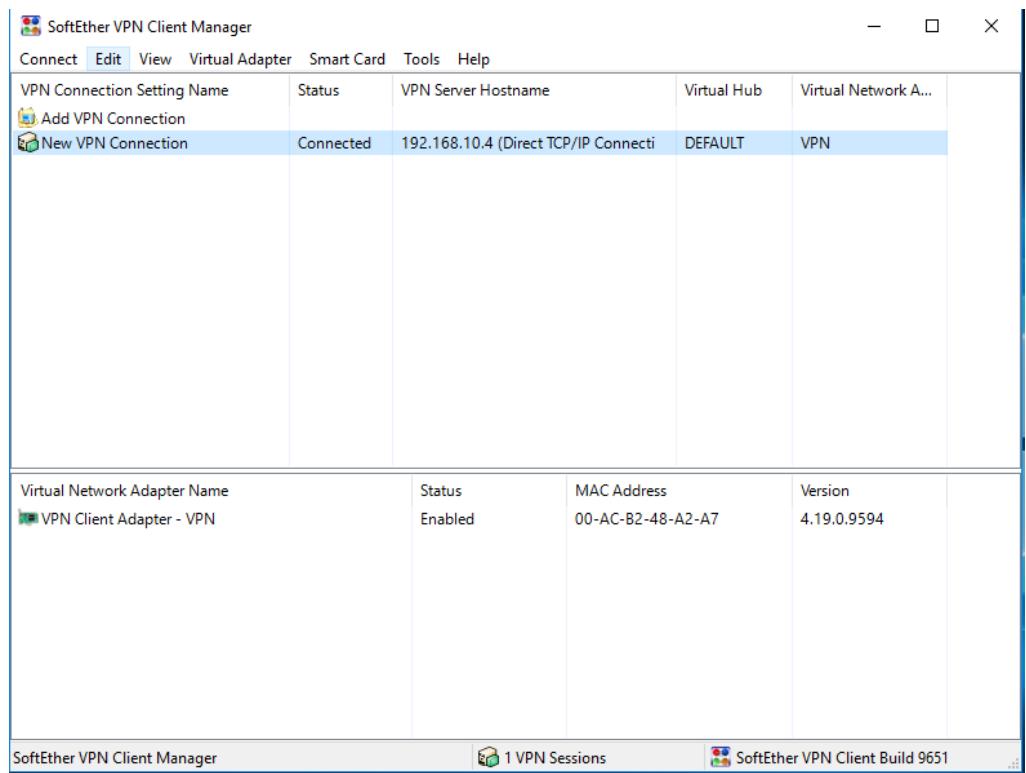


Figure 373: VPN is now connected

Step 20 : VPN is now connected.

5.3.25 Port Security

Step 1 : Open PuTTY and enter the switch.

Step 2 : Then, enter command errdisable as it will detect an error condition.

```
max Addresses limit in system (excluding one mac per port) : 61
g4switch(config)#errdisable recovery cause psecure-violation
g4switch(config)#errdisable recovery interval 60
```

Figure 374: Errdisable command

Step 3 : Firstly, make sure which port that we use for every server.

Step 4 : Enable port security on Windows Server (interface fa0/2 – 4).

Windows Server use fa0/4. Set the violation to restrict and allow maximum 2 number of address.

```
g4switch(config-if-range)#exit
g4switch(config)#int range fa0/2-3
g4switch(config-if-range)#switchport mode access
g4switch(config-if-range)#switchport port-security
g4switch(config-if-range)#switchport port-security max 2
g4switch(config-if-range)#switchport port-security mac-address sticky
g4switch(config-if-range)#switchport port-security violation restrict
g4switch(config-if-range)#end
g4switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
g4switch(config)#int fa0/4
g4switch(config-if)#switchport mode access
g4switch(config-if)#switchport port-security
g4switch(config-if)#switchport port-security max 10
g4switch(config-if)#switchport port-security mac-address sticky
g4switch(config-if)#switchport port-security violation restrict
g4switch(config-if)#end
```

Figure 375: Port security on Windows server interface

Step 5 : After that, do the same step to another server. Enable port security for Ubuntu server (interface fa0/5 – 7). Set the violation to restrict and allow maximum of 1 address only.

```
g4switch(config)#int range fa0/5-7
g4switch(config-if-range)#switchport mode access
g4switch(config-if-range)#switchport port-security
g4switch(config-if-range)#switchport port-security max 1
g4switch(config-if-range)#switchport port-security mac-address sticky
g4switch(config-if-range)#switchport port-security violation restrict
g4switch(config-if-range)#end
g4switch#conf t
```

Figure 61: Port security on Ubuntu server interface

- Step 6** : Enable port security on Fedora (interface fa0/8 – 10). Set the violation to restrict and allow maximum of 1 address only.

```
g4switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
g4switch(config)#int range fa0/8-10
g4switch(config-if-range)#switchport mode access
g4switch(config-if-range)#switchport port-security
g4switch(config-if-range)#switchport port-security max 1
g4switch(config-if-range)#switchport port-security mac-address sticky
g4switch(config-if-range)#switchport port-security violation restrict
g4switch(config-if-range)#exit
```

Figure 377: Port security on Fedora server interface

5.3.26 VLAN Security

Step 1 : Set interface as Ethernet trunk port. Trunk port can carry one or more VLANs on same physical link.

Step 2 : Set VLAN allowed for the trunk.

```
G4Switch#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
G4Switch(config)#int fa0/24  
G4Switch(config-if)#switchport mode trunk  
G4Switch(config-if)#switchport trunk allowed vlan 10,20,30,50,51  
G4Switch(config-if)#[
```

Figure 62: VLAN allowed for trunk

Step 3 : Set native VLAN for the trunk by command **switchport trunk native vlan** (vlan no).

```
G4Switch(config-if-range)#switchport trunk native vlan 3  
G4Switch(config-if-range)#exit  
G4Switch(config)#sh vlan
```

Figure 63: Setting native VLAN

Step 4 : Prevent VLAN hopping.

```
G4Switch(config-if)#switchport nonegotiate  
G4Switch(config-if)#no shut  
G4Switch(config-if)#[
```

Figure 64: VLAN hopping prevention

5.3.27 Router Hardening

Installation

Enable Login Banner

Banner is acting to inform an unauthorized user that an offense of unauthorized access can only be committed if the offender knew at the access he intended to obtain was unauthorized.

Step 1: Open PuTTY Configuration and login with username “Group4”, then enter password.

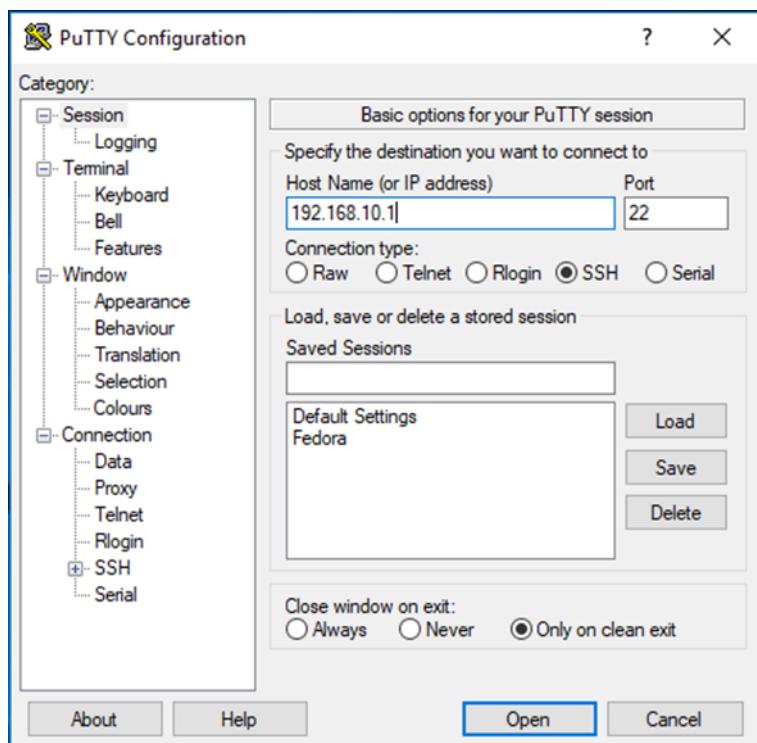


Figure 381: Putty Login

Step 2: Get into terminal and type “banner motd * ” to enter login banner.

```
G4Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
G4Router(config)#banner motd *
Enter TEXT message. End with the character '**'.
$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
$      WELCOME TO WORKSHOP 2      $
$      GROUP 4      $
$      UNAUTHORIZED USER IS PROHIBITED  $
$      $
$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
*
G4Router(config) #
```

Figure 382: Banner motd

Disable log to console or monitor sessions

It is always advised to send to send logging information to the local log buffer, which can be viewed with the show logging command rather than to send log messages to monitor and console sessions. The monitor and console sessions are interactive management sessions and it can elevate the CPU load of router.

Step 1: Type “show log” to show system log.

```

login as: syafiq
syafiq@192.168.10.1's password:

$ WELCOME TO WORKSHOP 2
$ GROUP 4
$ UNAUTHORIZED USER IS PROHIBITED
$ $$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
G4Router#
G4Router#
G4Router#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
G4Router(config)#exit
G4Router#show log
Syslog logging: enabled (11 messages dropped, 1 messages rate-limited,
          0 flushes, 0 overruns, xml disabled, filtering disabled)
  Console logging: disabled
  Monitor logging: disabled
  Buffer logging: disabled, xml disabled,
                  filtering disabled
  Logging Exception size (4096 bytes)
  Count and timestamp logging messages: disabled

No active filter modules.

Trap logging: level informational, 39 message lines logged
G4Router#exit

```

Figure 383: System Log

Step 2: Then get into configuration and type “no logging console” and “no logging monitor” to disable console and monitor logs.

```

G4Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
G4Router(config)#
G4Router(config)#
G4Router(config)#no logging console
G4Router(config)#no logging monitor
G4Router(config)#exit
G4Router#show log
Syslog logging: enabled (11 messages dropped, 1 messages rate-limited,
          0 flushes, 0 overruns, xml disabled, filtering disabled)
  Console logging: disabled
  Monitor logging: disabled
  Buffer logging: disabled, xml disabled,
                  filtering disabled
  Logging Exception size (4096 bytes)
  Count and timestamp logging messages: disabled

No active filter modules.

Trap logging: level informational, 35 message lines logged
G4Router#

```

Figure 384: Disable console and monitor logs

Enable configuration change notification and logging

To send notification of configuration changes to the software system logging (syslog) process. Syslog notifications allow monitoring of the configuration log information without performing polling and information gathering tasks. Then, it allows the tracking of configuration changes entered by users on a per-session and per-user basis. This tool allows administrators to track any configuration change made to the software running configuration, and identify the user that made that change.

Step 1: Get into PuTTY configuration and enter following commands.

```
G4Router#  
G4Router#config t  
Enter configuration commands, one per line. End with CNTL/Z.  
G4Router(config)#archive  
G4Router(config-archive)#log config  
G4Router(config-archive-log-cfg)#logging enable  
G4Router(config-archive-log-cfg)#logging size 300  
G4Router(config-archive-log-cfg)#hidekeya  
^  
% Invalid input detected at '^' marker.  
  
G4Router(config-archive-log-cfg)#hidekeys  
G4Router(config-archive-log-cfg)#notify syslog  
G4Router(config-archive-log-cfg)#end  
G4Router#  
G4Router#  
G4Router#  
G4Router#
```

Figure 385: Enable syslog

Step 2: Then type “*show archive log config 1 5*” to show archive from line 1 to line 5.

```
G4Router#  
G4Router#show archive log config 1 2  
idx sess user@line Logged command  
1 1 SYAFIQ@vty0 | logging enable  
2 1 SYAFIQ@vty0 | logging size 300  
  
G4Router#  
G4Router#  
G4Router#show archive log config 1 5  
idx sess user@line Logged command  
1 1 SYAFIQ@vty0 | logging enable  
2 1 SYAFIQ@vty0 | logging size 300  
3 1 SYAFIQ@vty0 | hidekeys  
4 1 SYAFIQ@vty0 | notify syslog  
  
G4Router#  
G4Router#show archive log config all provisioning  
archive  
log config  
logging enable  
logging size 300  
hidekeys  
notify syslog  
  
G4Router#
```

Figure 386: Show Archive log config

5.3.28 Linux Server1 Hardening

Step 1 : Go to the Terminal in Fedora.

```

root@Fedora:~#
File Edit View Search Terminal Help
[g4-15@Fedora ~]$ su -l
Password:
Last login: Tue Nov 13 15:53:02 +08 2018 on pts/0
[root@Fedora ~]# dnf update
Repository PlexRepo is listed more than once in the configuration
Waiting for process with pid 2242 to finish.
Last metadata expiration check: 0:00:00 ago on Tue 13 Nov 2018 03:56:27 PM +08.
Dependencies resolved.
=====
  Package          Arch    Version      Repository   Size
=====
Installing:
  kernel           x86_64  4.18.17-200.fc28      updates   100 k
  kernel-core       x86_64  4.18.17-200.fc28      updates   24 M
  kernel-modules    x86_64  4.18.17-200.fc28      updates   28 M
  kernel-modules-extra x86_64  4.18.17-200.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 65: Change user to root

Step 2 : Enter command su -l and dnf update to install the new updates.

```

root@Fedora:~#
File Edit View Search Terminal Help
Removing:
  kernel           x86_64  4.18.10-200.fc28      @updates   0
  kernel-core       x86_64  4.18.10-200.fc28      @updates   60 M
  kernel-modules    x86_64  4.18.10-200.fc28      @updates   27 M
  kernel-modules-extra x86_64  4.18.10-200.fc28      @updates 2.1 M
Transaction Summary
=====
Install  5 Packages
Upgrade  97 Packages
Remove   4 Packages
Total download size: 386 M
Is this ok [y/N]: y
Downloading Packages:
(1/102): evolution-langpacks-3.28.5-1.fc28 3.28.5-2.fc28.noarch.rpm: 20 kB/s | 21 kB  00:01
(2/102): libmspack-0.7-0.1.alpha.fc28 0.9.1-0.1.alpha.fc28.x86_64.rpm: 50 kB/s | 31 kB  00:00
(3/102): evolution-3.28.5-1.fc28 3.28.5-2.fc28.x86_64.rpm: 58 kB/s | 510 kB  00:08
[DRPM 1/4] evolution-langpacks-3.28.5-1.fc28 3.28.5-2.fc28.noarch.rpm: done
[DRPM 2/4] libmspack-0.7-0.1.alpha.fc28 0.9.1-0.1.alpha.fc28.x86_64.rpm: done
(4/102): kernel-4.18.17-200.fc28.x86_64.rpm: 24 kB/s | 100 kB  00:04
(5/102): evolution-help-3.28.5-1.fc28 3.28.5-2.fc28.noarch.rpm: 33 kB/s | 618 kB  00:19
[DRPM 3/4] evolution-3.28.5-1.fc28 3.28.5-2.fc28.x86_64.rpm: done
[DRPM 4/4] evolution-3.28.5-1.fc28 3.28.5-2.fc28.x86_64.rpm: done
(6/102): kernel-modules-extra-4.18.17-200.fc28.x86_64.rpm: 33 kB/s | 2.2 MB  01:08
(7/102): zchunk-libs-0.9.14-1.fc28.x86_64.rpm: 30 kB/s | 44 kB  00:01
(8/102): NetworkManager-1.10.12-2.fc28.x86_64.rpm: 39 kB/s | 1.8 MB  00:46
(9/102): NetworkManager-libnm-1.10.12-2.fc28.x86_64.rpm: 33 kB/s | 1.3 MB  00:41
(10/102): NetworkManager-wwan-1.10.12-2.fc28.x86_64.rpm: 33 kB/s | 154 kB  00:04
(11/102): NetworkManager-wifi-1.10.12-2.fc28.x86_64.rpm: 32 kB/s | 163 kB  00:05
(12/102): NetworkManager-team-1.10.12-2.fc28.x86_64.rpm: 32 kB/s | 131 kB  00:04
(13/102): NetworkManager-bluetooth-1.10.12-2.fc28.x86_64.rpm: 15 kB/s | 150 kB  00:09
(14/102): NetworkManager-adsl-1.10.12-2.fc28.x86_64.rpm: 70 kB/s | 128 kB  00:01
(15/102): NetworkManager-config-connectivity-fedora-1.10.12-2.fc28.noarch.rpm: 51 kB/s | 111 kB  00:02
(16/102): SDL2-2.0.9-1.fc28.x86_64.rpm: 53 kB/s | 444 kB  00:08
(17/102): autocorr-en-6.0.6.2-3.fc28.noarch.rpm: 46 kB/s | 216 kB  00:04
(18-20/102): cpp-8.2.1-5.fc28.x86_64.rpm: 113 kB/s | 46 MB  49:38 ETA

```

Figure 66: Installing the new updates

Step 3 : Type command “chage -l group4” to view current status.

```
[root@Fedora ~]# chage -l group4
Last password change : Nov 13, 2018
Password expires : never
Password inactive : never
Account expires : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
```

Figure 67: View the current status

Step 4 : Next, to edit the details, enter command as below.

```
[root@Fedora ~]# chage -I 31 group4
[root@Fedora ~]# chage -m 5 group4
[root@Fedora ~]# chage -E 22/12/2018 group4
[root@Fedora ~]# chage -M 14 group4
[root@Fedora ~]# █
```

Figure 68: Edit the details command

Step 5 : After editing, check the changes that has been made.

```
[root@Fedora ~]# chage -l group4
Last password change : Nov 13, 2018
Password expires : Nov 27, 2018
Password inactive : Dec 28, 2018
Account expires : Oct 12, 2019
Minimum number of days between password change : 5
Maximum number of days between password change : 14
Number of days of warning before password expires : 7
```

Figure 69: Checking the changes

Step 6 : Next, disable the unnecessary services.

```
[root@Fedora g4-15]# yum install nmap
Repository PlexRepo is listed more than once in the configuration
Last metadata expiration check: 2:22:46 ago on Tue 13 Nov 2018 07:21:59 PM +08.
Dependencies resolved.
=====
 Package      Arch      Version       Repository      Size
=====
 Installing:
  nmap        x86_64    2:7.60-12.fc28   fedora          5.7 M
Transaction Summary
=====
 Install 1 Package

Total download size: 5.7 M
Installed size: 22 M
Is this ok [y/N]: y
```

Figure 70: Install the Nmap

Step 7 : Firstly, install the Nmap.

```
[root@Fedora g4-15]# nmap -v -sT localhost
Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-13 21:45 +08
Initiating Connect Scan at 21:45
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 445/tcp on 127.0.0.1
Discovered open port 22/tcp on 127.0.0.1
Discovered open port 21/tcp on 127.0.0.1
Discovered open port 139/tcp on 127.0.0.1
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 443/tcp on 127.0.0.1
Discovered open port 3306/tcp on 127.0.0.1
Discovered open port 631/tcp on 127.0.0.1
Discovered open port 3128/tcp on 127.0.0.1
Discovered open port 10002/tcp on 127.0.0.1
Completed Connect Scan at 21:45, 0.03s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00024s latency).
Other addresses for localhost (not scanned): ::1
```

Figure 71: Display list of scan port

Step 8 : Then, enter command `nmap -v -sT localhost` to display list of scan ports.

Step 9 : The, study each of the following open and running ports and identify which one is unneeded service and can be disabled it.

Port 21 ftp

The File Transfer Protocol (FTP) is a standard network protocol used for the transfer of computer files between a client and server on a computer network. FTP is built on a client-server model architecture using separate control and data connections between the client and the server. FTP clients connect to port 21 of remote FTP servers to initiate file transfer operations.

Port 22 open SSH

Used for Secure Shell (SSH), secure logins, file transfers (scp, sftp) and port forwarding

Port 80 open http

Port 80 is the port number assigned to commonly used internet communication protocol, Hypertext Transfer Protocol (HTTP). It is the port from which a computer sends and receives Web client-based communication and messages from a Web server and is used to send and receive HTML pages or data.

Port 139 open netbios-ssn

Used for NETBIOS Session Service. TCP NetBIOS connections are made over this port, usually with Windows machines but also with any other system running Samba (SMB). These TCP connections form "NetBIOS sessions" to support connection-oriented file sharing activities

Port 443 open https

TCP port 443 is the standard TCP port that is used for website which use SSL.

Port 445 open Microsoft-ds

TCP port 445 runs server message block (SMB) over TCP/IP

Port 631 tcp open ipp

Internet Printing Protocol (IPP) for communication between computers and printers

Port 3128 open squid-http

Squid is a caching proxy for HTTP, HTTPS and FTP, providing extensive access controls. By default, Squid binds to port 3128.

Port 3306 open mysql

Used for MYSQL service.

Port 10002 open documentum

Runs documentum service. Documentum provides management capabilities for all types of content. The core of Documentum is a repository in which the content is stored securely under compliance rules and a unified environment, although content may reside on

multiple servers and physical storage devices within a networked environment

Step 10 : Disable CUPS service, open Terminal and run command as shown below.

```
[root@Fedora g4-15]# service cups stop
Redirecting to /bin/systemctl stop cups.service
```

Figure 72: Disable CUPS service

```
[root@Fedora g4-15]# nmap -v -sT localhost
Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-13 21:50 +08
Initiating Connect Scan at 21:50
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 21/tcp on 127.0.0.1
Discovered open port 3306/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 80/tcp on 127.0.0.1
Discovered open port 139/tcp on 127.0.0.1
Discovered open port 443/tcp on 127.0.0.1
Discovered open port 10002/tcp on 127.0.0.1
Discovered open port 3128/tcp on 127.0.0.1
Completed Connect Scan at 21:50, 0.02s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00013s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 991 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
3128/tcp  open  squid-http
3306/tcp  open  mysql
10002/tcp open  documentum

