



FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

**SEMESTER 1 2019/2020
BITU 3923 - WORKSHOP II**

**FINAL REPORT
IPSEC VIRTUAL PRIVATE NETWORK(VPN)**

PREPARED BY: GROUP 4

NAME	MATRIC NO	COURSE
MUHAMMAD ARIEF BIN MOHD ISA	B031820014	BITC
MUHAMMAD HAFIZ BIN JAMIL	B031820048	BITC
NUR ARDINA AIN BINTI ABD RAOFF	B031710221	BITC
NUR ASHYQIN BINTI MOHD ZAMRI	B031810457	BITC
AMIR ZAKI BIN MAT ALI	B031810026	BITC
NIRESHA A/P ARUMUGAM	B031710025	BITC
AMMAR AFIQ BIN SHAHRUL AZMAN	B031710341	BITZ
MUHAMAD AZIM BIN AZMAN	B031710430	BITZ
CHONG POH THENG	B031710150	BITZ

SUPERVISOR: DR. ZURINA BINTI SA'AYA

EVALUATOR: DR. SITI RAHAYU BINTI SELAMAT

ACKNOWLEDGMENT

In the name of Allah, Most gracious, Most Merciful. all praises belong to Allah. Firstly, we would like to thank to Allah the Al Mighty, who made us capable to complete the Workshop II services in timely manner. Next, we would like to thank to our supervisor, Dr. Zurina Binti Sa'aya for her excellent supervision, guidance, supporting and encouragement towards completing Workshop II projects. May Allah reward her with a reply that much better than what all she has done. We would like to thank ourselves (all group members of Group 4; Azim, Ammar, Amir, Arief, Ashyqin, Ardina, Hafiz, Niresha and Poh Theng), without sheer cooperation between ourselves, this Workshop II project would not be possible. Our special thanks go to all other teams in Workshop II's Computer System and Networking lab for technical assistance all around when we are facing problems whilst completing all required 30 services to pass the Workshop II course. Finally, we would like to thank our family for their perpetual encouragement and support, that was crucial for the completion of this Workshop II projects. Thank you.

ABSTRACT

The main objectives for this Workshop 2 are to design network infrastructure by using available equipment, implementing designated network services and configure the network infrastructure correctly, installing and integrating network infrastructure, services and configuration based on the requirement of the network environment, and managing the network infrastructure, services and configuration. Our group consists of 4 students, which are Muhamad Azim Bin Azman as the Project Manager, Muhammad Arief Bin Mohd Isa, Muhammad Hafiz Bin Jamil, Nur Ardina Ain Binti Abd Raoff, Nur Ashyqin Binti Mohd Zamri, Amir Zaki Bin Mat Ali, Niresha A/P Arumugam, Ammar Afiq Bin Shahrul Azman and Chong Poh Theng as our technical team members.

We are required to install and configure 30 designated network services including Network Management System, Web SSL & Virtual Hosting, Linux Email Server, Dynamic Routing (OSPF) and Network Address Translation(NAT), IPv6 Web with IPv6 Tunneling, IPSec Site-to-Site Tunneling, Proxy Server, Server Virtualization, Access Control List(ACL), Cloud Server, Active Directory & GPO, Dynamic Name Server, Dynamic Host Configuration Protocol(DHCP), Wireless Authentication using Radius Server, Authorization Authentication Accounting(AAA) using Radius, Windows Server Hardening, IPSec Virtual Private Network, Vlan & Port Security, Server Virtualization, Quota Screening, Syslog, Samba & Samba Security, Intrusion Detection System(IDS) & Port Mirroring, Linux Server Hardening, Secure FTP, User Authentication by integrating Active Directory with Linux, Web Hardening, Linux Email Server and Trivial FTP.

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 2019, Linux Ubuntu (Desktop Version), Linux Ubuntu (Live Server Version) 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 merekabentuk infrastruktur rangkaian dengan menggunakan peralatan yang tersedia, melaksanakan perkhidmatan rangkaian yang ditetapkan dan mengkonfigurasi infrastruktur rangkaian dengan betul, memasang dan mengintegrasikan infrastruktur rangkaian, perkhidmatan dan konfigurasi berdasarkan keperluan persekitaran rangkaian, dan menguruskan rangkaian infrastruktur, perkhidmatan dan konfigurasi. Kumpulan kami terdiri daripada 4 pelajar, iaitu Muhamad Azim Bin Azman sebagai Pengurus Projek, Muhammad Arief Bin Mohd Isa, Muhammad Hafiz Bin Jamil, Nur Ardina Ain Binti Abd Raoff, Nur Ashyqin Binti Mohd Zamri, Amir Zaki Bin Mat Ali, Niresha A / P Arumugam, Ammar Afiq Bin Shahrul Azman dan Chong Poh Theng sebagai ahli pasukan teknikal kami.

Kami dikehendaki untuk memasang dan mengkonfigurasi 30 perkhidmatan rangkaian yang ditetapkan termasuk *Network Management System, Web SSL & Virtual Hosting, Linux Email Server, Dynamic Routing (OSPF) and Network Address Translation(NAT), IPv6 Web with IPv6 Tunneling, IPSec Site-to-Site Tunneling, Proxy Server, Server Virtualization, Access Control List(ACL), Cloud Server, Active Directory & GPO, Dynamic Name Server, Dynamic Host Configuration Protocol(DHCP), Wireless Authentication using Radius Server, Authorization Authentication Accounting(AAA) using Radius, Windows Server Hardening, IPSec Virtual Private Network, Vlan & Port Security, Server Virtualization, Quota Screening, Syslog, Samba & Samba Security, Intrusion Detection System(IDS) & Port Mirroring, Linux Server Hardening, Secure FTP, User Authentication by integrating Active Directory with Linux, Web Hardening, Linux Email Server and Trivial FTP.* Seorang pengurus projek telah ditugaskan dari kumpulan untuk memimpin ahli-ahli kumpulan di seluruh bengkel tersebut. Kami telah menyediakan peralatan yang terdiri daripada (3) servers, satu (1) Cisco 2800 router (2 Fast Ethernet), satu (1) Cisco 2960 manageable switch, 15 meter UTP cable, 12 keping RJ-45, NIC card, Access Point (AP) dan satu set crimping tool. Sistem operasi yang digunakan dalam pelayan adalah Windows Server 2019, Ubuntu Linux (Versi Desktop), Ubuntu Linux (Versi Server Live) Setelah menyusun semua konfigurasi, infrastruktur dan perkhidmatan rangkaian, 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	ii
Abstract	iii
Abstrak	iv
Table of contents	v
List of figures	ix
List of tables	xxiv
Chapter 1: INTRODUCTION	1
1.1 Introduction	1
1.2 Objective	2
1.3 Project Plan / Schedule	2
1.4 Organization Chart	3
1.5 Conclusion	3
Chapter 2: PROJECT REQUIREMENT	4
2.1 Introduction	4
2.2 Types of Operating System	4
2.3 Operating system background	5
2.3.1 Windows Server 2012 R2	6
2.3.2 Ubuntu	6
2.3.3 Debian 9.3	6
2.4 Hardware requirement	7
2.5 Hardware justification	7
2.5.1 Router	7
2.5.2 Switch	8
2.5.3 Unshielded Twisted Pair (UTP Cable)	8
2.5.4 RJ-45 Connector	8
2.5.5 Ethernet Cable	9
2.5.6 Crimping Tool	10
2.6 Conclusion	10
Chapter 3: DESIGN	11
3.1 Introduction	11
3.2 Security Policy	11
3.2.1 Acceptable Encryption Policy	12
3.2.2 Password Protection Policy	12
3.2.3 Password Creation	12
3.2.4 Password Protection	12
3.2.5 Server security policy	13
3.2.6 Router and Switch Security Policy	13
3.2.7 Remote Access Policy	14
3.2.8 Application Security	14
3.2.8.1 Hardening Service Policy	14
3.2.8.2 Access Security	15
3.2.8.3 DNS Service Policy	15
3.2.8.4 VLAN Service Policy	16
3.2.8.5 Proxy Server Service Policy	16
3.2.8.6 Secure File Transfer Protocol (SFTP) Service Policy	16

3.2.8.7 Virtual Private Network (VPN) Service Policy	17
3.2.8.8 Authentication using Radius Server Service Policy	17
3.2.8.9 Active Directory Security Policy	18
3.2.8.10 Samba Security	18
3.3 Physical Security	18
3.4 Physical Design	20
3.5 Logical Design	21
3.6 Conclusion	22
Chapter 4: SERVICES	23
4.1 Introduction	23
4.2 List of services	23
4.3 Brief overview for services	24
4.3.1 Domain Name System (IPv4 & IPv6)	24
4.3.2 Dynamic Host Configuration Protocol (IPv4 & IPv6)	24
4.3.3 Active Directory	25
4.3.4 Secured FTP	25
4.3.5 Web, SSL & Virtual Hosting	25
4.3.6 TFTP	26
4.3.7 Linux Mail Server	26
4.3.8 Inter VLAN and VLSM addressing	27
4.3.9 Syslog	27
4.3.10 IPSec site-to-site tunnelling	27
4.3.11 Routing & NAT	28
4.3.12 Proxy Server	28
4.3.13 Network Management System	28
4.3.14 Server Virtualization	29
4.3.15 Security Policy	29
4.3.16 Linux Server Hardening	29
4.3.17 Windows Server Hardening	30
4.3.18. Authentication user by integrating AD with Linux	31
4.3.19 Wireless user authentication using Radius server	31
4.3.20 IDS with Port Mirror	31
4.3.21 IPSec VPN for remote employees	32
4.3.22 Samba Security	33
4.3.23 VLAN & Port Security	33
4.3.24 AAA	34
4.3.25 Quota Screening	34
4.3.26 Cloud Server	35
4.3.27 Access Control List	35
4.3.28 Web Hardening	35
4.3.29 IPv6 Tunnelling	36
4.4 Conclusion	36
Chapter 5: INSTALLATION AND CONFIGURATION	37
5.1 Introduction	37
5.2 Services testing and individual who responsible for the testing	37
5.3 Installation and Configuration	39
5.3.1 AAA	39
5.3.2 Server Virtualization	54

5.3.3 Active Directory with UAC/GPO	72
5.3.4 Domain Name System	86
5.3.5 Linux Email Server	99
5.3.6 IDS with Port Mirror	105
5.3.7 Wireless User Authentication user Radius Server	111
5.3.8 Network Management System	140
5.3.9 Secure FTP	152
5.3.10 Dynamic Host Configuration Protocol (IPv4 and IPv6)	155
5.3.11 Web, SSL and Virtual Hosting	164
5.3.12 Syslog	168
5.3.13 Dynamic Routing and Network Address Translation	170
5.3.14 Proxy Server	173
5.3.15 Access Control List	175
5.3.16 Trivial File Transfer Protocol	177
5.3.17 Quota Screening	179
5.3.18 IPv6 Web with IPv6 Tunneling	189
5.3.19 IPsec Site-to-Site Tunelling	191
5.3.20 Cloud Server	192
5.3.21 Web Hardening	196
5.3.22 Samba and Samba Security Services	209
5.3.23 Linux Server Hardening	213
5.3.24 User Authentication by Integrating Active Directory with Linux	218
5.3.25 Windows Server Hardening	222
5.3.26 IPsec VPN server for remote employees	247
5.3.27 VLAN and Port Security	270
5.3 Conclusion	272
Chapter 6: TESTING	273
6.1 Introduction	273
6.2 Services testing	273
6.2.1 Domain Name Server (IPV4 & IPV6) Testing	273
6.2.2 Dynamic Host Configuration Protocol (IPv4 & IPv6) Testing	274
6.2.3 Vlan & Port Security Testing	275
6.2.4 Web, SSL & Virtual Hosting Testing	278
6.2.5 Syslog Testing	280
6.2.6 Network Monitoring System	281
6.2.7 Wireless User Authentication by using RADIUS Server Testing	287
6.2.8 IPsec VPN Server for Remote Employee Testing	289
6.2.9 Reverse Proxy Server Testing	294
6.2.10 Trivial File Transfer Protocol (TFTP) Testing	295
6.2.11 IPsec Site-To-Site Testing	296
6.2.12 Windows Server Hardening Testing	297
6.2.13 Authentication, Authorization and Accounting (AAA) Using Radius Testing	299
6.2.14 Authentication User by Integrating Active Directory with Linux	300
6.2.15 Quota Screening	301

6.2.16 Testing Server Virtualization	303
6.2.17 Inter VLAN and VLSM Addressing	308
6.2.18 Web Hardening	308
6.2.19 IDS Port Mirror	311
6.2.20 Samba	312
6.2.21 Linux Server Hardening	317
6.2.22 Dynamic Routing & NAT	318
6.2.23 Linux Email Server	322
6.2.24 Cloud Server	325
6.2.25 Active Directory & GPO	329
6.2.26 Secured FTP Server	335
6.2.27 Access Control List	338
6.2.28 IPv6 Tunnel and IPv6 Web Testing	341
6.3 Conclusion	342
Chapter 7 : CONCLUSION	343
7.1 Introduction	343
7.2 Project advantages	343
7.3 Project disadvantages	344
7.4 Project limitation	344
7.5 Conclusion	344
REFERENCES	345
APPENDIX	347

LIST OF FIGURES

Figure 3.4.1: Physical Design	20
Figure 3.5.1: Logical Design	21
Figure 5.3.1.1: Server Manager	39
Figure 5.3.1.2: Add roles and features	39
Figure 5.3.1.3: Select server roles	40
Figure 5.3.1.4: Installation progress	40
Figure 5.3.1.5: Network Policy Server	41
Figure 5.3.1.6: Enable NPS (Network Policy Server)	41
Figure 5.3.1.7: New Radius Client	42
Figure 5.3.1.8: New Network Policies	43
Figure 5.3.1.9: Policy Name	44
Figure 5.3.1.10: Specify Condition	44
Figure 5.3.1.11: Select Group	45
Figure 5.3.1.12: Check Names	45
Figure 5.3.1.13: User Groups	46
Figure 5.3.1.14: Access Permission	46
Figure 5.3.1.15: Authentication Method	47
Figure 5.3.1.16: Configure Constraint	47
Figure 5.3.1.17: Configure Settings	48
Figure 5.3.1.18: Attribute Information	48
Figure 5.3.1.19 : Vendor Specific	49
Figure 5.3.1.20: Attribute Value	50
Figure 5.3.1.21: Successfully Creating Network Policy	50
Figure 5.3.1.22: Accounting in Network Policy Server	51
Figure 5.3.1.23: Introduction In Accounting Configuration	51
Figure 5.3.1.24: Select Accounting Option	52
Figure 5.3.1.25: Configuring File Logging	52
Figure 5.3.1.26: Conclusion	53
Figure 5.3.2.1 : Install Hyper-V	54
Figure 5.3.2.2: Installation type	54
Figure 5.3.2.3: Select destination server	55
Figure 5.3.2.4 : Select Hyper-V	55
Figure 5.3.2.5: Add features	56
Figure 5.3.2.6 : Select server roles	56
Figure 5.3.2.7: Select features	57
Figure 5.3.2.8 : Hyper-V information	57
Figure 5.3.2.9 : Server roles	58
Figure 5.3.2.10: Virtual machine migration	58
Figure 5.3.2.11 : Default stores	59
Figure 5.3.2.12 : Installation progress	59
Figure 5.3.2.13: Add new virtual machine	60
Figure 5.3.2.14 : Specify name and location	60
Figure 5.3.2.15: Specify generation	61
Figure 5.3.2.16: Assign memory	61
Figure 5.3.2.17: Configuring networking	62
Figure 5.3.2.18 : Connect virtual hard disk	62
Figure 5.3.2.19: Installation options	63

Figure 5.3.2.20: Summary of selection	63
Figure 5.3.2.21: Virtual machine installed	64
Figure 5.3.2.22: Connect virtual machine	64
Figure 5.3.2.23: Start the virtual machine	65
Figure 5.3.2.24: Front screen virtual machine	65
Figure 5.3.2.25: Install DHCP	66
Figure 5.3.2.26: Installation type	66
Figure 5.3.2.27: Destination server	67
Figure 5.3.2.28: Select server roles	67
Figure 5.3.2.29: Select features	68
Figure 5.3.2.30 : DHCP information	68
Figure 5.3.2.31: Confirmation installation	69
Figure 5.3.2.32 : Installation progress	69
Figure 5.3.2.33 : DHCP installed	70
Figure 5.3.2.34 : Configure failover	70
Figure 5.3.2.35 : New failover relationship	71
Figure 5.3.2.36 : Log of various task	71
Figure 5.3.3 1: Add Roles and Features Active Directory	72
Figure 5.3.3.2: Install Active Directory Domain Services	72
Figure 5.3.3.3: Confirmation Installation Active Directory	73
Figure 5.3.3.4 Installation Progress Active Directory Domain Services	73
Figure 5.3.3.5: Deployment Configuration Active Directory Domain Services	74
Figure 5.3.3.6: Setting Domain Controller Active Directory Services	74
Figure 5.3.3.7: Additional Options Active Directory Services	75
Figure 5.3.3.8: Configuration Paths Active Directory Domain Services	75
Figure 5.3.3.9: Review Options Active Directory	76
Figure 5.3.3.10: User and Computer Active Directory	77
Figure 5.3.3.11: New Object – User	77
Figure 5.3.3.12: Insert default password the user	78
Figure 5.3.3.13: List User Active Directory	78
Figure 5.3.3.14: Create new Organizational Unit	79
Figure 5.3.3.15: Insert the name Organizational Unit	79
Figure 5.3.3.16: Move the user Active Directory	80
Figure 5.3.3.17: Move the user to the new Organizational Unit	80
Figure 5.3.3.18 Group Policy Management Menu	81
Figure 5.3.3.19 Create new GPO policy	81
Figure 5.3.3.20: Edit the group policy	82
Figure 5.3.3.21: List policies in group policy management editor	82
Figure 5.3.3.22: List of policy in System	83
Figure 5.3.3.23: Enable the policy command prompt	83
Figure 5.3.3.24 List of policy Removable Storage Access	84
Figure 5.3.3.25 Enable the policy All Removable Storage Access	84
Figure 5.3.3.26 Summary update policy	85
Figure 5.3.3.27: Update policy on the command prompt	85
Figure 5.3.4.1: Add Roles for DNS Server	86
Figure 5.3.4.2: DNS Server Installation Progress	86
Figure 5.3.4.3: Option to Configure DNS	87
Figure 5.3.4.4: DNS Manager	87

Figure 5.3.4.5: New Zone Wizard	88
Figure 5.3.4.6: Select Zone Type	88
Figure 5.3.4.7: Set Zone Name	89
Figure 5.3.4.8: Set New File	89
Figure 5.3.4.9: Completed Forward Lookup	90
Figure 5.3.4.10: New Zone Wizard for Reverse Lookup	90
Figure 5.3.4.11: Reverse Lookup Zone Name	91
Figure 5.3.4.12: Enter Network ID	91
Figure 5.3.4.13: Create Zone File	92
Figure 5.3.4.14: Enable Dynamic Updates	92
Figure 5.3.4.15: Completed IPv4 Reverse Lookup	93
Figure 5.3.4.16: Add New Zone	93
Figure 5.3.4.17: New Zone for IPv6 Reverse Lookup	94
Figure 5.3.4.18: Select Reverse Lookup Zone Name	94
Figure 5.3.4.19: Set IPv6 Address Prefix	95
Figure 5.3.4.20: Select Zone File	95
Figure 5.3.4.21: Completed IPv6 Reverse Lookup	96
Figure 5.3.4.22: DNS Resources	96
Figure 5.3.4.23: DNS Resources	97
Figure 5.3.4.24: Server Record	97
Figure 5.3.4.25: Terminal	98
Figure 5.3.5.1: Installing email services command	99
Figure 5.3.5.2: Select mail type for auto configuration by Postfix	99
Figure 5.3.5.3: Enable secure SMTP and locate the certificate.	100
Figure 5.3.5.4: Enable submission port and disable regular SMTP port 25	100
Figure 5.3.5.5: Enable plain login when connecting using telnet	101
Figure 5.3.5.6: Allow email spooling	101
Figure 5.3.5.8: Disable other port except 143 for incoming email	101
Figure 5.3.5.9: Enable secure IMAP and locate the certificate	102
Figure 5.3.5.10: Roundcube webmail installation command	102
Figure 5.3.5.31: Specifies the host for Roundcube connection to email server	103
Figure 5.3.5.12: Specifies the SMTP server for Roundcube connection	103
Figure 5.3.5.13: Enable virtual hosting for Roundcube webmail	104
Figure 5.3.6.1: Install prerequisite snort	105
Figure 5.3.6.2: Download DAQ packages	106
Figure 5.3.6.3: Install DAQ	106
Figure 5.3.6.4: Download Snort Package	106
Figure 5.3.6.5: Create Symlink	107
Figure 5.3.6.6: Create directory and file	107
Figure 5.3.6.7: Change file permission	107
Figure 5.3.6.8: Copy necessary file	108
Figure 5.3.6.9: Snort configuration file	108
Figure 5.3.6.10: Validate Snort	109
Figure 5.3.6.11: Setup port mirror configuration	110
Figure 5.3.6.12: Validate port mirror	110
Figure 5.3.7.1: Access Point Web	111
Figure 5.3.7.2: Basic Setup for Access Point	112
Figure 5.3.7.3: Wireless Physical Interface info of AP	113

Figure 5.3.7.4: Wireless Security Information of AP	113
Figure 5.3.7.5: Create New Object - Group	114
Figure 5.3.7.6: Information of New Group	114
Figure 5.3.7.7: Create New Object - User	115
Figure 5.3.7.8: Information of New User	115
Figure 5.3.7.9: Creating password to the user	116
Figure 5.3.7.10: Confirmation of User	116
Figure 5.3.7.11: Members of group4	117
Figure 5.3.7.12: Add Roles and Features Wizard	118
Figure 5.3.7.13: Select Installation Type	119
Figure 5.3.7.14: Select Destination Server	120
Figure 5.3.7.15: Select Server Roles	121
Figure 5.3.7.16: Adding Features for AD CS	121
Figure 5.3.7.17: Installation Progress	122
Figure 5.3.7.18: Role Services Configuration	123
Figure 5.3.7.19: Select Role Services for AD CS	123
Figure 5.3.7.20: Setup Type of CA	124
Figure 5.3.7.21: CA Type Specification	125
Figure 5.3.7.22: Choosing the Private Key	125
Figure 5.3.7.23: Selecting Cryptography for CA	126
Figure 5.3.7.24: Specify Validity Period	126
Figure 5.3.7.25: Specify Database Location	127
Figure 5.3.7.26: Confirmation of AD CS Configuration	127
Figure 5.3.7.27: Results of AD CS Configuration	128
Figure 5.3.7.28: Console Root Page	128
Figure 5.3.7.29: Adding or Remove snap-ins	129
Figure 5.3.7.30: Choosing Certificates Snap In	129
Figure 5.3.7.31: Select Local Computer to manage snap-in	130
Figure 5.3.7.32: Loading the Certificate into Consolz	131
Figure 5.3.7.33: Beginning of Certificate Enrolment	132
Figure 5.3.7.34: Selecting Certificate Enrolment Policy	132
Figure 5.3.7.35: Requesting Certificates	133
Figure 5.3.7.36: Installation of Certificate	133
Figure 5.3.7.37: Network Policy server page	134
Figure 5.3.7.38: Select 802.1X Connection Type	134
Figure 5.3.7.39: Setting up new RADIUS Client	135
Figure 5.3.7.40: Add RADIUS Client	135
Figure 5.3.7.41: Select the PEAP type for the policy	136
Figure 5.3.7.42: Specify user Group	136
Figure 5.3.7.43: Completing the RADIUS Client	137
Figure 5.3.7.44: Certificate Export Wizard	137
Figure 5.3.7.45: Choose to not export private key	138
Figure 5.3.7.46: Selecting export file format	138
Figure 5.3.7.46: Select File Name to export Certificate	139
Figure 5.3.7.47: Completing the Certificate export wizard	139
Figure 5.3.8.1: Show the installation of apache2, mysql and php	140
Figure 5.3.8.2: Show the opening file and change the time zone in the php.ini file.	140

Figure 5.3.8.3: Show the download from the repo and depackage the downloaded file	140
Figure 5.3.8.4: Show the installation of Zabbix agent, mysql and the frontend	140
Figure 5.3.8.5: Show the database and the user is created	141
Figure 5.3.8.6: Show the open file of ‘Zabbix_server.conf’ and change database name,host,user and the password	141
Figure 5.3.8.7: Show the restart of all Zabbix service	141
Figure 5.3.8.8: Show the copy file	142
Figure 5.3.8.9: Show the opening setup page for Zabbix	142
Figure 5.3.8.10: Show the check for pre-requisites	143
Figure 5.3.8.11: Show the configure of database connection	143
Figure 5.3.8.12: Show the Zabbix server details	144
Figure 5.3.8.13: Show the pre-installation summary	144
Figure 5.3.8.14: Show the login page for Zabbix	145
Figure 5.3.8.15. Show Zabbix dashboard	145
Figure 5.3.8.16: Show the Zabbix agent for Windows	146
Figure 5.3.8.17: Show the update of configuration	146
Figure 5.3.8.18: Show the installation of the Zabbix agent	146
Figure 5.3.8.19: Show to stop and start Zabbix agent service using command line	14
Figure 5.3.8.20: Show to stop and start Zabbix agent using task manager	147
Figure 5.3.8.21: Show the full coding of the installation, stop and start of the Zabbix agent	148
Figure 5.3.8.22: Show the installation of zabbix agent for Ubuntu from repositories	149
Figure 5.3.8.23: Show the depackage downloaded file	149
Figure 5.3.8.24: Show the installation of Zabbix agent.	1491
Figure 5.3.8.25: Show the way to open the zabbix_agentd.conf file	149
Figure 5.3.8.26: Show the server is set into Zabbix server ip	150
Figure 5.3.8.27: Show the hostname is set to hostname of the client	150
Figure 5.3.8.28: Show the enable, start, stop and status of the Zabbix agent	151
Figure 5.3.9.1: The command to install and enable service	152
Figure 5.3.9.2: The configuration file of vsftpd	152
Figure 5.3.9.3: The command to store certificate	153
Figure 5.3.9.4: The vsftpd configuration file	153
Figure 5.3.9.5: The certificate prompted	154
Figure 5.3.10.1: Adding role for DHCP	155
Figure 5.3.10.2: Select features for DHCP	155
Figure 5.3.10.3: DHCP role to be completed	156
Figure 5.3.10.4: DHCP configuration page	156
Figure 5.3.10.5: Create scope name for New Scope Wizard	157
Figure 5.3.10.6: Create scope name for New Scope Wizard	157
Figure 5.3.10.7: Set IP Address Range	158
Figure 5.3.10.8: Set the lease duration	158
Figure 5.3.10.9: Configure DHCP options	159
Figure 5.3.10.10: Add IP for Router	159
Figure 5.3.10.11: Set Domain Name and DNS Server	160
Figure 5.3.10.12: Completed New Scope Wizard	160
Figure 5.3.10.13: Add New Scope	161
Figure 5.3.10.14: New Scope Wizard	161

Figure 5.3.10.15: Set Scope Name	162
Figure 5.3.10.16: Set Prefix	162
Figure 5.3.10.17: Set Scope Lease for IPv6	163
Figure 5.3.10.18: Completed New Scope Wizard	163
Figure 5.3.11.1: Show the IIS Manager	164
Figure 5.3.11.2: Show the server certificate	164
Figure 5.3.11.3: Show the create certificate	165
Figure 5.3.11.4: Show the select of certificate	165
Figure 5.3.11.5: Show the integrated SSL on Debian	166
Figure 5.3.11.6: Show the directory and copy the file	166
Figure 5.3.11.7: Show the coding put into the vhost-group4.conf file	166
Figure 5.3.11.8: Show the deactivate and activate the virtual host	167
Figure 5.3.11.9: Show the open for index.php	167
Figure 5.3.11.10: Show the setup of index.php	167
Figure 5.3.12.1: Show the configure rsyslog.conf.	168
Figure 5.3.12.2: Show the trap information for router.	169
Figure 5.3.13.1: OSPFv2 running configuration with created process and advertised network	170
Figure 5.3.13.2: OSPFv3 running configuration with created process and router-id	170
Figure 5.3.13.3: Advertised interfaces	171
Figure 5.3.13.4: The highlighted statement matched internal network	171
Figure 5.3.13.5: Translate all the internal network to public IP address on interface serial0/2/0.	171
Figure 5.3.13.6: MAP the proxy server to a single public IP address	172
Figure 5.3.13.7: Set interface serial0/2/0 as an outside interface	172
Figure 5.4.14.1: shows installation of nginx	173
Figure 5.3.14.2: shows the configuration of the nginx	173
Figure 5.3.14.3: shows the active (running) of the nginx.	174
Figure 5.3.14.3: shows the active (running) of the nginx.	175
Figure 5.3.15.2: ip access-group	175
Figure 5.3.15.3: ACL command	176
Figure 5.3.15.4: show access-list	176
Figure 5.3.16.1: installed tftpd-hpa	177
Figure 5.3.16.2: show configuration of tftp	177
Figure 5.3.16.3: show active (running) tftp	178
Figure 5.3.17.1: Add roles and features	179
Figure 5.3.17.2: Installation type	179
Figure 5.3.17.3: Select destination server	180
Figure 5.3.17.4: Server roles	180
Figure 5.3.17.5: Select server roles	181
Figure 5.3.17.6: Features	181
Figure 5.3.17.7: Confirmation of selections	182
Figure 5.3.17.8: Installation progress	182
Figure 5.3.17.9: Quota Management	183
Figure 5.3.17.10: Quota Template	183
Figure 5.3.17.11: New Quota Template	184
Figure 5.3.17.12: Quota Path	184
Figure 5.3.17.13: New Quota List	185