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)
```

Figure 73: Checking the status

Step 11 : Check status after disabling cups service.

5.3.29 Windows Server Hardening

Step 1 : Go to Start > Administrative Tools > Security Configuration Wizard.

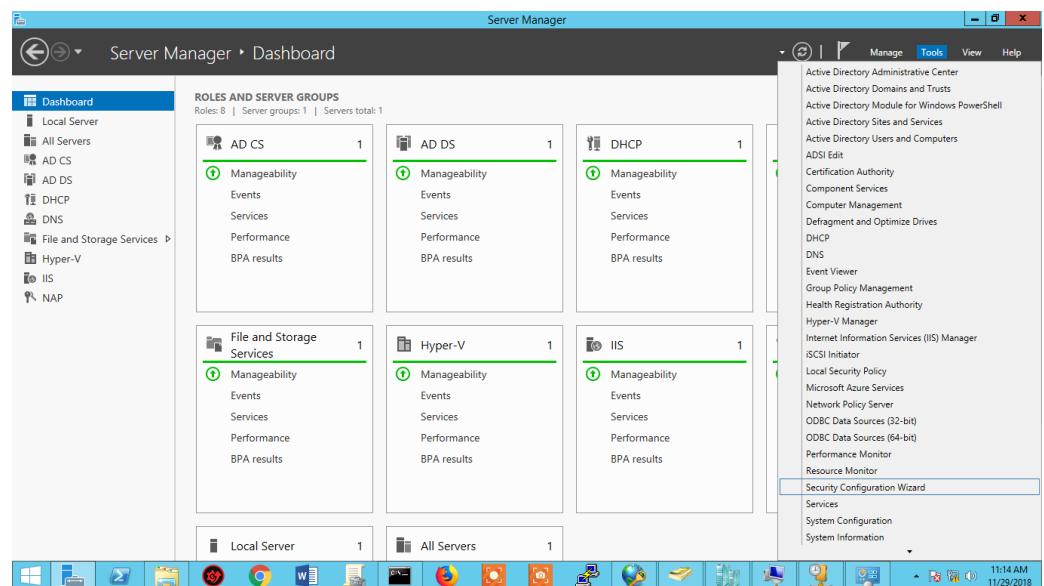


Figure 396: Server Manager Dashboard

Step 2 : This is the open page of the Security Configuration Wizard. Click

Next to go to the next page.



Figure 74: Security configuration wizard

Step 3 Select create a new security policy and click Next.

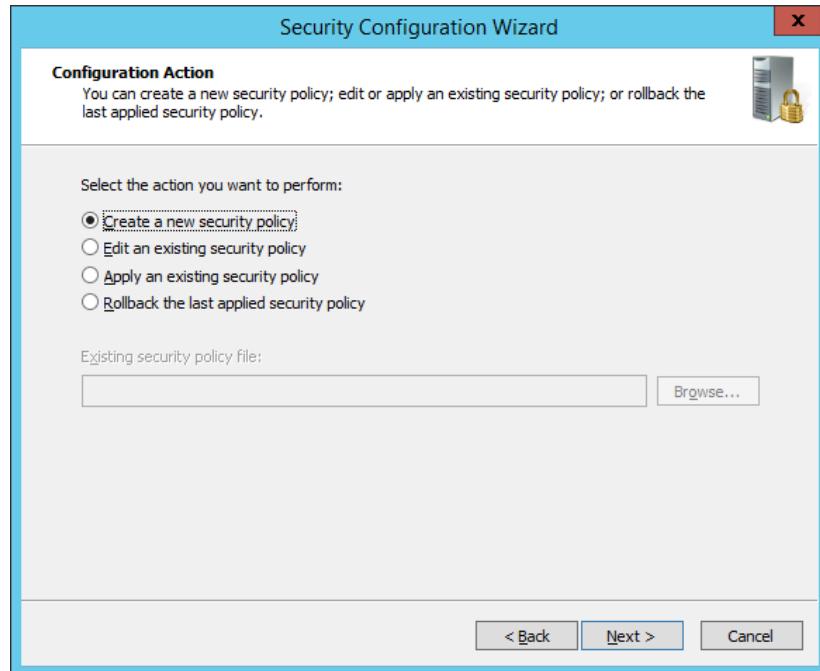


Figure 75: Create new security policy

Step 4 : Insert the server name and click Next.

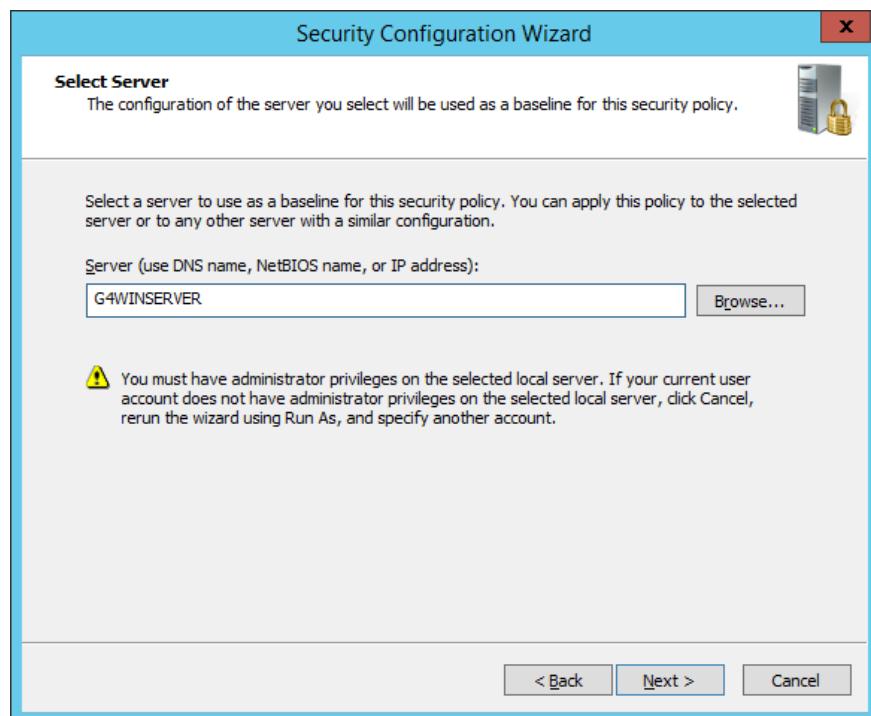


Figure 76: Insert server name

Step 5 : Wait until the Processing complete and after its complete, click Next.

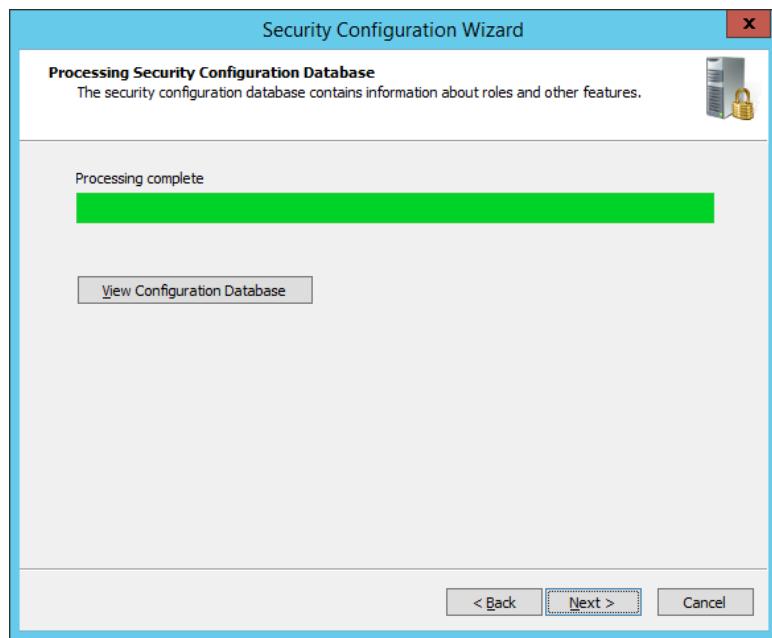


Figure 400: Complete the processing

Step 6 : Role-Based Service Configuration will be shown up and click Next.

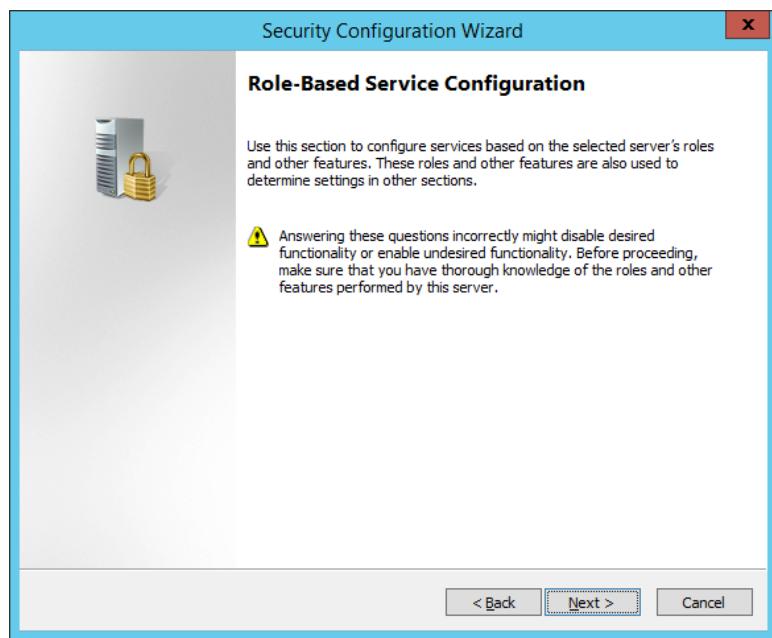


Figure 401: Role based service configuration

Step 7 : Select the server roles that the selected server performs and click Next.

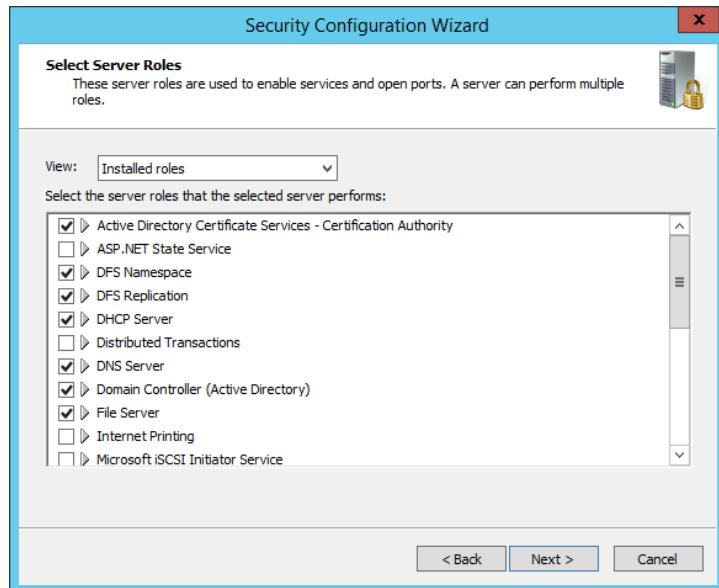


Figure 402: Select server roles

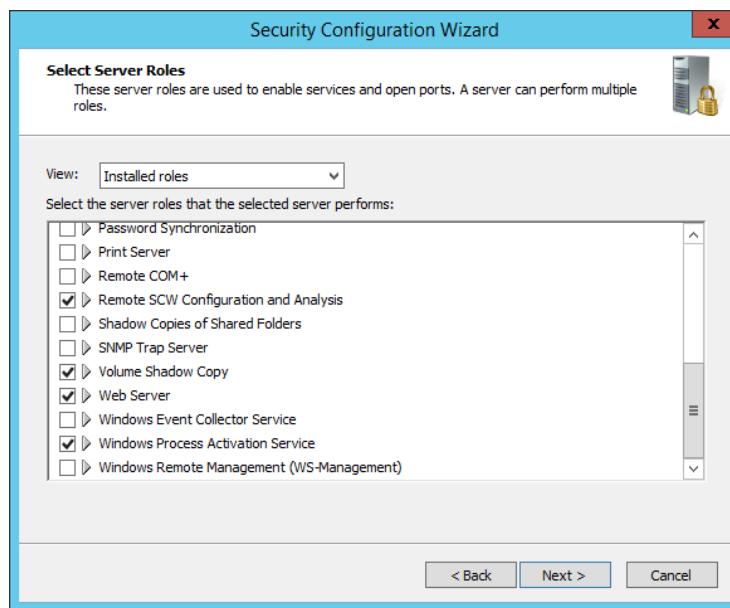


Figure 403: Select server roles

Step 8 : Select the client features that the selected server performs. Click Next.

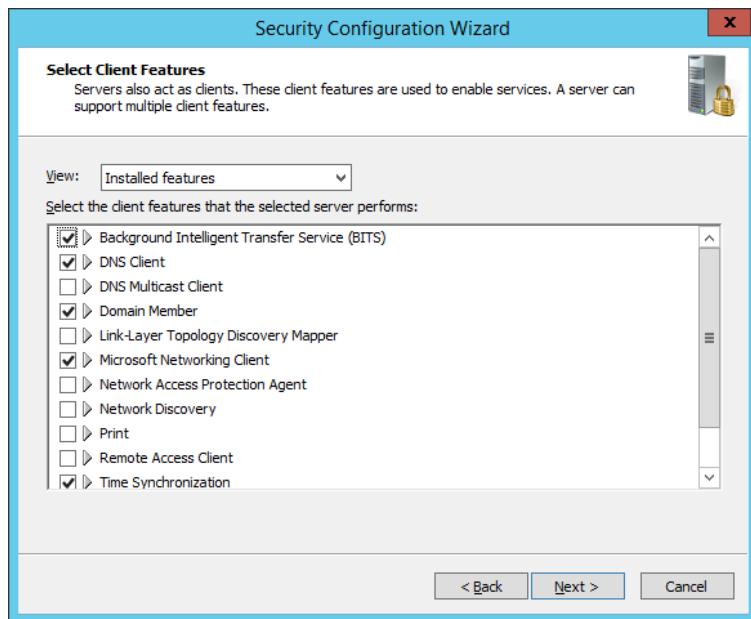


Figure 404: Select client features

Step 9 : Select the options used to administrate the selected server and click Next > Next > Next.

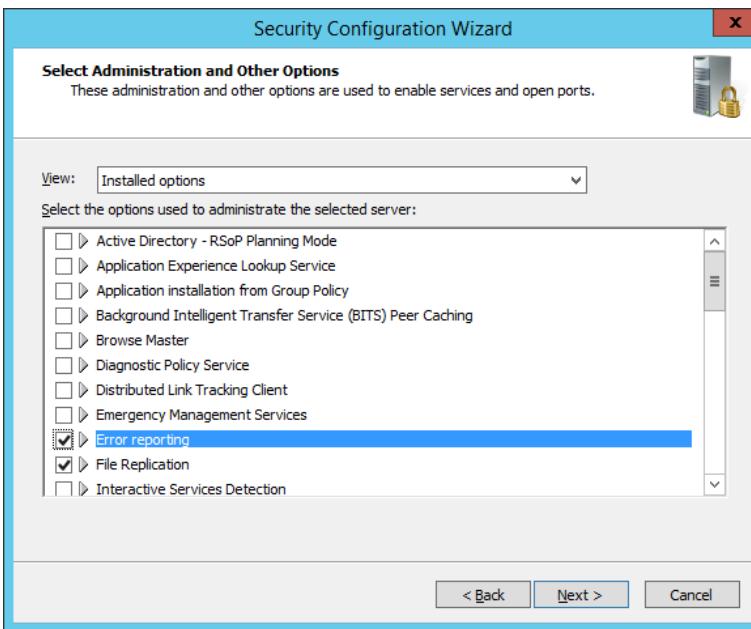


Figure 405: Select options used to administrate the selected server

Step 10 : Select the additional services that the selected server requires and click Next.

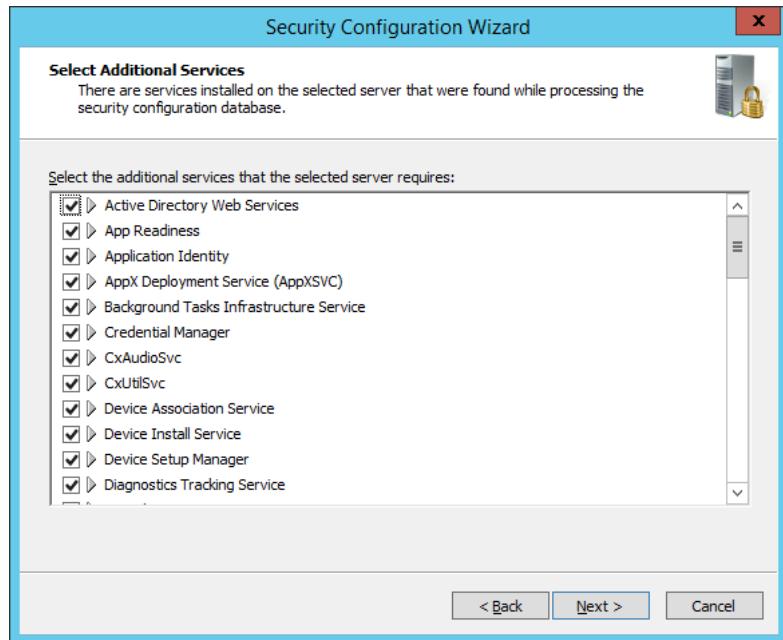


Figure 406: Select additional services

Step 11 : Select the Do not change the start-up mode of the service and click Next.

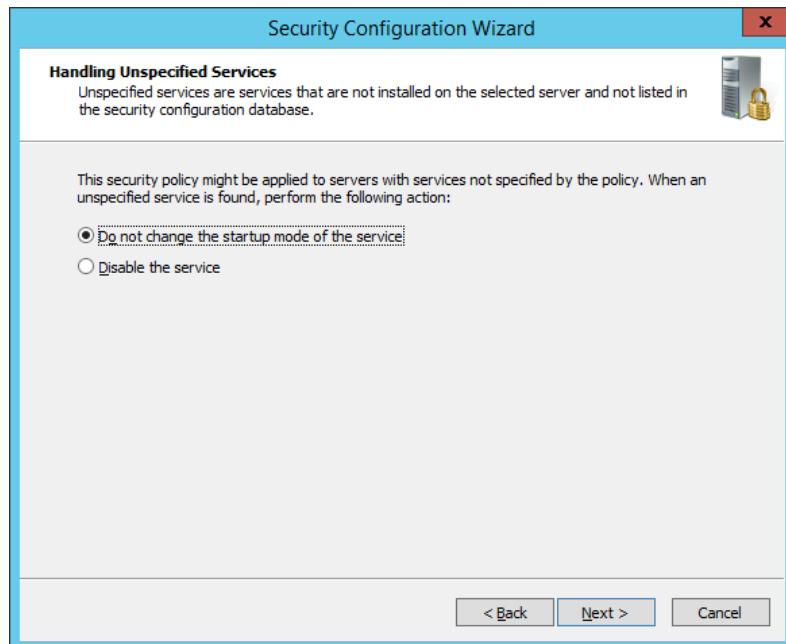


Figure 407: Select Handling Unspecified services

Step 12 : Confirm the service changes then click Next.

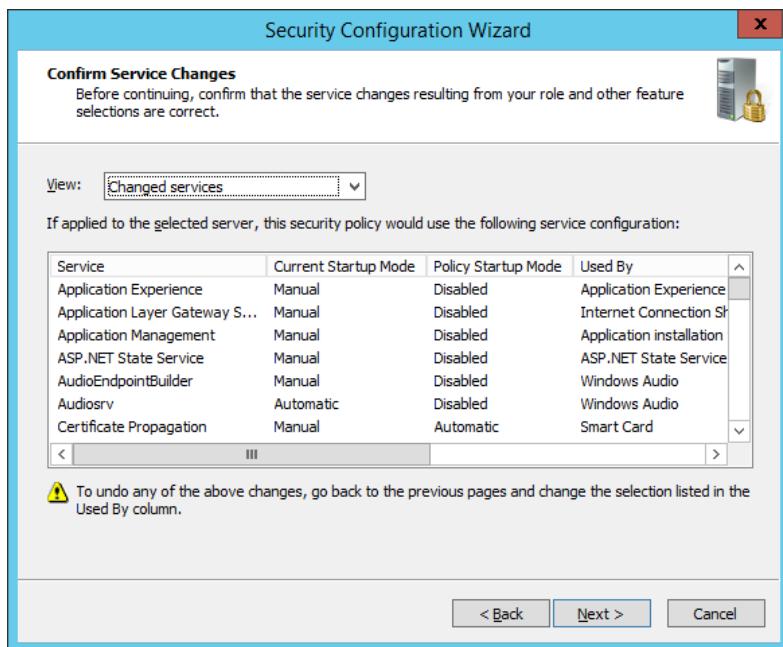


Figure 408: Confirm service changes

Step 13 : The first page of Network Security will show and click Next.

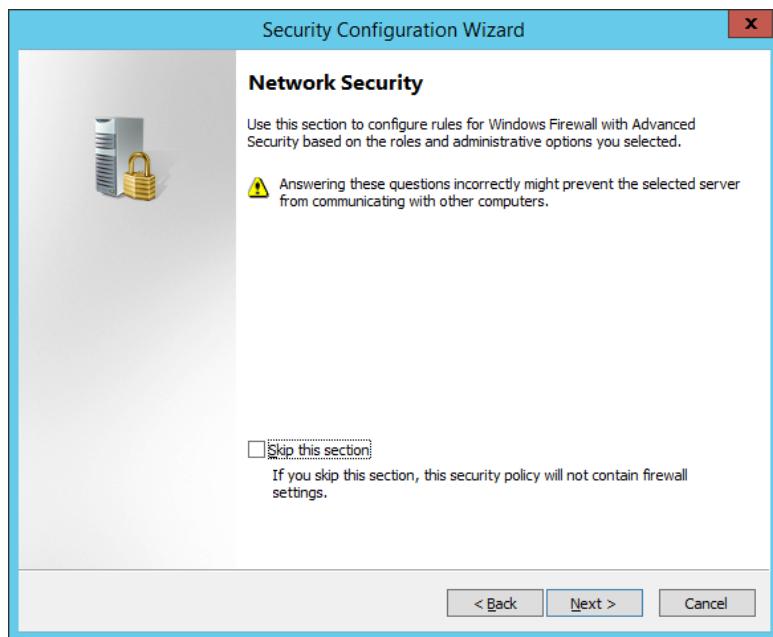


Figure 409: Network security first page

Step 14 : Select the network security rules and click Next.

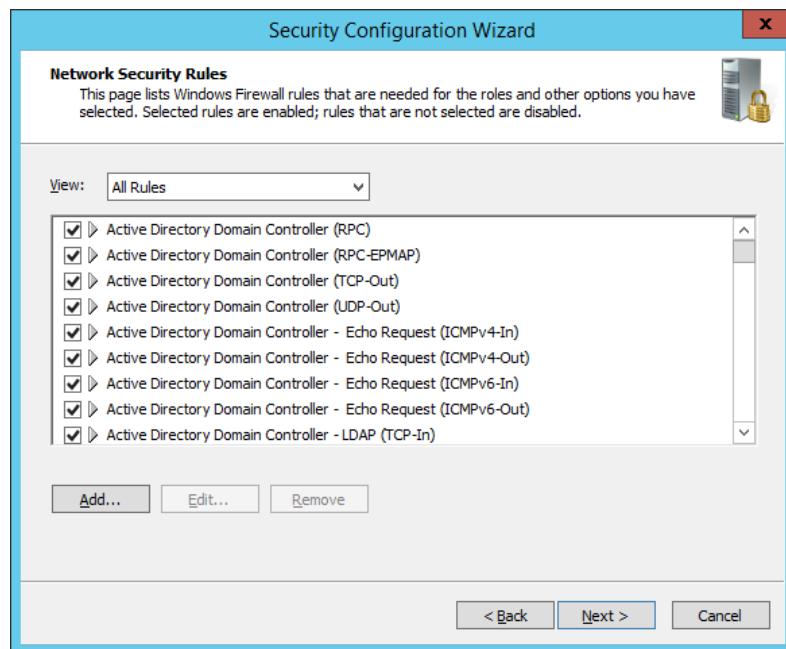


Figure 410: Select network security rules

Step 15 : The first page of the registry setting will be show up. Click Next.

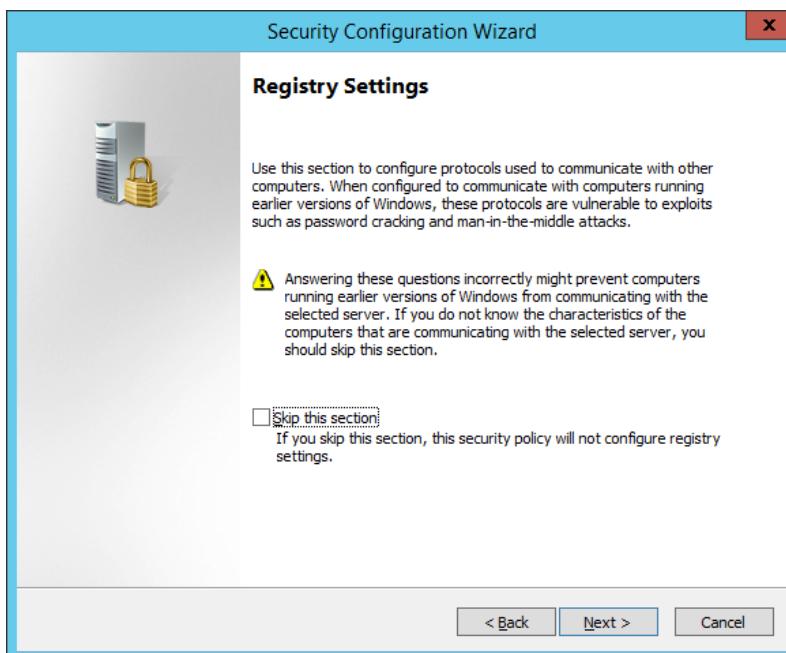


Figure 411: Registry setting first page

Step 16 : Select the attributes that is needed for the Server Message Block (SMB) Security Signatures and click Next.

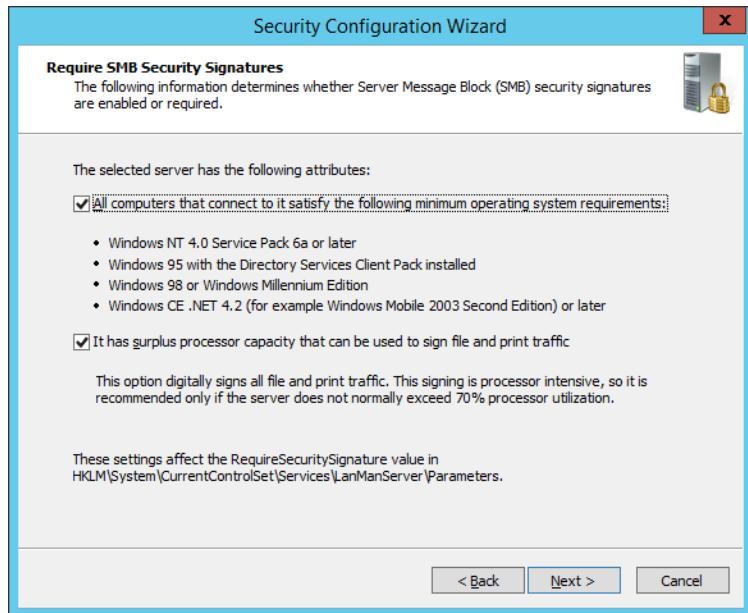


Figure 412: Select attributes needed for SMB Security Signature

Step 17 : Determines whether LDAP Signing is required by the security policy and click Next.

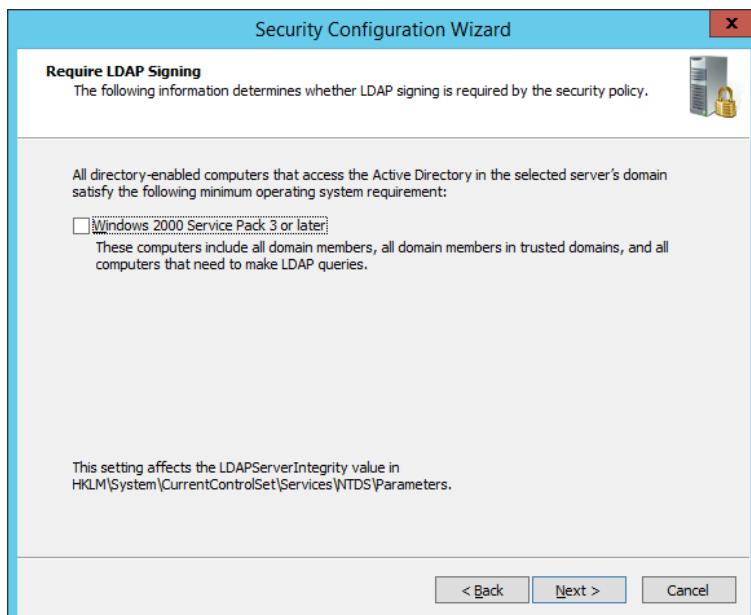


Figure 413: Determine LDAP Signing

Step 18 : Select the Domain Accounts as the methods uses to authenticate with remote computers and click Next.

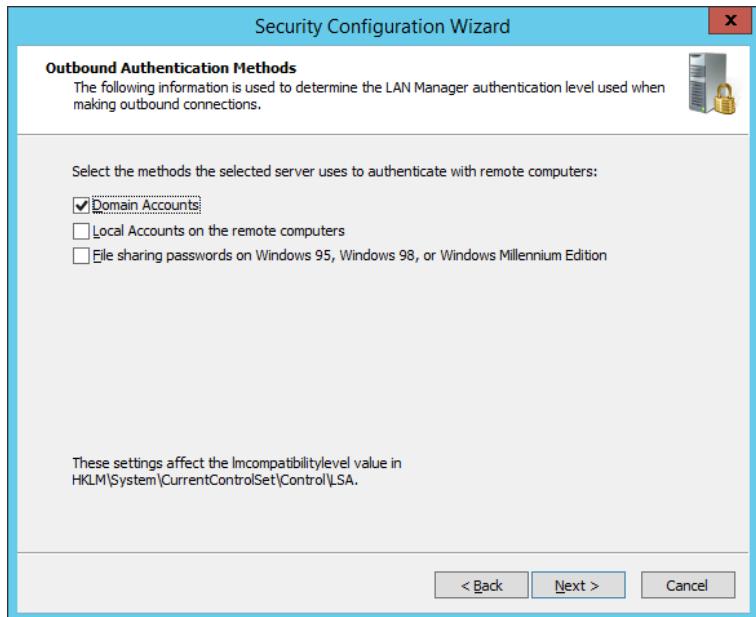


Figure 414: Select outbound authentication method

Step 19 : Select Windows NT 4.0 Service Pack 6a or later operating systems and then click Next.

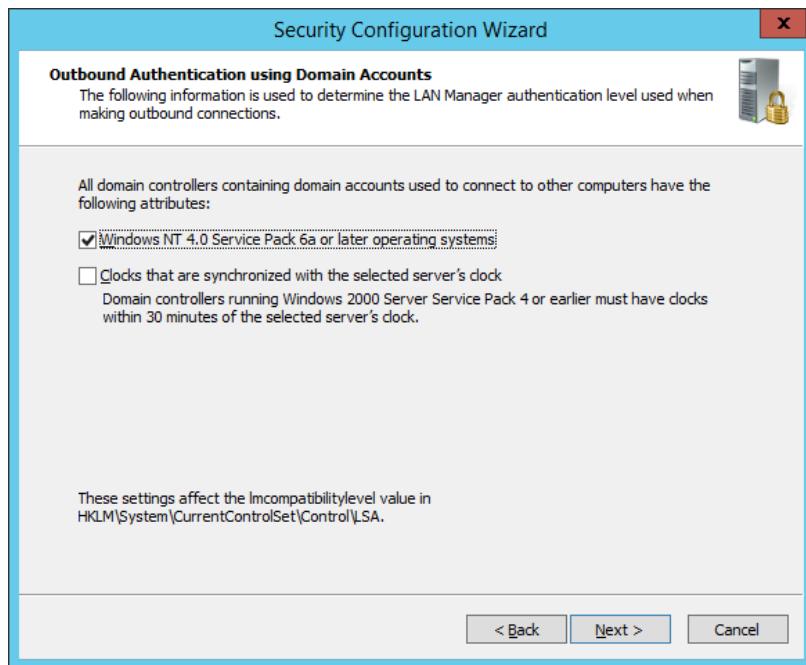


Figure 415: Select outbound authentication using Domain Accounts

Step 20 Then, it will show the registry settings summary and click Next.

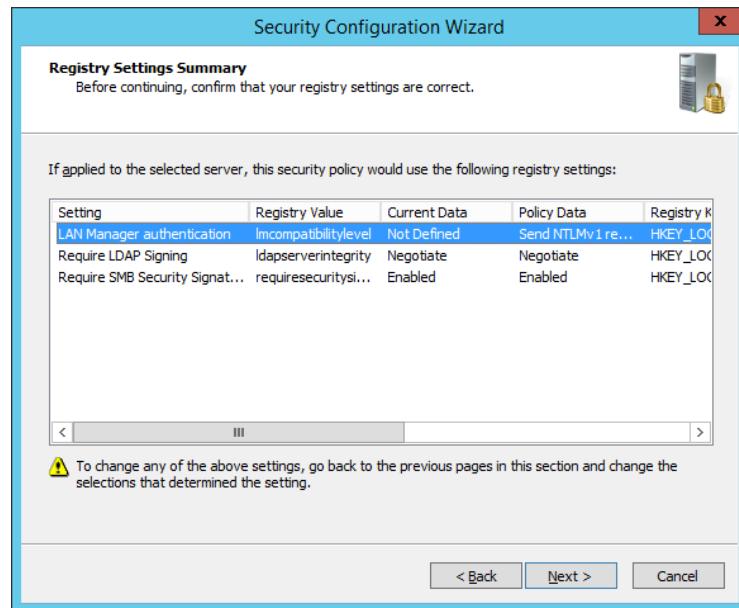


Figure 416: Registry setting summary

Step 21 : The first page of the Audit Policy will be shown and click Next.

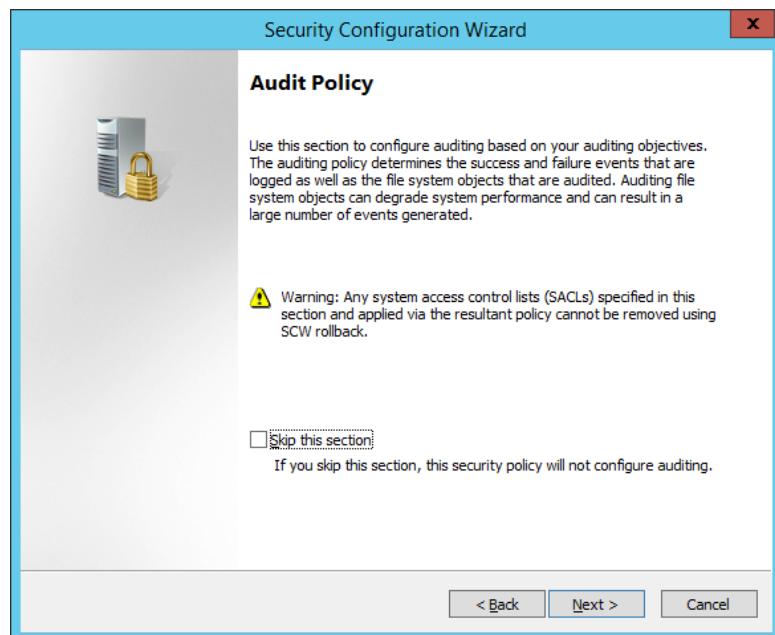


Figure 417: First page of audit policy

Step 22 : Then, select the Audit successful and unsuccessful activities and then click Next.

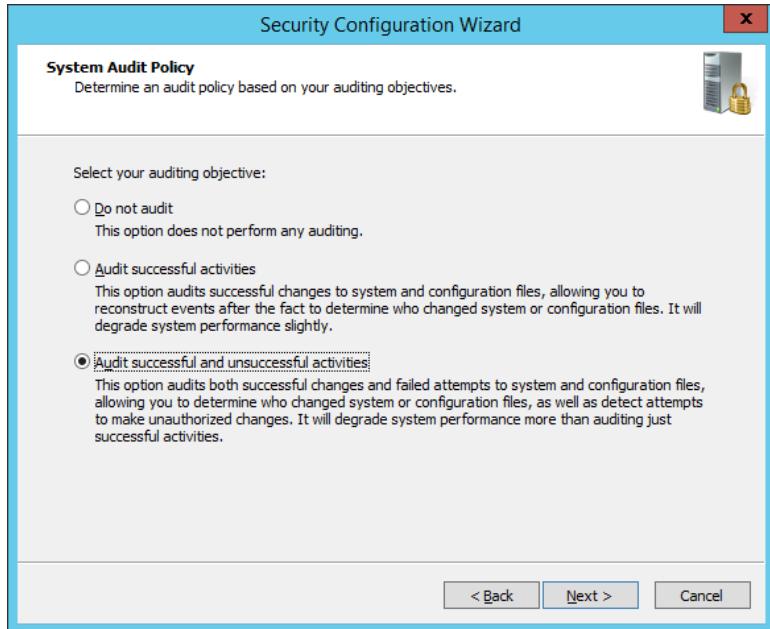


Figure 418: Select system audit policy

Step 23 : This page shows the summary of the audit policy and then click Next.

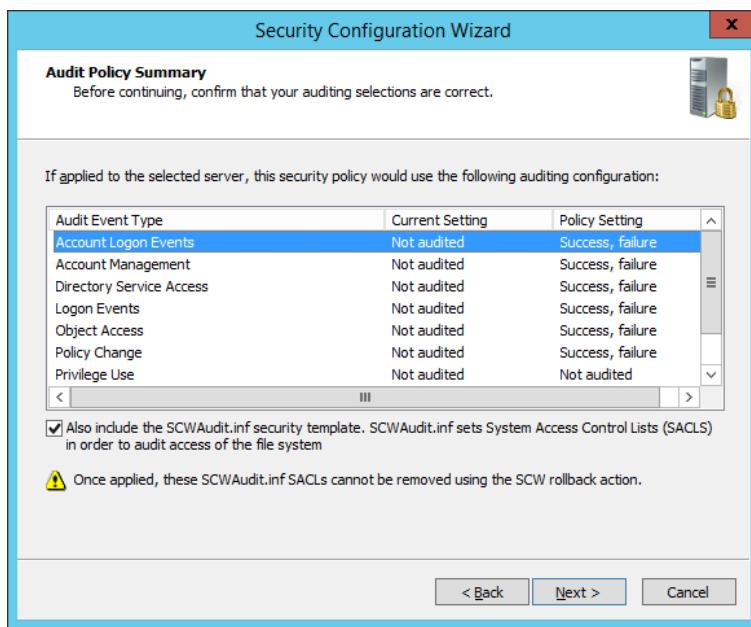


Figure 419: Summary of audit policy

Step 24 : This page show that the security policy has been save. Then, click Next.

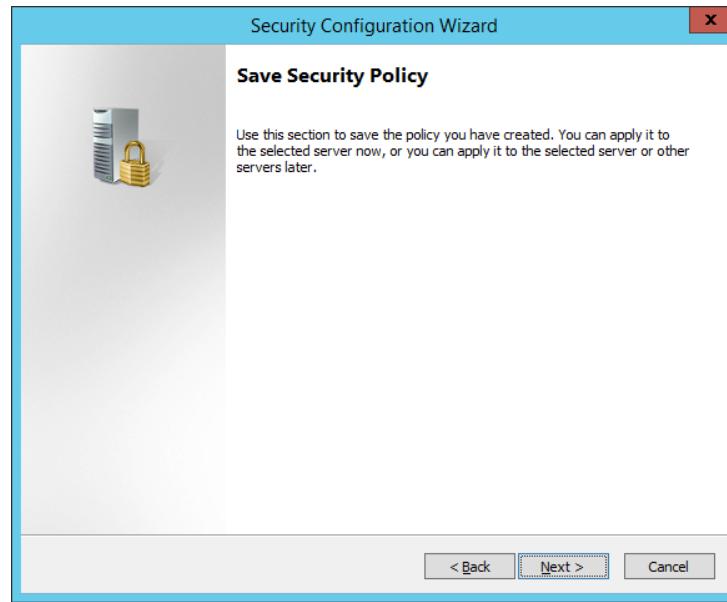


Figure 420: Security policy that has need to be save

Step 25 : Save the name and location for the security policy file. Then, click Next.

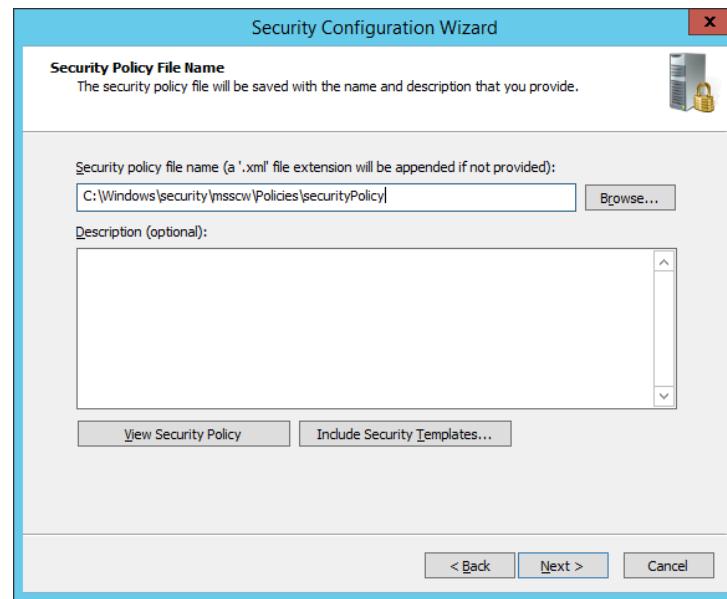


Figure 77: Save the name and location

Step 26 : Then, select Apply Now to apply the security policy and click Next.

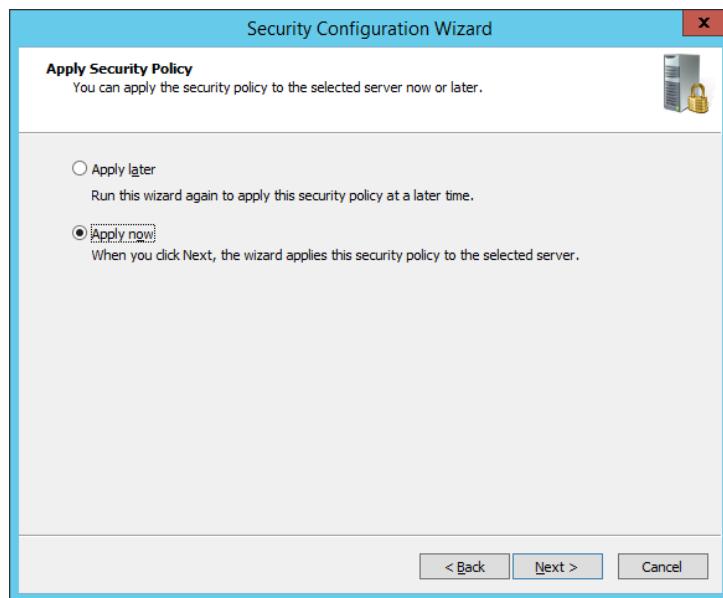


Figure 78: Select to apply security policy

Step 27 : This page show that Security Configuration Wizard has been completed successful. Click Finish.

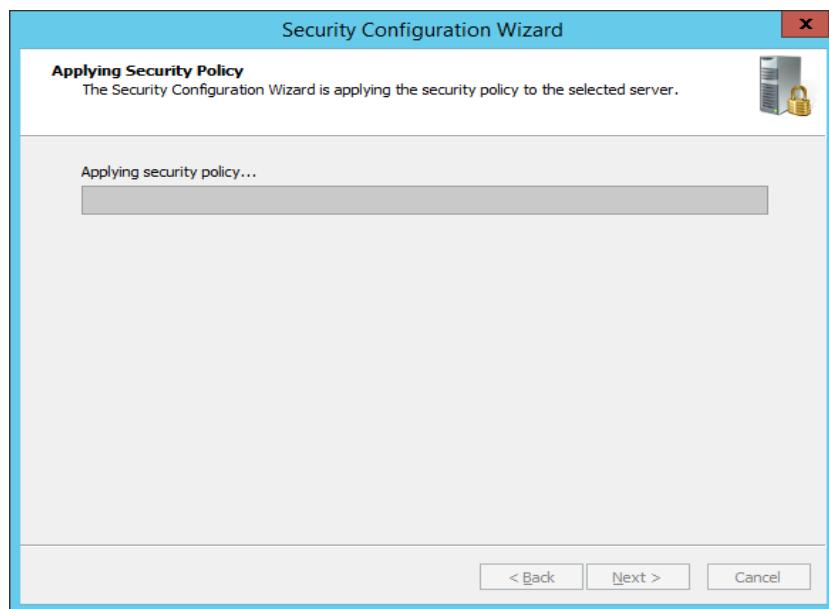


Figure 79: Security configuration Wizard has completed

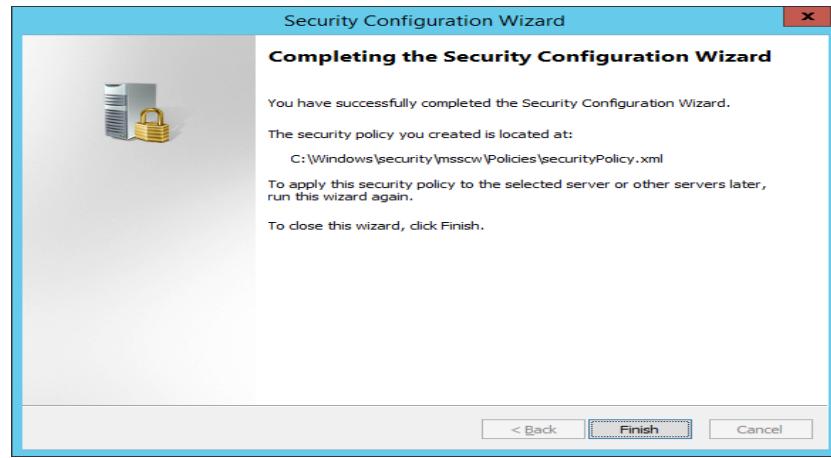


Figure 80: Security configuration wizard is complete

Disable or Delete Unnecessary Accounts.

Step 1 : Go to Server Manager > Active Directory Domain Service > Active Directory Users and Computer > group4.com > Users.