Figure 5.3.17.14: File Screening Management	185
Figure 5.3.17.15: New File Screen Template	186
Figure 5.3.17.16: Create File Screen Template	186
Figure 5.3.17.18: File Group Properties	187
Figure 5.3.17.18: Named template	187
Figure 5.3.17.19: File Screen Path	188
Figure 5.3.17.20: New File Screen Template List	188
Figure 5.3.18.1: Tunnel 0 configuration on router	189
Figure 5.3.18.2: OSPFv3 configuration	189
Figure 5.3.18.3: Advertise OSPFv3	190
Figure 5.3.19.1: Configure ISAKMP	191
Figure 5.3.19.2: Set the acl to allow the specific network	191
Figure 5.3.19.3: Apply the ipsec	191
Figure 5.3.20.1: Install Apache server	192
Figure 5.3.20.2: Install php extension server	192
Figure 5.3.20.3: Install MariaDB server	193
Figure 5.3.20.4: Install MariaDB database server	193
Figure 5.3.20.5: Unpacking nextcloud server	194
Figure 5.3.20.6: NextCloud setup wizard interface	195
Figure 5.3.21.4 : Check for updates	196
Figure 5.3.21.5 : Install updates	196
Figure 5.3.21.6 : Install updates	197
Figure 5.3.21.7 : Install updates	197
Figure 5.3.21.8 : Install updates	198
Figure 5.3.21.9: Reboot server	198
Figure 5.3.21.10 : Install ufw	198
Figure 5.3.21.11 : Check ufw status	199
Figure 5.3.21.12 : Modify default rules	199
Figure 5.3.21.13 : Enable port	199
Figure 5.3.21.14 : Set port nummber	199
Figure 5.3.21.15: Enable ufw	199
Figure 5.3.21.16 : Create a non-root account	200
Figure 5.3.21.17 : Change user default mode	200
Figure 5.3.21.18 : Test new user	200
Figure 5.3.21.19 : Check updates	201
Figure 5.3.21.20 : Install apache2	201
Figure 5.3.21.21 : Install Certbot	202
Figure 5.3.21.22 : Install Certbot	202
Figure 5.3.21.23 : Run Certbot	203
Figure 5.3.21.24 : Enable HTTP/2 module and restart apache2	203
Figure 5.3.21.25 : Enter config file	204
Figure 5.3.21.26 : Apply settings	204
Figure 5.3.21.27 : Create password file	205
Figure 5.3.21.25: Restart Apache2	205
Figure 5.3.21.28 : Configure Apache Password Authentication	205
Figure 5.3.21.29 : Enable Clickjacking Protection	205
Figure 5.3.21.30 : Restart Apache2	206
Figure 5.3.21.31 : Enable XSS Protection	206

Figure 5.3.21.32 : Disable directory browser listing	206
Figure 5.3.21.33 : Restart Apache2	206
Figure 5.3.21.34 : System settings protection	207
Figure 5.3.21.35 : Install ModSecurity	207
Figure 5.3.21.36 : Open config file	208
Figure 5.3.21.37 : Edit settings	208
Figure 5.3.21.38 : Restart Apache2	208
Figure 5.3.21.39 : Apply a small bash script	208
Figure 5.3.22.1: Installation Of Samba	209
Figure 5.3.22.2: Status Running Of Samba	209
Figure 5.3.22.3: Allow SAMBA in Firewall	210
Figure 5.3.22 4: Integrate Active Directory with Samba	210
Figure 5.3.22 4: Samba group configuration	210
Figure 5.3.22.5: Create samba directory	210
Figure 5.3.22.6:Change file permission and owner	210
Figure 5.3.22.7: Shared path	211
Figure 5.3.22.8: Restart samba	211
Figure 5.3.22 9: Samba group configuration	211
Figure 5.3.22 10: Create group	212
Figure 5.3.22 11: Add member to group	212
Figure 5.3.22 12: Change group owner	212
Figure 5.3.22 13: Assign valid user	212
Figure 5.3.23.1: Install System Update	213
Figure 5.3.23.2: Updating system done	213
Figure 5.3.23.3: Check vulnerability	214
Figure 5.3.23.4: Done updating system and upgrade bash	214
Figure 5.3.23.5: View password current status	215
Figure 5.3.23.6: Command for change expiration date	215
Figure 5.3.23.7: Change expiration date of password	215
Figure 5.3.23.8: Changing system update	216
Figure 5.3.23.9: Install UFW firewall	216
Figure 5.3.23.10: Allow SSH and HTTP services	217
Figure 5.3.23.11: Enable firewall and check status	217
Figure 5.3.24 1: Install Winbind Kerberos	218
Figure 5.3.24 2: Insert requirement for installation	218
Figure 5.3.24 3: Setting on Global Setting	219
Figure 5.3.24 4: Setting the nsswitch.conf file	219
Figure 5.3.24 5: Adding session option in common-session file	220
Figure 5.3.24 6: Verifying status is active	220
Figure 5.3.24 7: Command to join domain	221
Figure 5.3.24 8: AD Users and Computer addition of Debian	221
Figure 5.3.25.1: Server Manager Dashboard	222
Figure 5.3.25 2: Security configuration wizard	222
Figure 5.3.25 3: Create new security policy	223
Figure 5.3.25 4: Insert Server name	223
Figure 5.3.25 5: Complete the processing	224
Figure 5.3.25 6: Role-based service configuration	224
Figure 5.3.25 7: Select server roles	225

Figure 5.3.25.8: Select server roles	225
Figure 5.3.25.9: Select client features	226
Figure 5.3.25.10: Select options used to administrate the selected server	226
Figure 5.3.25.11: Select Additional services	227
Figure 5.3.25.12: Select Handling Unspecified Services	227
Figure 5.3.25.13: Confirm service changes	228
Figure 5.3.25.14: Network security first page	228
Figure 5.3.25.15: Select network security rules	229
Figure 5.3.25.16: Registry setting first page	229
Figure 5.3.25.17: Select attributes needed for SMB Security Signature	230
Figure 5.3.25.18: Determine: LDAP Signing	230
Figure 5.3.25.19: Select outbound authentication method	231
Figure 5.3.25.20: Select outbound authentication using Domain Accounts	231
Figure 5.3.25.21: Registry setting summary	232
Figure 5.3.25.22: First page of Audit Policy	232
Figure 5.3.25.23: Select system audit policy	233
Figure 5.3.25.24: Summary of audit policy	233
Figure 5.3.25.25: Saving Security policy	234
Figure 5.3.25.26: Saving the policy name and file location	234
Figure 5.3.25.27: Select to apply security policy	235
Figure 5.3.25.28: Security Configuration Wizard has completed	235
Figure 5.3.25.29: Server Manager Dashboard	236
Figure 5.3.25.30: Disable account for hafiz	236
Figure 5.3.25.31: Local security policy	237
Figure 5.3.25.32: Audit Policy	237
Figure 5.3.25.33: Local security setting for audit privilege use	238
Figure 5.3.25.34: Search for Windows Update	239
Figure 5.3.25.35: Change the setting of installation updates	239
Figure 5.3.25.36: Check for available updates	240
Figure 5.3.25.37: Server Manager Dashboard	240
Figure 5.3.25.38: Enabling firewall	241
Figure 5.3.25.39: Search for services.msc	241
Figure 5.3.25.40: Change the Startup Type of Distributed Transaction Coordinator Properties	242
Figure 5.3.25.41: Change the Startup Type of KtmRm for Distributed Transaction Coordinator Properties	242
Figure 5.3.25.42: Search for Services.msc	243
Figure 5.3.25.43: Change the Startup Type of Windows Error Reporting Service	243
Figure 5.3.25.44: Change the Startup Type of Secure Socket Tunneling Protocol Service Properties	244
Figure 5.3.25.45: Change the Startup Type of Certificate Propagation Service Properties	244
Figure 5.3.25.46: Change the Startup Type of Netlogon Service Properties	245
Figure 5.3.25.47: Windows Error Reporting	245
Figure 5.3.25.48: Check the status of Certificate Propagation	246
Figure 5.3.25.49: Checking on NetLogon startup type	246
Figure 5.3.26.40 : Go to website and click download	247
Figure 5.3.26.41 : Download SoftEther VPN	247

Figure 5.3.26.42 : Choose requirement	248
Figure 5.3.26.43 : Download section	248
Figure 5.3.26.44: Choose software component to install	249
Figure 5.3.26.45 : Agree to End user Agreement	249
Figure 5.3.26.46 : Important Notice	250
Figure 5.3.26.47 : Path Selection	250
Figure 5.3.26.48 : Wait for installation	251
Figure 5.3.26.49 : Finish installation	251
Figure 5.3.26.50 : Select local host	252
Figure 5.3.26.51 : Set up local host	252
Figure 5.3.26.52 : Set administrator password	253
Figure 5.3.26.53 : Set up bridge	253
Figure 5.3.26.54 : Set up confirmation notice	254
Figure 5.3.26.55 : Setup Virtual Hub Name	254
Figure 5.3.26.56 : Disable VPN Azure Services	254
Figure 5.3.26.57 : Create a new user	255
Figure 5.3.26.58 : Set up new user	255
Figure 5.3.26.59 : Confirmation alert of user created	256
Figure 5.3.26.60 : Manage user	256
Figure 5.3.26.61 : Set up local bridge	257
Figure 5.3.26.62: Manage Virtual Hub	257
Figure 5.3.26.63 : Enable SecureNAT	258
Figure 5.3.26.64 : Enable SecureNAT alert	258
Figure 5.3.26.65 : Ip address provided by SecureNAT	259
Figure 5.3.26.66 : Manage encryption and network	259
Figure 5.3.26.67 : Select Encryption and Network	260
Figure 5.3.26.68 : Modify encryption algorithm name	260
Figure 5.3.26.69 : Select IPsec / L2TP Setting	261
Figure 5.3.26.70 : Virtual Hub is created	261
Figure 5.3.26.71 : Go to website and click download	262
Figure 5.3.26.72 : Download SoftEther VPN	262
Figure 5.3.26.73 : Choose requirement	263
Figure 5.3.26.74 : Download section	263
Figure 5.3.26.75 : Choose software component to install	264
Figure 5.3.26.76 : Agree to End user Agreement	264
Figure 5.3.26.77 : Important Notice	265
Figure 5.3.26.78 : Path Selection	265
Figure 5.3.26.79 : Wait for installation	266
Figure 5.3.26.80 : Finish installation	266
Figure 5.3.26.81 : GUI of SoftEther VPN Client Manager	267
Figure 5.3.26.82 : Create new Virtual Network Adapter	267
Figure 5.3.26.83 : Set up Virtual Network Adapter name	268
Figure 5.3.26.84 : New virtual network adapter	268
Figure 5.3.26.85 : Set up VPN Connection	269
Figure 5.3.26.86 : VPN Connection created	269
Figure 5.3.27.87 : Switchport Nonegotiate Command	270
Figure 5.3.27.88 : VLAN list	270
Figure 5.3.27.89 : create VLAN 15	270

Figure 5.3.27.90 : Suspend VLAN 15	270
Figure 5.3.27.91: Configure unused ports in VLAN 15	271
Figure 5.3.27.92 : Assign VLAN into trunk port	271
Figure 6.2.1.1: Testing DNS	273
Figure 6.2.2.1: Show port-security address command	274
Figure 6.2.3.1: Show VLAN command	275
Figure 6.2.3.2: ipconfig command	275
Figure 6.2.3.3: interface trunk command	275
Figure 6.2.3.4: Show Port-security	276
Figure 6.2.3.5: Show port-security address command	276
Figure 6.2.3.6: Show physical address	277
Figure 6.2.3.7: Shows MAC address port	277
Figure 6.2.3.8: Err-Dissabled Status	277
Figure 6.2.3.9: Security violation alert	278
Figure 6.2.4.1: Show the list of certificate	278
Figure 6.2.4.2: Show the https is secure.	279
Figure 6.2.4.3: URL Testing	279
Figure 6.2.5.1: Show the log for the switch	280
Figure 6.2.5.2: Show the ping to the internet access	280
Figure 6.2.6.1: Show the login page of zabbix.	281
Figure 6.2.6.2: Show the dashboard of the zabbix.	281
Figure 6.2.6.3: Show the configuration of the Ubuntu host.	282
Figure 6.2.6.4: Show the templates of Ubuntu server.	283
Figure 6.2.6.5: Show the graph of Ubuntu server	283
Figure 6.2.6.6: Show the configuration of the Windows server host	284
Figure 6.2.6.7: Show the templates of Windows server.	285
Figure 6.2.6.8: Show the graph of Windows server	285
Figure 6.2.6.9: Show the switch's graph.	286
Figure 6.2.6.10: Show the list of host in zabbix	286
Figure 6.2.7.1: Insert identity and password	287
Figure 6.2.7.2: Wireless authentication successful	288
Figure6.2.8.1: GUI of SoftEther VPN Client Manager	289
Figure 6.2.8.2: Connect to VPN	290
Figure 6.2.8.3: Connected to VPN	290
Figure 6.2.8.4: Connection sucessful	290
Figure 6.2.8.5: Verify VPN Connection	291
Figure 6.2.8.6: Verify IP address	291
Figure 6.2.8.7: GUI of SoftEther VPN Client Manager	291
Figure6.2.8.8: Properties of G4-OutsideNet	292
Figure 6.2.8.9: Connect to VPN Server	292
Figure 6.2.8.10: VPN Connection Established	293
Figure 6.2.8.11: Verify ip address in cmd	293
Figure 6.2.9.1: Reverse Proxy Status.	294
Figure 6.2.9.2: Requested Website	294
Figure 6.2.10.1: Tftp Status	295
Figure 6.2.10.2: command to save the switch configuration.	295
Figure 62.2.11.1: show crypto ipsec sa.	296
Figure 6.2.11.2: Show crypto session	296

Figure 6.2.11.3: ping 192.168.3.2	296
Figure 6.2.12.1: Windows Error Reporting	297
Figure 6.2.12.2: Check the status of Certificate Propagation	297
Figure 6.2.12.3: Checking on NetLogon startup type	298
Figure 6.2.12.4: Show crypto ipsec sa	298
Figure 6.2.13.1: Show crypto ipsec sa	299
Figure 6.2.14.1: User Login	300
Figure 6.2.14.2: Enter User Password	300
Figure 6.2.15.1: Test Quota	301
Figure 6.2.15.2: Test Quota	301
Figure 6.2.15.3: Create new Text Document	302
Figure 6.2.15.4: Change extension fail	302
Figure 6.2.16.1: Hostname IP address on primary server	303
Figure 6.2.16.2: IP address for primary server	303
Figure 6.2.16.3: Stop DHCP from primary server	304
Figure 6.2.16.4: Wait to stop	304
Figure 6.2.16.5: DHCP failure on primary server	305
Figure 6.2.16.6: ipconfig /release	305
Figure 6.2.16.7: ipconfig /renew	306
Figure 6.2.16.8: Hostname IP address has changed	306
Figure 6.2.16.9: Virtual Machine IP Address	307
Figure 6.2.17.1: Assign VLAN	308
Figure 6.2.18.1: Status of Apache2	308
Figure 6.2.18.2: Display username and password prompt	309
Figure 6.2.18.3: Not found error displayed	309
Figure 6.2.18.5: HTTP respond	310
Figure 6.2.19.1: Ping Ubuntu	311
Figure 6.2.19.2: Snort detection	311
Figure 6.2.19.3: Snort's log file	312
Figure 6.2.20.1: Status of Samba	312
Figure 6.2.20.2: Map Network drive	313
Figure 6.2.20.3: Choose network foleder	313
Figure 6.2.20.4: File samba share	314
Figure 6.2.20.5: connecting samba from linux	314
Figure 6.2.20.6: log in samba interface	315
Figure 6.2.20.7: Run dialog box	315
Figure 6.2.20.8: Run dialog box	315
Figure 6.2.20.9: Run dialog box	316
Figure 6.2.20.10: Log in user	316
Figure 6.2.20.11: Network drive where the file saved	317
Figure 6.2.21.1: Check status of password expire	317
Figure 6.2.21.2: Check status of firewall	318
Figure 6.2.22.94: OSPF process created	318
Figure 6.2.22.2: Advertised IPv4 network.	319
Figure 6.2.22.3: Neighbor for IPv4 and IPv6 fully exchange routing information.	319
Figure 6.2.22.4: Internal client able to reach remote network	320
Figure 6.2.22.5: Internal client able to reach public network.	321