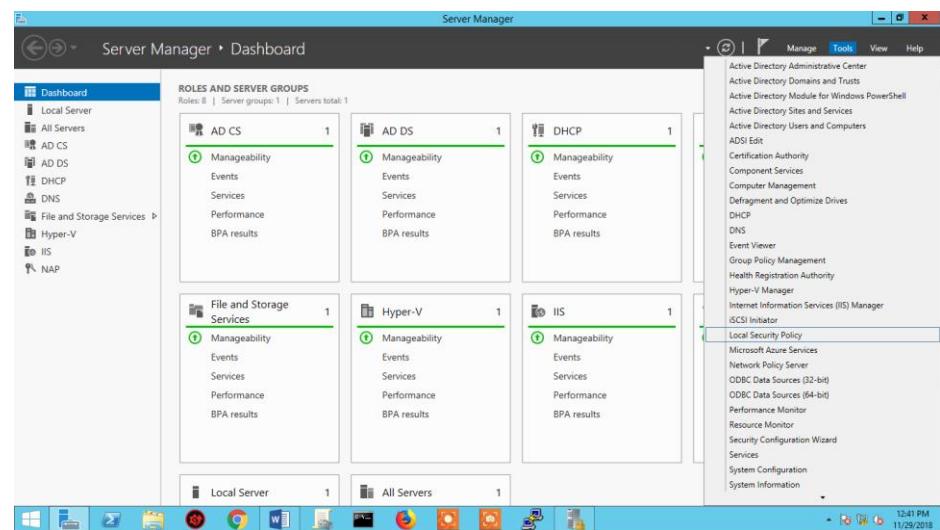


Figure 81: Server Manager dashboard

Step 2 : Right click Guest and choose Disable Account.

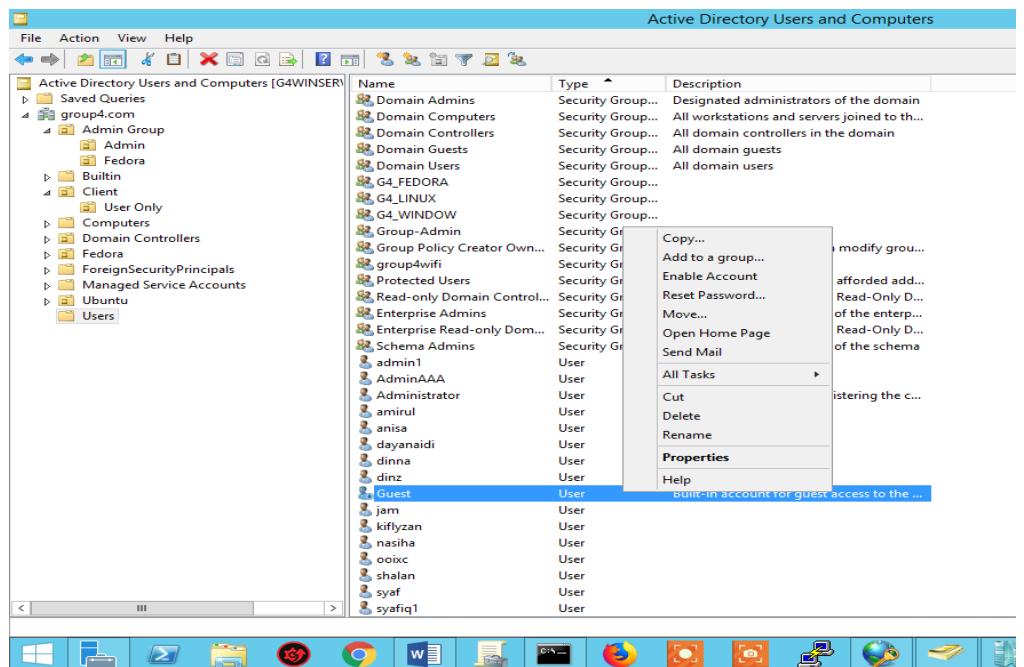


Figure 82: Disable account for guest

Configuring Auditing

Step 1 : Go to Start > Administrative Tools > Local Security Policy.

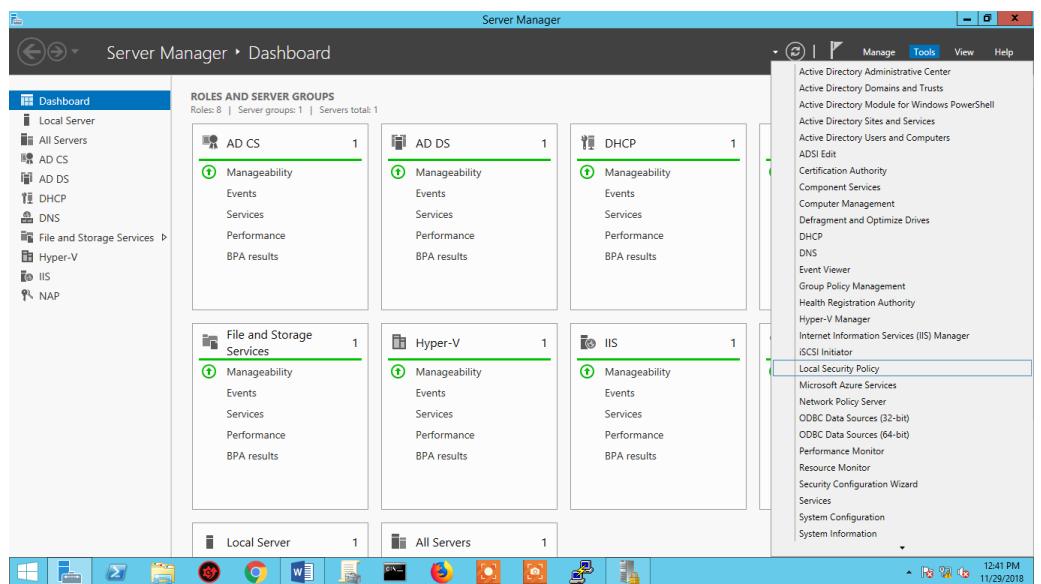


Figure 427: Local security policy

Step 2 : Go to Security Setting > Local Policies > Audit Policies.

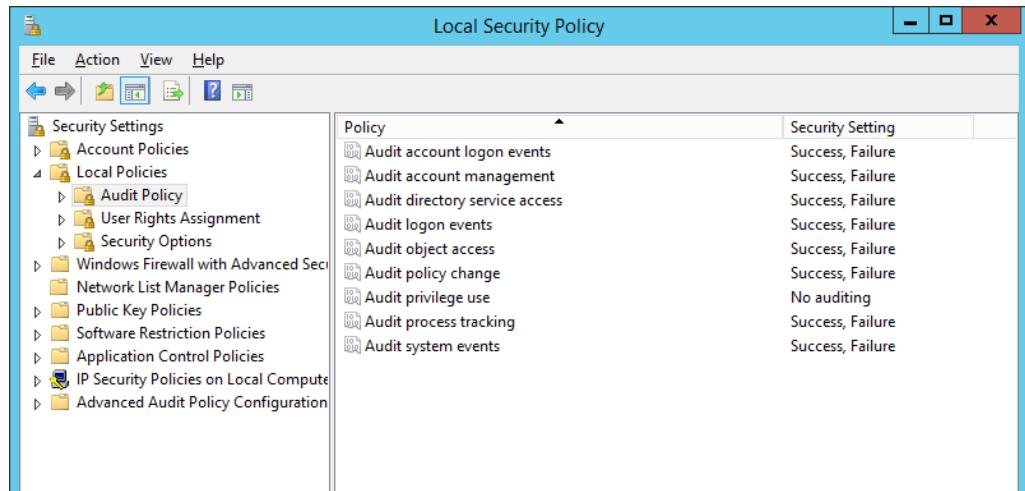


Figure 428: Audit policy

Step 3 : By default, Audit Policy setting in Windows Server 2012 have already attempt success and failure for each audit policy but only Audit Privilege use are not. Double click on Audit Privilege use then select Success and Failure.

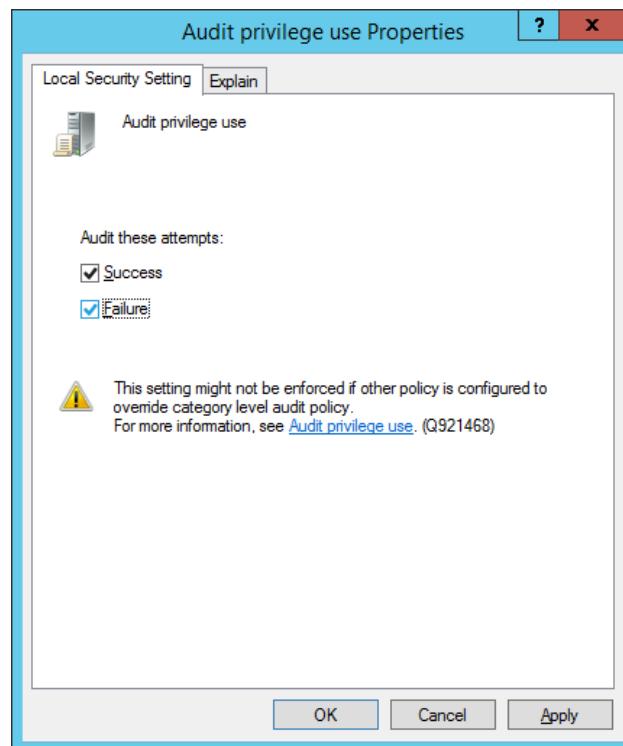


Figure 429: Local security setting for audit privilege use

Updates and Patches

Step 1 : Go to Start > search for Windows Update.

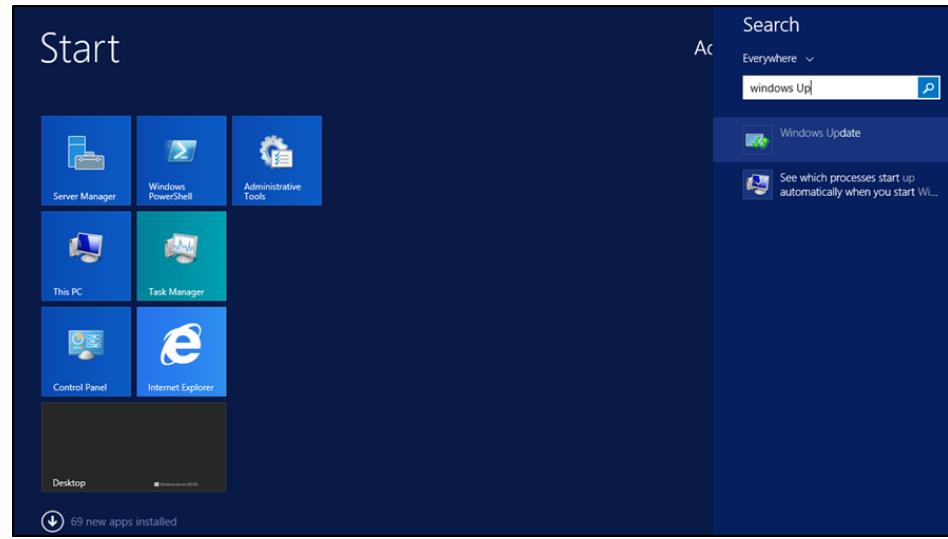


Figure 83: Search for Windows Update

Step 2 : Change the settings become Install updates automatically and click OK.

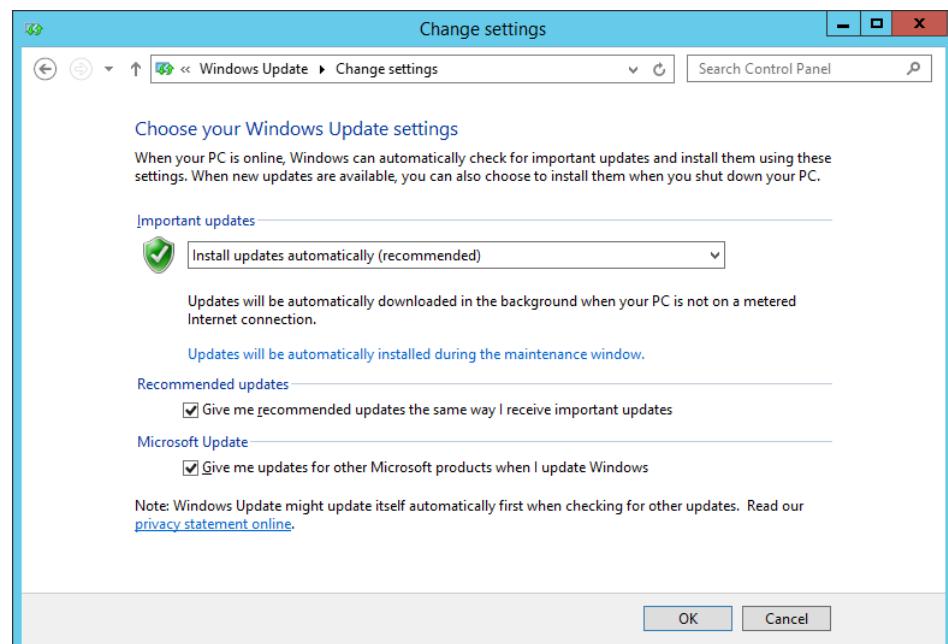


Figure 84: Change the setting of Installation updates

Step 3 : Check for view available updates to check the updates.

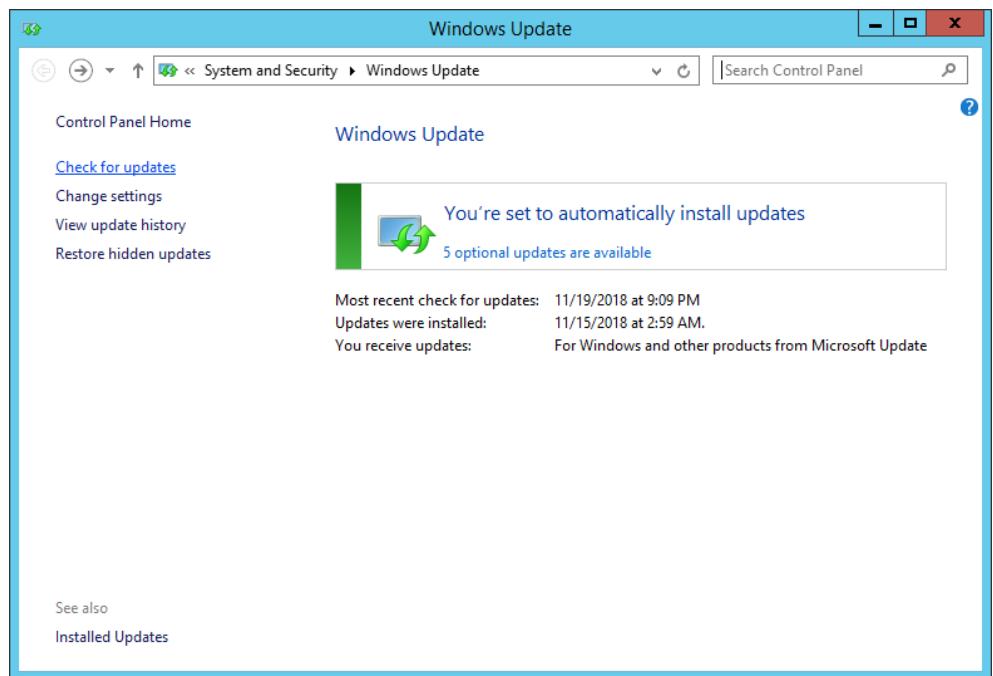


Figure 85: Check for available updates

Step 4 : Choose the updates that is needed to install and click Install.

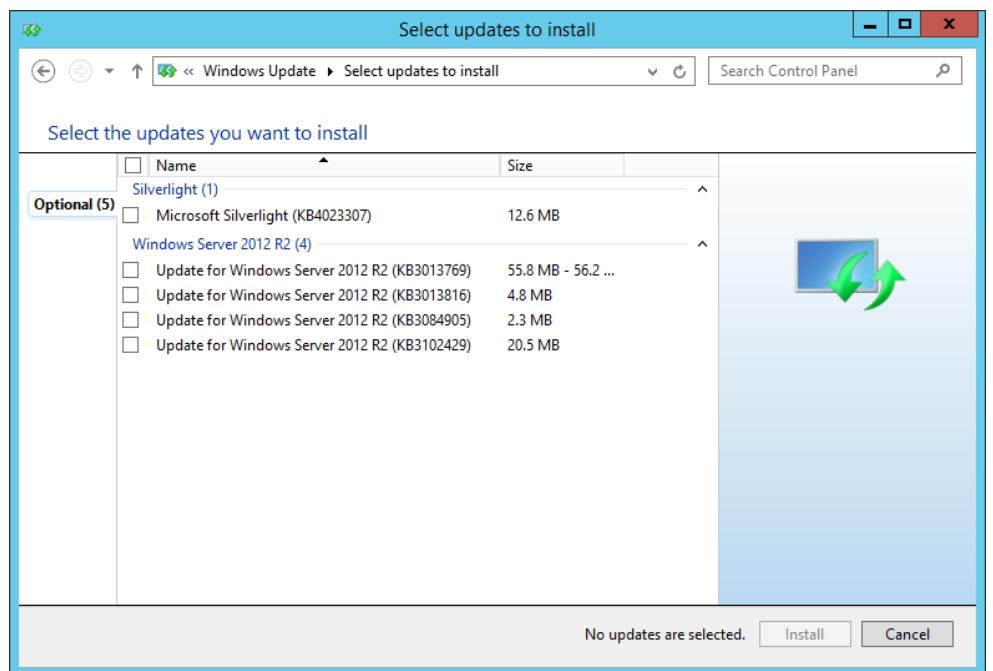


Figure 86: Choose the updates that need to be installed

Enable Windows Firewall

Step 1 : Open Windows Firewall with Advanced Security.

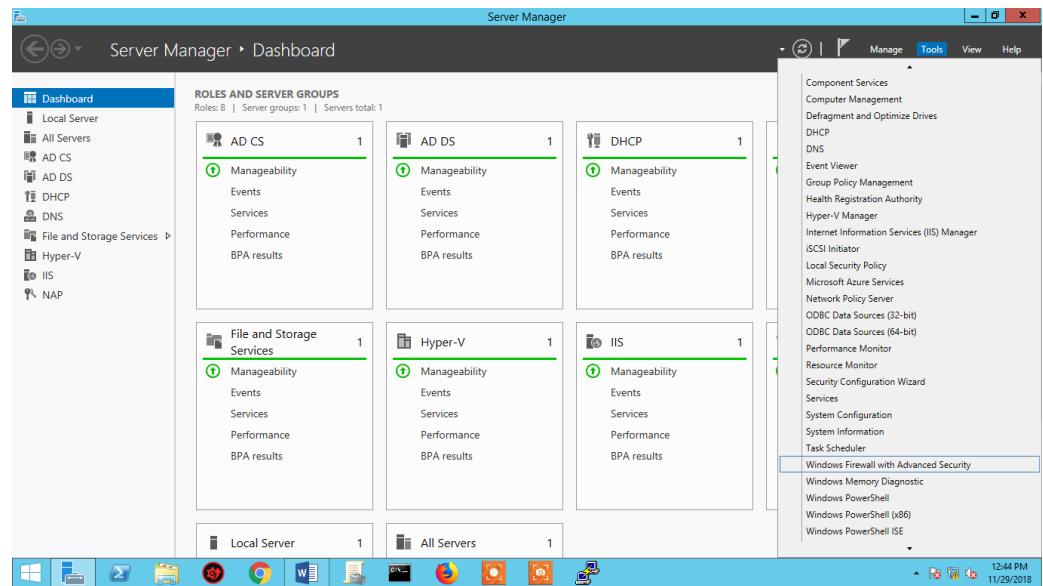


Figure 87: Server Manager dashboard

Step 2 : Enable the firewall.

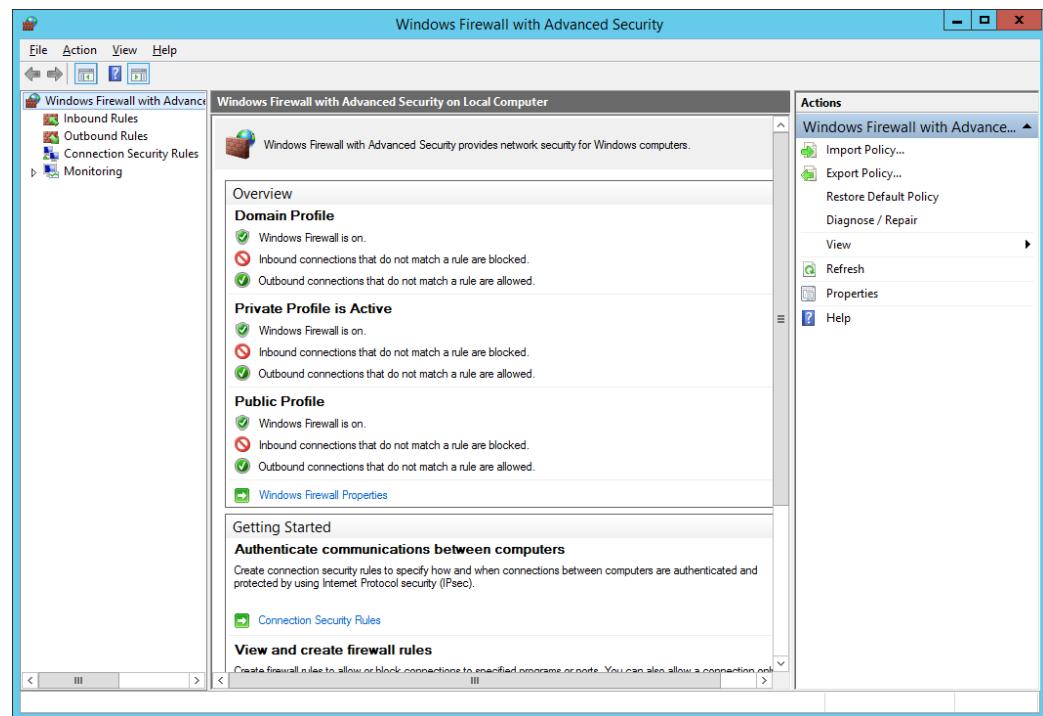


Figure 88: Enabling Firewall

Disable Automatic Services

Step 1 : Go to start and open Run, type in services.msc to open Services.

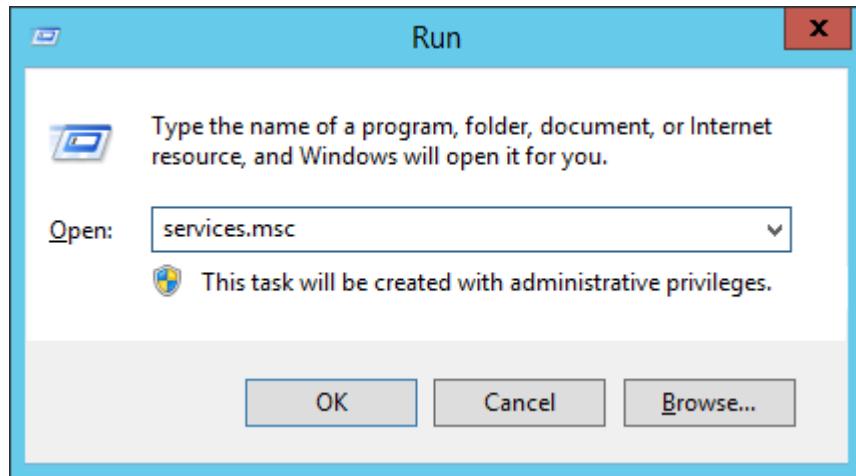


Figure 89: Search for services.msc

Step 2 : Change the Startup Type of Distributed Transaction Coordinator Properties from Automatic to Disabled.

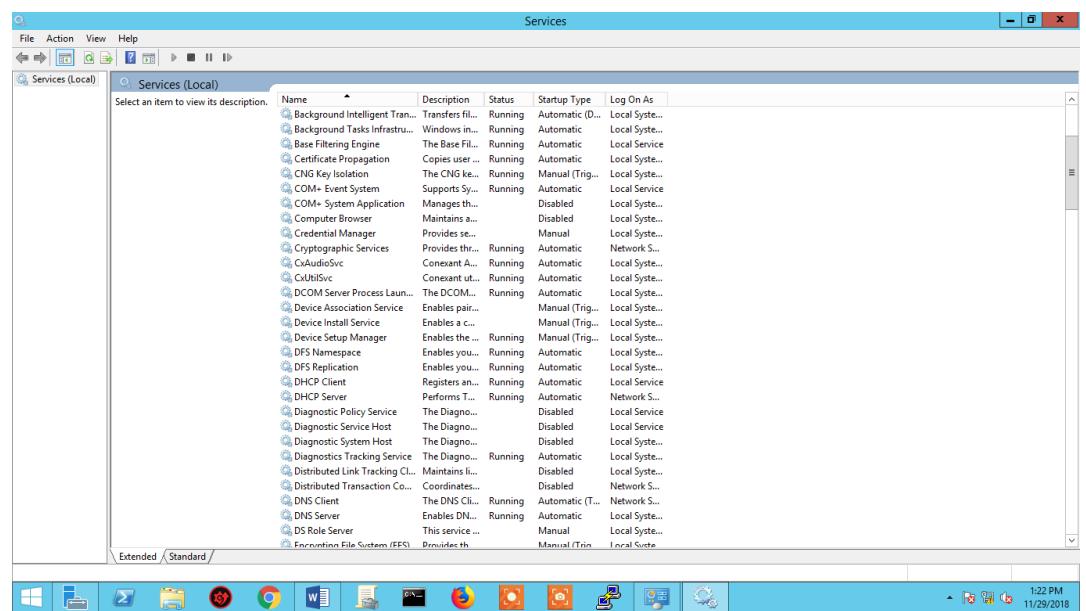


Figure 90: Change the Startup Type of Distributed Transaction Coordinator Properties

Step 3 Change the Startup Type of KtmRm for Distributed Transaction Coordinator Properties from Automatic to Disabled.

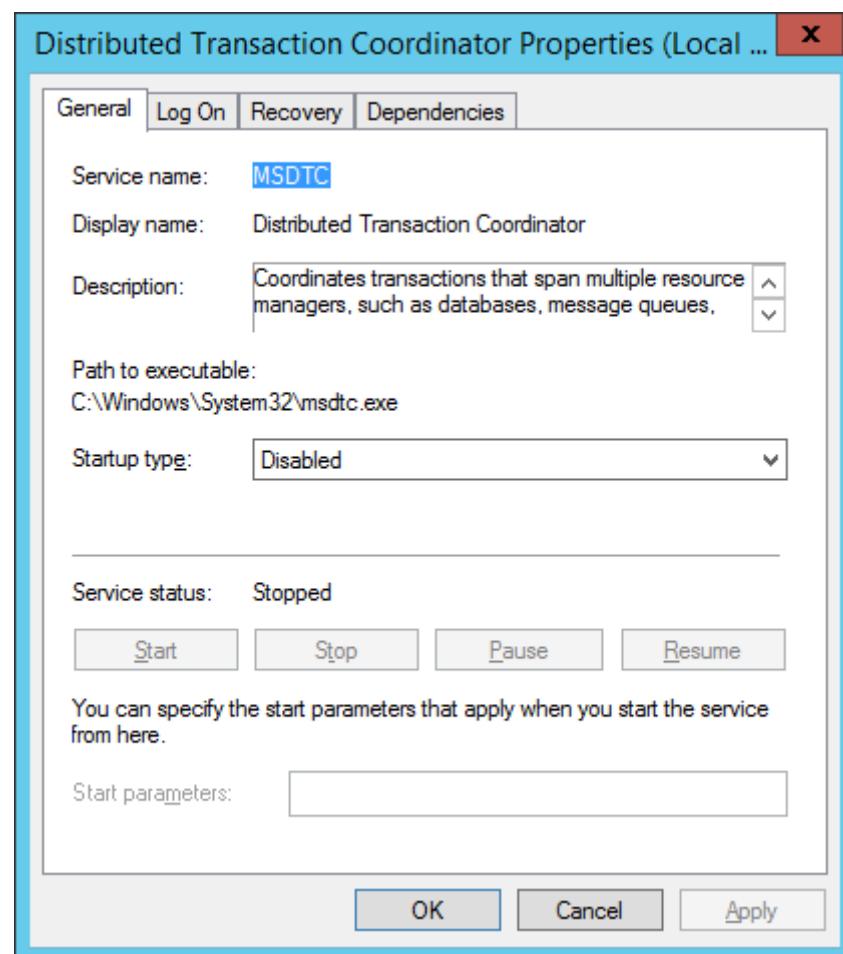


Figure 91: Change the Startup Type of KtmRm for Distributed Transaction Coordinator Properties

Step 4 : Change the Startup Type of Print Spooler Properties from Automatic to Disabled.

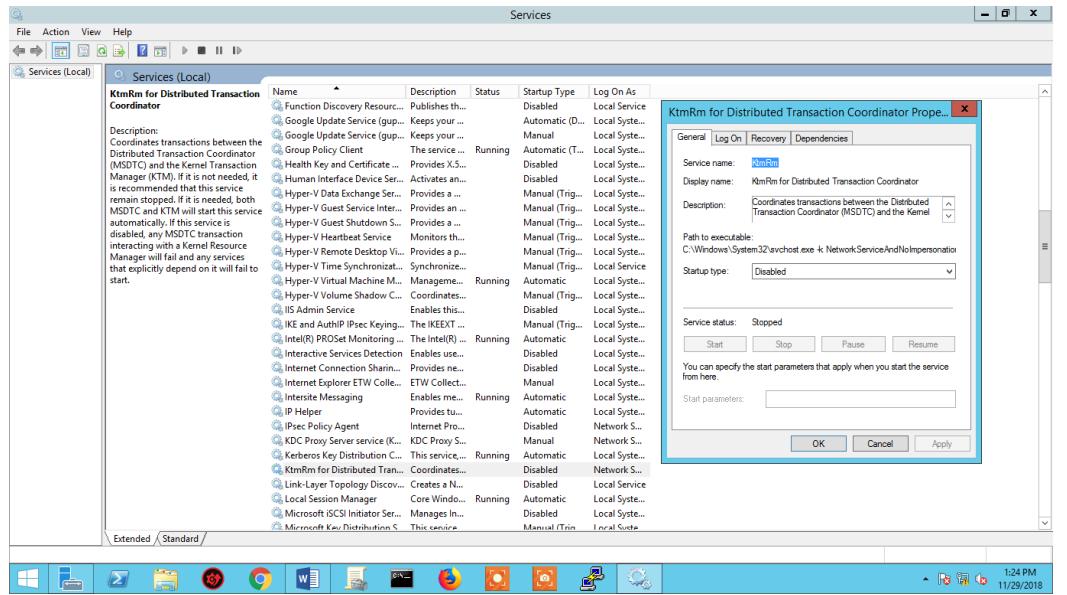


Figure 92: Change the Startup Type of Print Spooler Properties

Do Automatic Services

Step 1 : Go to Start and open Run. Then, type in services.msc to open Services.

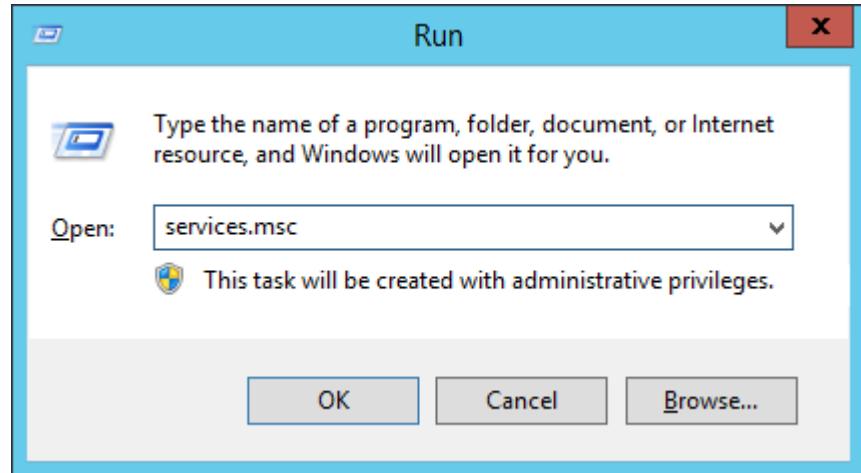


Figure 93: Search for services.msc

Step 2 : Change the Startup Type of Windows Error Reporting Service to Automatic and start the service.

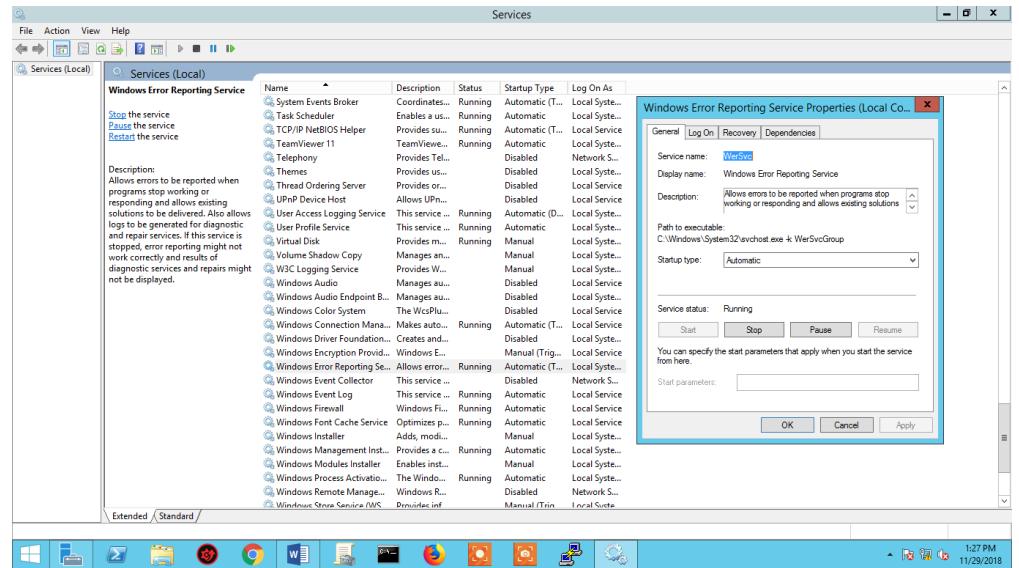


Figure 94: Change the Startup Type of Windows Error Reporting Service

Step 3 : Change the Startup Type of Secure Socket Tunneling Protocol Service Properties to Automatic and start the service.

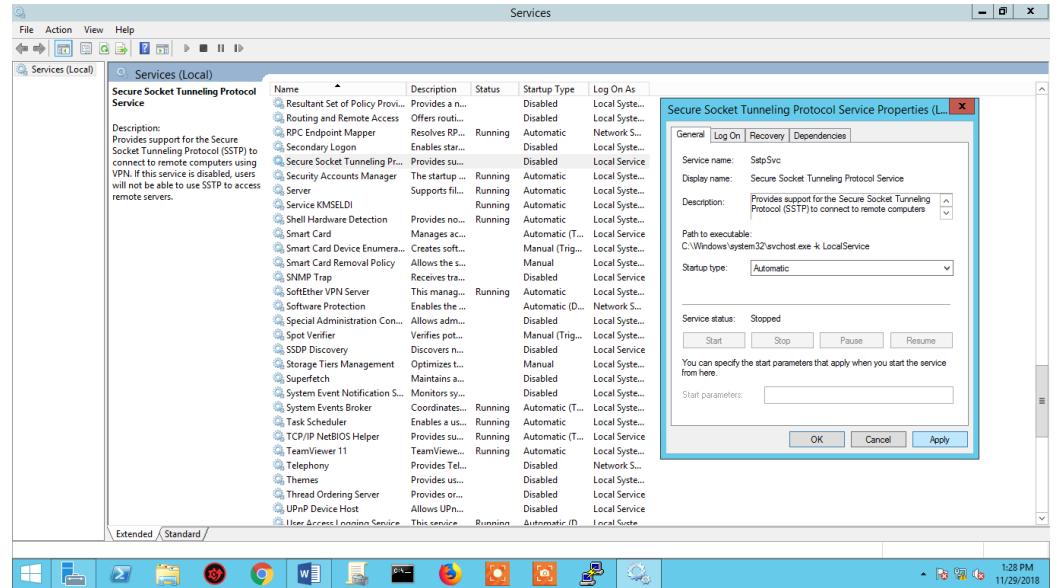


Figure 442: Change the Startup Type of Secure Socket Tunneling Protocol Service Properties

Step 4 : Change the Startup Type of Certificate Propagation Properties to Automatic and start the service.

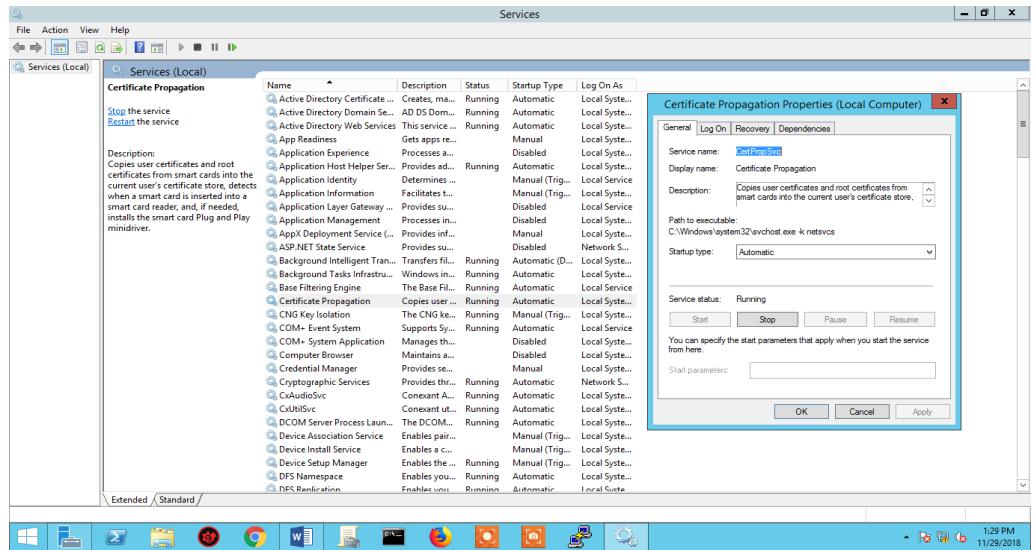


Figure 443: Change the Startup Type of Certificate Propagation Properties

Step 5 : Change the Startup Type of NetLogon to Automatic and start the service.

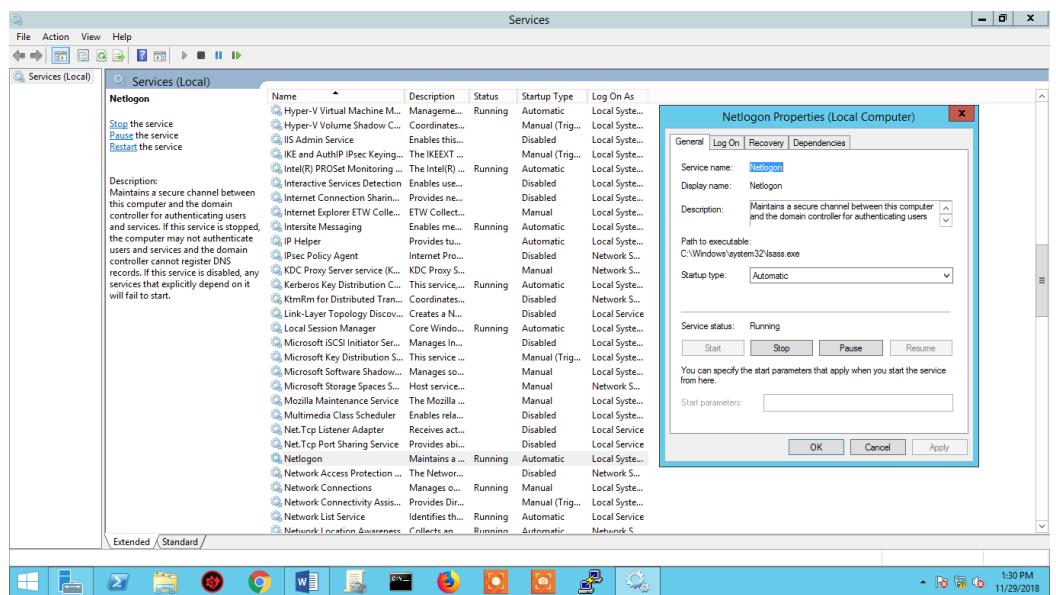


Figure 95: Change the Startup Type of NetLogon

Check Enabled Services

Step 1 : Ensure Windows Error Reporting Service startup type is Automatic and started. It has to be enabled so that it will capture software crash data and support end-user reporting of crash information.

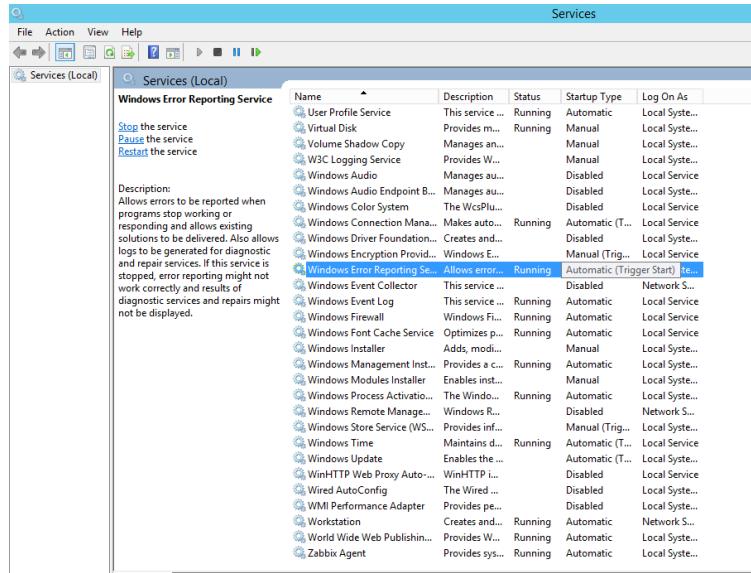


Figure 96: Windows Error Reporting Service

Step 2 : Check the status of Certificate Propagation. The startup has been changed to Automatic and started. It is used for Smart Card certificate handling. Smart-cards are used sometimes for log in instead of a password.

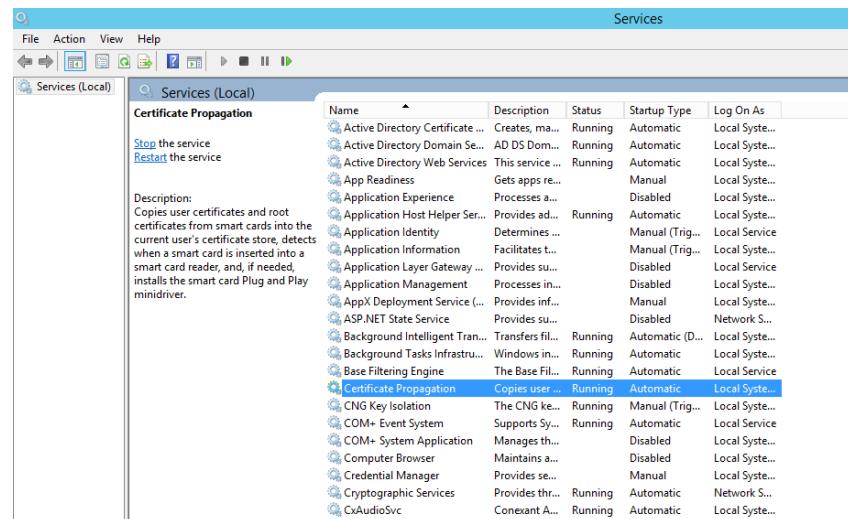


Figure 97: Check the status of Certificate Propagation

Step 3 : Ensure NetLogon startup type is Automatic and started. This maintains a channel between computer and domain controller. The NetLogon sub-key stores information for the NetLogon service. The Net Log on service verifies log-on requests and it registers, authenticates and locates domain controllers.

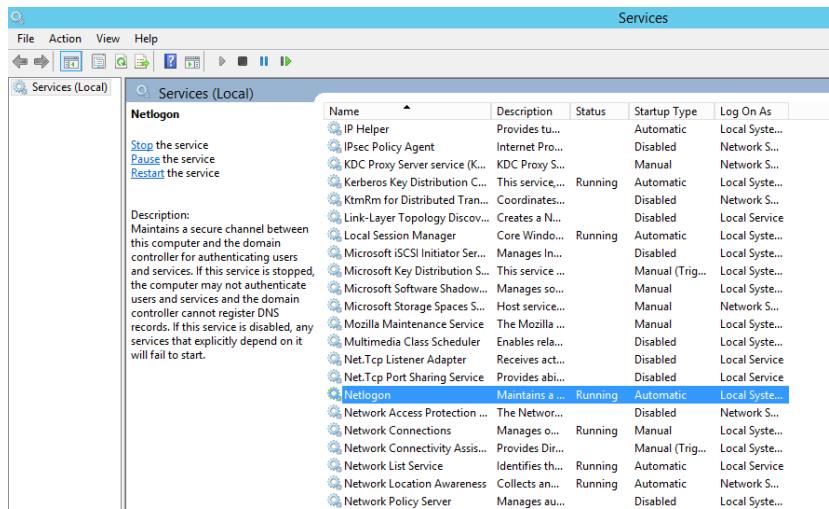


Figure 98: Ensure NetLogon startup type

5.4 Conclusion

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

6.0 TESTING

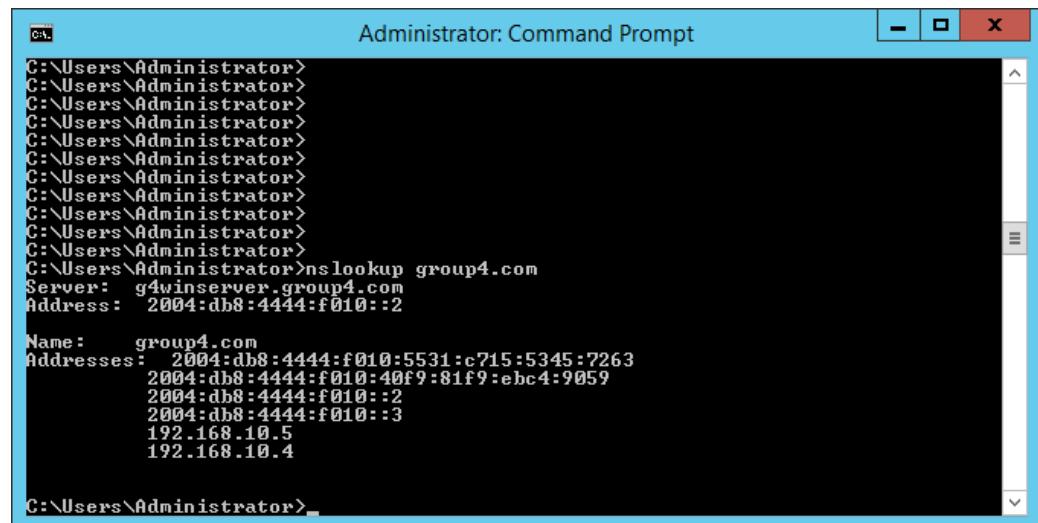
6.1 Introduction

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

6.2 Services Testing

6.2.1 Domain Name System (IPv4 & IPv6)

Step 1 : User nslookup. Both primary and secondary DNS for IPV4 and IPV6 should be listed here.