Figure 6.2.22.6: Output above shows translated IP address from internal "10.1.1.2" to "113.114.115.1" using different port number.	321
Figure 6.2.23.1: Webmail for email services	322
Figure 6.2.23.2: Login Active Directory	322
Figure 6.2.23.3: Sending email from hafiz to ammar	323
Figure 6.2.23.4: Email from hafiz received on ammar account.	323
Figure 6.2.23.5: Using telnet to list the email sent from hafiz	324
Figure 6.2.23.6: SMTP forwarded the email from hafiz to correct destination domain.	324
Figure 6.2.24.1: Create new user	325
Figure 6.2.24.2: Files in nextcloud	325
Figure 6.2.24.3: Files in nextcloud	326
Figure 6.2.24.4: Files in nextcloud	326
Figure 6.2.24.5: Login Page	327
Figure 6.2.24.6: Client dashboard	327
Figure 6.2.24.7: Files in nextcloud	328
Figure 6.2.25.1: Details of the user on the Active Directory to test	329
Figure 6.2.25.2: List of the policy that have been enable at the setting	330
Figure 6.2.25.3: List of the policy that have been enable at the setting	330
Figure 6.2.25.4: The text that have been set on the GPO once user login	331
Figure 6.2.25.5: The new user login dashboard.	332
Figure 6.2.25.6: Shared folder home that have been shared on the new user by the admin.	332
Figure 6.2.25.7: Dashboard of the new user shared folder home	333
Figure 6.2.25.8: The desktop background options are not enable for user to change	333
Figure 6.2.25.9: The desktop dashboard of the new user	334
Figure 6.2.26.1: Show the list of file created on FTP user.	335
Figure 6.2.26.2: The new file in the ftp user that have been created.	335
Figure 6.2.26.3: The dashboard of the log in user	336
Figure 6.2.26.4: The entry password dashboard in client interface.	336
Figure 6.2.26.5: The client and remote dashboard interface	337
Figure 6.2.26.6: The client is successful transfer the file from the ftp remote.	337
Figure 6.2.27.1: Testing SSH	338
Figure 6.2.27.2: Testing icmp	338
Figure 6.2.27.3: Matches on icmp increase	338
Figure 6.2.27.4: Testing telnet	339
Figure 6.2.27.5: Matches on telnet increase	339
Figure 6.2.27.6: Testing ftp	340
Figure 6.2.27.7: Matches on ftp increase	340
Figure 6.2.27.8: Saving configuration	340
Figure 6.2.28.1: group4.com website with IPv6 Address	341
Figure 6.2.28.2: Tunnel0 status	341
Figure 6.2.28.3: Ping status success	342
Figure 6.2.1.1: Testing DNS	273
Figure 6.2.2.1: Show port-security address command	274
Figure 6.2.3.1: Show VLAN command	275
Figure 6.2.3.2: ipconfig command	275
Figure 6.2.3.3: interface trunk command	275

Figure 6.2.3.4: Show Port-security	276
Figure 6.2.3.5: Show port-security address command	276
Figure 6.2.3.6: Show physical address	277
Figure 6.2.3.7: Shows MAC address port	277
Figure 6.2.3.8: err-dissabled status	277
Figure 6.2.3.9: Security violation alert	278
Figure 6.2.4.1: Show the list of certificate	278
Figure 6.2.4.2: Show the https is secure.	279
Figure 6.2.4.3: URL Testing	279
Figure 6.2.5.1: Show the log for the switch	280
Figure 6.2.5.2: Show the ping to the internet access	280
Figure 6.2.6.1: Show the login page of zabbix.	281
Figure 6.2.6.2: Show the dashboard of the zabbix.	281
Figure 6.2.6.3: Show the configuration of the Ubuntu host.	282
Figure 6.2.6.4: Show the templates of Ubuntu server.	283
Figure 6.2.6.5: Show the graph of Ubuntu server	283
Figure 6.2.6.6: Show the configuration of the Windows server host	284
Figure 6.2.6.7: Show the templates of Windows server.	285
Figure 6.2.6.8: Show the graph of Windows server	285
Figure 6.2.6.9: Show the switch's graph.	286
Figure 6.2.6.10: Show the list of host in zabbix	286
Figure 6.2.7.1: Insert identity and password	287
Figure 6.2.7.2: Wireless authentication successful	288
Figure 6.2.8.1: GUI of SoftEther VPN Client Manager	289
Figure 6.2.8.2: Connect to VPN	290
Figure 6.2.8.3: Connected to VPN	290
Figure 6.2.8.4: Connection sucessful	290
Figure 6.2.8.5: Verify VPN Connection	291
Figure 6.2.8.6: Verify IP address	291
Figure 6.2.8.7: GUI of SoftEther VPN Client Manager	291
Figure 6.2.8.8: Properties of G4-OutsideNet	292
Figure 6.2.8.9: Connect to VPN Server	292
Figure 6.2.8.10: VPN Connection Established	293
Figure 6.2.8.11: Verify ip address in cmd	293
Figure 6.2.9.1: Reverse Proxy Status.	294
Figure 6.2.9.2: Requested Website	294
Figure 6.2.10.1: Tftp Status	295
Figure 6.2.10.2: command to save the switch configuration.	295
Figure 6.2.11.1: show crypto ipsec sa.	296
Figure 6.2.11.2: Show crypto session	296
Figure 6.2.11.3: ping 192.168.3.2	296
Figure 6.2.12.1: Windows Error Reporting	297
Figure 6.2.12.2: Check the status of Certificate Propagation	297
Figure 6.2.12.3: Checking on NetLogon startup type	298
Figure 6.2.12.4: Show crypto ipsec sa	298
Figure 6.2.13.1: Show crypto ipsec sa	299
Figure 6.2.14.1: User Login	300
Figure 6.2.14.2: Enter User Password	300

Figure 6.2.15.1: Test Quota	301
Figure 6.2.15.2: Test Quota	301
Figure 6.2.15.3: Create new Text Document	302
Figure 6.2.15.4: Change extension fail	302
Figure 6.2.16.1: Hostname IP address on primary server	303
Figure 6.2.16.2: IP address for primary server	303
Figure 6.2.16.3: Stop DHCP from primary server	304
Figure 6.2.16.4: Wait to stop	304
Figure 6.2.16.5: DHCP failure on primary server	305
Figure 6.2.16.6: ipconfig /release	305
Figure 6.2.16.7: ipconfig /renew	306
Figure 6.2.16.8: Hostname IP address has changed	306
Figure 6.2.16.9: Virtual Machine IP Address	307
Figure 6.2.17.1: Assign VLAN	308
Figure 6.2.18.1: Status of Apache2	308
Figure 6.2.18.2: Display username and password prompt	309
Figure 6.2.18.3: Not found error displayed	309
Figure 6.2.18.5: HTTP respond	310
Figure 6.2.19.1: Ping Ubuntu	311
Figure 6.2.19.2: Snort detection	311
Figure 6.2.19.3: Snort's log file	312
Figure 6.2.20.1: Status of Samba	312
Figure 6.2.20.2: Map Network drive	313
Figure 6.2.20.3: Choose network foleder	313
Figure 6.2.20.4: File samba share	314
Figure 6.2.20.5: connecting samba from linux	314
Figure 6.2.20.6: log in samba interface	315
Figure 6.2.20.7: Run dialog box	315
Figure 6.2.20.8: Run dialog box	315
Figure 6.2.20.9: Run dialog box	316
Figure 6.2.20.10: Log in user	316
Figure 6.2.20.11: Network drive where the file saved	317
Figure 6.2.21.1: Check status of password expire	317
Figure 6.2.21.2: Check status of firewall	318
Figure 6.2.22.94: OSPF process created	318
Figure 6.2.22.2: Advertised IPv4 network.	319

LIST OF TABLE

Table 1: Windows Server	5
Table 2 : Ubuntu	6
Table 3: Services and Corresponding Person-In-Charge	38

CHAPTER 1: INTRODUCTION

1.1 Introduction

This Workshop II (BITU 3923) is a required subject that must be taken by every student of the Faculty of Information and Technology, UTeM. It was first being introduced to all third year students of Bachelor Degree as a platform to prepare them before undergo their Final Year Project and Industrial Training. During Workshop II, the students will be working in a group. They will be needed to develop a project based on their course. Workshop II provides an opportunity for the students to practice their knowledge and gain experience from their previous subject taken. Students are also be able to develop their understanding in problem solving techniques to solve problem based on their demanded project.

The main goal for this Workshop II is to let the students design the network infrastructure by using available basic equipment and be able to put into selected network services and also to install and integrate network services infrastructure to suit the network environment while maintaining and control the network services infrastructure. Students from BITZ should be able to input the security features into networking infrastructure. The group of Workshop II consists of 9 students, 6 students from BITC and 3 students from BITZ. We have been given the equipment that consists of three servers, 1 Cisco 2811 router (2 Fast Ethernet), one Cisco 2960 manageable switch, 15 meters UTP cable, 12 pieces of RJ-45 and one set crimping tool.

By using the equipment above, we are needed to design, set up, maintain and monitor a network environment with basic server applications and basic services. There are 18 network services and 12 security services are required to be implement in the network infrastructure. Three operating systems are used in the servers which are Microsoft Windows Server 2012, Ubuntu 16.04 and Debian.

1.2 Objective

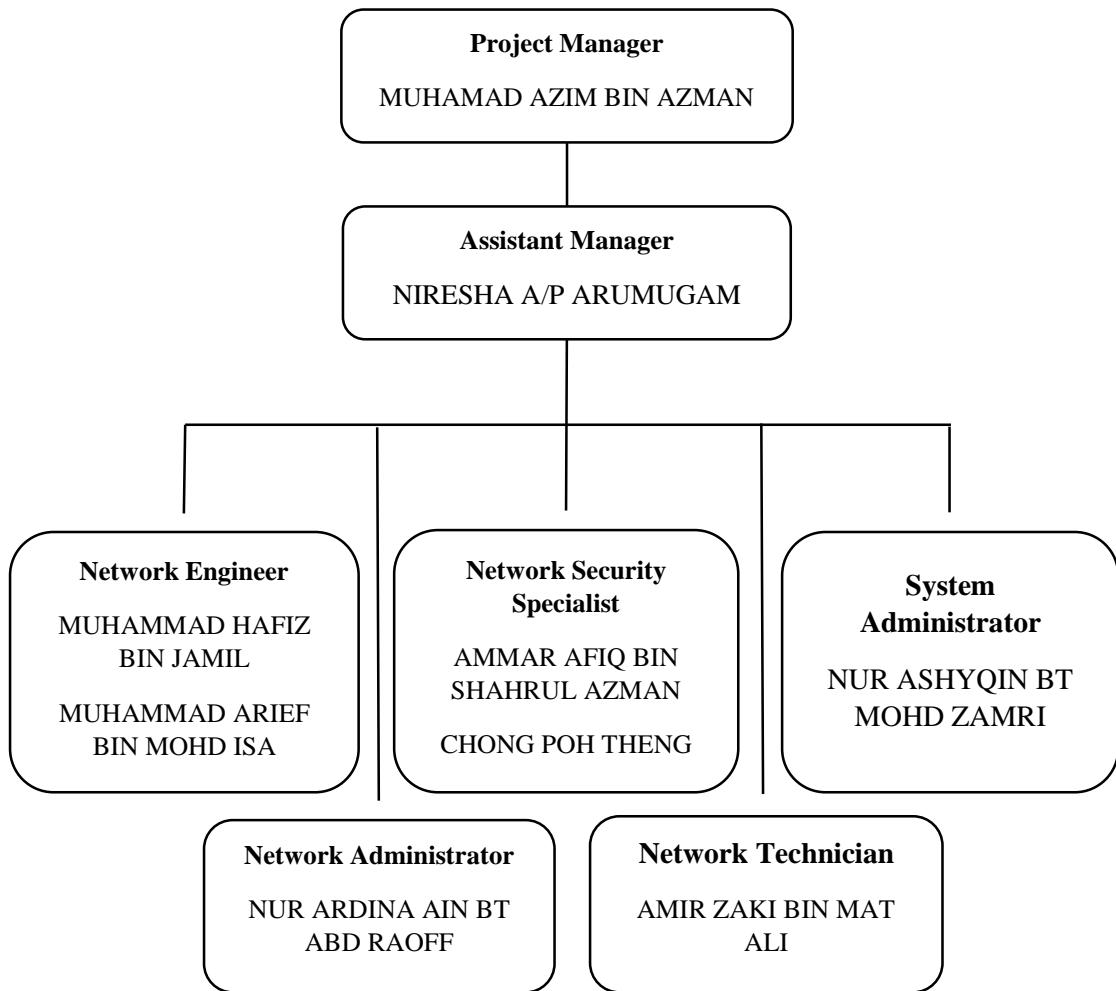
The main objectives of our group in Workshop II are:

- 1) To build and configured the network environment with 30 services including 18 services of network services and 12 services of security services..
- 2) To make sure the security services that had been chosen compatible with the network infrastructure.
- 3) To secure all the server from any possible threat that can disrupt the network infrastructure.

1.3 Project Plan

In week 1 and 2, we will submit a proposal to Dr. Zurina Binti Sa'aya for the approval. So that we can borrow the equipment that we all needed for our workshop 2 subject. The equipment that we borrowed such as routers, switch and servers from the faculty. Then we will setup all the hardware by following the physical network design that have been planned. During week 2 until week 5, we will proceed to set up the services needed for this project. There are 8 services that we plan to install during this period. The services include DNS, DHCP, Inter VLAN and VLSM addressing, Active directory, Server virtualization, service for video and Security Policy. From week 6 to week 10, we plan to proceed to set up the 27 other services. The services are; IPsec between server and user, proxy server, install Samba Security services, set up web, SSL and virtual hosting and wireless user authentication using radius server. During week 11 to week 12, we will proceed towards completing the setup of the whole network and setup of all services required. At the same time, 3 we prepared a video and a poster that shows one of the services that has been set up. After the completion of the network, we will demonstrate our respective task individually to the supervisor and evaluator while the video and poster prepared will be presented during the project demonstration for the purpose of updates for the final exhibition at week 14. At week 13, the final report and individual log book been revised if there is any error and improved. At week 14, will be a video and poster exhibition for workshop 2. The completed video and poster will be evaluated by the supervisors and evaluator.

1.4 Organization Chart



1.5 Conclusion

As a conclusion, the benefit that we will gained from this project is, we will able to apply the theory that we have learnt in subject Internet Technology, Local Area Network, Wide Area Network, Operating System, Network Analysis, Design and Computer Organization and Structure into this project. The practically practice from this project would give us the fact of real working environment that definitely would help us to solve problem especially about networking. We will further understand how to implement each network service and network security in this project. If there is a problem, we are able to solve it by discuss it in a group.

CHAPTER 2: PROJECT REQUIREMENT

2.1 Introduction

In this Workshop II, we have been provided with basic equipment such as three servers with combination of different platforms, 1 Cisco 2811 router (2 Fast Ethernet), 1 Cisco 2960 manageable switch, 15 meter UTP cable, 12 pieces of RJ45 and one set of crimping tool. By using the equipment provided above, we are required to design a secure network infrastructure. The network to be developed will be consists of 30 services that will be divided among three servers. There are 18 services for computer networking and 12 services for computer security students that are required to be implement in the network infrastructure.

2.2 Types of Operating System

Operating system (OS) is the software that allows a user to run other applications on the computing device. The operating system manages a computer's hardware resources, including the input and output devices, network devices and storage devices. OS also provides services to facilitate the efficient execution and management of, and memory allocations for, any additional installed software application programs. There are three different servers with different platform of operating system being used in this project. The operating systems uses in the project are:

- i. Windows Server 2012 R2
- ii. Ubuntu 16.04
- iii. Debian

2.3 Operating System Background

2.3.1 Windows Server 2012 R2

Windows Server 2012 being used because it can support many services including all the basic services used in this project. Thus, it is the most stable and familiar OS that can we used compared others. The operating system is also built to run constantly and packed with all the basic features required to run a server.

Server Configuration	
Processor	2 GHz or faster
Memory	2 GB or greater
Operating System	Window Server 20012 R2
Chassis Configuration	Tower Chassis Orientation
Hard Drive	40 GB or greater
Drive	DVD-ROM drive
Display	Super VGA (800 × 600) or higher resolution monitor

Table 1: Windows Server

2.3.2 Ubuntu

Ubuntu is an open source operating system for software and also supported on network server and personal computer. The package is always updated. Every Ubuntu packages that had update are security fixes, high-impact bug fixes and conservative, substantially beneficial low risk bug fixes.

Ubuntu supports multiple workspaces and it also provides an enterprise administrative tool of its own that can perform tasks. It also installs some hardware drivers that are available only in binary format, but such packages are clearly marked in the restricted component. Intuitive dash interface making it easy to find applications, files and other things with a great set of keyboard shortcuts.

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 2: Windows Server

2.3.3 Debian 9.3

The Debian Project is an association of individuals who have made common cause to create an open source operating system. Debian has access to online repositories that contain over 51,000 packages making it the largest collection of software in the world. Debian officially contains only free software, but non-free software can be downloaded and installed from the Debian repositories. At the core of an operating system is the kernel. Debian systems currently use the Linux kernel or the FreeBSD kernel. Linux is a piece of software started by Linus Torvalds and supported by thousands of programmers worldwide. So, the Debian OS can be stable as it quite popular OS server also it has all the services need in this project.

2.4 Hardware Requirement

In Workshop II, we have been provided with the equipment which are four desktop computers, one Cisco 1941 router (2 Gigabit Ethernet), one Cisco 2960 manageable switch, 15 meters UTP cable, one set crimping tool, one NIC, and one Access Point. These hardware are 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.

2.5 Hardware Justification

2.5.1 Router

A router is a networking device that forwards data packets between computer networks. A router is connected to two or more data lines from different networks. (NAT and Routing). Wire-speed performance for concurrent services such as security and voice, and advanced services to multiple T1/E1/xDSL WAN rates. Optional Layer 2 switching support with Power over Ethernet (PoE) (as an option)

- Security: Antivirus defence support through Network Admission Control (NAC) o Support of up to 1500 VPN tunnels with the AIM-EPII-PLUS Module o Intrusion Prevention as well as stateful Cisco IOS Firewall support and many more essential security features
- Voice: Analog and digital voice call support Optional support for Cisco Call Manager Express for ocal call processing in stand-alone business for up to 36 IP Phones. Optional voice mail support

2.5.2 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.

2.5.3 Unshielded Twisted Pair (UTP Cable)

We are given 15 meters UTP cable in Workshop II. UTP cable is a type of wiring in which two conductors of a single circuit are twisted together for the purposes 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.

2.5.4 RJ-45 Connector

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

2.5.5 Ethernet Cable

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) 568A (Cross-Over cable)
 - Connect between router and router (NAT and Routing)
 - Connect between servers (Testing services)
- 2) 568B (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.

2.5.6 Crimping Tool

A crimping tool is a tool used to fastening a connector as far as possible of a link. While creasing the link, we need to choose which link type we should utilize: straight through or hybrid. At the point when the link is utilized to interface two gadget at various system layer e.g. change to switch, we should utilize straight through link. When we interface two gadgets at same system layer, e.g. change to switch, we should utilize hybrid link. A cable tester is provided to ensure the cable is functional.

2.6 Conclusion

For the completion of this Workshop II, we have to define, design, implement and manage the network services. Before installing the Operating System needed, one should ensure that the computer meet the requirements. It tends to be 15 complicated to coordinate three different type of Operating System with 30 distinct administrations and design in a system foundation. We need to think about the similarity and execution of the server and choose which benefit have a place with which server.

CHAPTER 3: DESIGN

3.1 Introduction

In this Workshop II, we have to define, design, implement and manage the network services. Each group in this Workshop II will be design their own security policy, physical network and logical network. Design phase is very crucial phase during the development process. The network design that we had done is based on Workshop II requirements, we need to set up a LAN (Local Area Network) which consists of three servers, one router, one switch and one client.

3.2 Security Policy

Security policy is a document that states in writing how a company plans to protect the company's physical and information technology assets. Security policy is the document that will be continuously update as the technology and employee requirement change.

There are several factors that security policy must follow, such as:

- i. It must provide the mission statement for the security
- ii. Developed to integrate security into all business functions and process
- iii. The policies must be review and modify as the company changes
- iv. It should represent business objectives.

There are three types of security policy:

- i. Regulatory policy: regulatory is the policy that follows the standards by specific industry regulations. This are the policies that an organization must implement due to compliance, regulation, or other legal requirements.
- ii. Advisory policy: These policy are not mandatory but strongly suggested for the behaviours and the activities of the employees that takes place within the organization.
- iii. Informative: The policies that exist to inform the reader or the user within the company or outside the company.

The main objective of the security policy are:

- i. To protect the company integrity, security, validity and the confidentiality of the data and the system
- ii. To ensure the smoothness of the company's operation and to minimize the damage or destruction to the company assets and network.
- iii. To prevent the misuse of the company assets and network.

3.2.1 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.

3.2.2 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.

3.2.3 Password Creation

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

3.2.4 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.

3.2.5 Server security policy

- Any services or applications that not being used should be disabled.
- Access to any services should be logged and protected through access-control methods such as firewall.
- The server’s operating system must be configured to prevent security weakness.
- If a methodology for secure channel connection is available privileged must be performed over secure channels.
- The servers must be located in an access-controlled area.

3.2.6 Router and Switch Security Policy

- The enable passwords on all router and switch must be encrypted.
- Access control lists must be used to limit sources and to reduce the risk of being infected by any threats from outside.
- All routing updates need to be done using secure routing updates.
- Router must be secured with password at both login mode and privileged mode.

- Apply login mode password on Console, AUX, and VTY (telnet/ssh).
- Set a correct time and date to ensure the log are correct.
- Make a complex password. Make sure to always use type 5 password encryption on the router.
- Use RADIUS for all user authentication.

3.2.7 Remote Access Policy

- It is a responsibility for any company with remote access privileges to other company's network to ensure that their access connection is given the same consideration.
- General access to the internet for recreational use through the company's networks strictly limited for the group member (refer to as "Authorized User").
- Secure remote access must be strictly controlled with strong and encrypted passwords.
- All hosts that are connected to the internal networks via remote access must use the up-to-date antivirus. All third party connections must comply with requirements.

3.2.8 Application Security

3.2.8.1 Hardening Service Policy

Hardening is the service that was provided in every server that we have. This hardening policy that each server must have are:

- i. Access Security
- ii. DNS Service Policy
- iii. Service Policy
- iv. Proxy Server Service Policy
- v. Authentication using Radius Server Service Policy.
- vi. User authentication and authorization Service Policy.

- vii. Secure file transfer protocol Service Policy.
- viii. Virtual private network (VPN) Service Policy.
- ix. Domain Name System.
- x. Samba Security.

3.2.8.2 Access Security

- 1) All physical entrance and video surveillance for any server access will be recorded.
- 2) The server access is governed by firewall.
- 3) Web server hardening:
 - Configure authorization rules.
 - Secure socket layer.
 - Configure server certificates.
 - Enable authentication.

3.2.8.3 DNS Service Policy

- a) DNS servers are configured to listen to specific IP addresses.
- b) Secure dynamic update is allowed for all DNS zones.
- c) All DNS servers in the network perform standard DNS resolution.
- d) All DNS servers limit transfer zone to servers listed in their zone records.

3.2.8.4 VLAN Service Policy

- a) VLAN must have at least one active port for a service policy to be configured.
- b) ACL logs can only support logging levels of 3 or later..
- c) Only one log message will be displayed until the flow stops and the rest is displayed later.
- d) TCAM (Ternary Content-Addressable Memory) must have enough free entries to configure the service policy on the VLAN.

3.2.8.5 Proxy Server Service Policy

- a) Port used for proxy server is 8080 and any unsecured website will be block.
- b) Ensuring appropriate types of authorization are used to access the services.
- c) Only allow certain clients to have the access to the proxy based on IPs.

3.2.8.6 Secure File Transfer Protocol (SFTP) Service Policy

- a) Disable anonymous access.
- b) Enable logging.
- c) Harden using access-list.
- d) Setup ftp site as blind put.
- e) Login time restriction.
- f) Restrict access by IP.
- g) Enable account lockout and account lockout threshold.

3.2.8.7 Virtual Private Network (VPN) Service Policy

- a) VPN should be use a one-time authentication.
- b) VPN user should be auto-disconnected after sometime of inactivity.
- c) Only one tunneling connection is allowed.
- d) Unauthorized user are not allowed to access internet network.

3.2.8.8 Authentication using Radius Server Service Policy

- a) RADIUS is a client/server protocol.
- b) Communications between a Network Access Server(NAS) from server to client.
- c) RADIUS server is based on the User Datagram Protocol(UDP).
- d) The protocol is consider a connectionless service.
- e) Router or switch can be the host for RADIUS.
- f) Access-Request packet contains username, encrypted password, NAS IP address and port.
- g) User login consists of a query (Access-Request) from the NAS to the RADIUS server and a corresponding response (Access-Accept or Access-Reject) from the server.
- h) RADIUS using UDP port number 1645 or 1812 for authentication port.
- i) It can support PPP, PAP, CHAP, UNIX login and other authentication mechanisms.
 - i. PAP: Password Authentication Protocol normally used with MAB and some devices use PAP for Web authentications.
 - ii. CHAP: Challenge Handshake Authentication Protocol. The username and the password are encrypt using a challenge sent from the server. CHAP was not often used with network access.

3.2.8.9 Active Directory Security Policy

- a) Change password every three months.
- b) Delete account when no log in activity more than one month.
- c) Only active directory user that being assigned by the administrator can have the access to use USB in Windows Client PC.
- d) Normal user cannot have the access to command prompt.

3.2.8.10 Samba Security

Several methods of authentication are apply:

- a) User-level authentication
Verifies user's username and password to allow access to the folder that being shared.
- b) Host-based protection
Use hosts allow and hosts deny command to access server from a specific range off networks. In our project, we allow network from VLAN Clients and VLAN Windows Server to access the Samba server.

3.3 Physical Security

Physical security can often 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
 - Each unit shall be distinctly and uniquely identified on all visible sides. Machines shall be housed in secured facilities (caged or locked).

2. Media

- Provisioning New storage media (whether disk or removable) shall be securely erased and reformatted before use.

3. Physical access

- 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.
- Access Authorization (Access to physical equipment must be authorized).
- Access Logging (All physical accesses are logged and reported to all).