```
C:\> Administrator: Command Prompt
C:\>Administrator>
C:\>Administrator>nslookup group4.com
Server: g4winserver.group4.com
Address: 2004:db8:4444:f010::2

Name: group4.com
Addresses: 2004:db8:4444:f010:5531:c715:5345:7263
           2004:db8:4444:f010:40f9:81f9:ebc4:9059
           2004:db8:4444:f010::2
           2004:db8:4444:f010::3
           192.168.10.5
           192.168.10.4

C:\>Administrator>
```

Figure 448: Nslookup

6.2.2 Dynamic Host Configuration Protocol (DHCP) IPv4 & IPV6

Open the network manager and look for DHCP enabled. It should be showing yes indicating the host is receiving IP address from the DHCP server.

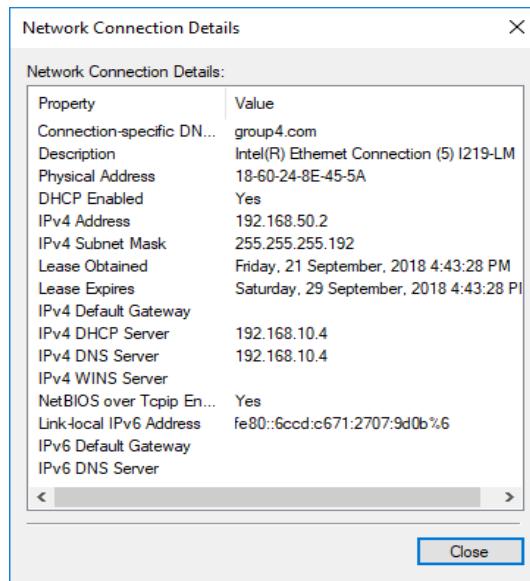


Figure 449: DHCP Testing

IPv6 Testing

Step 1: Successfully connect to wired_user_ipv6

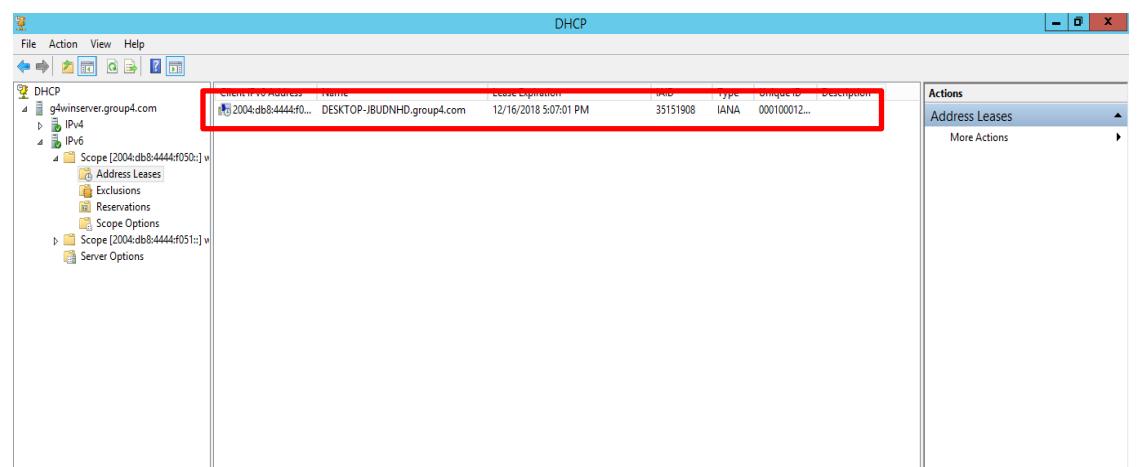


Figure 450: wired_user_ipv6 connected

Step 2: Successfully connect to wireless_user_ipv6

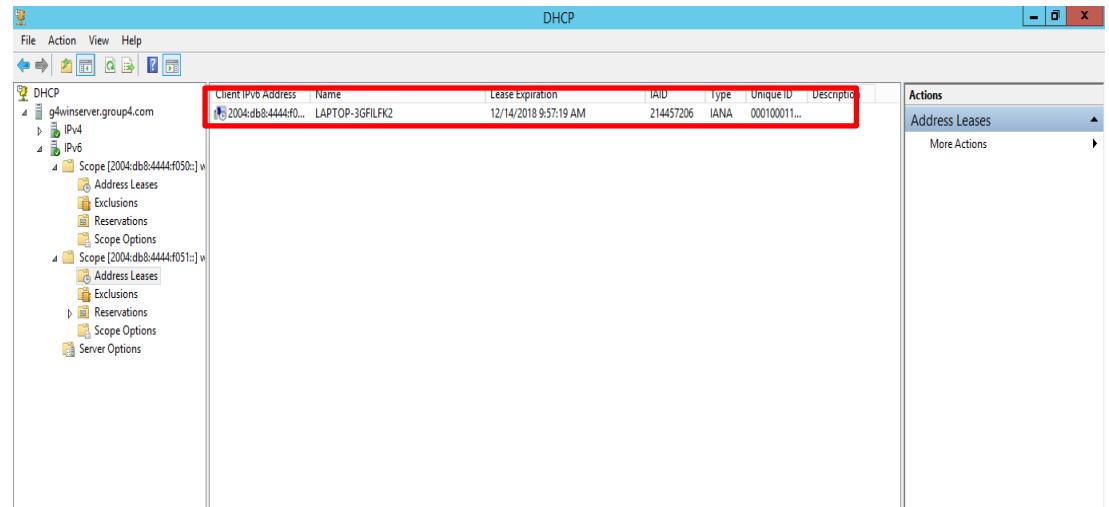


Figure 451: wireless_user_ipv6 connected

6.2.3 INTERVLAN and VLSM Addressing

Step 1: Insert command “*show run*”, then *Enter*.

```
G4Switch#sh vlan
VLAN Name Status Ports
---- --
1 default active Fa0/1, Fa0/13, Fa0/18, Fa0/19
                  Fa0/20, Fa0/21, Fa0/22, Fa0/23
                  Fa0/24, Gi0/1, Gi0/2
3 trunk active Fa0/2, Fa0/3, Fa0/4
10 windows active Fa0/5, Fa0/6, Fa0/7
20 ubuntu active Fa0/8, Fa0/9, Fa0/10
30 fedora active Fa0/14, Fa0/15, Fa0/16, Fa0/17
50 user active Fa0/11, Fa0/12
51 AP act/unsup
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Transl Trans2
---- --
1 enet 100001 1500 -- -- -- -- -- 0 0
3 enet 100003 1500 -- -- -- -- -- 0 0
10 enet 100010 1500 -- -- -- -- -- 0 0
20 enet 100020 1500 -- -- -- -- -- 0 0
30 enet 100030 1500 -- -- -- -- -- 0 0
50 enet 100050 1500 -- -- -- -- -- 0 0
51 enet 100051 1500 -- -- -- -- -- 0 0
1002 fddi 101002 1500 -- -- -- -- -- 0 0
1003 tr 101003 1500 -- -- -- ieee -- 0 0
1004 fdnet 101004 1500 -- -- -- ibee -- 0 0
1005 trnet 101005 1500 -- -- -- ibm -- 0 0

Remote SPAN VLANs

Primary Secondary Type Ports
---- --

```

Figure 452: Command to see VLAN Configuration

The command on the highlight line appeared:

```
COM4 - PuTTY

!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
!
interface FastEthernet0/1.3
encapsulation dot1Q 3
ip address 192.168.3.1 255.255.255.248
!
interface FastEthernet0/1.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.248
!
interface FastEthernet0/1.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.248
!
interface FastEthernet0/1.30
encapsulation dot1Q 30
ip address 192.168.30.1 255.255.255.248
!
interface FastEthernet0/1.50
encapsulation dot1Q 50
ip address 192.168.50.1 255.255.255.192
!
interface FastEthernet0/1.51
encapsulation dot1Q 51
ip address 192.168.51.1 255.255.255.192
!
interface Serial0/2/0
no ip address
shutdown
clock rate 2000000
!
```

Figure 453: Command to see trunking configuration

6.2.4 Routing & NAT

Step 1: Access any server from the neighbour or island and view the IP translation from router.

```
COM6 - PuTTY
G4Router#sh ip nat trans
G4Router#sh ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
icmp 200.200.202.4:1   192.168.10.4:1   200.200.202.11:1  200.200.202.11:1
udp 200.200.202.4:53  192.168.10.4:53   200.200.202.8:54828 200.200.202.8:54828
udp 200.200.202.4:53  192.168.10.4:53   200.200.202.8:54873 200.200.202.8:54873
udp 200.200.202.4:53  192.168.10.4:53   200.200.202.8:54938 200.200.202.8:54938
udp 200.200.202.4:53  192.168.10.4:53   200.200.202.8:54947 200.200.202.8:54947
udp 200.200.202.4:53  192.168.10.4:53   200.200.202.8:54950 200.200.202.8:54950
udp 200.200.202.4:53  192.168.10.4:53   200.200.202.8:54987 200.200.202.8:54987
udp 200.200.202.4:53  192.168.10.4:53   200.200.202.8:55022 200.200.202.8:55022
udp 200.200.202.4:53  192.168.10.4:53   200.200.202.8:55030 200.200.202.8:55030
udp 200.200.202.4:53  192.168.10.4:53   200.200.202.8:55158 200.200.202.8:55158
udp 200.200.202.4:53  192.168.10.4:53   200.200.202.8:55170 200.200.202.8:55170
udp 200.200.202.4:53  192.168.10.4:53   200.200.202.8:55227 200.200.202.8:55227
```

Figure 454: Show IP NAT Translation

6.2.5 Active Directory (AD)

Step 1 : From client, right-click Computer > Change Settings > System Properties > click button Change



Figure 455: System properties

Step 2 Click radio box Domain at Member of and named the group domain which are group4.com. Then, click OK button.



Figure 456: Computer Name/Domain Changes

Step 3 : A pop-up window will appear and prompt the username and password. Use AD account that have been created to fill in the username and password field. Then, click Enter button on the keyboard.

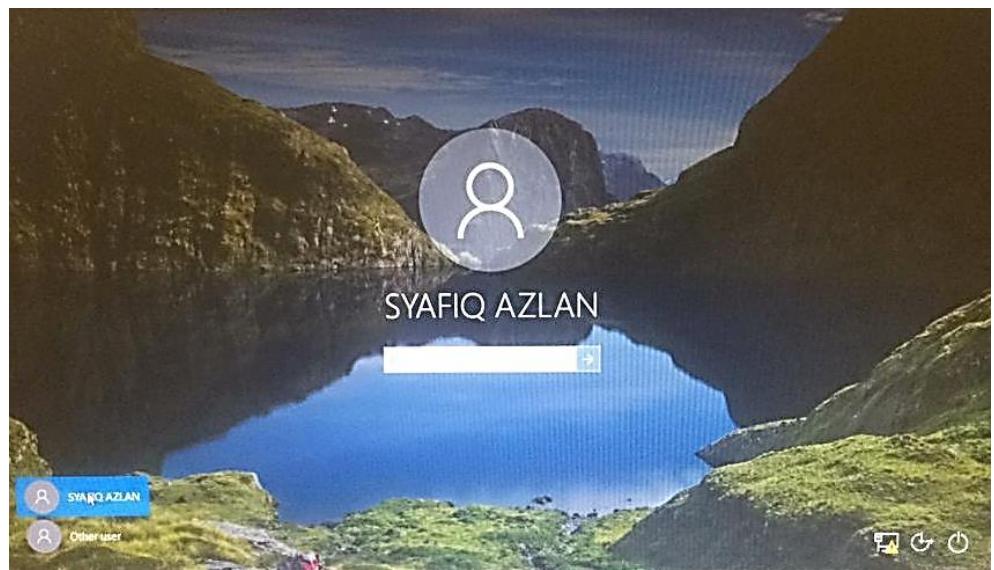


Figure 457: AD user account

Group Policy Object

Step 1 : From the client, login as client user.

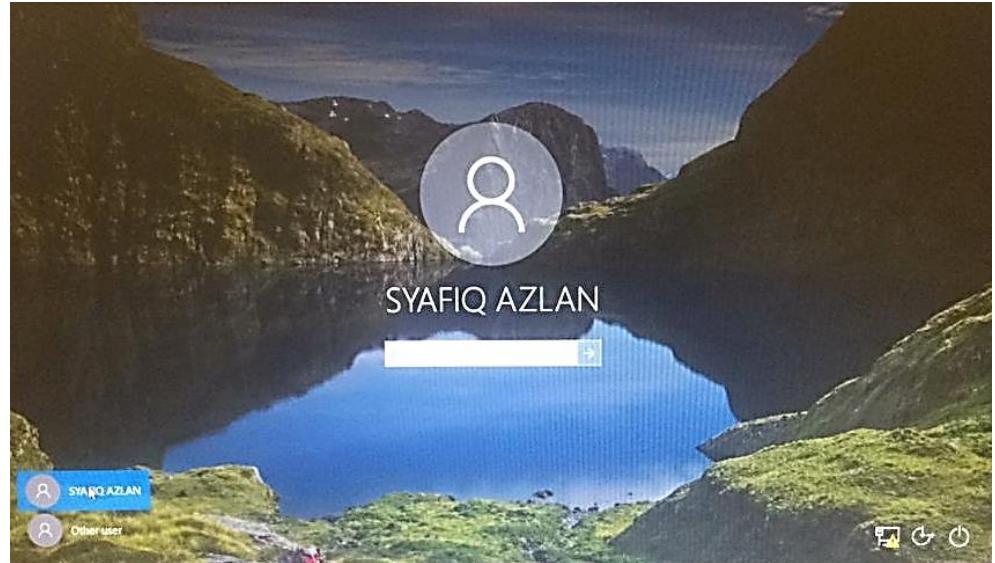


Figure 458: Login User Account

Step 2 : Firstly, open the file explorer.

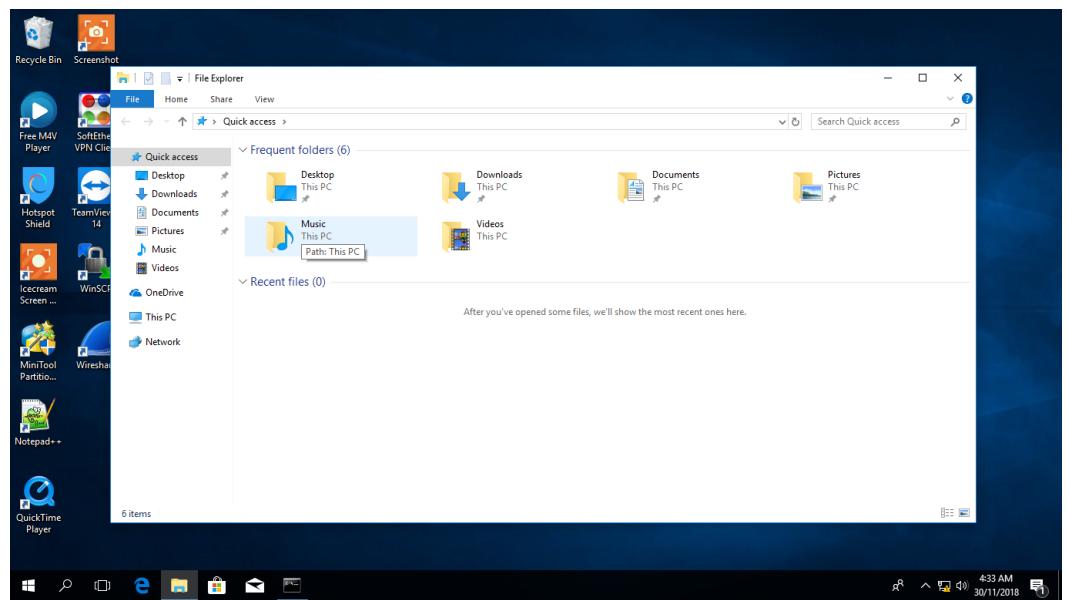


Figure 459: File Explorer

Step 3 : Next, connect the external hard disk or USB to this computer and click on This PC to check whether the USB are connected or not.

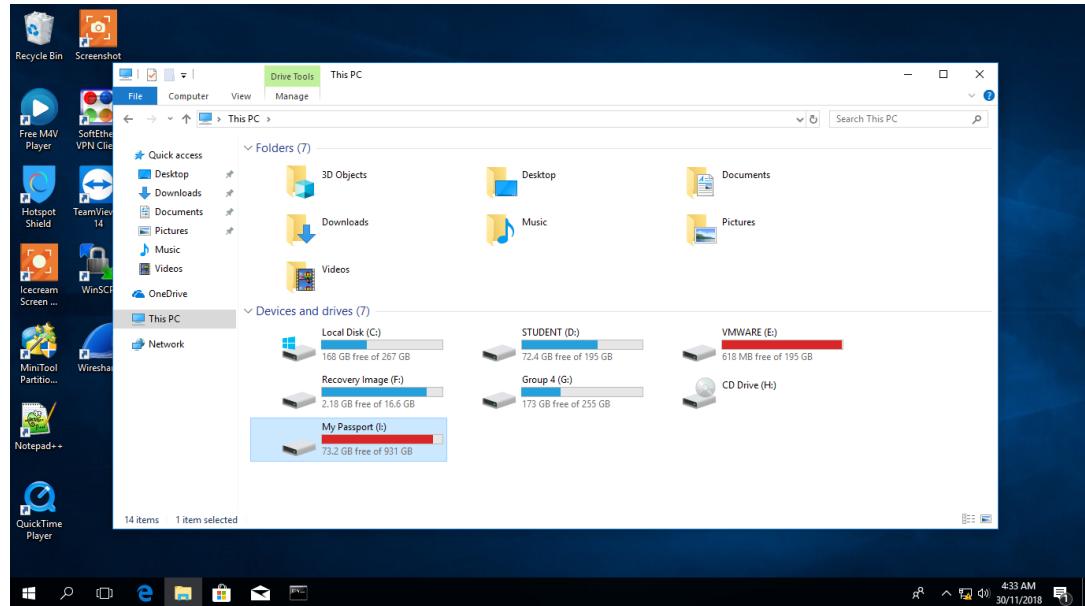


Figure 460: Connect to external hard disk/USB

Step 4 : Lastly, click on the external hard disk and then, the pop-up access denied will show that client is under control by group policy administration.

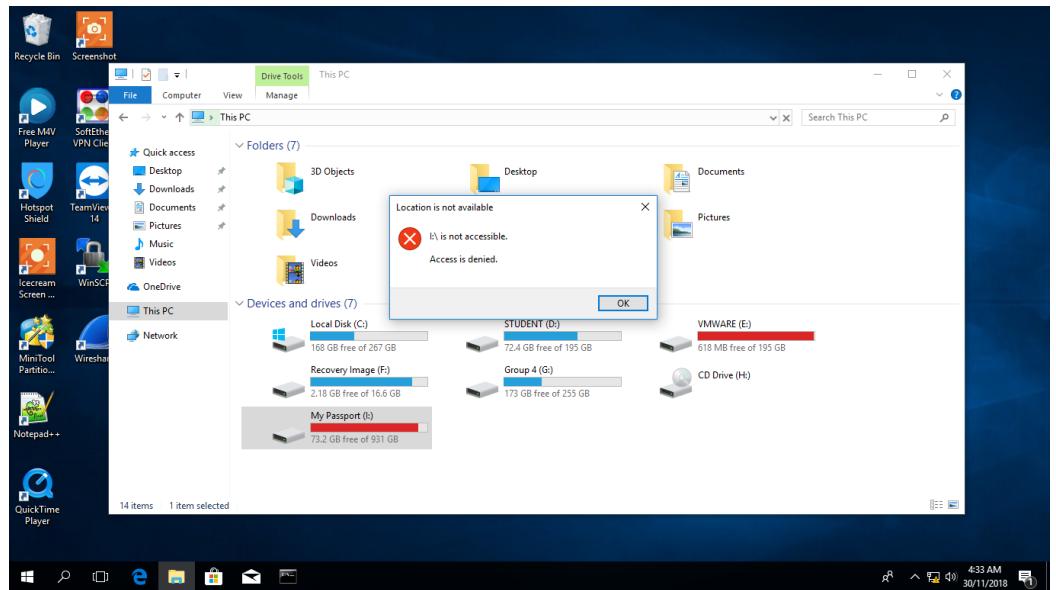


Figure 461: Pop-up Access Denied

6.2.6 Authentication User by Integrating AD with Linux

Step 1: Log in as “*Anisa*”

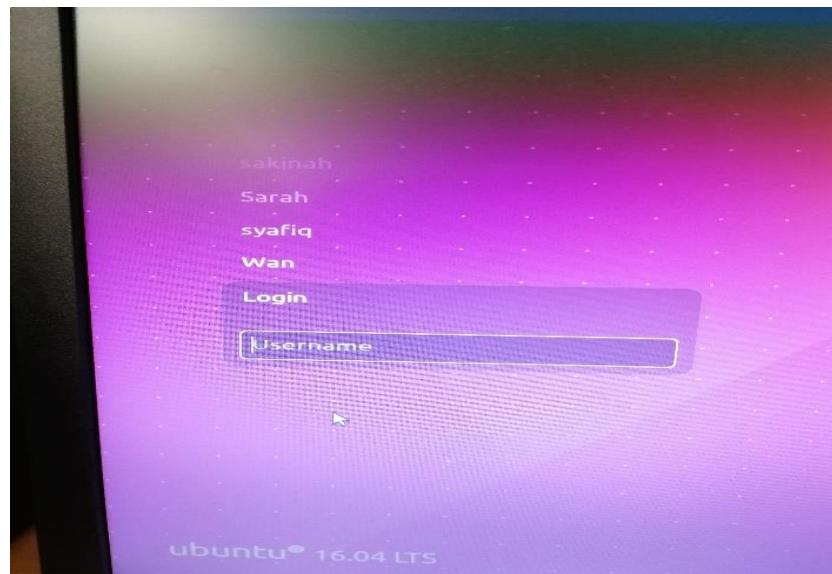


Figure 462: Log in username

Step 2: Enter the password for “*Anisa*” user.

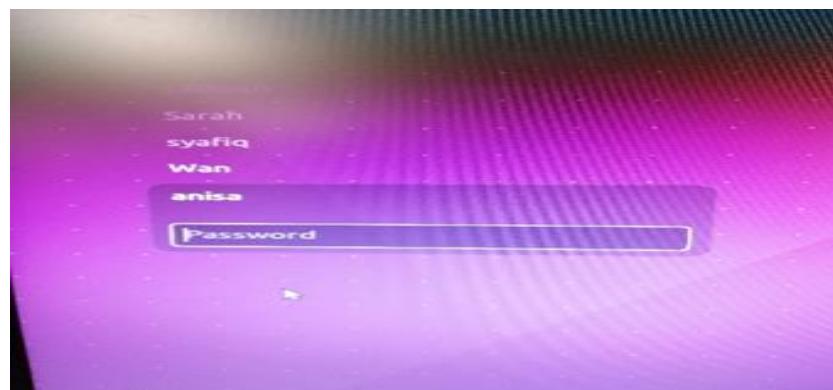


Figure 463: Enter the password

Step 3: Successfully access



Figure 464: Successfully access

6.2.7 Proxy Server

Check the status of proxy service and make sure the service is active.