3.4 Physical Design

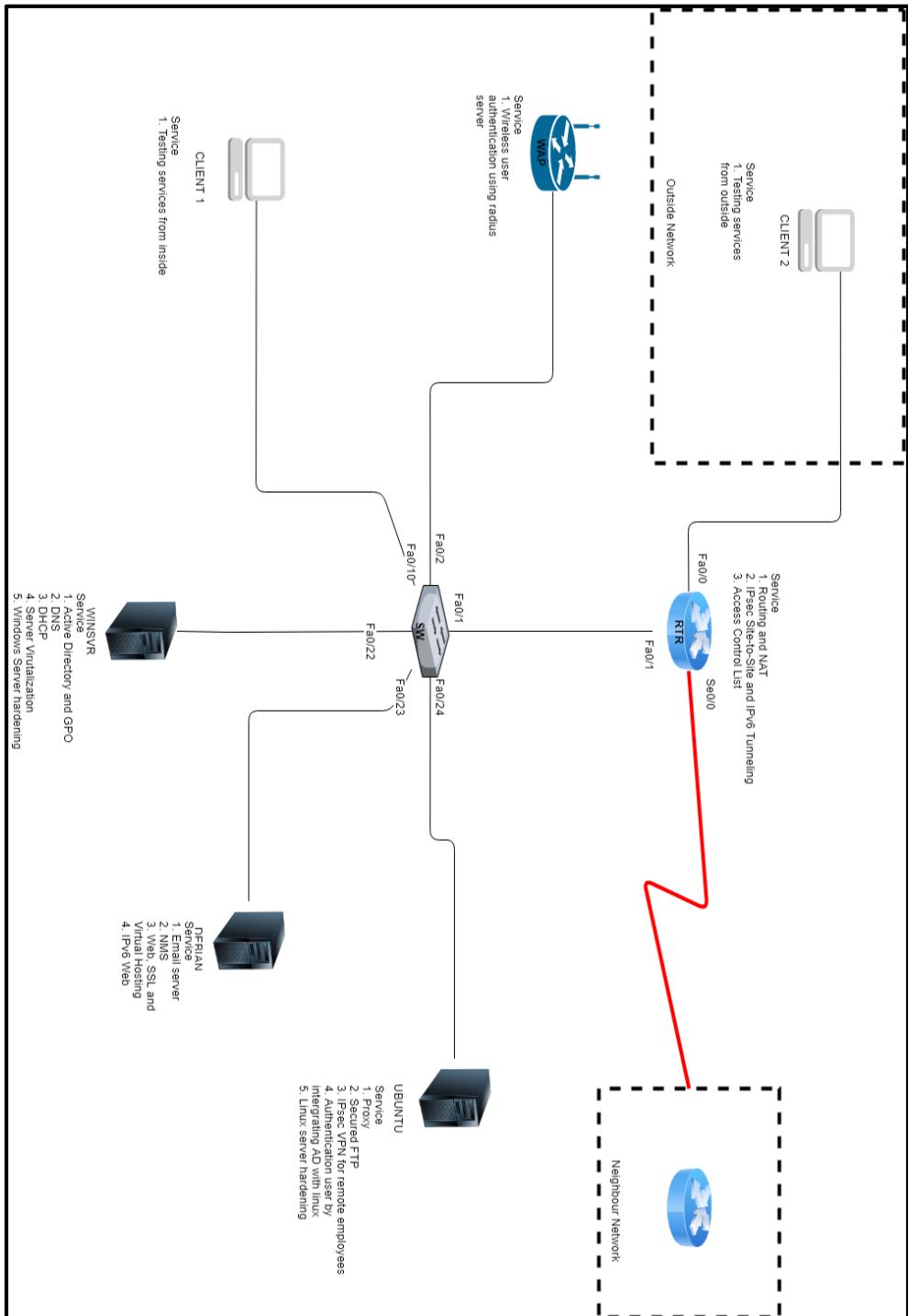


Figure 3.4.1: Physical Design

3.5 Logical Design

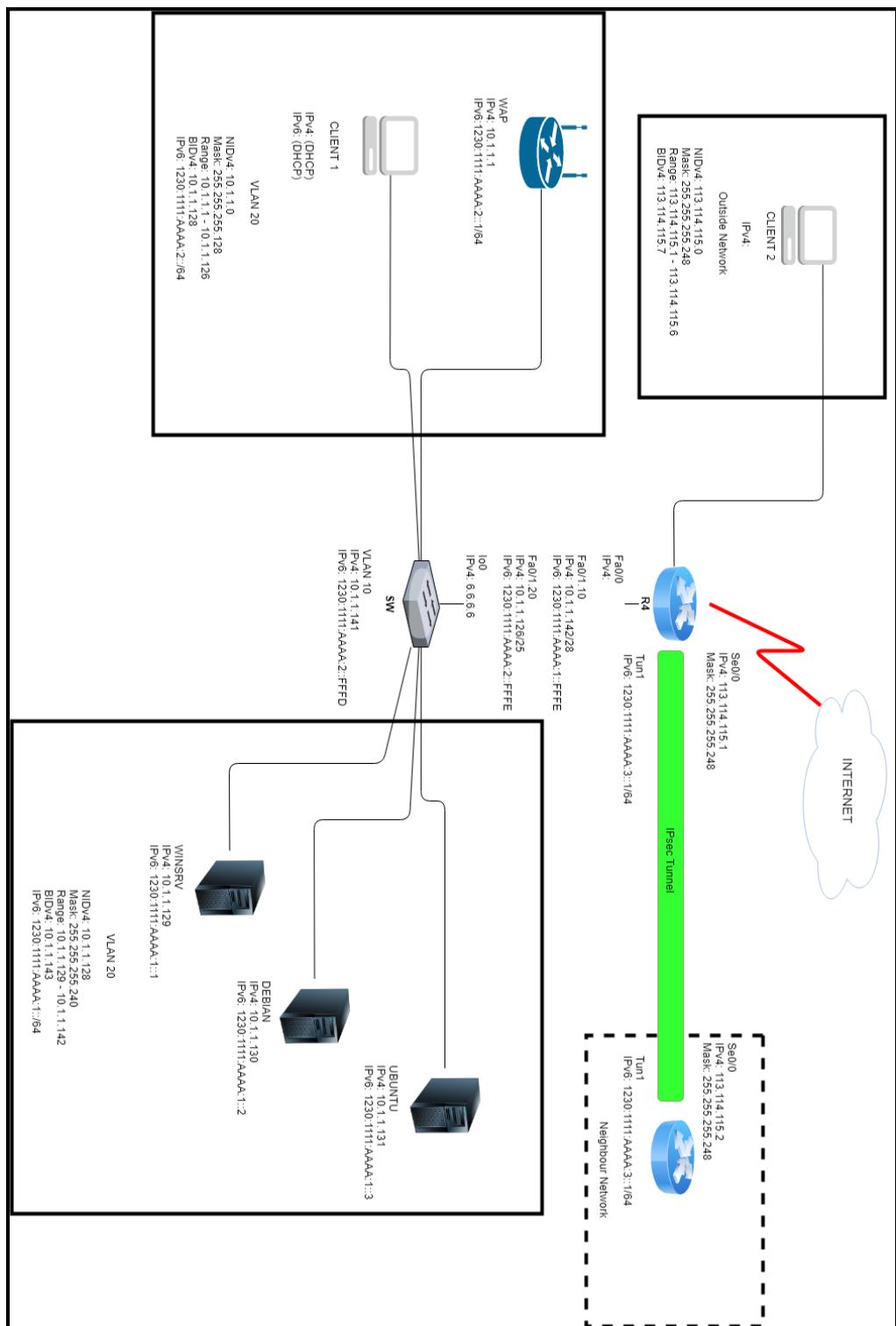


Figure 3.5.1: Logical Design

3.6 Conclusion

Network design is an important part before creating a real network. The first step of implementing a network design are the physical and logical design. A good network design must be functional, expandable for future implementation and should be easy to be maintain. A good network infrastructure design also must include the planning of the network complexity, redundancy, standards and maintenances factor. After considering on those factors, we will implement the design that we had discussed and being approve by our supervisor to the next level.

CHAPTER 4: SERVICES

4.1 Introduction

This chapter will provide a list of services that will be implemented by our group to fulfil the requirement for Workshop II. We will also provide a brief overview of the services that will be implemented.

4.2 List of Services

- 1) DNS (IPv4 & IPv6)
- 2) DHCP (IPv4 & IPv6)
- 3) Active Directory
- 4) Secured FTP
- 5) Web, SSL & Virtual Hosting
- 6) Linux Email Server
- 7) Linux Server Hardening
- 8) Syslog
- 9) IPv6 Web with IPv6 Tunneling
- 10) Dynamic Routing & NAT
- 11) Proxy Server
- 12) Samba
- 13) Network Management System
- 14) Server Virtualization
- 15) Web Hardening
- 16) Access Control List
- 17) Windows Server Hardening
- 18) Authentication user by integrating AD with Linux
- 19) Wireless user authentication using RADIUS server
- 20) IDS with port mirror
- 21) IPsec VPN for remote employees
- 22) VLAN & Port Security
- 23) TFTP

- 24) IPsec site-to-site
- 25) Quota Screening
- 26) AAA
- 27) Cloud Server
- 28) InterVlan Routing
- 29) VLSM Addressing
- 30) Security Policy

4.3 Brief Overview of the Services

4.3.1 Domain Name System (IPv4 & IPv6)

Domain Name System (DNS) is a hierarchical distributed naming system for computers and services. DNS is a service that translates internet domain and host names to respective IP addresses. This is necessary because domain names are easy for people to remember, computers or machines, access websites or network resources based on IP addresses.

4.3.2 Dynamic Host Configuration Protocol (IPv4 & IPv6)

DHCP (Dynamic Host Configuration Protocol) is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers configured for a given network. DHCP assigns a local IP address to devices connected to the local network from DHCP address pool. Network clients will be configured automatically by the DHCP service. When a computer uses a static IP address, it means that the computer is manually configured to use a specific IP address. Using DHCP to dynamically assign IP addresses minimizes these conflicts.

4.3.3 Active Directory

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.

4.3.4 Secured FTP

Very Secure File Transfer Protocol Daemon (VSFTPD) is a secure version of File Transfer Protocol (FTP), it is a GPL licensed FTP server for UNIX systems. It is secure and extremely fast and stable. VSFTPD is a mature and trusted solution which support virtual users with PAM (pluggable authentication modules). 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. VSFTPD is essential as a mean to transfer files between servers and client or network equipment without compromising on security and confidentiality.

4.3.5 Web, SSL & Virtual Hosting

SSL(Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. Virtual hosting is a method for hosting multiple domain names on a single server. This allows one server share its resources such as memory and

processor cycles, without requiring all services provided to use the same host name. The term virtual hosting is usually used in reference to web servers but the principles do carry over to other internet services. Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network. As the Internet Information Services (IIS) Manager is already been downloaded, proceed to open the IIS Manager to request certificate at Windows server.

4.3.6 TFTP

Trivial File Transfer Protocol (TFTP) is a simple protocol used for transferring files. TFTP uses the User Datagram Protocol (UDP) to transport data from one end to another. TFTP is mostly used to read and write files/mail to or from a remote server. TFTP is very useful for boot computers and devices that do not have hard disk drives or storage devices because it can easily be implemented using a small amount of memory. Data transfer through TFTP is usually initiated through port 69. However, the data transfer ports are selected by the sender and receiver when the connection is initialized.

4.3.7 Linux Mail Server

The backbone of the mail system is the Mail Transport Agent (MTA). It will handle message transfer agent software that transfers electronic mail messages from one computer to another using a client–server application architecture. MTA implements both the client (sending) and server (receiving) portions of the Simple Mail Transfer Protocol. Mail is read either through direct access (shell login) or mailbox protocols like POP and IMAP.

4.3.8 Inter VLAN and VLSM addressing

Virtual Local Area Network (VLAN) is a broadcast domain that is partitioned in a computer network at the data link layer. It is to subdivide a network into virtual LAN, one configures a network switch or router. Variable Length Subnet Masks (VLSM) is a technique that allows network administrator to divide an IP address to subnets into different sizes.

4.3.9 Syslog

Syslog stands for System Logging Protocol and is a standard protocol used to send system log or event messages to a specific server, called a syslog server. It is primarily used to collect various device logs from several different machines in a central location for monitoring and review. Syslog uses the UDP protocol on port 514 but can be configured to use any port. Syslog packet transmission is asynchronous. What causes a syslog message to be generated is configured within the router, switch, or server itself. Unlike other monitoring protocols, such as SNMP, there is no mechanism to poll the syslog data. In some implementations, SNMP may be used to set or modify syslog parameters remotely.

4.3.10 IPSec site-to-site tunnelling

IPSec site-to-site tunneling is a security feature that allow to create secure communication link also called VPN Tunnel between two different networks located at different sites. Site-to-Site IPSec VPN Tunnels are used to allow the secure transmission of data, voice and video between two sites (e.g offices or branches). The VPN tunnel is created over the Internet public network and encrypted using a number of advanced encryption algorithms to provide confidentiality of the data transmitted between the two sites.

4.3.11 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.

4.3.12 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 component of firewall. Proxy server provides security and able to improve performance through caching in the network.

4.3.13 Network Management System

NMS is combination of hardware and software that allows an IT professional to supervise the individual components of a network within a larger network management framework. Network monitoring is part of NMS which is constantly monitors a computer network for slow or failing components and that notifies the network administrators (via email, SMS or other alarms) in case of outages. In order to monitor the network, our group has decided to use Nagios monitoring tool. Nagios is a monitoring tool that will monitor the entire IT infrastructure to ensure systems, applications, services and business processes are functioning properly. In the event of a failure, Nagios will be sending an alert to notify the user when there is a problem arise.

4.3.14 Server Virtualization

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

4.3.15 Security Policy

Security policy is a secure for the system, organization or other entity which come in a set of rules defining who is authorized to access what and under which conditions, and the criteria under which such authorization is given or cancelled. For systems, the security policy addresses constraints on functions and flow among them, constraints on access by external systems and adversaries including programs and access by external systems and adversaries including programs and access to data by people. For an organization, it addresses the constraints on behavior of its members as well as constraints imposed on adversaries by mechanisms such as doors, locks, keys and walls. Mostly, security policy will be update from time to time, as technology and system requirements always changing.

4.3.16 Linux Server Hardening

Hardening is a process of securely configuring vulnerability point of a system like there maybe unused port, services or useless software running that may create vulnerability point in the system. This vulnerability point may be used by others to enter the system. For example in Linux systems there is a file called /etc/hosts to allow or disallow users as a policy. So, it may need to change the permissions of this file chmod 700 /etc/hosts.allow or chmod 000 /etc/hosts.allow. Below are the primary ways to hardening linux and to prevent attackers from gaining access to the systems:

- Encrypt all data transmitted over the network. Encrypting authentication information (such as passwords) is particularly important.
- Minimize the amount of software installed and running in order to minimize vulnerability.
- Use security-enhancing software and tools whenever available (e.g SELinux).
- Run each network service on a separate server whenever possible. This minimizes the risk that a compromise of one service could lead to a compromise of others.
- Maintain user accounts. Create a good password policy and enforce its use. Delete unused user accounts.
- Review system and application logs on a routine basis. Send logs to a dedicated log server. This prevents intruders from easily avoiding detection by modifying the local logs.
- Never log in directly as root, unless absolutely necessary. Administration should use sudo to execute commands as root when required.

4.3.17 Windows Server Hardening

Windows Server 2012 operating system reduces the attack surface by disabling functionality that is not required while maintaining the minimum functionality that is required. This service is to implement secure procedures from the initial installation. New machines should be installed on an isolated network, well protected from possible hostile traffic until the operating system is hardened. Step to harden the Windows Server:

- Configure a security policy
- Disable or delete unnecessary accounts, ports and services Uninstall Unnecessary Applications
- Configure the windows 2012 Firewall Configure Auditing
- Disable unnecessary shares

- Configure Encryption on 2012 server Updates amp; Hot fixes
- Anti-Virus amp; NAP Least Privilege

4.3.18. Authentication user by integrating AD with Linux

Active Directory (AD) serve 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 34 type, assigning and enforcing security policies for all computers in a network and installing or updating software on network computers. Active directory uses Lightweight Directory Access Protocol (LDAP) version2.3 and DNS. At this project, we need to integrate Active Directory with Linux.

4.3.19 Wireless user authentication using Radius server

Remote Authentication Dial-In User Service (RADIUS) is a client, server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it's easier to track usage for billing and for keeping network statistics.

4.3.20 IDS with Port Mirror

An intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. Anomaly detection and reporting is the main function, certain IDS are capable of taking actions when malicious activity or anomalous traffic in network is

detected and also blocking traffic sent from suspicious IP addresses. It is also will log any packet flow whether suspicious websites, blacklisted IP or any breach attempt. Port mirroring is a method of monitoring network traffic. With port mirroring enabled, the switch sends a copy of all network packets seem on one port or an entire VLAN to another port, where the packet can be analyzed. Its function is best described when comparing regular switch and switch mirroring support. With regular switch the network traffic is visible only to computers, which directly participate in a communication. Other computers do not see the traffic that is not destined for them.

4.3.21 IPSec VPN for remote employees

IPSec (Internet Protocol Security) is a framework for a set of protocols for security at the network or packet processing layer of network communication. It helping to ensure private, secure communications over Internet Protocol (IP) networks through the use of cryptographic security services. IPSec supports network-level data integrity, data confidentiality, data origin authentication, and replay protection. Because IPSec is integrated at the Internet layer (layer 3), it provides security for almost all protocols in the TCP/IP suite, and because IPSec is applied transparently to applications, there is no need to configure separate security for each application that uses TCP/IP. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. The uses of IPsec are to fulfil security requirements, or simply enhance the security of your application. IPsec helps provide defence-in-depth against:

- Network-based attacks from untrusted computers, attacks that can result in the denial of-service of applications, services, or the network
- Data corruption
- Data theft
- User-credential theft
- Administrative control of servers, other computers, and the network.

4.3.22 Samba Security

Samba is an open-source software that runs on UNIX or Linux based platforms to enable communication with Windows clients like a native application. It is provided secure, stable and fast file and print services for all clients by employing the Common Internet File System (CIFS). At the heart of CIFS is the latest incarnation of the Server Message Block (SMB) protocol, which has a long and tedious history. Samba acts similar as File Transfer Protocol (FTP) but the advantage of Samba is Client and Server can simply communicate between them without need authorization. This is the reason why Samba needs to be more secure in terms of internetworking.

4.3.23 VLAN & Port Security

Port Security is a dynamic feature that can be used to limit and identify the MAC addresses of the stations that allow access to the same physical port. When an administrator assigns secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses. If a port is configured as a secure port and the maximum number of secure MAC addresses is reached, a MAC address of a station attempting to access the port that is different from any of the identified secure MAC addresses triggers a security violation. To configure port security, three steps are required:

1. Define the interface as an access interface by using the switch port mode access interface subcommand
2. Enable port security by using the switch port port-security interface subcommand
3. Define which MAC addresses are allowed to send frames through this interface by using the switch port port-security mac-address MAC_ADDRESS interface subcommand or using the switchport, port security mac-address sticky interface subcommand to dynamically learn the MAC address of the currently connected host.

A virtual LAN (Local Area Network) is a logical subnetwork that can group together a collection of devices from different physical LANs. Larger business computer networks often set up VLANs to re-partition their network for improved traffic management. When deploying VLANs, here are five key considerations to address:

1. Links on VLAN switches
2. Native VLAN, ISL and 802.1Q
3. Virtual trunk protocol and VTP pruning

4.3.24 AAA

Authentication, authorization, and accounting (AAA) is a term for a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. Authentication provides a way of identifying a user, typically by having the user enter a valid user name and valid password before access is granted. After logging into a system, for instance, the user may try to issue commands. The authorization process determines whether the user has the authority to issue such commands. Simply put, authorization is the process of enforcing policies: determining what types or qualities of activities, resources, or services a user is permitted. Accounting is carried out by logging of session statistics and usage information and is used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities.

4.3.25 Quota Screening

A disk quota provides a fixed and limited amount of storage. Disk quotas are assigned to home directories, file shares and email mailboxes. By assigning quotas, no single user or area can consume enough space to cause an outage to the system or impact other users. Configure file screens with File Server Resource Manager (FSRM) in Windows Server 2016 to automatically deny users from saving files with a specific file extension or string in the file name.

While this can be useful to a degree, a savvy user will be able to simply modify the file name or extension and save the file anyway, as the contents of the files themselves are not checked with this feature of FSRM.

4.3.26 Cloud Server

A cloud server is a virtual server (rather than a physical server) running in a cloud computing environment. It is built, hosted and delivered via a cloud computing platform via the internet, and can be accessed remotely. They are also known as virtual servers. Cloud servers have all the software they require to run and can function as independent units. Cloud servers are stable, fast and secure. They avoid the hardware issues seen with physical servers, and they are likely to be the most stable option for businesses wanting to keep their IT budget down.

4.3.27 Access Control List

Access Control Lists “ACLs” are network traffic filters that can control incoming or outgoing traffic. ACLs work on a set of rules that define how to forward or block a packet at the router’s interface. An ACL is the same as a Stateless Firewall, which only restricts, blocks, or allows the packets that are flowing from source to destination. The devices that are facing unknown external networks, such as the Internet, need to have a way to filter traffic. So, one of the best places to configure an ACL is on the edge routers.

4.3.28 Web Hardening

Windows Server hardening involves identifying and remediating security vulnerabilities. Security is complex and constantly changing. This standard was written to provide a minimum standard for the baseline of Window Server Security and to help Administrators avoid some of the common configuration flaws that could leave systems more exposed. This hardening standard, in part, is taken from the guidance of the Center for Internet Security and is the result

of a consensus baseline of security guidance from several government and commercial bodies. Other recommendations were taken from the Windows Security Guide, and the Threats and Counter Measures Guide developed by Microsoft. Hardening of the OS is the act of configuring an OS securely, updating it, creating rules and policies to help govern the system in a secure manner, and removing unnecessary applications and services. This is done to minimize a computer OS's exposure to threats and to mitigate possible risk.

4.3.29 IPv6 Tunnelling

Tunnelling provides a way to use an existing IPv4 routing infrastructure to carry IPv6 traffic. The key to a successful IPv6 transition is compatibility with the existing installed base of IPv4 hosts and routers. Maintaining compatibility with IPv4 while deploying IPv6 streamlines the task of transitioning the Internet to IPv6. While the IPv6 infrastructure is being deployed, the existing IPv4 routing infrastructure can remain functional, and can be used to carry IPv6 traffic.

4.4 Conclusion

This chapter provide a brief explanation about all the services that will be implement for this Workshop II. This chapter provide a clearer picture about each service. These administrations are regular in industry. So, this basic knowledge about all the services will be very helpful for us before going for industry training.

CHAPTER 5: INSTALLATION AND CONFIGURATION

5.1 Introduction

This chapter will list out list of services being implemented in Workshop II and the corresponding person-in-charge for the services. All service installation and configuration will be show and explain in this chapter.

5.2 Services and Corresponding Person-In-Charge

No	Name	Services
1	MUHAMMAD ARIEF BIN MOHD ISA	<ul style="list-style-type: none"> • Network Management System (main) • Web, SSL & Virtual Hosting • Syslog
2	MUHAMMAD HAFIZ BIN JAMIL	<ul style="list-style-type: none"> • Linux Email Server (main) • Dynamic routing (OSPF or EIGRP) and Network Address Translation (NAT) • IPv6 Web with IPv6 Tunneling (testing IPv6 Web from remote site)
3	NUR ARDINA AIN BINTI ABD RAOFF	<ul style="list-style-type: none"> • IPSec site-to-site tunneling (main) • Proxy Server • TFTP
4	NUR ASHYQIN BINTI MOHD ZAMRI	<ul style="list-style-type: none"> • Server Virtualization (main) • Access Control List (ACL) • Quota Screening
5	AMIR ZAKI BIN MAT ALI	<ul style="list-style-type: none"> • Cloud server (main) • Secure FTP with authentication and encryption

		<ul style="list-style-type: none"> • Active Directory with UAC/GPO
6	NIRESHA A/P ARUMUGAM	<ul style="list-style-type: none"> • DNS (IPv4 & IPv6) • DHCP (IPv4 & IPv6) • Wireless user authentication using Radius server
7	AMMAR AFIQ BIN SHAHRUL AZMAN	<ul style="list-style-type: none"> • IDS with port mirror (main) • Samba and Samba security services • Linux Server Hardening
8	MUHAMAD AZIM BIN AZMAN	<ul style="list-style-type: none"> • AAA (Authentication, Authorization, and Accounting) using Radius (main) • User authentication by integrating Active Directory with linux • Windows Server Hardening
9	CHONG POH THENG	<ul style="list-style-type: none"> • IPsec VPN server for remote employees (main) • VLAN and Port Security • Web hardening

Table 3: Services and Corresponding Person-In-Charge

5.3 Installation and Configuration

5.3.1 AAA (Authentication, Authorization and Accounting) using Radius

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

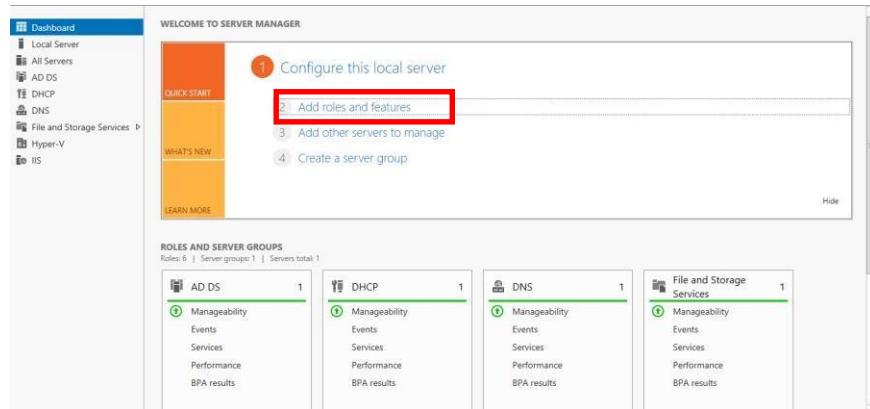


Figure 5.3.1.1: Server Manager

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

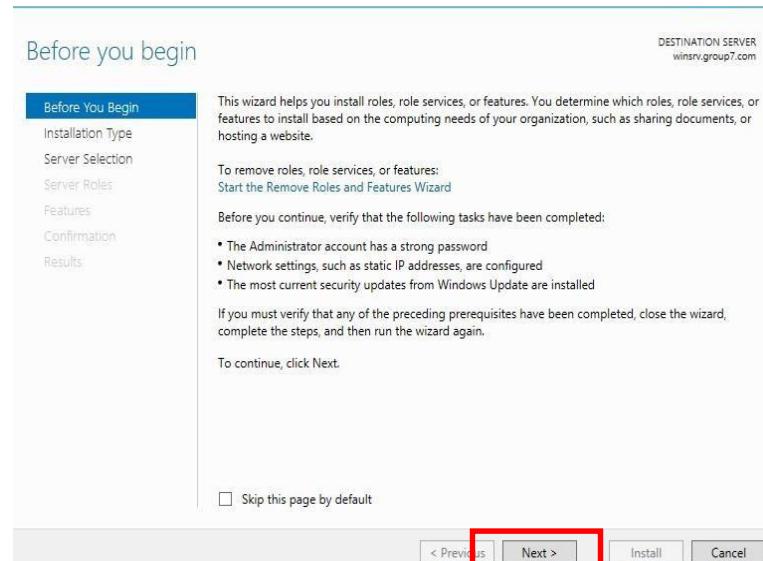


Figure 5.3.1.2: Add roles and features

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

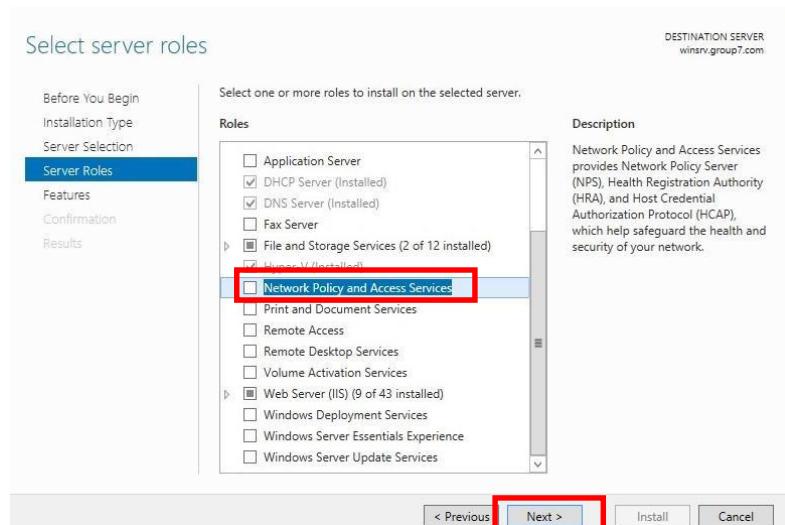


Figure 5.3.1.3: Select server roles

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

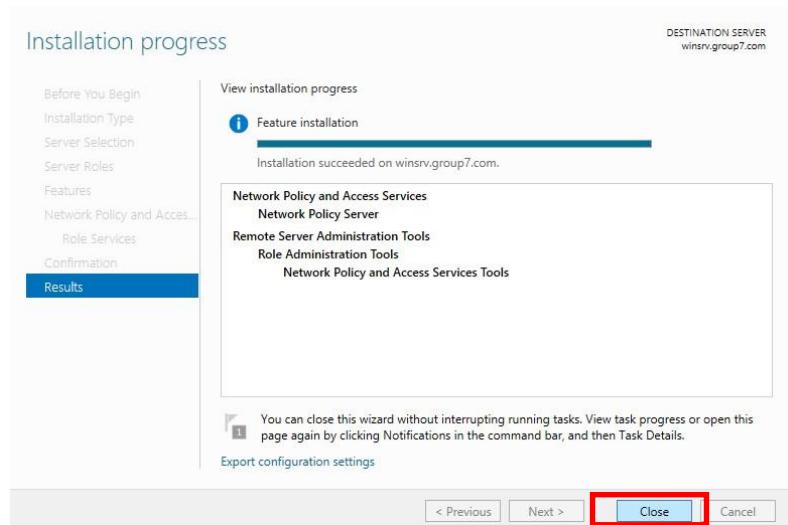


Figure 5.3.1.4: Installation progress

Step 5: Right click on **NAP**, and then click **Network Policy Server**, then click to **register server in Active Directory**. When Network Policy Server (NPS) is a member of an Active Directory Domain Services (AD DS) domain, NPS performs

authentication by comparing user credentials that it receives from network access servers with the credentials that are stored for the user account in AD DS. In addition, NPS authorizes connection requests by using network policy and by checking user account in AD DS.