```
File Edit View Search Terminal Tabs Help
g4-15@Fedora... × g4-15@Fedora... × g4-15@Fedora... × g4-15@Fedora... × g4-16@ubuntu... × g4-15@Fedora...
[g4-15@Fedora httpd]$ sudo su
[sudo] password for g4-15:
[root@Fedora httpd]# cd /etc/squid
[root@Fedora squid]# systemctl status squid.service
● squid.service - Squid caching proxy
   Loaded: loaded (/usr/lib/systemd/system/squid.service; enabled; vendor preset: disabled)
     Active: active (running) since Wed 2018-12-05 11:19:24 +08; 19min ago
       Process: 16420 ExecStop=/usr/sbin/squid -k shutdown -f $SQUID_CONF (code=exited, status=0/SUCCESS)
       Process: 16426 ExecStart=/usr/sbin/squid $SQUID_OPTS -f $SQUID_CONF (code=exited, status=0/SUCCESS)
       Process: 16421 ExecStartPre=/usr/libexec/squid/cache_swap.sh (code=exited, status=0/SUCCESS)
     Main PID: 16427 (squid)
        Tasks: 3 (limit: 4915)
       Memory: 20.1M
      CGroup: /system.slice/squid.service
              └─16427 /usr/sbin/squid -f /etc/squid/squid.conf
                  ├─16429 (squid-1) --kid squid-1 -f /etc/squid/squid.conf
                  └─16430 (logfile-daemon) /var/log/squid/access.log

Dec 05 11:19:24 Fedora systemd[1]: Starting Squid caching proxy...
Dec 05 11:19:24 Fedora squid[16427]: Squid Parent: will start 1 kids
Dec 05 11:19:24 Fedora squid[16427]: Squid Parent: (squid-1) process 16429 started
Dec 05 11:19:24 Fedora systemd[1]: Started Squid caching proxy.
[root@Fedora squid]#
```

Figure 465: Proxy Status

"*instagram.com*" is one of the website that has been blocked by the proxy server.

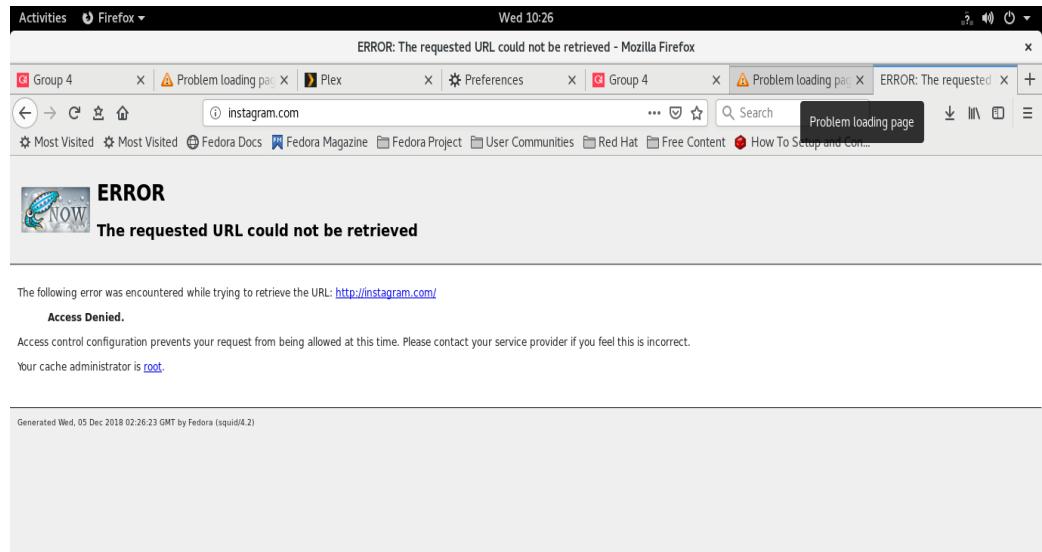


Figure 466: Blocked Website by Proxy

6.2.8 Samba

Client PC

Step 1: Go to client pc explorer and type the host IP address of Fedora terminal which that installed and configured the samba services \\192.168.30.4. A small window network credentials will pop up asking for user name and password. Enter the user added into samba group. The shared folder will be shown.

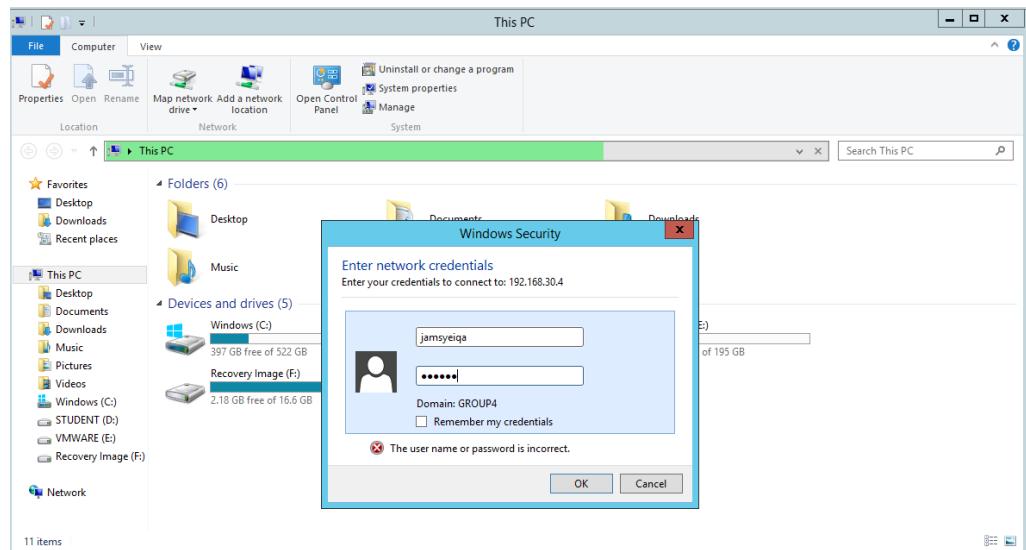


Figure 467: Enter username and password for authorized to access Samba

Step 2: The shared folder is visible and accessible. The user can add, edit, delete and view the file in the folder.

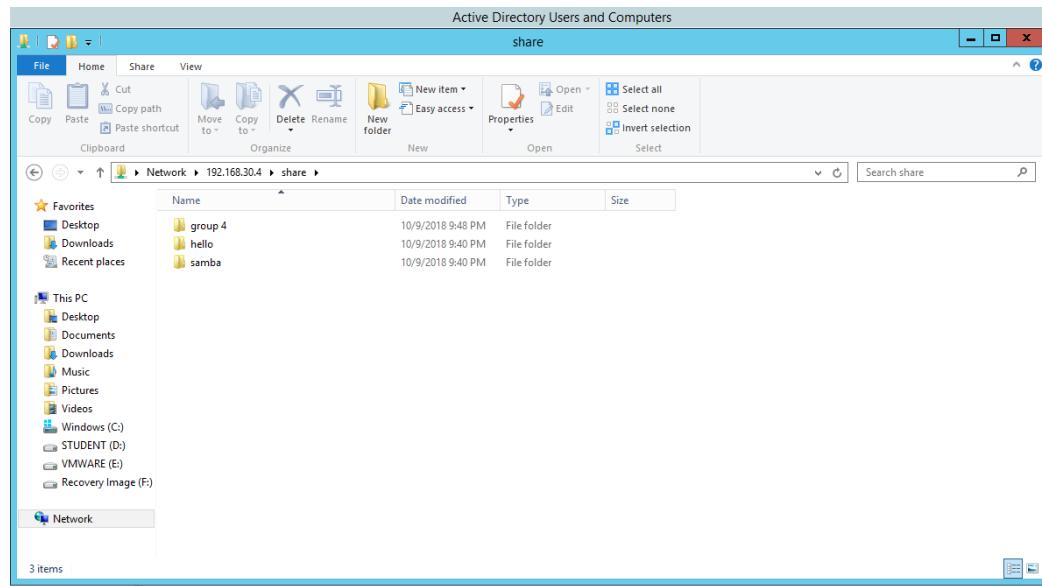


Figure 468: Shared files in Samba Folder

Ubuntu Server

Step 1: Go to *Connect to Server* in Ubuntu and click on it. Enter *smb://samba server IP address* and click “*Connect*”.

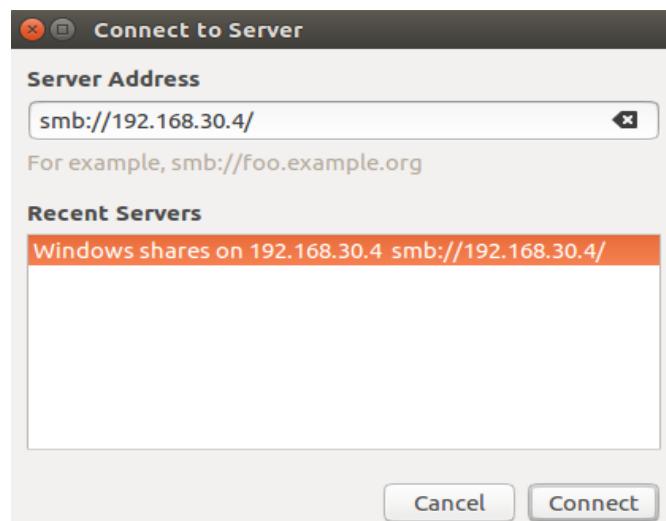


Figure 469: Connect to Samba Server

Step 2: The shared folder will be shown after that.

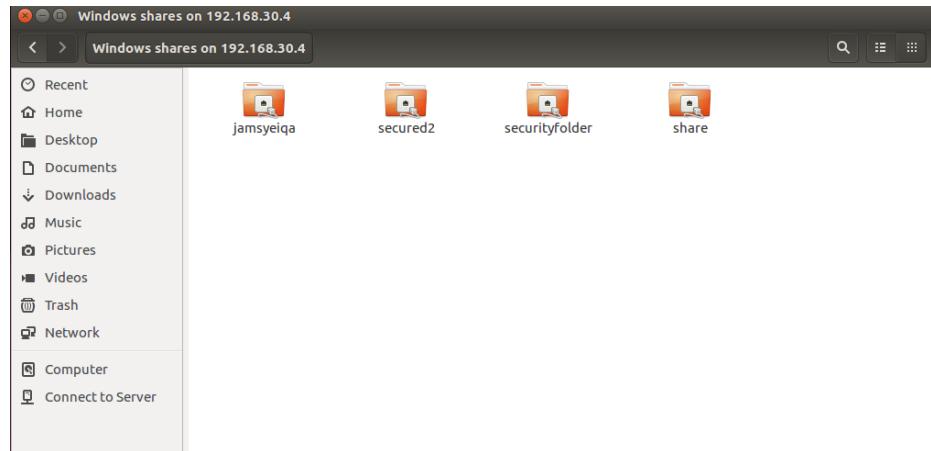


Figure 470: The shared folder is visible

Step 3: Enter the username and password added into Samba group. The password can be chosen to be forgotten immediately. After log out or remember forever. Choose the desired selection and click “Connect”.

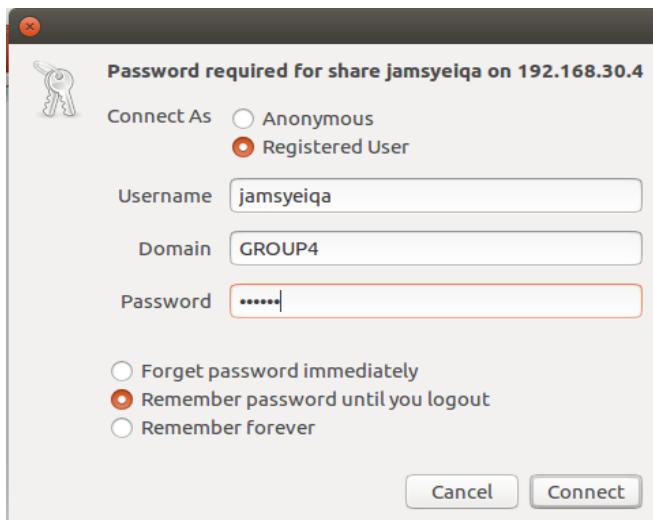


Figure 471: Enter username and password

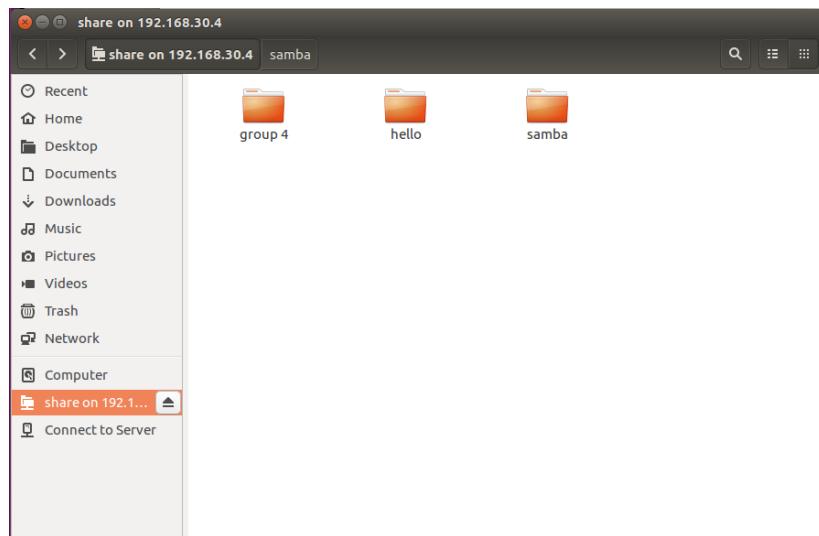


Figure 472: Shared files in Samba shared folder

6.2.9 Samba Security Services

Step 1: Enter ip address “smb://192.168.30.4/” on server connection option.

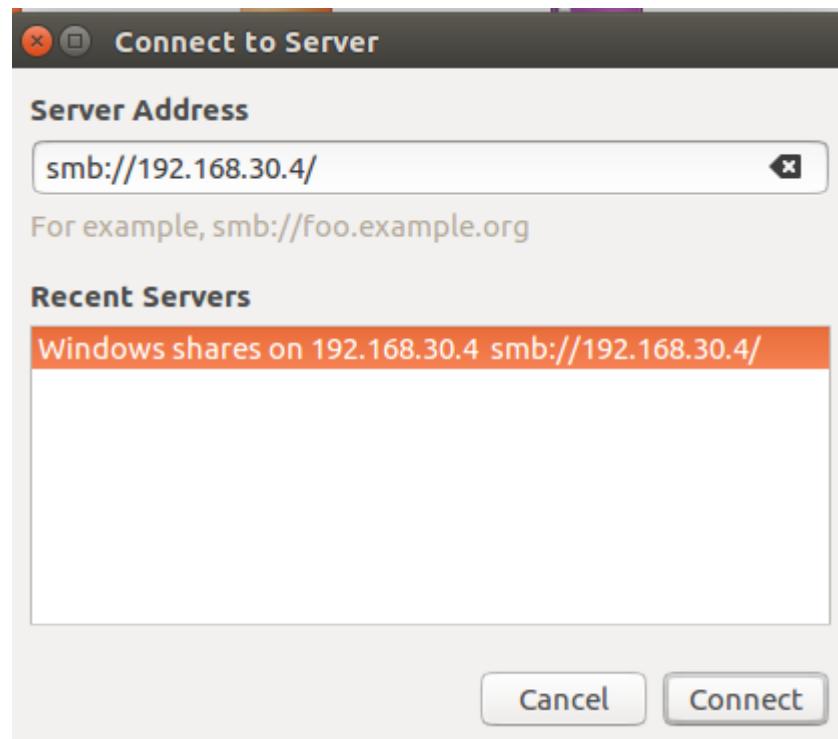


Figure 473: Enter IP Address and connect

Step 2: Open Secure folder and click anonymous.

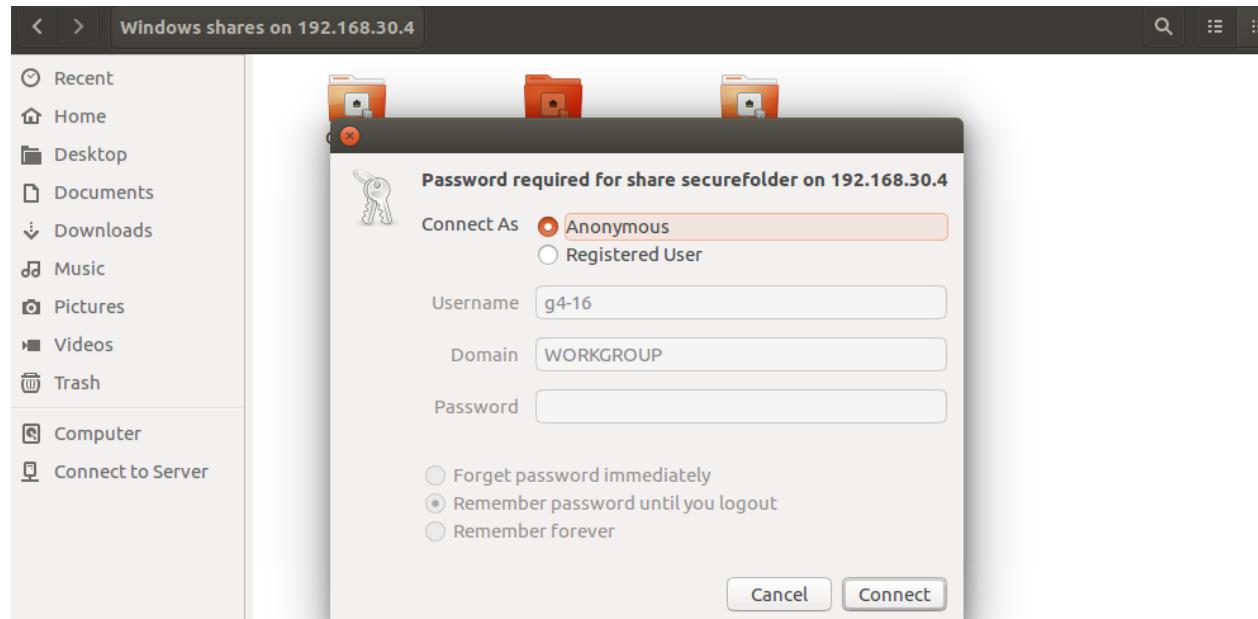


Figure 474: Input username and password

Step 3: The file in security folder cannot be accessed because it is not the allowed host to view file.

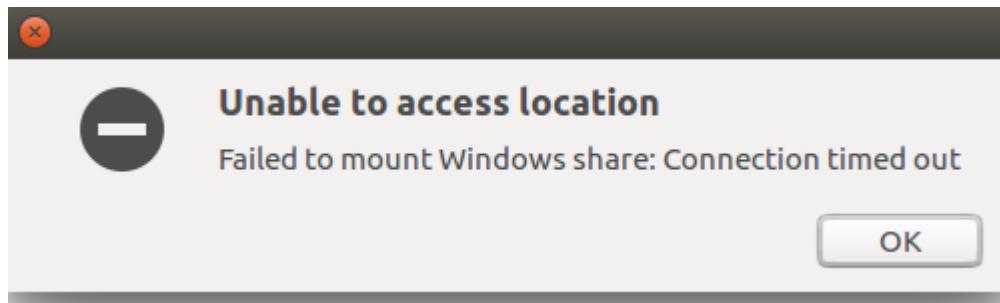


Figure 475: Failed to open file.

Step 4: Type the samba IP address in Windows Explorer and click on Secure folder.

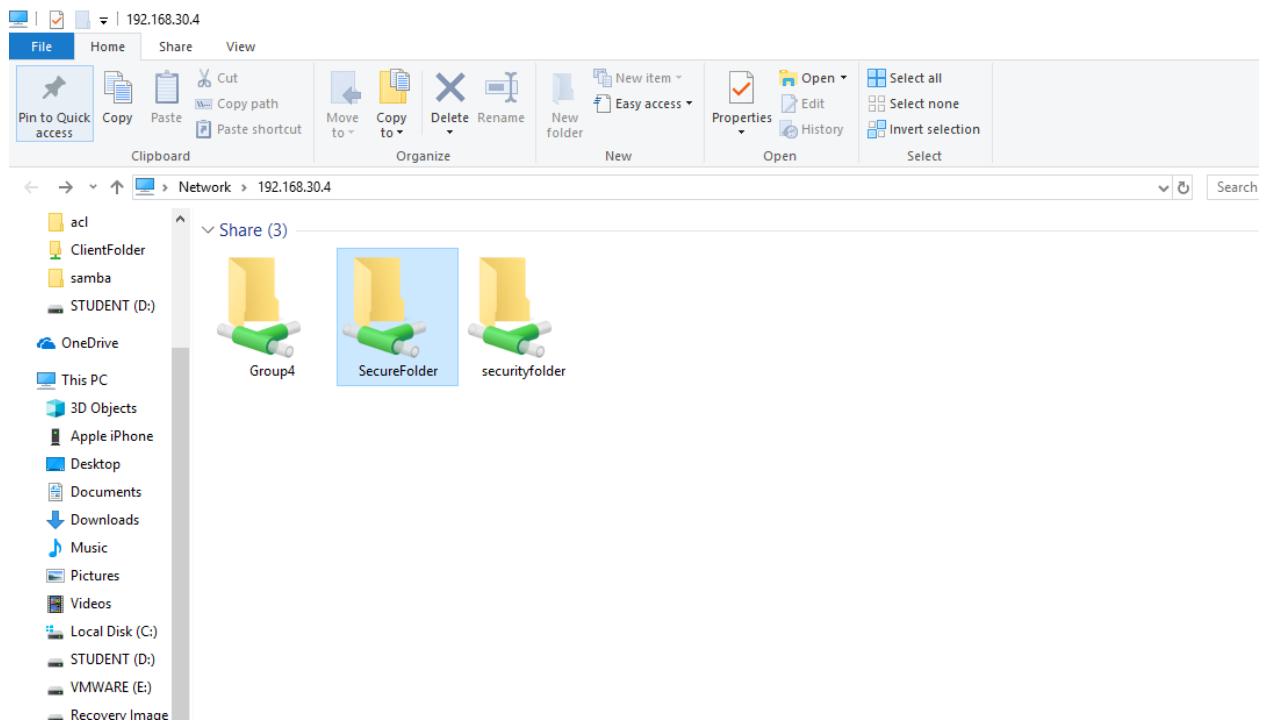


Figure 476: Open Secure Folder in Windows

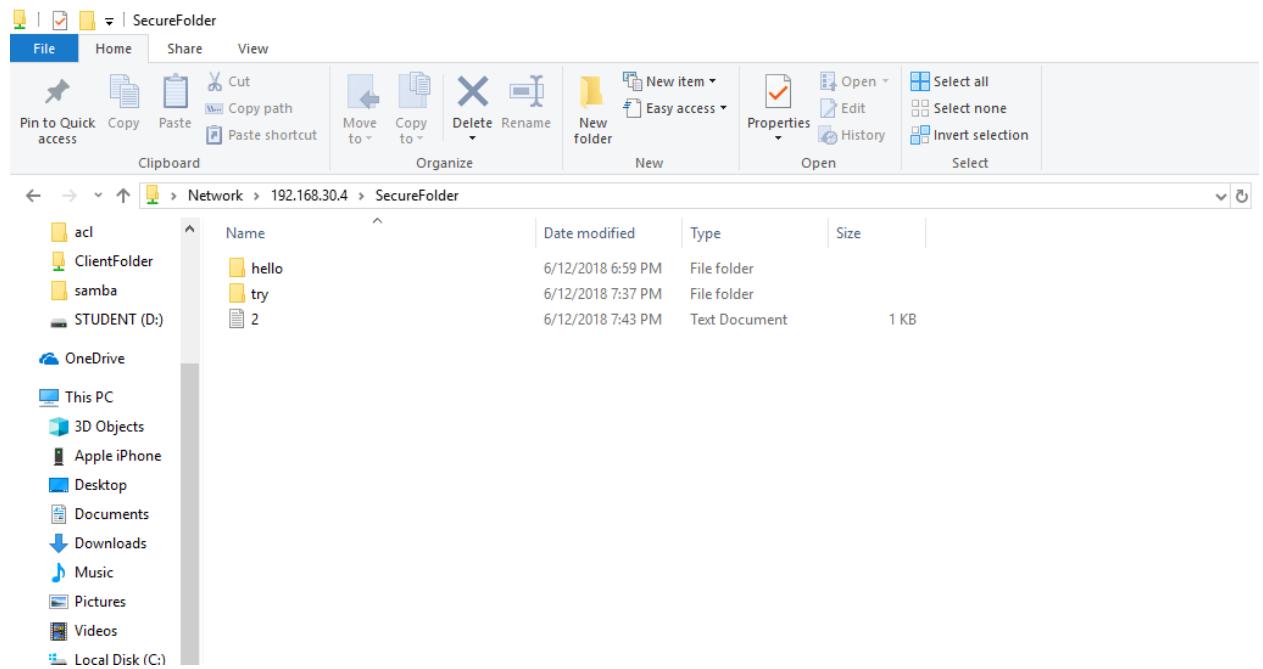


Figure 477: Samba can be opened in Windows

6.2.10 Network Management System

Step 1: Open web browser and type `zabbix.group4.com`. Insert Username and Password by default “`admin`” and “`g4123456@`”

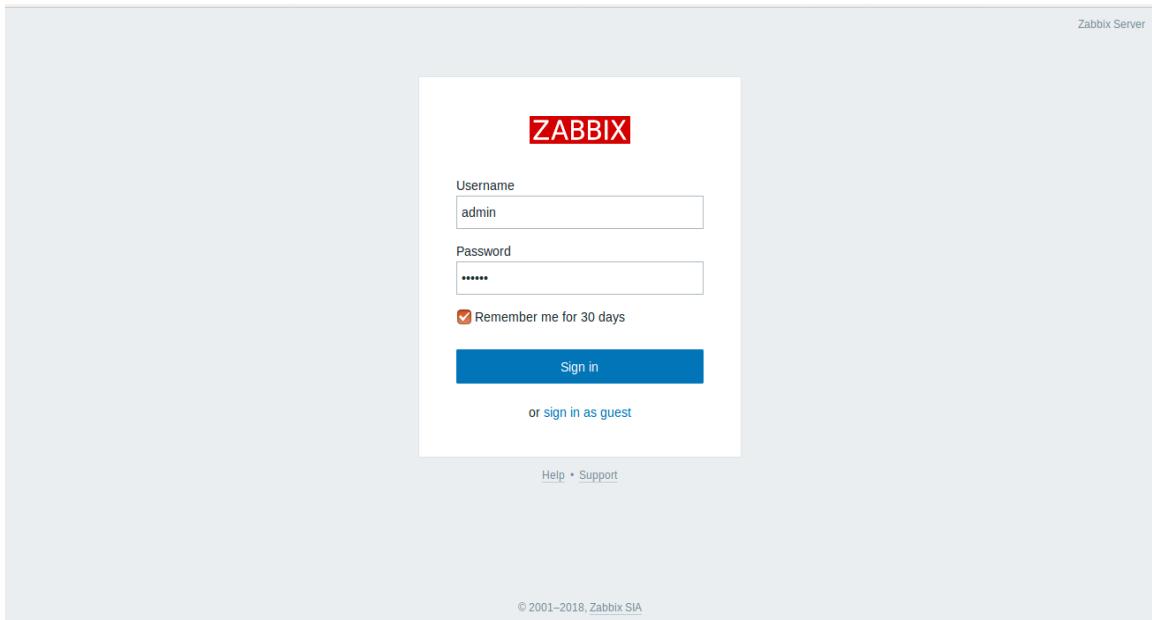


Figure 478: Open browser and login a username and password

Step 2: Go to configuration and then host. It shows the preferred server for monitoring.

The screenshot shows the Zabbix Server: Configuration of hosts - Mozilla Firefox window. The URL is zabbix.group4.com/hosts.php?ddreset=1. The page title is "ZABBIX Monitoring". The main content area is titled "Hosts" and displays a table of host configurations. The columns include Name, Applications, Items, Triggers, Graphs, Discovery, Web, Interface, Templates, Status, Availability, Agent encryption, and Info. The table lists five hosts: Fedora Server, Router, SWITCH, Ubuntu Server, and Windows Server, each with its respective details and status.

Name	Applications	Items	Triggers	Graphs	Discovery	Web	Interface	Templates	Status	Availability	Agent encryption	Info
Fedora Server	Applications 10	Items 53	Triggers 21	Graphs 11	Discovery 2	Web 192.168.30.4:10050		Template OS Linux (Template App Zabbix Agent)	Enabled	ZBX SNMP JMX IPMI	NONE	
Router	Applications 2	Items 102	Triggers 12	Graphs 12	Discovery 1	Web 192.168.10.1:161		Template SNMP Device (Template SNMP Generic, Template SNMP Interfaces)	Enabled	ZBX SNMP JMX IPMI	NONE	
SWITCH	Applications 2	Items 270	Triggers 33	Graphs 33	Discovery 1	Web 192.168.20.2:161		Template SNMP Device (Template SNMP Generic, Template SNMP Interfaces)	Enabled	ZBX SNMP JMX IPMI	NONE	
Ubuntu Server	Applications 10	Items 41	Triggers 17	Graphs 8	Discovery 2	Web 192.168.20.4:10050		Template OS Linux (Template App Zabbix Agent)	Enabled	ZBX SNMP JMX IPMI	NONE	
Windows Server	Applications 9	Items 95	Triggers 14	Graphs 35	Discovery 2	Web 192.168.10.4:10050		Template OS Windows (Template App Zabbix Agent)	Enabled	ZBX SNMP JMX IPMI	NONE	

Figure 479: Zabbix NMS

6.2.11 Server Virtualization

Testing Web and SSL in Hyper-V

Web Testing

The web testing <http://www.group4webhv.com> was successfully can be browse in a web browser on three servers and client.

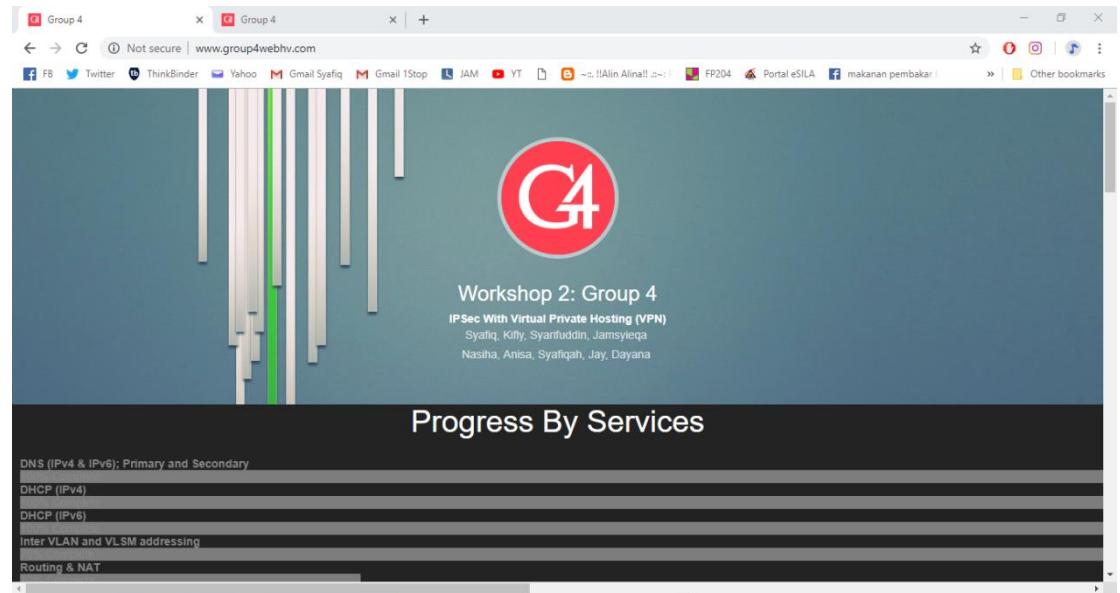


Figure 480: Web Hyper-V testing

SSL Testing

The SSL testing <https://www.group4webhv.com> was successfully can be browse in the web browser on three servers and client. The website has been secured by added the https for SSL.

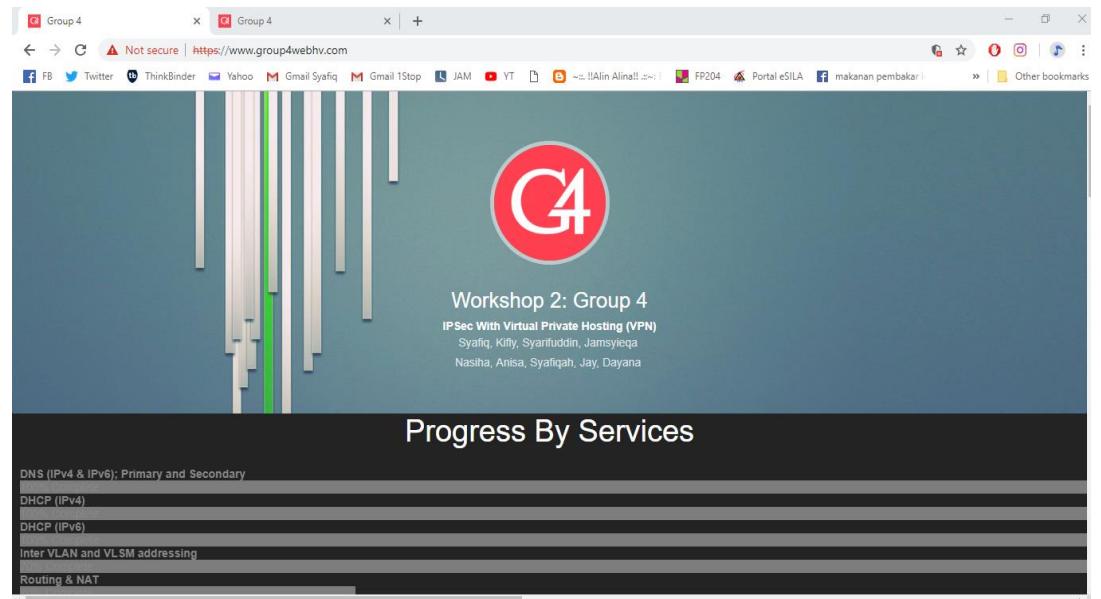


Figure 481 Secure Browsing Hyper-V Testing

6.2.12 AAA (Authentication, Authorization and Accounting) using Radius

User need to login the username and password that already set which a username is “**AdminAAA**” and password “**g4123456@**”.



Figure 482: Result at putty when user trying to login into the router

6.2.13 Wireless User Authentication using Radius Server

Step 1 : Open Wi-Fi in your mobile devices or laptop. Insert your identity and password.

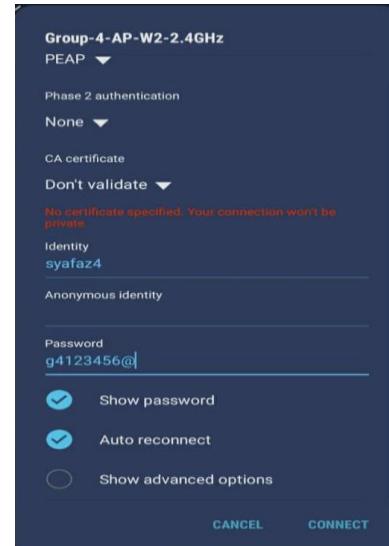


Figure 483: Insert identity and password

Step 2 : If connected, then, your wireless authentication is successful.

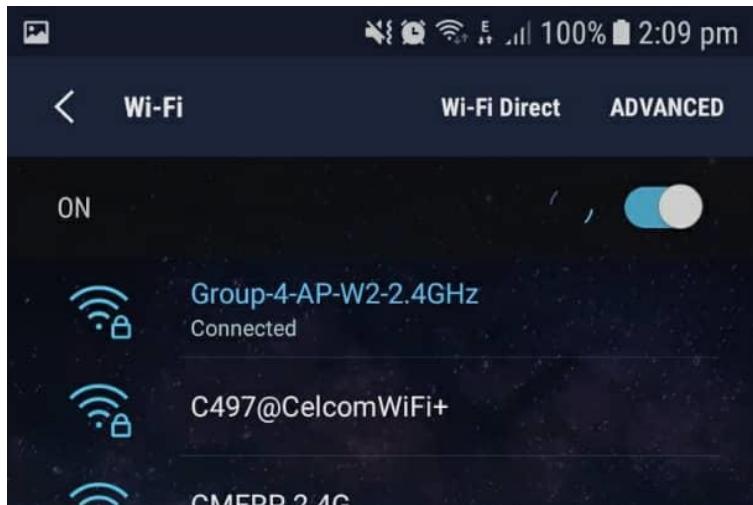


Figure 484: Wireless authentication successful

6.2.14 Access Control List (ACL)

Step 1: ACL can be test using command show ip access-list in the cisco router.

Step 2: Number of the matches shows there are packets was passing through the permitted services via interface f0/0.

```
access-list 104 permit tcp any 200.200.202.0 0.0.0.15 eq 443
access-list 104 deny   tcp any 200.200.202.0 0.0.0.15 eq 22
access-list 104 deny   tcp any 200.200.202.0 0.0.0.15 eq www
access-list 104 deny   tcp any host 200.200.202.6 eq 445
access-list 104 permit ip any any
```

Figure 485: ACL Configuration

Step 3: Our ACL will block http website in local area network to access outside.

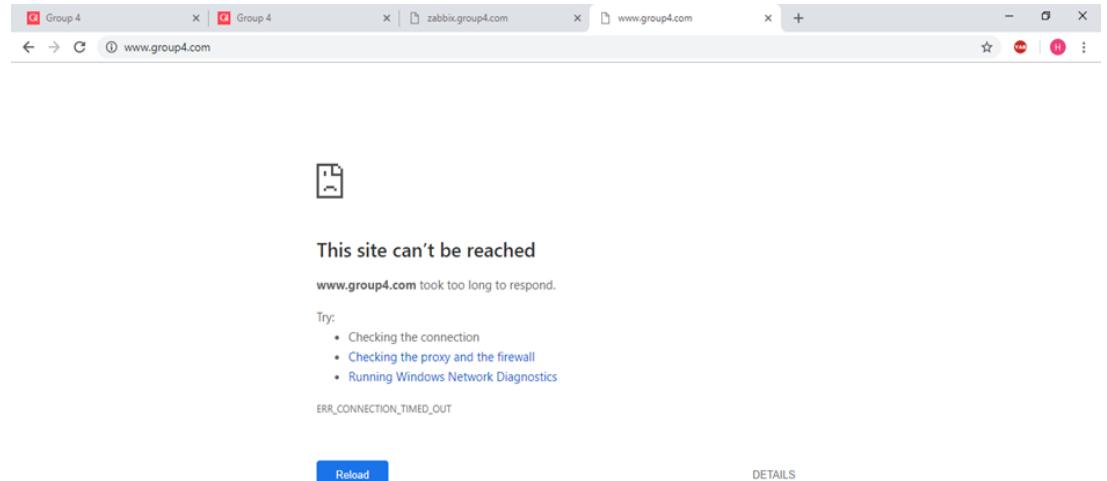


Figure 486: Open browser

Step 4: Our ACL permit HTTPS in local area network to access outside network.

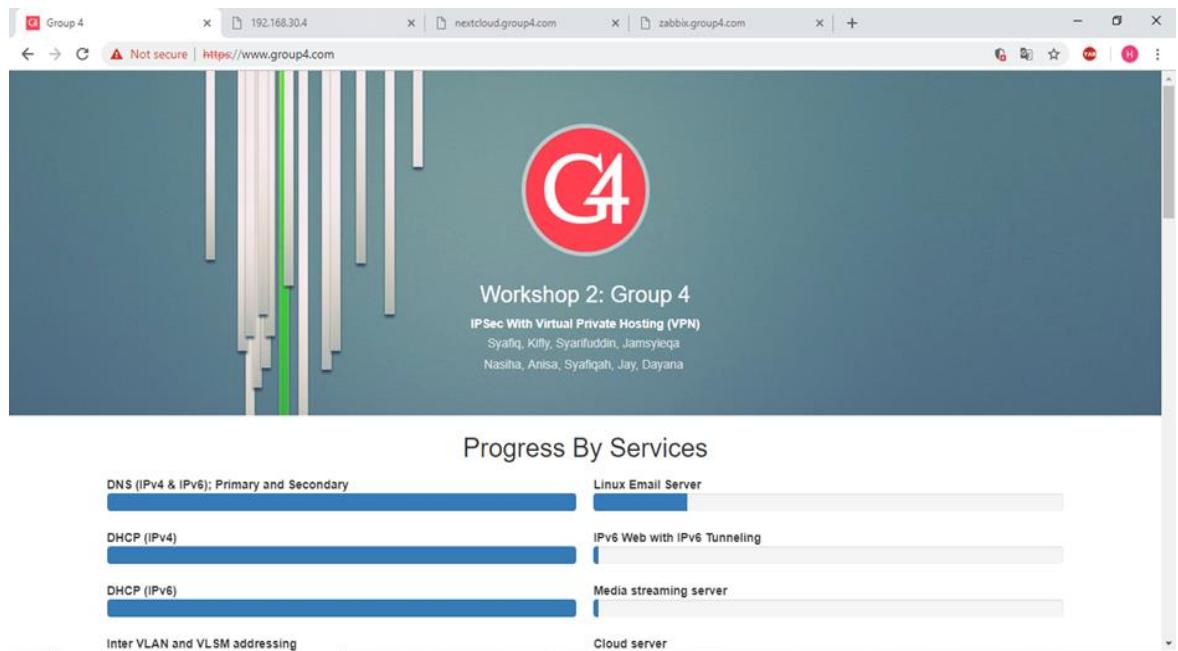


Figure 487: Display on other group browser.

Step 5: Our ACL will block Samba in local area network to access outside network.

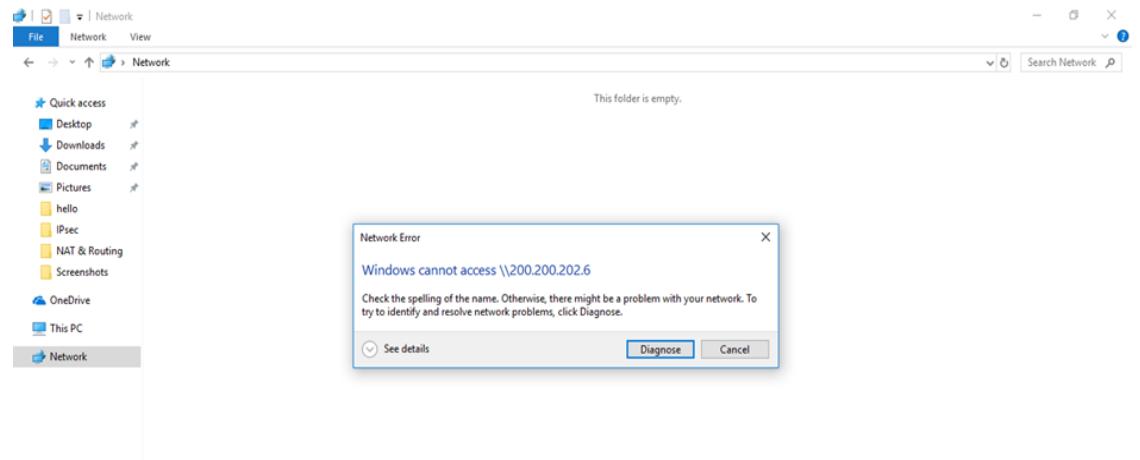


Figure 488: Folder Samba can't be access

Step 6: Our ACL will block the SSH in local area network to access outside network.

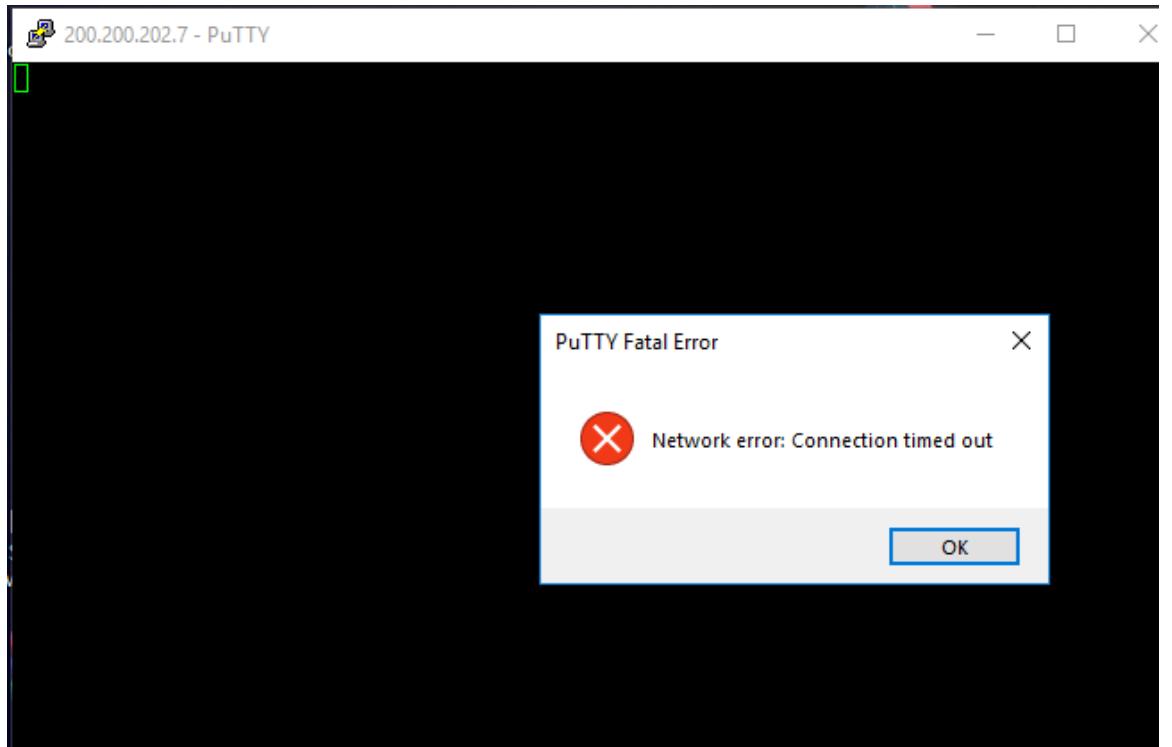
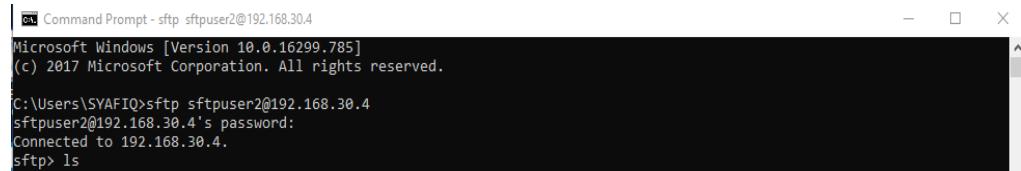


Figure 489: Samba can't be access

6.2.15 Secured FTP

Step 1: Open command prompt and insert command to access secure ftp.

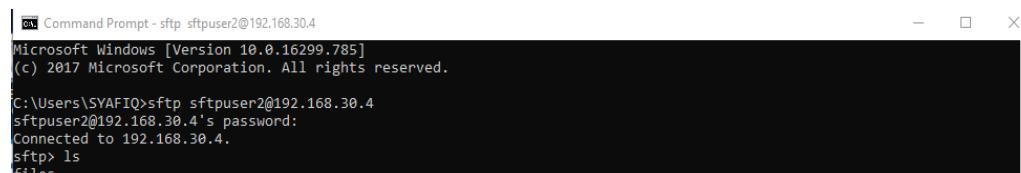


```
Command Prompt - sftp sftpuser2@192.168.30.4
Microsoft Windows [Version 10.0.16299.785]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\SYAFIQ>sftp sftpuser2@192.168.30.4
sftpuser2@192.168.30.4's password:
Connected to 192.168.30.4.
sftp> ls
```

Figure 490: Command for access “sftp sftpuser2@192.168.30.4”

Step 2: Check secure ftp for make sure that only have files that only user can access.

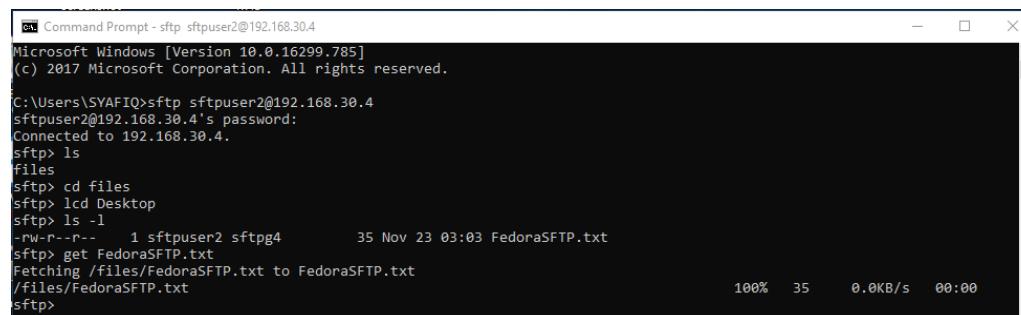


```
Command Prompt - sftp sftpuser2@192.168.30.4
Microsoft Windows [Version 10.0.16299.785]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\SYAFIQ>sftp sftpuser2@192.168.30.4
sftpuser2@192.168.30.4's password:
Connected to 192.168.30.4.
sftp> ls
files
```

Figure 491: List only one folder that name files

Step 3: Change directory from folder to files while get access desktop client and take file.txt at client.



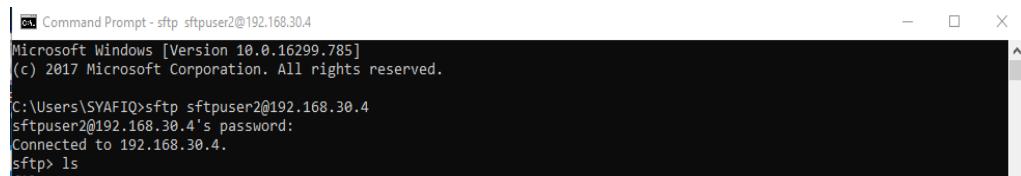
```
Command Prompt - sftp sftpuser2@192.168.30.4
Microsoft Windows [Version 10.0.16299.785]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\SYAFIQ>sftp sftpuser2@192.168.30.4
sftpuser2@192.168.30.4's password:
Connected to 192.168.30.4.
sftp> ls
files
sftp> cd files
sftp> lcd Desktop
sftp> ls -l
-rw-r--r-- 1 sftpuser2 sftpg4          35 Nov 23 03:03 FedoraSFTP.txt
sftp> get FedoraSFTP.txt
Fetching /files/FedoraSFTP.txt to FedoraSFTP.txt
/Files/FedoraSFTP.txt
100%   35      0.0KB/s  00:00
sftp>
```

Figure 492: Get File FedoraSFTP.txt

Testing upload Files from Fedora Server to Windows Client

Step 1: Open command prompt and insert command to access secure ftp.

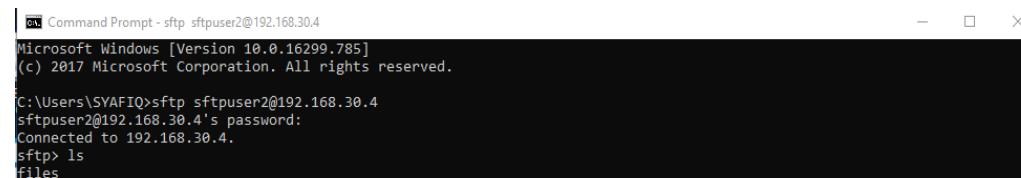


```
Command Prompt - sftp sftpuser2@192.168.30.4
Microsoft Windows [Version 10.0.16299.785]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\SYAFIQ>sftp sftpuser2@192.168.30.4
sftpuser2@192.168.30.4's password:
Connected to 192.168.30.4.
sftp> ls
```

Figure 493: Command for access “[sftp sftpuser2@192.168.30.4](#)”

Step 2: Check secure ftp for make sure that only have files that only user can access.



```
Command Prompt - sftp sftpuser2@192.168.30.4
Microsoft Windows [Version 10.0.16299.785]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\SYAFIQ>sftp sftpuser2@192.168.30.4
sftpuser2@192.168.30.4's password:
Connected to 192.168.30.4.
sftp> ls
files
```

Figure 494: List only one folder that name files

Step 3: Change directory from folder to files while get access desktop client and send file.txt at client.

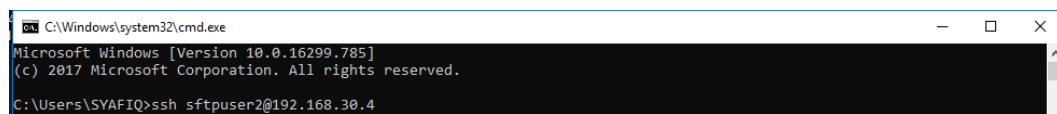


```
sftp> put ClientSFTP.txt
Uploading ClientSFTP.txt to /files/ClientSFTP.txt
ClientSFTP.txt                                         100%   21      0.0KB/s  00:00
sftp>
```

Figure 495: Send file [FedoraSFTP.txt](#)

Test to access SSH using secure FTP User account

Step 1: Open command prompt and insert command to access SSH.

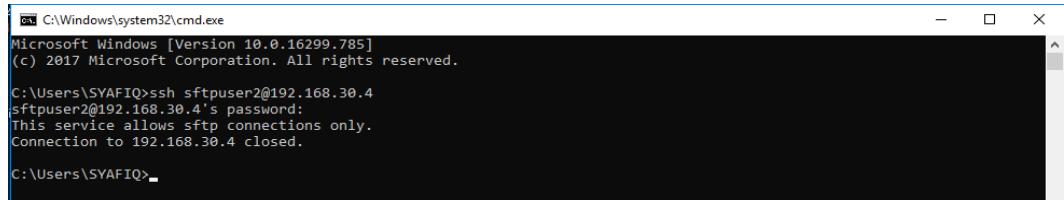


```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.16299.785]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\SYAFIQ>ssh sftpuser2@192.168.30.4
```

Figure 496: Command for access “[ssh sftpuser2@192.168.30.4](#)”

Step 2: When access SSH using Secure ftp account the access will block by secure ftp because this account can't access SSH because don't have permission.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.16299.785]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\SYAFIQ>ssh sftpuser2@192.168.30.4
sftpuser2@192.168.30.4's password:
This service allows sftp connections only.
Connection to 192.168.30.4 closed.

C:\Users\SYAFIQ>
```

Figure 497: Close the connection SSH for secure ftp user

Test to Access secure FTP by FileZilla at Client

Step 1: Using FileZilla Client software and connect to group4 network.

Step 2: Put in the hostname: 192.168.30.4 (IP vsftpd server)

Step 3: Put in username: sftpuser2

Step 4: Key in password

Step 5: Click connect

Step 6: Successful connected

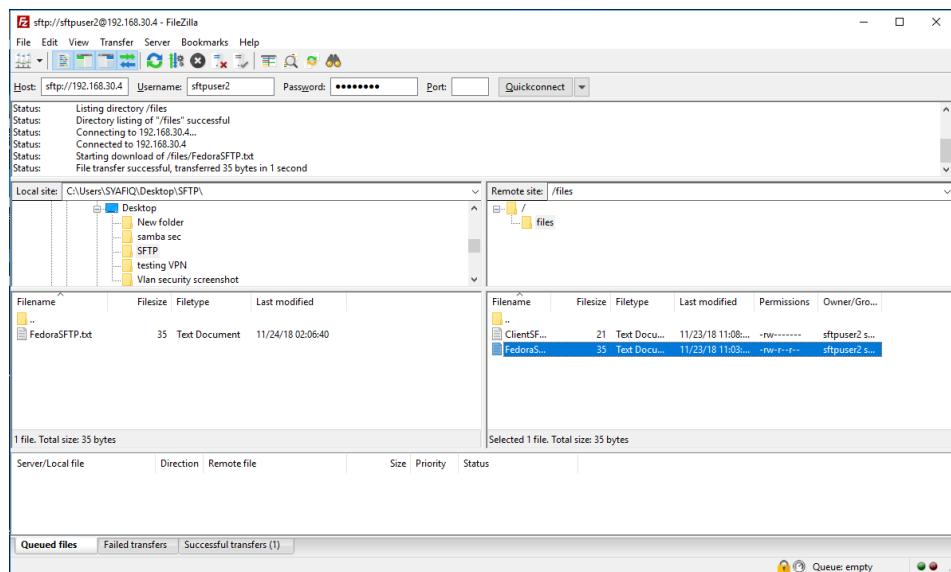


Figure 498: FileZilla Client software and connect to group4 network

6.2.16 Web, SSL & Virtual Hosting

Browse <http://www.group4.com>

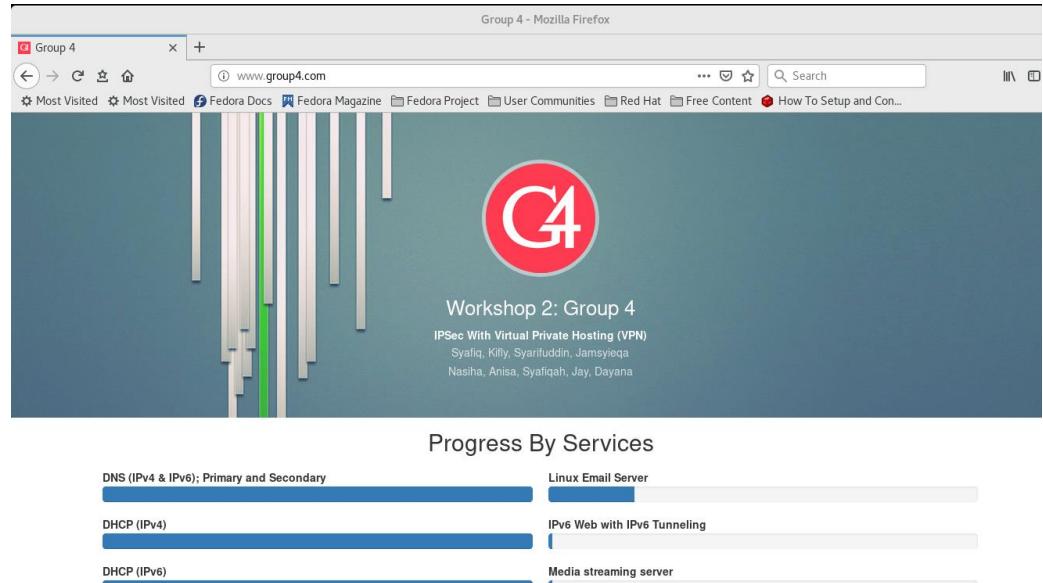


Figure 499: Web browser

Browse <https://www.group4.com> as secure browser.



Figure 500: SSL secure browser

Browse <http://www.group4virtualweb.com>

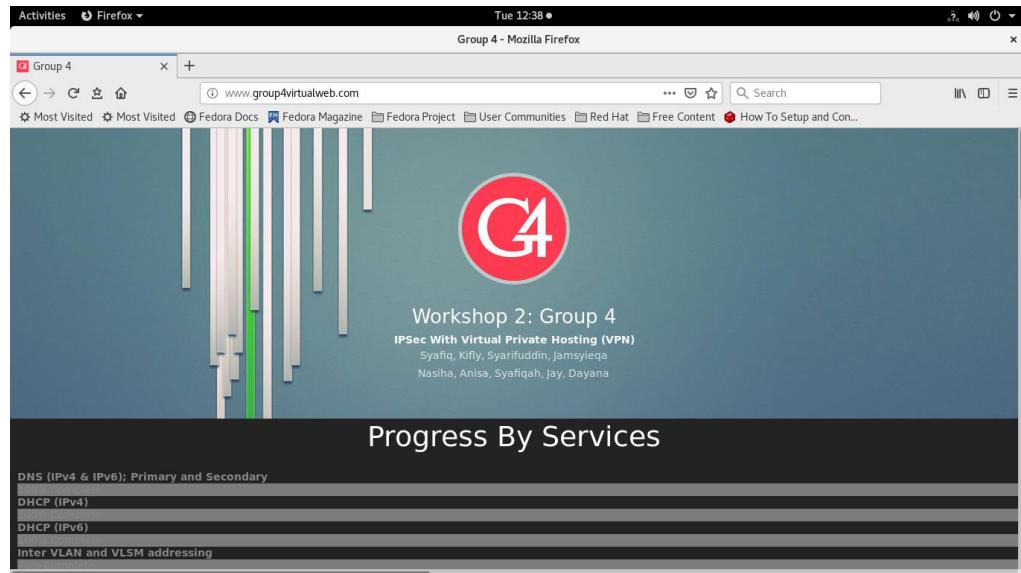


Figure 501: Virtual hosting browser

6.2.17 Linux Email Server

Step 1: Open browser and open following url

'<http://mail.group4.com/?admin>'. Login as **admin** and default password is **12345**.

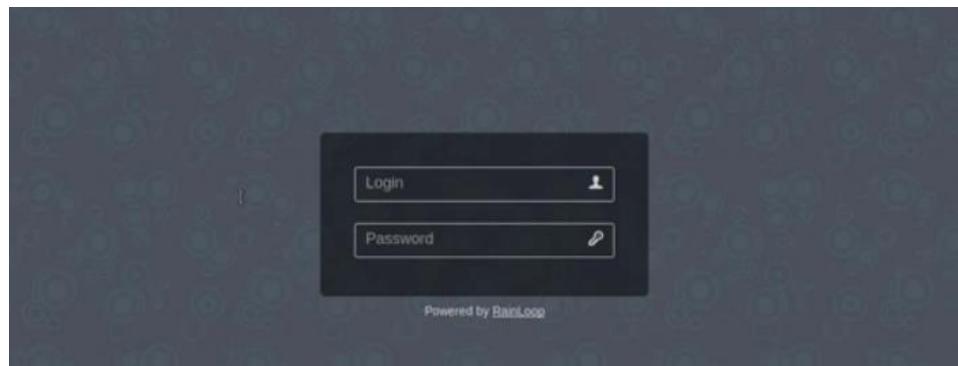


Figure 502: user login and password

Step 2: Next, change the password. Tick ‘Allow 2-step Verification’ and ‘Enforce 2-Step Verification’. Then, update password.

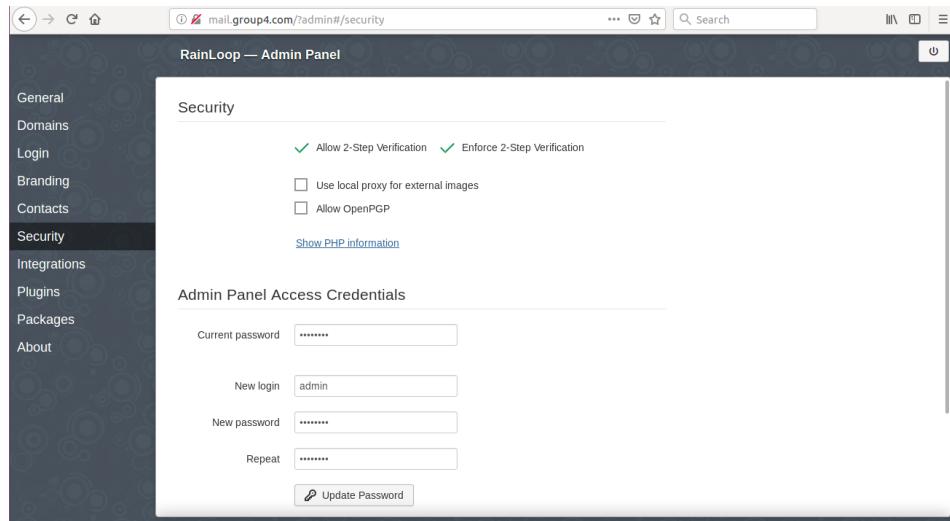


Figure 503: change and update password

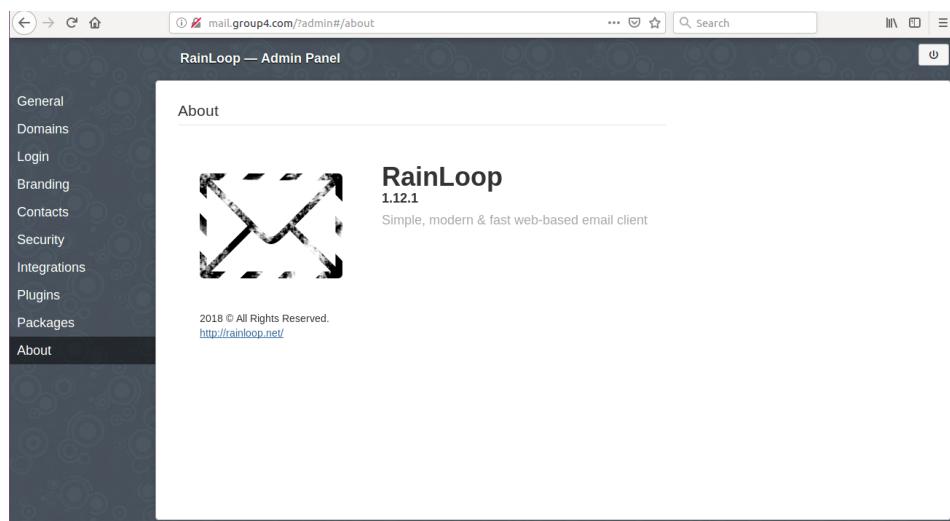


Figure 504: Rainloop – Admin Panel

Step 3: Send email to other user by clicking new. Email send to puteri@group4.com

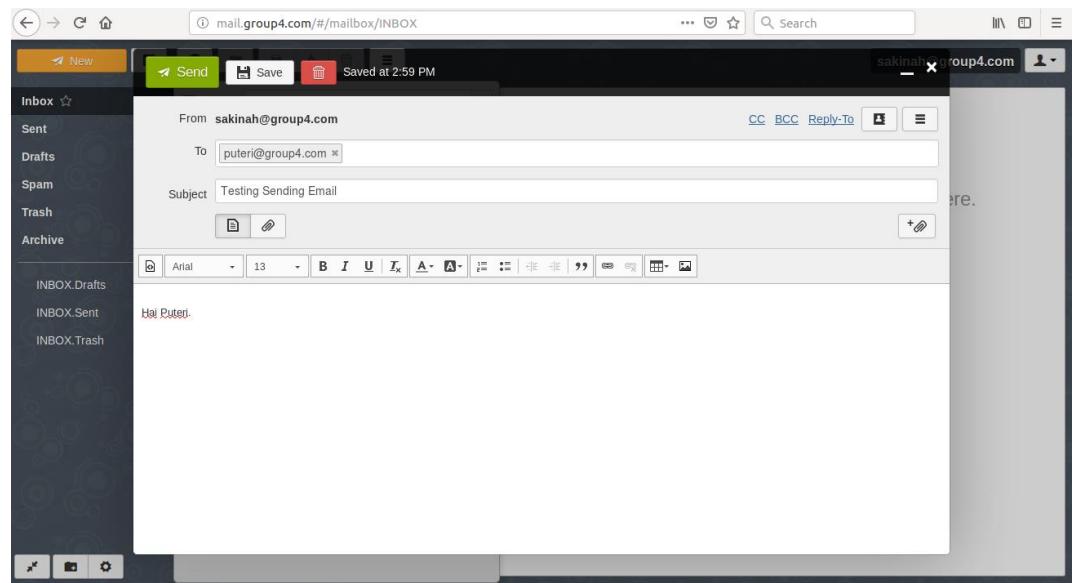


Figure 505: Send email to user

Step 4: Open new email using other user.

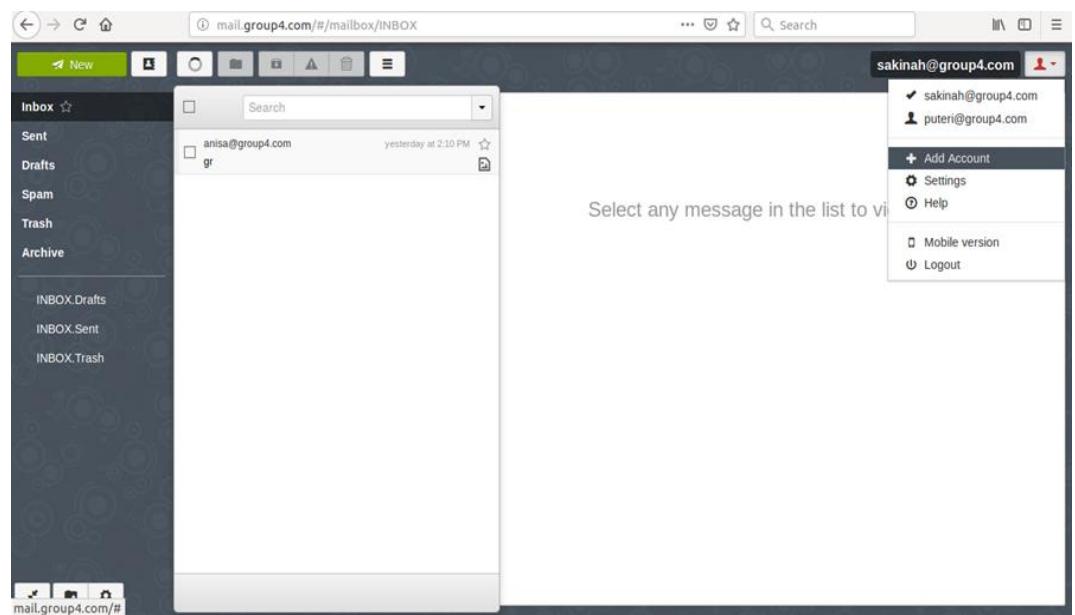


Figure 506: Add user account

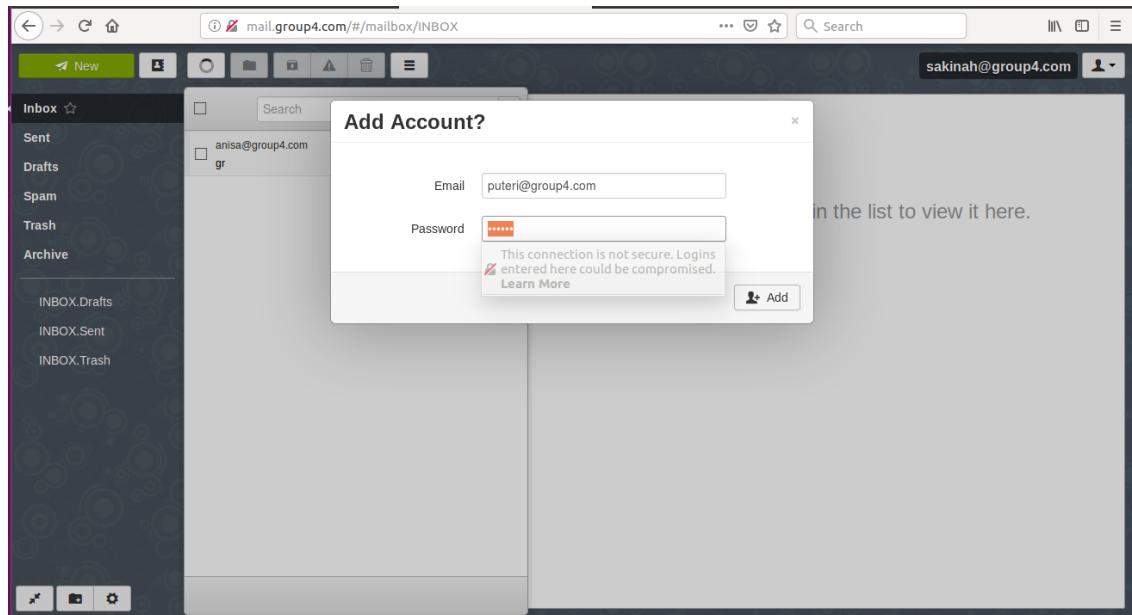


Figure 507: Add account by adding email and password

Step 4: Email successfully receive from sakinah@group4.com

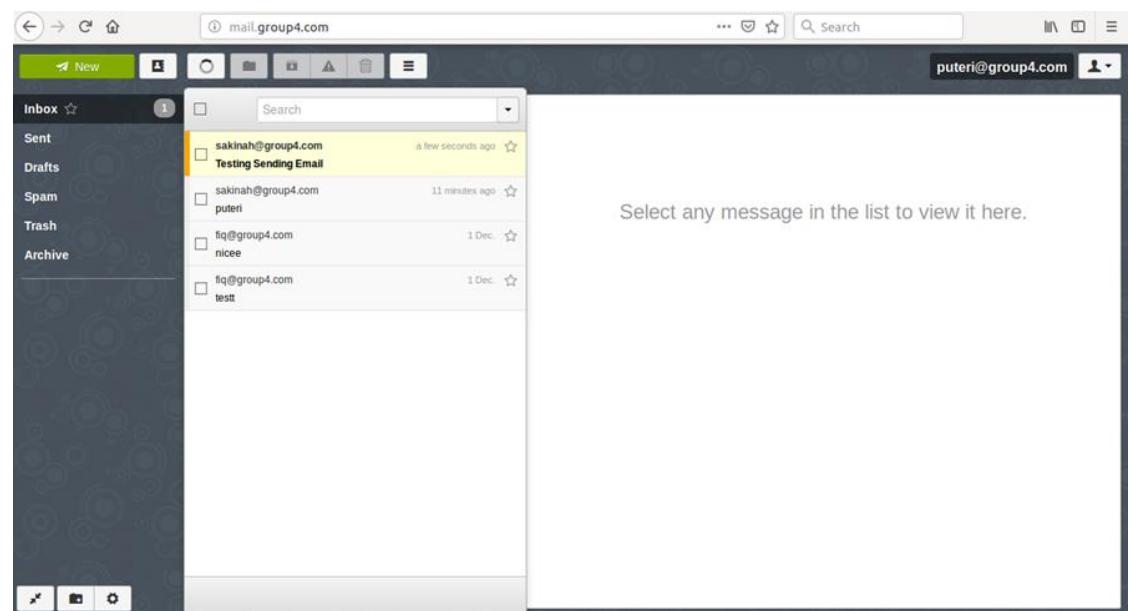


Figure 508: Successfully received email

6.2.18 IPv6 Web with IPv6 Tunnelling

IPv6 Web Testing

The website <http://www.group4ipv6.com> and [http://\[2004:db8:4444:f010::3\]](http://[2004:db8:4444:f010::3]) was tested successfully on three servers which is Fedora, Windows Server, Ubuntu and client.

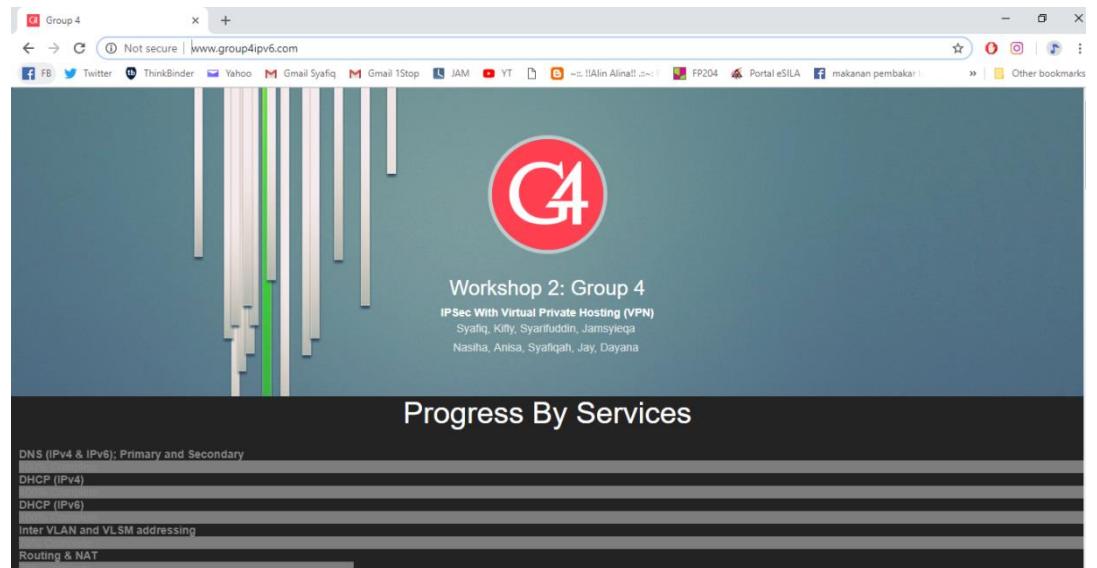


Figure 509: Web testing using domain name

IPv6 Tunneling Testing

Type the neighbor's website which is <http://www.ipv6web.group3.com> in the web browser. The group 3 website already popup in the browser after insert the website URL and the tunneling process is successfully completed.

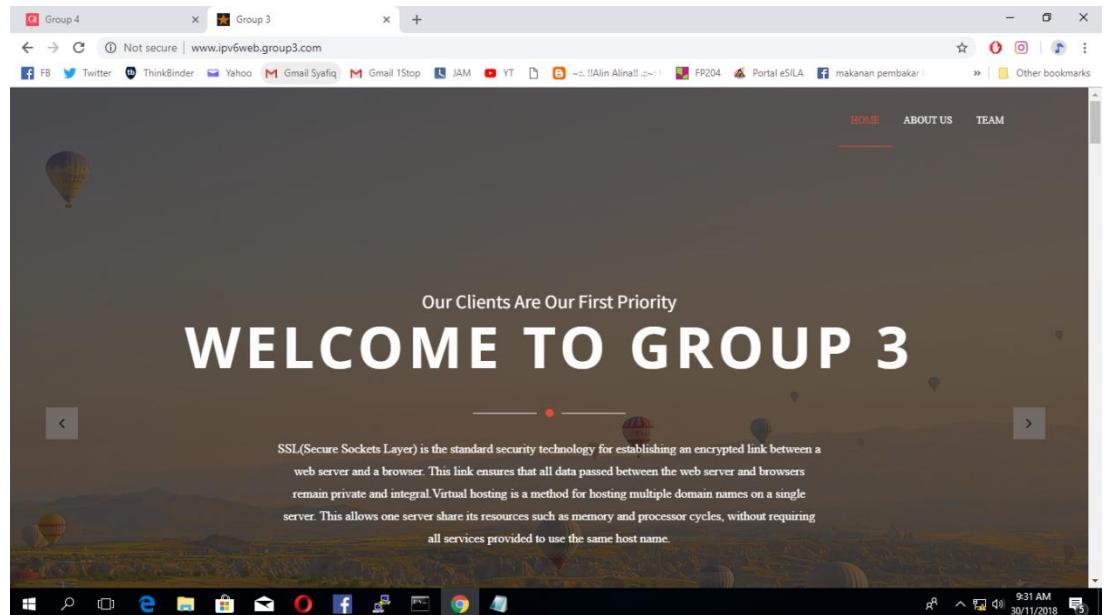


Figure 510: Group 3 access website

6.2.19 Media Streaming Server

Step 1: Before configuring the Plex media server, make sure we have an account for Plex and then login to our account. If we're a registered user and logged in with our browser, we can open our Plex media server installation url in the following way, which is <http://192.168.30.4:32400/web/> and we will be redirected to the Plex login as below. Then, click the ‘SIGN IN’ button.

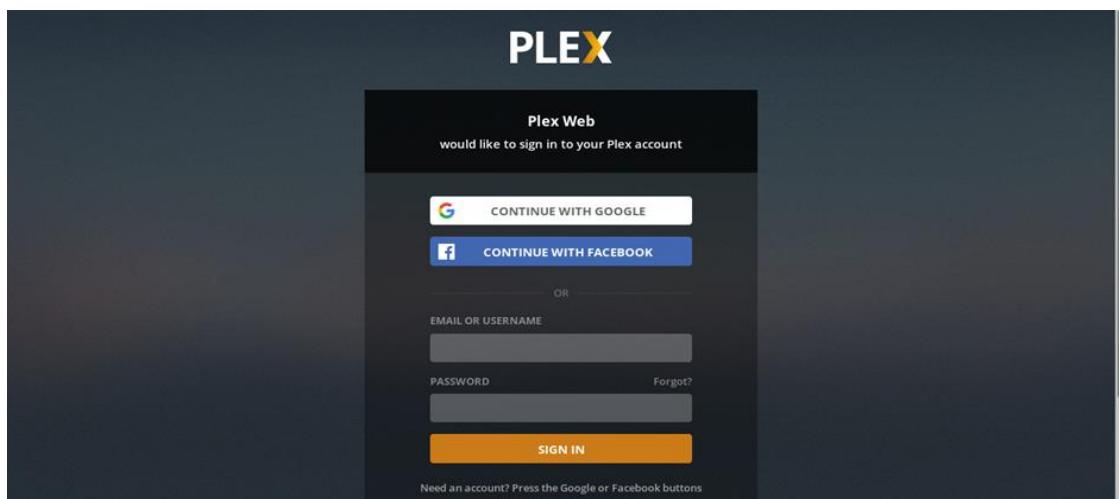


Figure 511: Plex Web

Step 2: Now, we can add media files to our Plex media server. Click ‘Add library’.

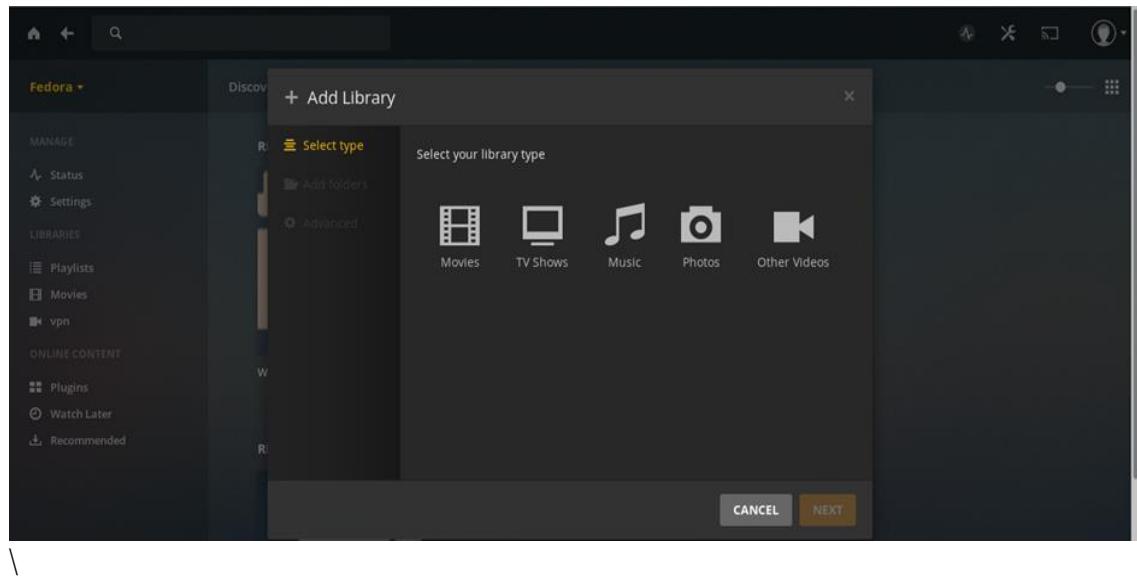


Figure 512: Add library for add media files

Step 3: Choose media that want to upload and click “Next”

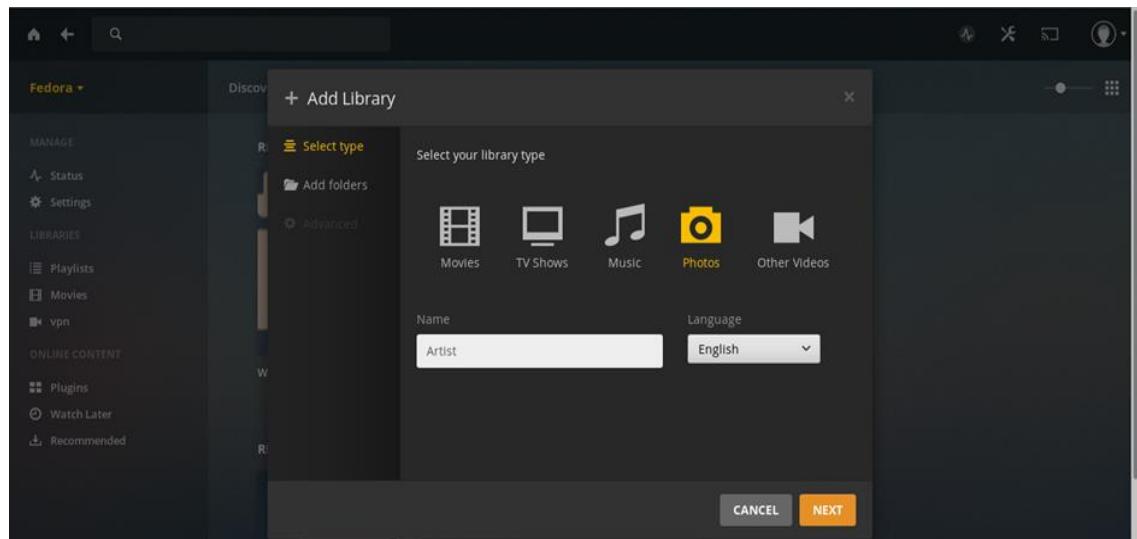


Figure 513: Choose media to upload

Step 4: Click “*Browse for Media Folder*”

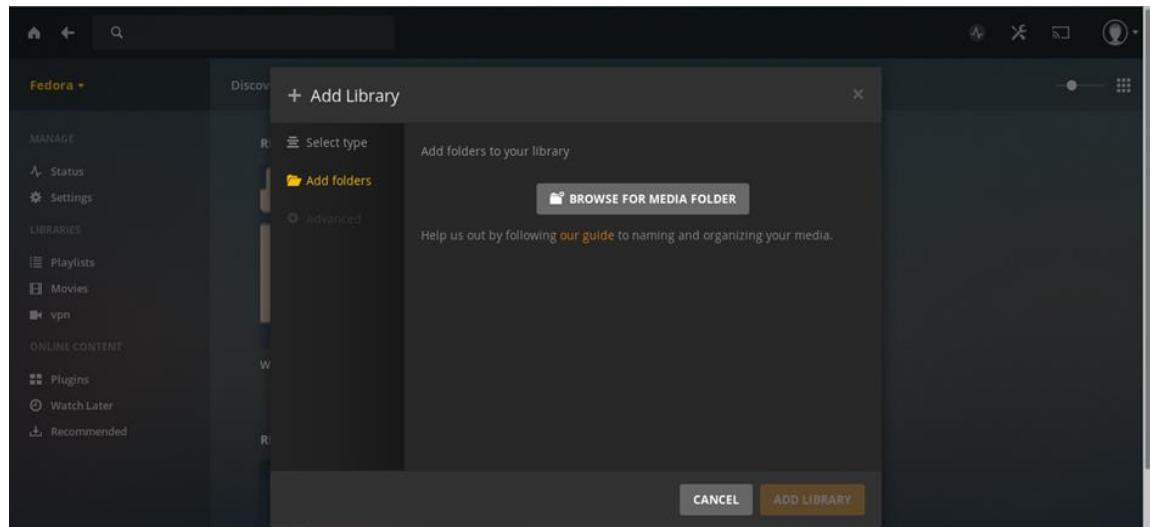


Figure 514: Browse media folder

Step 5: Choose the media and click “*Add*”

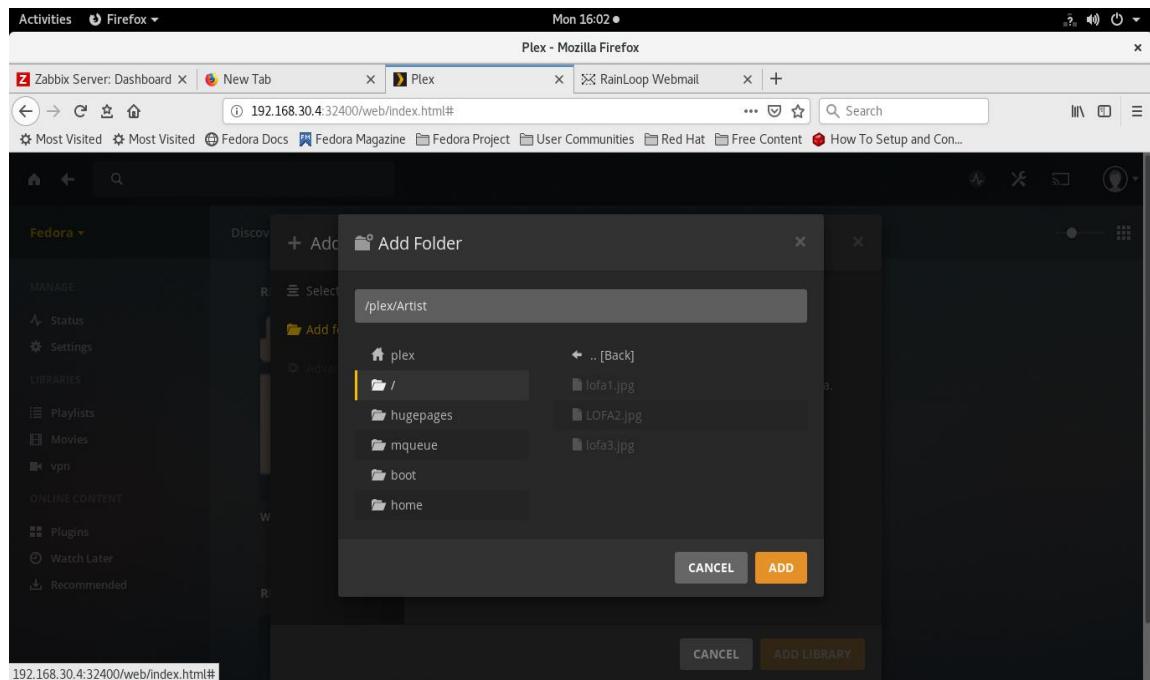


Figure 515: Add the media

Step 6: Last step click “*Add Library*”

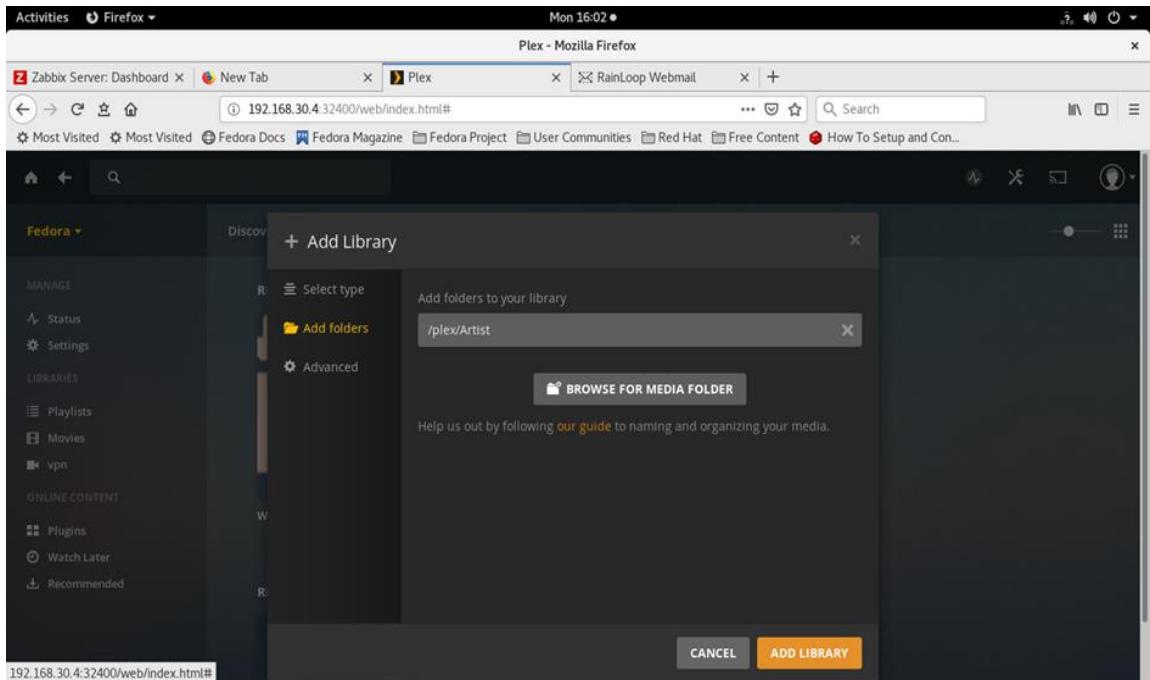


Figure 516: Add Library

Step 7: Photo successfully uploaded.

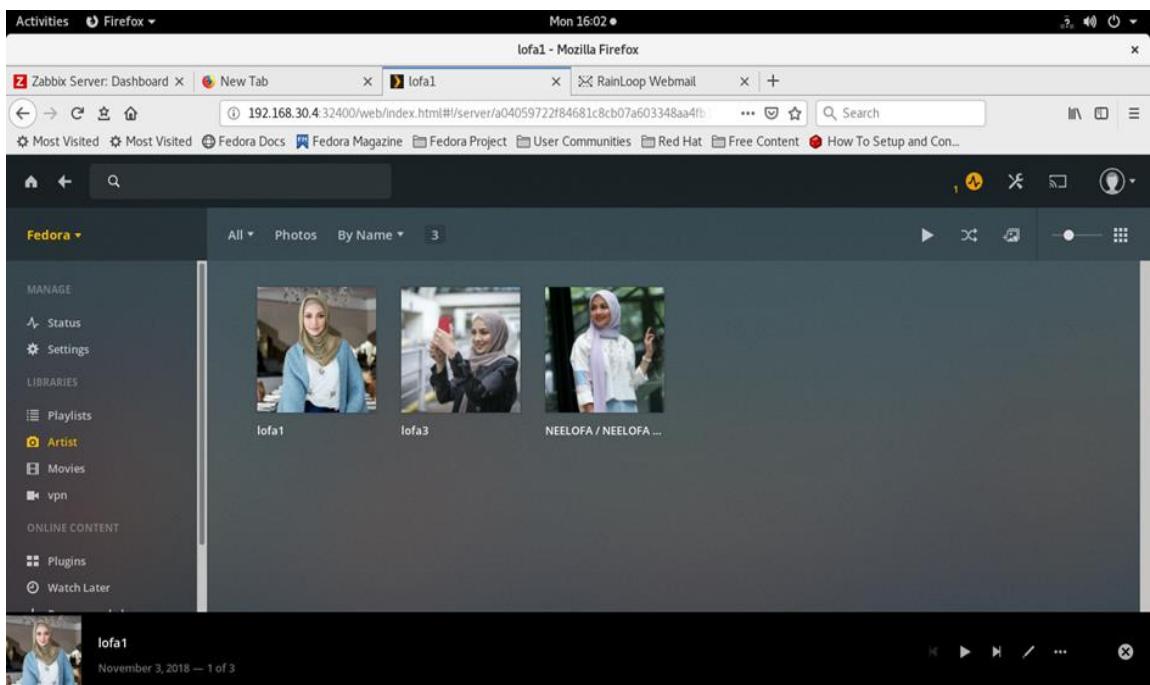


Figure 517: Successfully photo uploaded

6.2.20 Cloud Server

Step 1: Access NextCloud via nextcloud.group4.com

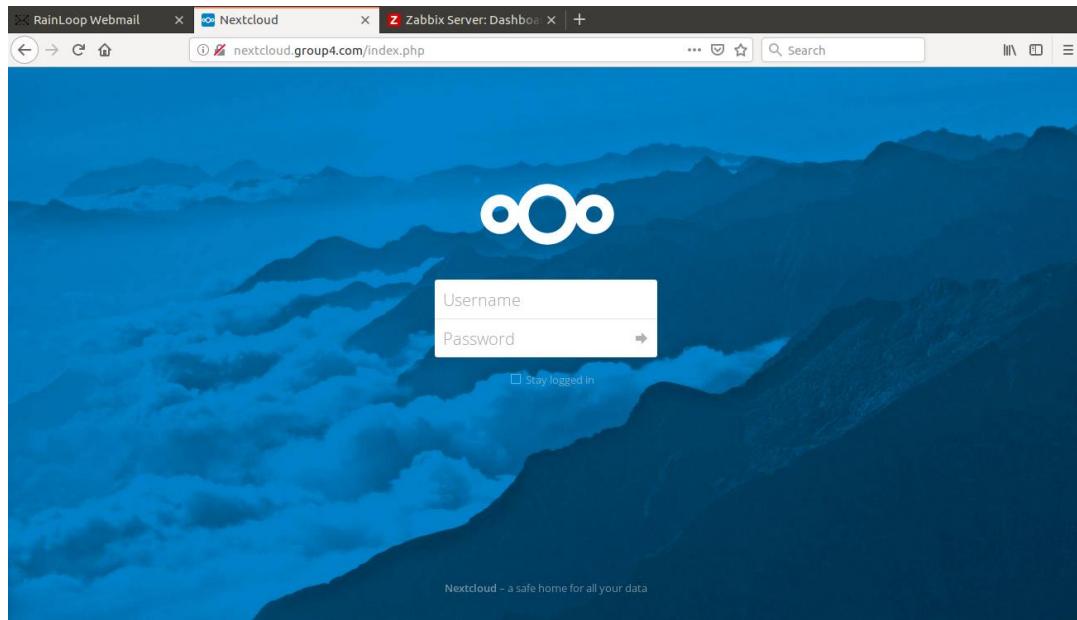


Figure 518: Login to NextCloud

Step 2: Login using previously created user and a Home page will be displayed.

	Name	Size	Modified
📁	Anime	1.9 GB	a month ago
📁	Documents	1.1 MB	a month ago
📁	g4www	7 MB	a month ago
📁	ipsec vpn	1.5 MB	12 days ago
📁	Photos	663 KB	2 months ago
📁	poster dinna	84 KB	12 days ago
📁	Poster IPSEC VPN	1.2 MB	10 days ago
📁	syafiq	38.9 MB	a month ago

Figure 519: Homepage upon login success

Step 3: Access from another host in the network.

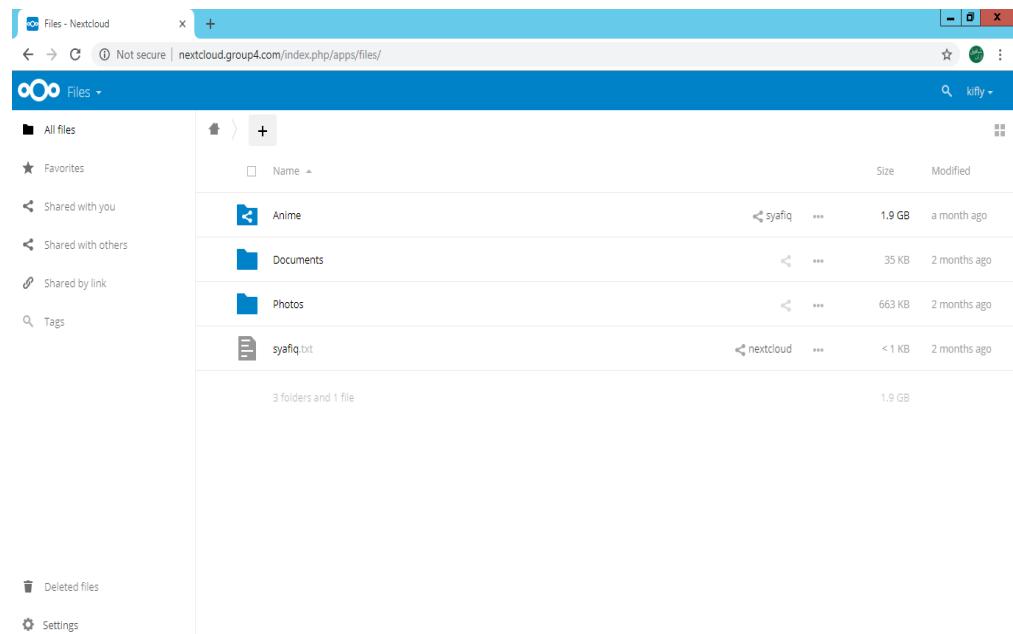


Figure 520: Access NextCloud from Windows Server

Step 4: Play/view/download any content over NextCloud.

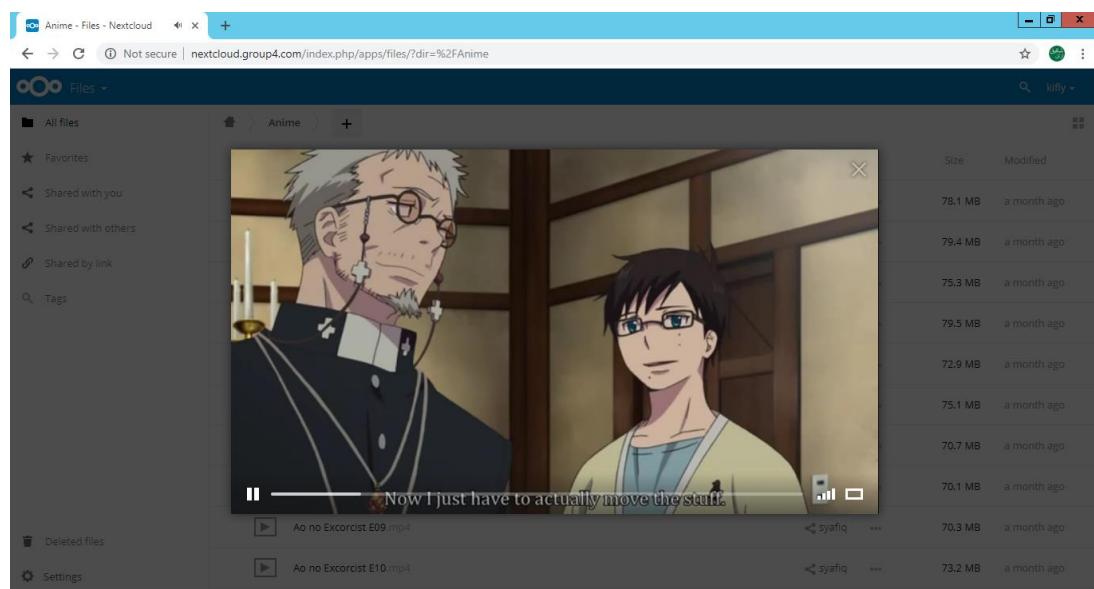


Figure 521: Test to access the content

6.2.21 Remote Login using SSH

Testing SSH in Fedora

Step 1 : Start the SSH service if it is not started.

```
g4-16@Ubuntu:~$ sudo systemctl start ssh
```

Figure 522: Start SSH

Step 2 : Login to Fedora from Ubuntu and create the file.

```
g4-16@Ubuntu:~$ ssh g4-15@192.168.30.4
g4-15@192.168.30.4's password:
Last login: Mon Oct 15 14:31:25 2018 from 192.168.50.4
[g4-15@Fedora ~]$ ls
Desktop      jcameron-key.asc  Public      webmin-current.rpm
Documents    Music            Templates   webmin-current.rpm.1
Downloads   Pictures         Videos     webmin-current.rpm.2
[g4-15@Fedora ~]$ cd Documents/
[g4-15@Fedora Documents]$ mkdir syaf
[g4-15@Fedora Documents]$ cd syaf/
[g4-15@Fedora syaf]$ touch syaf.txt
[g4-15@Fedora syaf]$ ls -la
total 8
drwxrwxr-x. 2 g4-15 g4-15 4096 Oct 15 14:43 .
drwxr-xr-x. 3 g4-15 g4-15 4096 Oct 15 14:43 ..
-rw-rw-r--. 1 g4-15 g4-15     0 Oct 15 14:43 syaf.txt
[g4-15@Fedora syaf]$
```

Figure 523: Login and create files

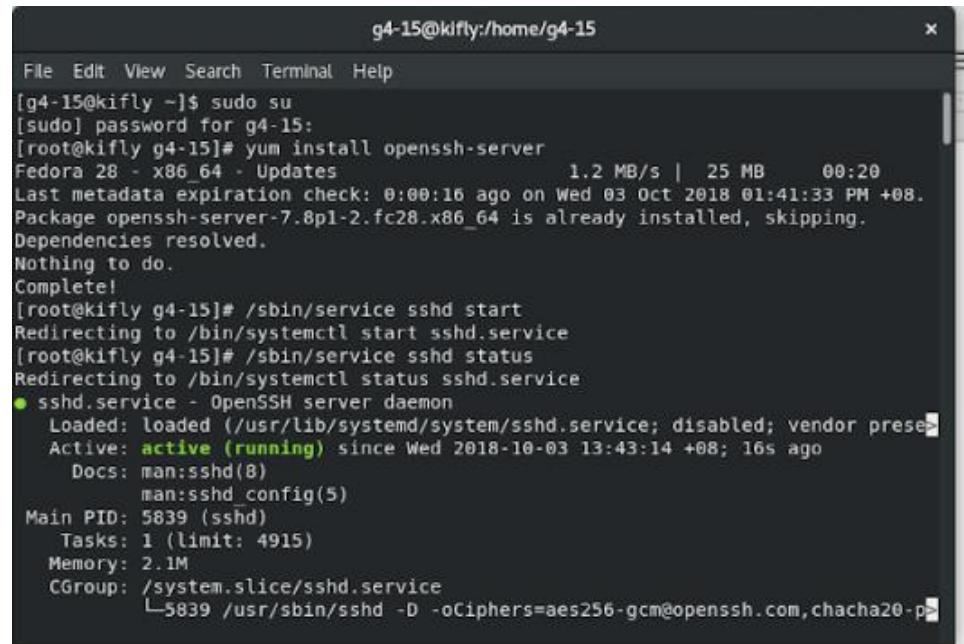
Step 3 : Check at Fedora whether the file that has been created exist or not.



Figure 524: Check file at Fedora

Testing SSH at Fedora

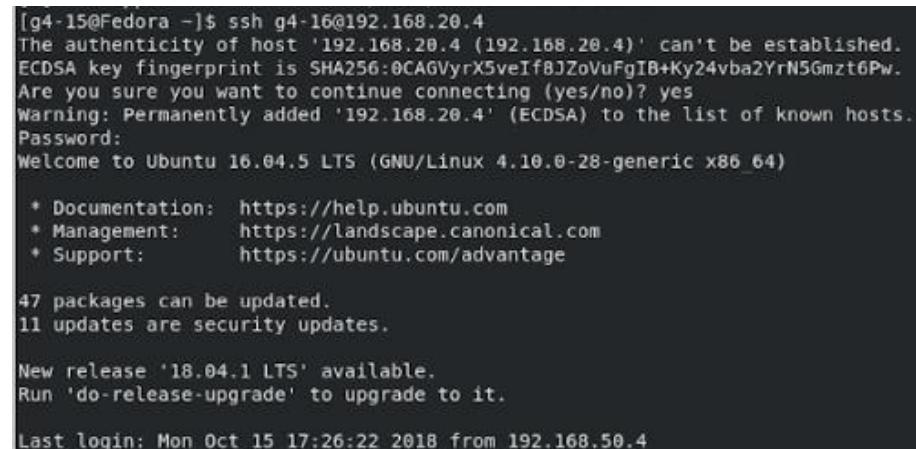
Step 1 : Start SSH at Fedora and check the status.



```
g4-15@kifly:/home/g4-15
File Edit View Search Terminal Help
[g4-15@kifly ~]$ sudo su
[sudo] password for g4-15:
[root@kifly g4-15]# yum install openssh-server
Fedora 28 - x86_64 - Updates           1.2 MB/s | 25 MB   00:20
Last metadata expiration check: 0:00:16 ago on Wed 03 Oct 2018 01:41:33 PM +08.
Package openssh-server-7.8p1-2.fc28.x86_64 is already installed, skipping.
Dependencies resolved.
Nothing to do.
Complete!
[root@kifly g4-15]# /sbin/service sshd start
Redirecting to /bin/systemctl start sshd.service
[root@kifly g4-15]# /sbin/service sshd status
Redirecting to /bin/systemctl status sshd.service
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; disabled; vendor prese>
   Active: active (running) since Wed 2018-10-03 13:43:14 +08; 16s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 5839 (sshd)
      Tasks: 1 (limit: 4915)
     Memory: 2.1M
    CGroup: /system.slice/sshd.service
           └─5839 /usr/sbin/sshd -D -oCiphers=aes256-gcm@openssh.com,chacha20-p>
```

Figure 525: start and check status SSH

Step 2 : Log in to Ubuntu from Fedora.



```
[g4-15@Fedora ~]$ ssh g4-16@192.168.20.4
The authenticity of host '192.168.20.4 (192.168.20.4)' can't be established.
ECDSA key fingerprint is SHA256:0CAGVyrX5veIf8JZoVuFgIB+Ky24vba2YrN5Gmzt6Pw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.20.4' (ECDSA) to the list of known hosts.
Password:
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.10.0-28-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

47 packages can be updated.
11 updates are security updates.

New release '18.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Mon Oct 15 17:26:22 2018 from 192.168.50.4
```

Figure 526: Login Ubuntu from Fedora

Step 3 Create the file at Ubuntu from Fedora.

```
g4-16@Ubuntu:~$ cd Desktop  
g4-16@Ubuntu:~/Desktop$ mkdir group4  
g4-16@Ubuntu:~/Desktop$ touch group4.txt  
g4-16@Ubuntu:~/Desktop$
```

Figure 527: Create Ubuntu file from Fedora

Step 4 : Check whether the file exist or not at the Desktop.

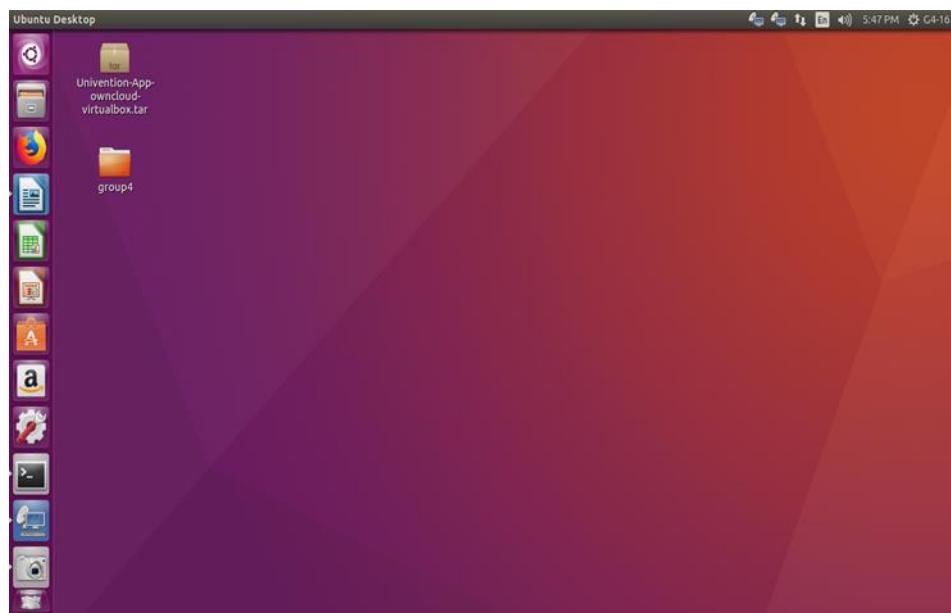


Figure 528: Check existing file at Desktop

6.2.22 IDS with Port Mirror

Step 1: Display monitor session interface.

```
Switch#  
Switch#show monitor session 1  
Session 1  
-----  
Type : Local Session  
Source Ports :  
    Both : Fa0/22  
Destination Ports : Fa0/5  
    Encapsulation : Native  
        Ingress: Disabled
```

Figure 529: Monitor session interface

Step 2: Type “ snort -c /etc/snort/snort.conf -K ascii ” to start IDS.

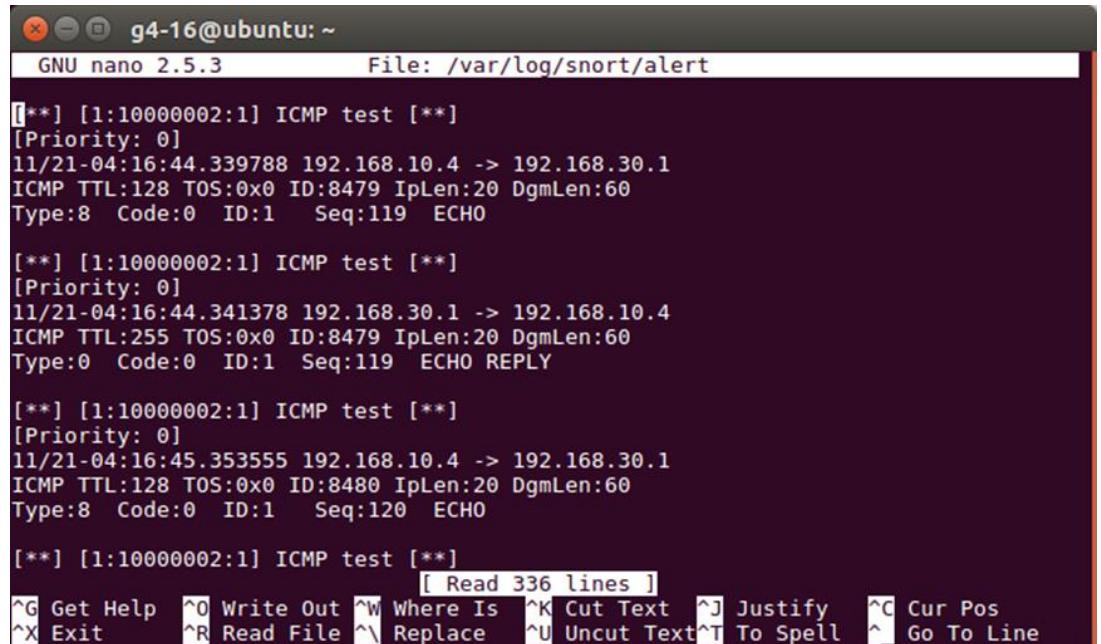
```
---- Initialization Complete ----

      -*> Snort! <-
o" ,,-)~ 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 reserv
ed.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.7.4
Using PCRE version: 8.41 2017-07-05
Using ZLIB version: 1.2.8

Commencing packet processing (pid=32313)
12/01-19:29:47.506339 192.168.20.4:80 -> 192.168.30.4:51174
```

Figure 530: Command to start the IDS

Step 3: Ping from any host from HOME_NET to other host from HOME_NET



```
g4-16@ubuntu: ~
GNU nano 2.5.3          File: /var/log/snort/alert

[**] [1:10000002:1] ICMP test [**]
[Priority: 0]
11/21-04:16:44.339788 192.168.10.4 -> 192.168.30.1
ICMP TTL:128 TOS:0x0 ID:8479 IpLen:20 DgmLen:60
Type:8 Code:0 ID:1 Seq:119 ECHO

[**] [1:10000002:1] ICMP test [**]
[Priority: 0]
11/21-04:16:44.341378 192.168.30.1 -> 192.168.10.4
ICMP TTL:255 TOS:0x0 ID:8479 IpLen:20 DgmLen:60
Type:0 Code:0 ID:1 Seq:119 ECHO REPLY

[**] [1:10000002:1] ICMP test [**]
[Priority: 0]
11/21-04:16:45.353555 192.168.10.4 -> 192.168.30.1
ICMP TTL:128 TOS:0x0 ID:8480 IpLen:20 DgmLen:60
Type:8 Code:0 ID:1 Seq:120 ECHO

[**] [1:10000002:1] ICMP test [**]
[ Read 336 lines ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit    ^R Read File ^\ Replace   ^U Uncut Text ^T To Spell ^_ Go To Line
```

Figure 531: ping from HOME_NET to other host

6.2.23 IPsec VPN for Remote Employees

Step 1: Add VPN on PC Client using IP of Softether server PC as server address and type correct username and password.

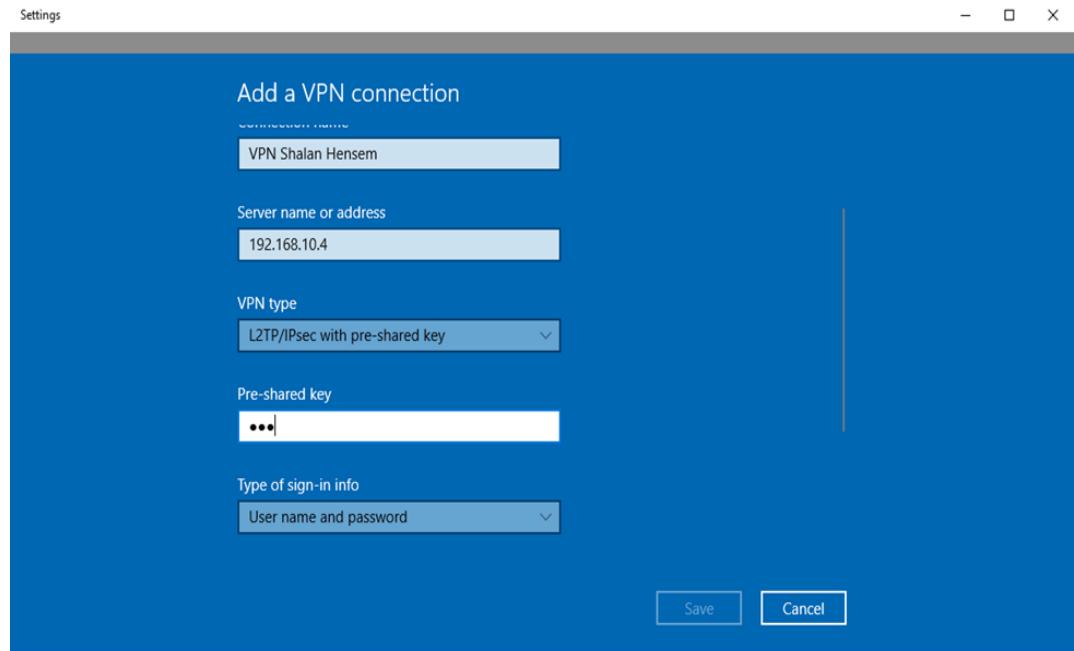


Figure 532: type correct information to add VPN on PC client

The screenshot shows a configuration dialog box for a VPN connection. The fields filled in are:

- IP address: 200.200.202.4
- VPN type: L2TP/IPsec with pre-shared key
- Pre-shared key: (redacted)
- Type of sign-in info: User name and password
- User name (optional): minthe
- Password (optional): (redacted)
- Remember my sign-in info

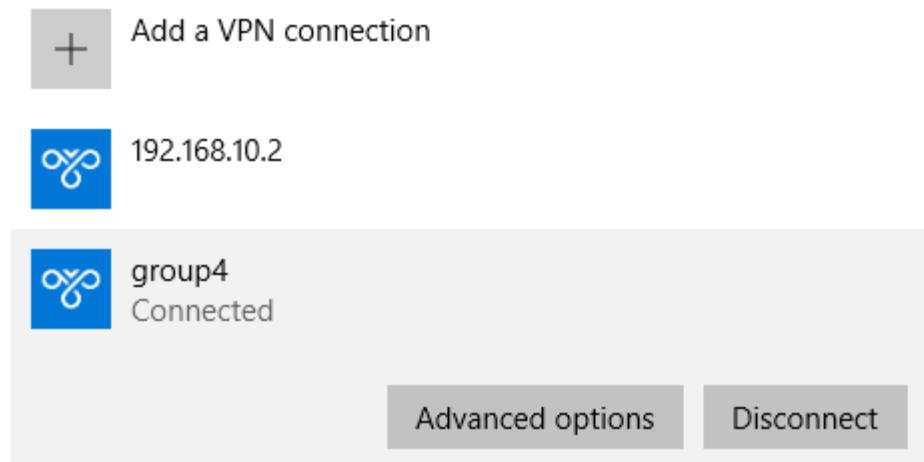
At the bottom right are two buttons: Save and Cancel.

Figure 533: Type correct information

Step 2: Verify that VPN is connected.

VPN

VPN



Advanced Options

Allow VPN over metered networks

On

Allow VPN while roaming

On

Figure 534: VPN is connected

Step 3: Check the connectivity in SoftEther Client Manager

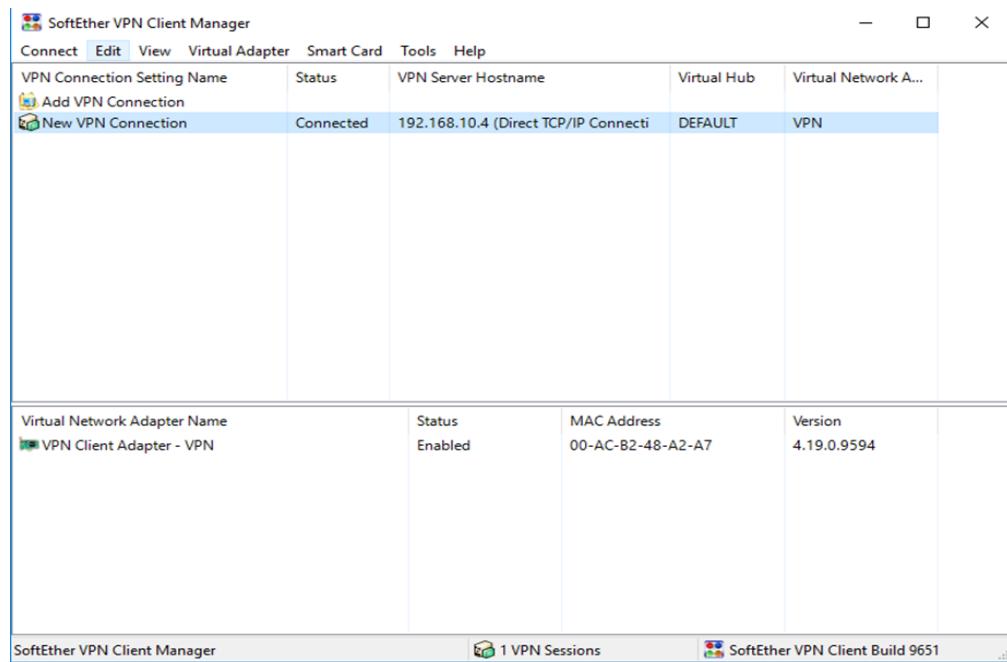


Figure 535: VPN in Client Manager Connected

6.2.24 Port Security

Step 1 : Check port security using command “sh port-security”.

```

g4switch#sh port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
          (Count)        (Count)        (Count)
-----
Fa0/2           2            0            0      Restrict
Fa0/3           2            0            0      Restrict
Fa0/4          10           2            0      Restrict
Fa0/5           1            1            0      Restrict
Fa0/6           1            0            0      Restrict
Fa0/7           1            0            0      Restrict
Fa0/8           1            1            0      Restrict
Fa0/9           1            0            0      Restrict
Fa0/10          1            0            0      Restrict
-----
Total Addresses in System (excluding one mac per port) : 1
Max Addresses limit in System (excluding one mac per port) : 8192
g4switch#wr
Building configuration...
[OK]
g4switch#

```

Figure 536: Check port-security status

6.2.25 VLAN Security

Step 1: Use command ‘sh int trunk’ to view trunk settings.

```
g4switch# sh int trunk

Port      Mode          Encapsulation  Status        Native vlan
Gi0/1    on           802.1q         trunking     3

Port      Vlans allowed on trunk
Gi0/1    1-4094

Port      Vlans allowed and active in management domain
Gi0/1    1,10,20,30,50-51

Port      Vlans in spanning tree forwarding state and not pruned
Gi0/1    1,10,20,30,50-51
```

Figure 537: Trunk setting in port

Step 2: Use command ‘sh run’ and check if commands about VLAN security already have been entered.

```
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
  switchport trunk native vlan 3
  switchport mode trunk
!
interface GigabitEthernet0/2
  switchport mode trunk
!
interface Vlan1
  no ip address
  no ip route-cache
!
interface Vlan10
  ip address 192.168.10.2 255.255.255.248
  no ip route-cache
!
interface Vlan20
  ip address 192.168.20.2 255.255.255.248
  no ip route-cache
!
interface Vlan30
  ip address 192.168.30.2 255.255.255.248
  no ip route-cache
!
interface Vlan50
  ip address 192.168.50.50 255.255.255.192
  no ip route-cache
!
interface Vlan51
  no ip address
  no ip route-cache
!
ip http server
ip http secure-server
snmp-server community group4 RO
```

Figure 538: Display sh run command

6.2.26 Router Hardening

Testing Log

Step 1: Go to PuTTY configuration and under the category > Session, select Logging. At Logging, click on Browse button to save log file.

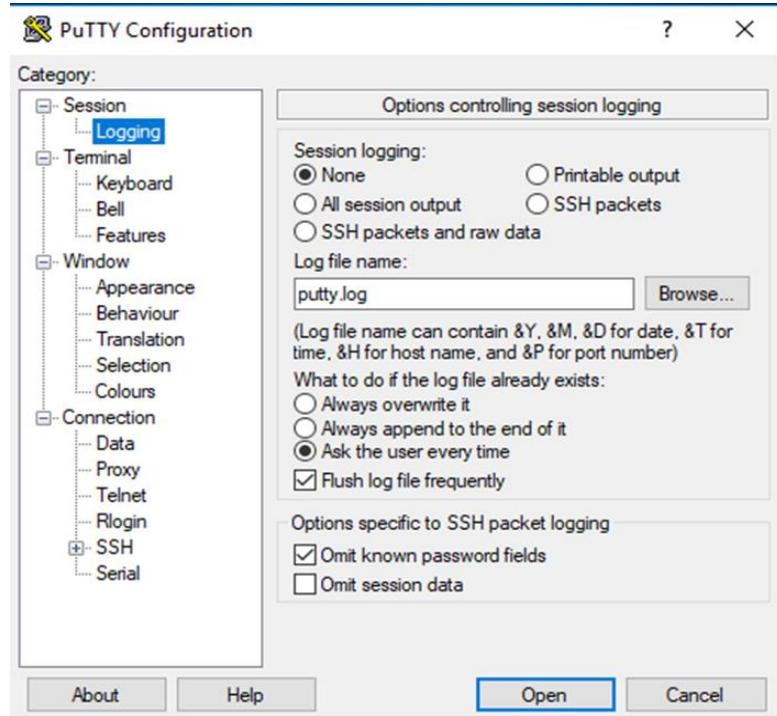


Figure 539: Options controlling session logging

Step 2: Type the log file name and save it.

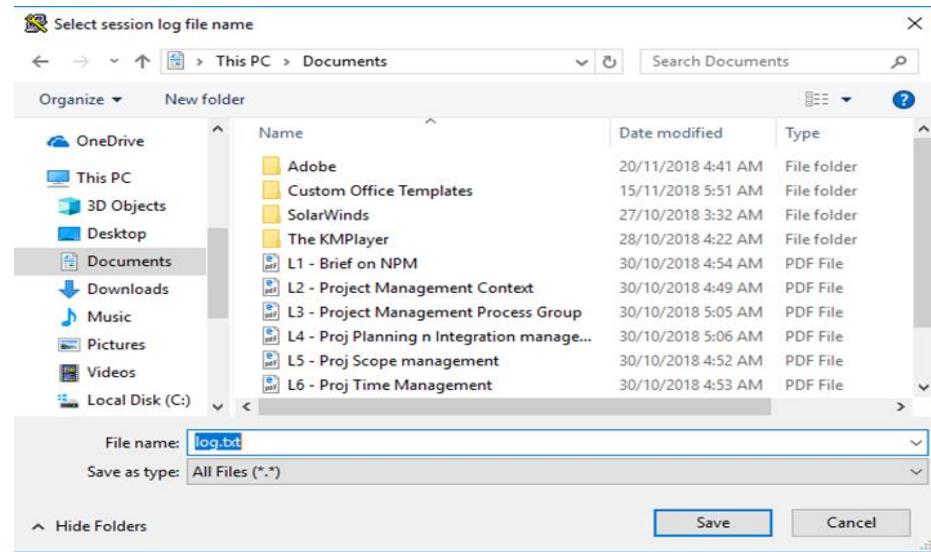


Figure 540: save log file name

Step 3: Then get into PuTTY and login to router. In the configuration, type something to create log file.

```
G4Router#  
G4Router#show log  
Syslog logging: enabled (11 messages dropped, 1 messages rate-limited,  
          0 flushes, 0 overruns, xml disabled, filtering disabled)  
  Console logging: level debugging, 30 messages logged, xml disabled,  
          filtering disabled  
  Monitor logging: level debugging, 0 messages logged, xml disabled,  
          filtering disabled  
  Buffer logging: disabled, xml disabled,  
          filtering disabled  
  Logging Exception size (4096 bytes)  
  Count and timestamp logging messages: disabled  
  
No active filter modules.  
  
  Trap logging: level informational, 34 message lines logged  
G4Router#
```

Figure 541: Create log file in router

Step 4: After log file created, exit configuration and go to location that save log file.

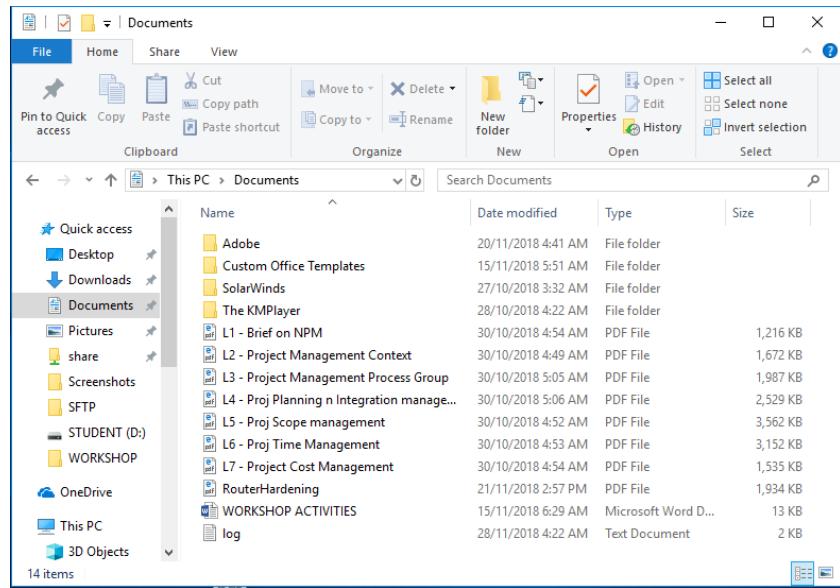


Figure 542: Location and save of log file

Step 5: Click the log file and it will show what we do just now in configuration.

```

log - Notepad
File Edit Format View Help
===== Putty log 2018.11.28 04:21:01 =====
login as: syafiq
syafiq@192.168.10.1's password:

$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
$ WELCOME TO WORKSHOP 2 $
$ GROUP 4 $

$ UNAUTHORIZED USER IS PROHIBITED $
$                               $
$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$

G4Router#
G4Router#
G4Router#conf t []
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
G4Router(config)#exit
G4Router#show log
Syslog logging: enabled (11 messages dropped, 1 messages rate-limited,
 0 flushes, 0 overruns, xml disabled, filtering disabled)
Console logging: disabled
Monitor logging: disabled
Buffer logging: disabled, xml disabled,
  filtering disabled
Logging Exception size (4096 bytes)
Count and timestamp logging messages: disabled

No active filter modules.

Trap logging: level informational, 39 message lines logged
G4Router#exit

```

Figure 543: Show the configuration of log file

6.2.27 Linux Server(Fedora) Hardening

Password Expiry

Previous

```
[root@Fedora ~]# chage -l group4
Last password change : Nov 13, 2018
Password expires      : never
Password inactive     : never
Account expires        : never
Minimum number of days between password change : 0
Maximum number of days between password change   : 99999
Number of days of warning before password expires : 7
```

Figure 544: Before change the password expiry

After

```
[root@Fedora ~]# chage -l group4
Last password change : Nov 13, 2018
Password expires      : Nov 27, 2018
Password inactive     : Dec 28, 2018
Account expires        : Oct 12, 2019
Minimum number of days between password change : 5
Maximum number of days between password change   : 14
Number of days of warning before password expires : 7
```

Figure 545: After change the password expiry

Disable Port

Previous

The screenshot shows a terminal window titled 'g4-15@Fedora:/home/g4-15'. The window displays the output of the Nmap command 'nmap -v -sT localhost'. The output shows that port 631/tcp is open on the local host. Other open ports listed include 21/tcp (ftp), 22/tcp (ssh), 80/tcp (http), 139/tcp (netbios-ssn), 443/tcp (https), 445/tcp (microsoft-ds), 3128/tcp (squid-http), 3306/tcp (mysql), and 10002/tcp (documentum). The Nmap version is 7.60, and the scan completed in 0.03 seconds.

```
g4-15@Fedora:/home/g4-15
File Edit View Search Terminal Help
Complete!
[root@Fedora g4-15]# nmap -v -sT localhost
Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-13 21:45 +08
Initiating Connect Scan at 21:45
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 445/tcp on 127.0.0.1
Discovered open port 22/tcp on 127.0.0.1
Discovered open port 21/tcp on 127.0.0.1
Discovered open port 139/tcp on 127.0.0.1
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 443/tcp on 127.0.0.1
Discovered open port 3306/tcp on 127.0.0.1
Discovered open port 631/tcp on 127.0.0.1
Discovered open port 3128/tcp on 127.0.0.1
Discovered open port 10002/tcp on 127.0.0.1
Completed Connect Scan at 21:45, 0.03s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00024s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 990 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
631/tcp   open  ipp
3128/tcp  open  squid-http
3306/tcp  open  mysql
10002/tcp open  documentum
```

Figure 546: Before disabling port

After

The screenshot shows a terminal window titled 'g4-15@Fedora:/home/g4-15'. The window displays the output of the Nmap command 'nmap -v -sT localhost'. The output is identical to Figure 546, showing that port 631/tcp is still open. This indicates that the port was not successfully disabled.

```
[root@Fedora g4-15]# nmap -v -sT localhost
Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-13 21:50 +08
Initiating Connect Scan at 21:50
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 21/tcp on 127.0.0.1
Discovered open port 3306/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 80/tcp on 127.0.0.1
Discovered open port 139/tcp on 127.0.0.1
Discovered open port 443/tcp on 127.0.0.1
Discovered open port 10002/tcp on 127.0.0.1
Discovered open port 3128/tcp on 127.0.0.1
Completed Connect Scan at 21:50, 0.02s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00013s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 991 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
3128/tcp  open  squid-http
3306/tcp  open  mysql
10002/tcp open  documentum

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)
```

Figure 547: After disabling port 631

6.2.28 Windows Server Hardening

Step 1: Ensure Windows Error Reporting Service start-up type is Automatic and started. It has to be enabled so that it will capture software crash data and support end-user reporting of crash information.

The screenshot shows the Windows Services (Local) window. The service 'Windows Error Reporting' is selected, highlighted with a blue border. Its status is 'Running' and its startup type is 'Automatic (Trigger Start)'. The 'Log On As' column shows 'Local System'. Other services listed include User Profile Service, Virtual Disk, Volume Shadow Copy, W3C Logging Service, Windows Audio, Windows Audio Endpoint B..., Windows Color System, Windows Connection Mana..., Windows Driver Foundation..., Windows Encryption Provid..., Windows Event Collector, Windows Event Log, Windows Firewall, Windows Font Cache Service, Windows Installer, Windows Management Inst..., Windows Modules Installer, Windows Process Activatio..., Windows Remote Manage..., Windows Store Service (WS...), Windows Time, Windows Update, WinHTTP Web Proxy Auto..., Wired AutoConfig, WMI Performance Adapter, Workstation, World Wide Web Publishin..., and Zabbix Agent. Most services are set to automatic startup.

Name	Description	Status	Startup Type	Log On As
User Profile Service	This service ...	Running	Automatic	Local Syste...
Virtual Disk	Provides m...	Running	Manual	Local Syste...
Volume Shadow Copy	Manages an...	Manual	Local Syste...	
W3C Logging Service	Provides W...	Manual	Local Syste...	
Windows Audio	Manages au...	Disabled	Local Service	
Windows Audio Endpoint B...	Manages au...	Disabled	Local Syste...	
Windows Color System	The WcsPlus...	Disabled	Local Service	
Windows Connection Mana...	Makes auto...	Running	Automatic (T...	Local Service
Windows Driver Foundation...	Creates and...	Disabled	Local Syste...	
Windows Encryption Provid...	Windows E...	Manual (Trig...	Local Service	
Windows Error Reporting	Allows error ...	Running	Automatic (Trigger Start)	Local System
Windows Event Collector	This service ...	Disabled	Network S...	
Windows Event Log	This service ...	Running	Automatic	Local Service
Windows Firewall	Windows Fi...	Running	Automatic	Local Service
Windows Font Cache Service	Optimizes p...	Running	Automatic	Local Service
Windows Installer	Adds, modifi...	Manual	Local Syste...	
Windows Management Inst...	Provides a c...	Running	Automatic	Local Syste...
Windows Modules Installer	Enables inst...	Manual	Local Syste...	
Windows Process Activatio...	The Windo...	Running	Automatic	Local Syste...
Windows Remote Manage...	Windows R...	Disabled	Network S...	
Windows Store Service (WS...)	Provides inf...	Manual (Trig...	Local Syste...	
Windows Time	Maintains d...	Running	Automatic (T...	Local Service
Windows Update	Enable the ...	Automatic	Automatic (T...	Local Syste...
WinHTTP Web Proxy Auto...	WinHTTP i...	Disabled	Local Service	
Wired AutoConfig	The Wired...	Disabled	Local Syste...	
WMI Performance Adapter	Provides pe...	Disabled	Local Syste...	
Workstation	Creates and...	Running	Automatic	Network S...
World Wide Web Publishin...	Provides W...	Running	Automatic	Local Syste...
Zabbix Agent	Provides sys...	Running	Automatic	Local Syste...

Figure 548: Services start-up type started and automatic

Step 2: Check the status of Certificate Propagation. The start-up have been changed to Automatic and started. It is used for Smart Card certificate handling. Smart-cards are used sometimes for log in instead of a password.

The screenshot shows the Windows Services (Local) window. The service 'Certificate Propagation' is selected, highlighted with a blue border. Its status is 'Running' and its startup type is 'Automatic'. The 'Log On As' column shows 'Local System'. Other services listed include Active Directory Certificate..., Active Directory Domain Se..., Active Directory Web Services, App Readiness, Application Experience, Application Host Helper Ser..., Application Identity, Application Information, Application Layer Gateway ..., Application Management, AppX Deployment Service (...), ASP.NET State Service, Background Intelligent Tran..., Background Tasks Infrastruc..., Base Filtering Engine, Certificate Propagation, CNG Key Isolation, COM+ Event System, COM+ System Application, Computer Browser, Credential Manager, Cryptographic Services, and CxAudioSvc. Most services are set to automatic startup.

Name	Description	Status	Startup Type	Log On As
Active Directory Certificate...	Creates, ma...	Running	Automatic	Local Syste...
Active Directory Domain Se...	AD DS Dom...	Running	Automatic	Local Syste...
Active Directory Web Services	This service ...	Running	Automatic	Local Syste...
App Readiness	Gets apps re...	Manual	Local Syste...	
Application Experience	Processes a...	Disabled	Local Syste...	
Application Host Helper Ser...	Provides ad...	Running	Automatic	Local Syste...
Application Identity	Determines ...	Manual (Trig...	Local Service	
Application Information	Facilitates ...	Manual (Trig...	Local Syste...	
Application Layer Gateway ...	Provides ...	Disabled	Local Service	
Application Management	Processes in...	Disabled	Local Syste...	
AppX Deployment Service (...)	Provides inf...	Manual	Local Syste...	
ASP.NET State Service	Provides ...	Disabled	Network S...	
Background Intelligent Tran...	Transfers fil...	Running	Automatic (D...	Local Syste...
Background Tasks Infrastruc...	Windows in...	Running	Automatic	Local Syste...
Base Filtering Engine	The Base Fil...	Running	Automatic	Local Service
Certificate Propagation	Copies user ...	Running	Automatic	Local Syste...
CNG Key Isolation	The CNG ke...	Running	Manual (Trig...	Local Syste...
COM+ Event System	Supports Sy...	Running	Automatic	Local Service
COM+ System Application	Manages th...	Disabled	Local Syste...	
Computer Browser	Maintains a...	Disabled	Local Syste...	
Credential Manager	Provides se...	Manual	Local Syste...	
Cryptographic Services	Provides thr...	Running	Automatic	Network S...
CxAudioSvc	Conexant A...	Running	Automatic	Local Syste...

Figure 549: Status of Certificate Propagation

Step 3: Ensure Net Logon start-up type is Automatic and started. This maintains a channel between computer and domain controller. The Net Logon sub-key stores information for the Net Logon service. The Net Logon service verifies log-on requests and it registers, authenticates and locates domain controllers.

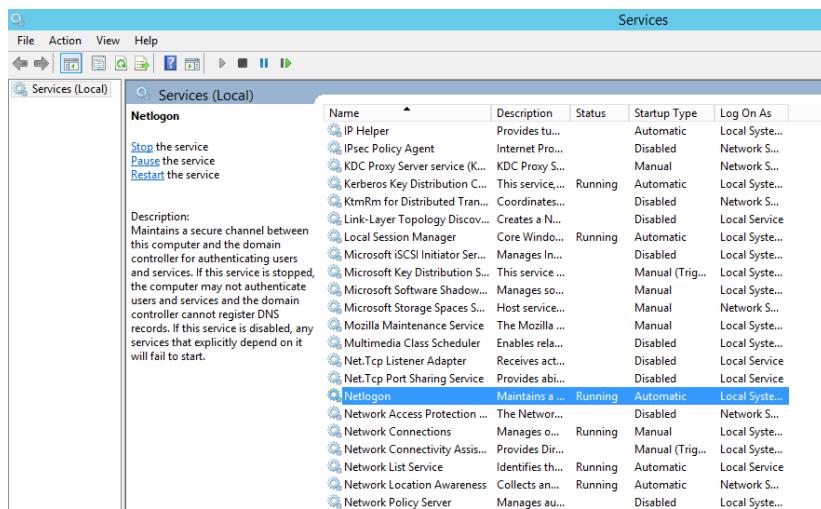


Figure 550: Net Logon information services

6.3 Conclusion

Testing is the practice of making objective judgments regarding the extent to which the system device meets, exceeds or fails to meet stated objectives. Moreover, testing is needed for risk assessment. A good testing program will allow administrator to determine errors and carry out modification for the best performance. Therefore, all of the services shall be carried out testing.

7.0 CONCLUSION

7.1 Introduction

Through these numerous weeks, a lot of things have been studied such as method to setup, configure, maintain, and troubleshoot and all of the basic of the services in this Workshop 2. All of the lessons learnt from this Workshop 2 is the prerequisite for industrial training.

To define, implement and manage this Workshop starting from selecting a leader to lead this project from the beginning until the end of the project. The overall performance of this workshop is acceptable. Our group has successfully done all of the services before the due date. Tasks have been distributed equally to each member and a schedule has been created to manage the flow of it. This is very important in managing and organizing every task in order to prevent the error from occurring before the due date.

This network is the combination of network and network security. This network is very suitable for Small and Medium Enterprise Business because it is easy to manage and implement. In this network, all of the basic services and security services are included to maintain and control the network services infrastructure. We are very grateful to gain all of the knowledge and experiences by accomplishing this project as to prepare each and every one of us for the industrial training.

7.2 Project Advantages

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

1. To design the network infrastructure for this project.
2. Learned to install and configure these services.
3. Learned how to design, monitor, and maintain a simple network.
4. Learned the methods to setup a small and simple network and the ways to manage the hardware like switch and router.
5. Learned to troubleshoot and overcome any problems during setup the services.
6. Know more about the configuration and functions of services that installed in the Windows Server 2012, Fedora, Linux Ubuntu.
7. Learned to develop a simple networking system to allow communication between computers in different platform.
8. Increase the communication between network student and security student in developing a good network environment.

7.3 Project Disadvantages

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

1. Lack of knowledge about some of the services done by other group member.
2. Some of the network equipment not in a good condition, it may not work as well as expected.
3. The servers provided to do this project are too old and causing the problems thus complicates the development of the project.
4. The students have to spend much time to setup the network.

5. The lab environment during the night time is very humid because the air condition is turned off and all of the servers are running causing the servers to heat up.

7.4 Project Limitation

These limitations prevent us to maximize the full potential of the project. Due to this limitation, we had to adapt and work harder to succeed. These limitations are:

1. The network only implemented in wired environment.
2. The equipment that provided to each group is not in good condition.
3. The network used in this project is small because it only involves 3 servers which is Windows Server, Ubuntu and Fedora. It is not really exposed to large network set ups and management.
4. Do not have chance and opportunity to try and implement any wireless technology.
5. The provided network equipment can only be used to build a small network.

7.5 Conclusion

Upon the completion of this Workshop 2, we are expected to be able to install, configure, set up, monitor and maintain own network given the necessary network equipment's. We will use heterogeneous operating system such as Microsoft Windows Server 2012 Server Enterprise Edition, Ubuntu 14.04 and Fedora. We also can design our own network and maintain a good network environment.

Moreover, in workshop 2, we learn to setup some security configuration such as server hardening, port security, access control list (ACL), and so forth to enhance the security level of our network and protect the network being access or hack by unauthorized access. To give an opportunity to apply the concept or knowledge that we learned during the lecture such as Local Area Network (LAN), Wide Area Network (WAN), Network analysis and Design, Data Communication and Networking, and so on.

Finally, this project is a very good real world exposure to us and at the end of this project we manage to complete all the tasks given and setup the network successfully. We have learned and understood the services from our supervisor and co-supervisor. We are very grateful and we appreciate our supervisor and co-supervisor for guiding us to a successful workshop completion.

BIBLIOGRAPHY

Anand Nayyar (October 10, 2016). How to install Zabbix Monitoring Server on Ubuntu 16.04 from <https://www.youtube.com/watch?v=jpj933xdaHc>

Rahul (November 27, 2018). How to install Zabbix Agent on Ubuntu 18.04 & 16.04 from <https://tecatmin.net/install-zabbix-agent-on-ubuntu-and-debian/>

Xiao Guo An (July 12, 2018). How to install RainLoop Webmail on Ubuntu 16.04 from <https://www.linuxbabe.com/mail-server/install-rainloop-webmail-ubuntu-16-04>

Michael Lenardson (October 6, 2017). How to install and configure Nextcloud on Ubuntu 16.04 from

<https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-nextcloud-on-ubuntu-16-04>

Boris Napernikov (February 19, 2002). Web Server hardening from <https://www.sans.org/reading-room/whitepapers/win2k/harden-iis-web-server-217>

ACL configuration from

<https://docs.oracle.com/cd/E19859-01/820-3252-11/FP44ucgACL.html>

About Samba. (n.d.). Retrieved from Samba <https://www.samba.org/samba/>

Harry, J. (August 20, 2009). "Configure a Cisco Router to use RADIUS for Authentication." from <http://blog.pluralsight.com/using-radius-for-authentication>.

Virtual NAT & Virtual DHCP Servers. (n.d.). Retrieved from SoftEther Project:

https://www.softether.org/index.php?title=4-docs/1-manual/3_SoftEther_VPN_Server_Manual/3.7_Virtual_NAT_%26_Virtual_DHCP_Servers

APPENDIX

No	Task name	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	Discussion with team members														
2	Proposal Preparation and Writing Proposal														
3	Submit Proposal Report														
4	Preparing Hardware and Setup Device														
5	Progress I														
6	Progress II														
7	Progress III														
8	Preparation for Video & Poster														
9	Editing the Report														
10	Final Presentation														
11	Submission of Final Report and Log Book														

Table 5: Gantt Chart