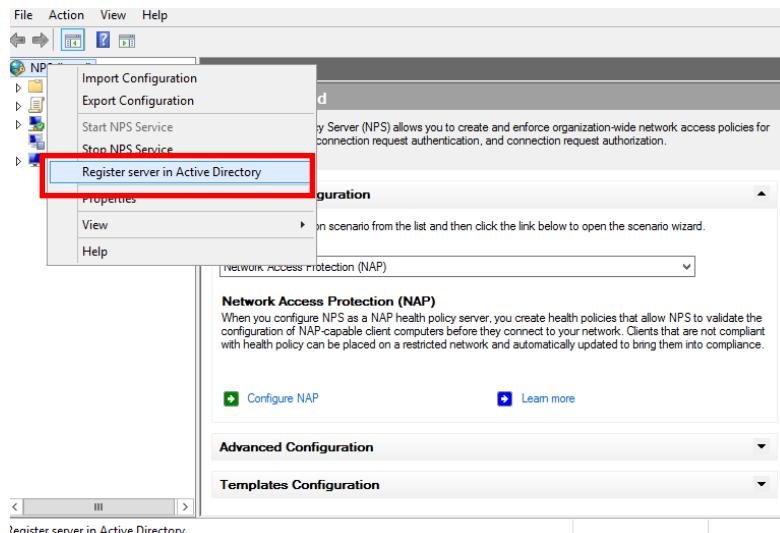


Figure 5.3.1.5: Network Policy Server

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

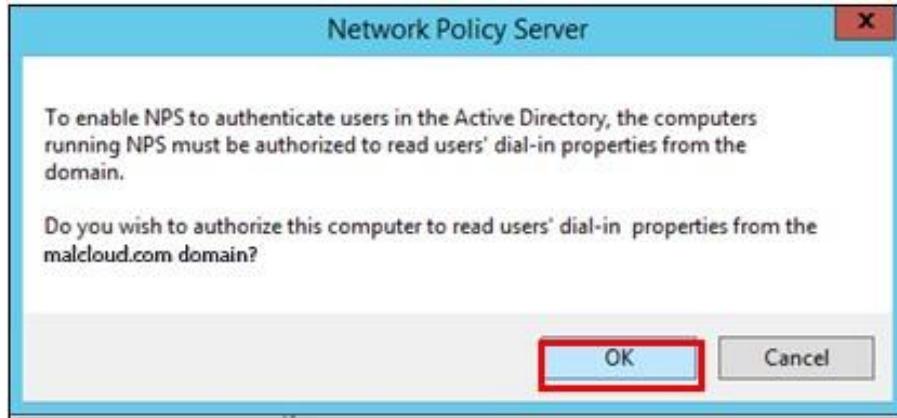


Figure 5.3.1.6: Enable NPS (Network Policy Server)

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

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

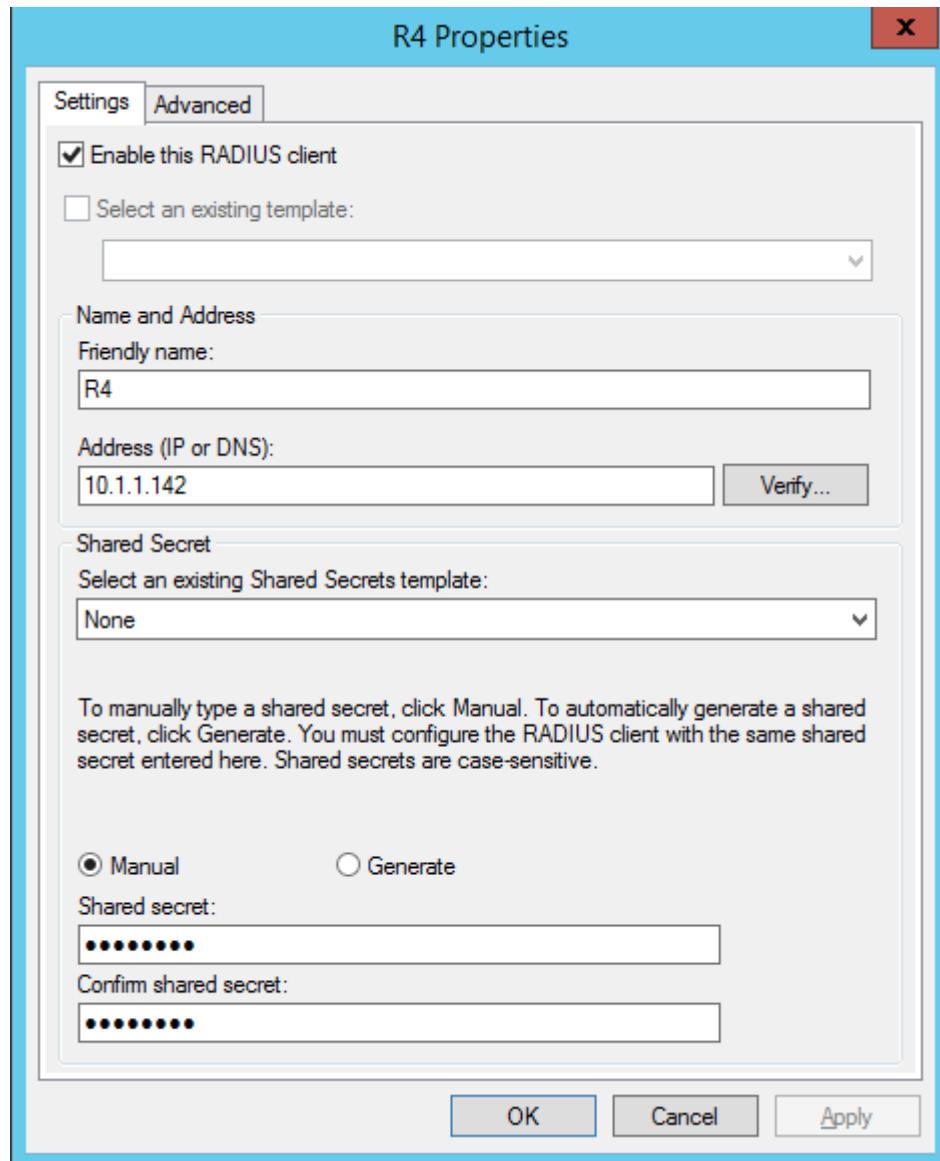


Figure 5.3.1.7: New Radius Client

Step 8: Next we need to create new network policies. To do that, go to the network policies and then right click on it, after that click New. Network policies are sets of conditions, constraints, and settings that allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect. When you deploy Network Access Protection (NAP), health policy is added to the network policy configuration so that Network Policy Server (NPS) performs client

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

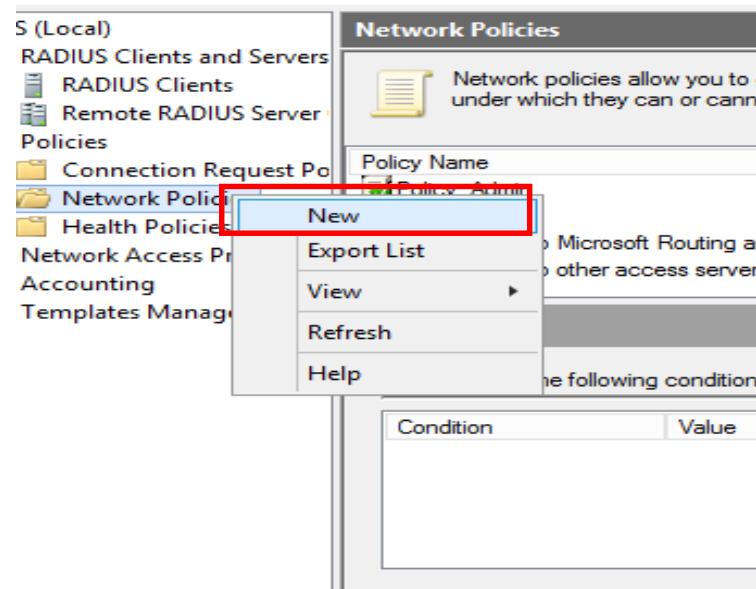


Figure 5.3.1.8: New Network Policies

Step 9: Enter the Policy Name and click **next**.

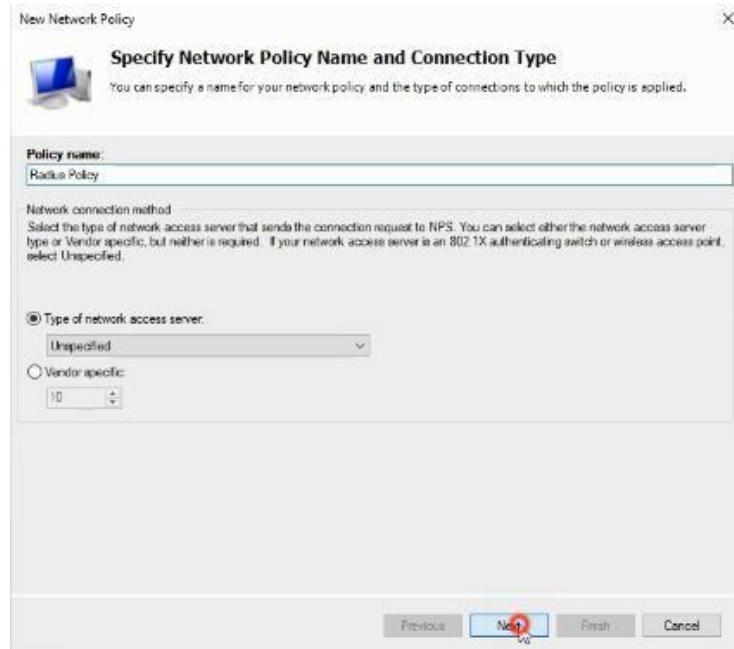


Figure 5.3.1.9: Policy Name

Step 10: Select the condition > User group then, click add. You can use this procedure to create a user or computer group in Active Directory Domain Services (AD DS) and then add the group as a condition in a Network Policy Server (NPS) network policy. Membership in Domain Users, or equivalent, is the minimum required to complete this procedure.

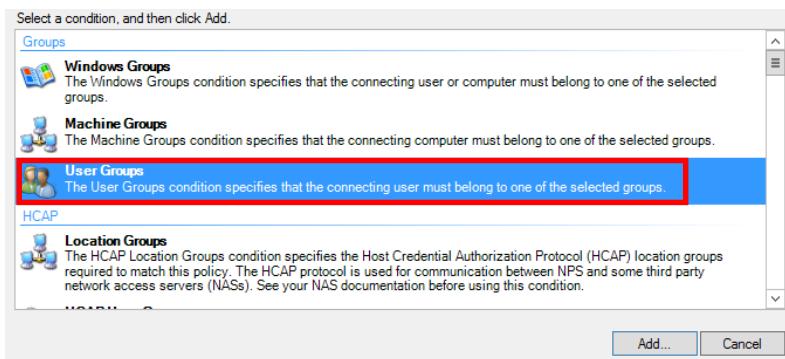


Figure 5.3.1.10: Specify Condition

Step 11: In User Groups page, click Add Groups. This step is to define which groups that can access the network.



Figure 5.3.1.11: Select Group

Step 12: Enter the object name to select > type “AAA” > click Check Names. Then, choose **Group4** and click **OK**.



Figure 5.3.1.12: Check Names

Step 13: Proceed to OK.

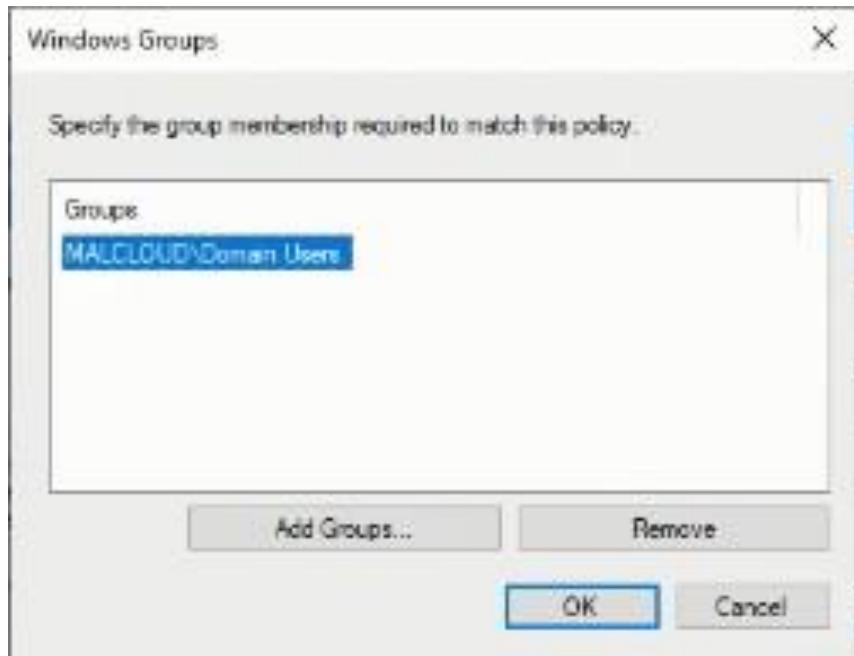


Figure 5.3.1.13: User Groups

Step 14: In **Specify Access Permission**, tick **Access granted**. Proceed to Next. This step is to configure whether you want to grant network access or deny network access if the connection request matches this policy.

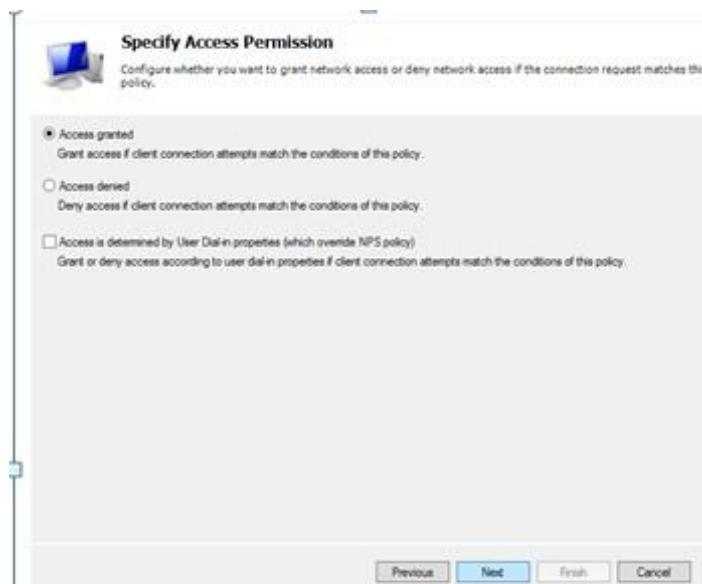


Figure 5.3.1.14: Access Permission

Step 15: On Configuration Authentication Methods, tick on Unencrypted Authentication (PAP, SPAP). Choosing this option because CISCO Router only support PAP and SPAP protocol. Proceed to Next. When Connection Request Policy windows appear, click no.

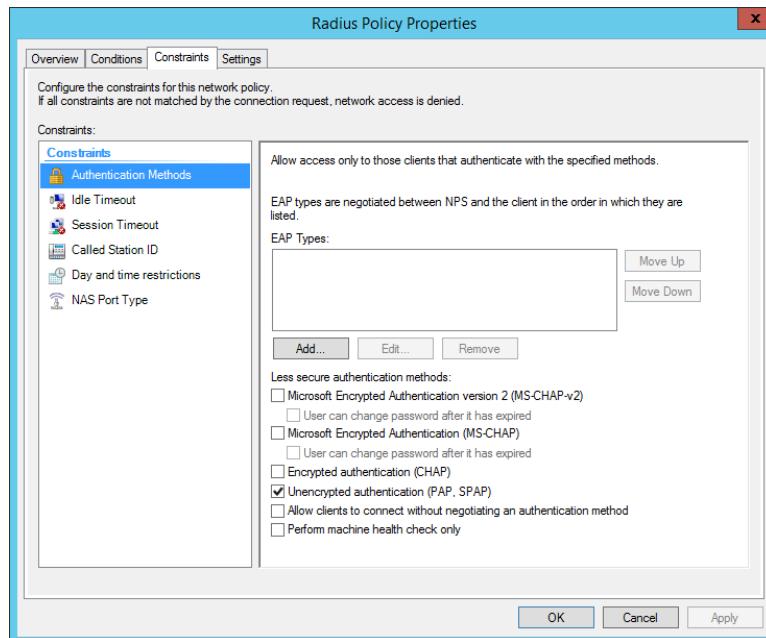


Figure 5.3.1.15: Authentication Method

Step 16: Configure Constraint page, proceed to Next, Constraint are additional parameters of the network policy that are required to match the connection request.

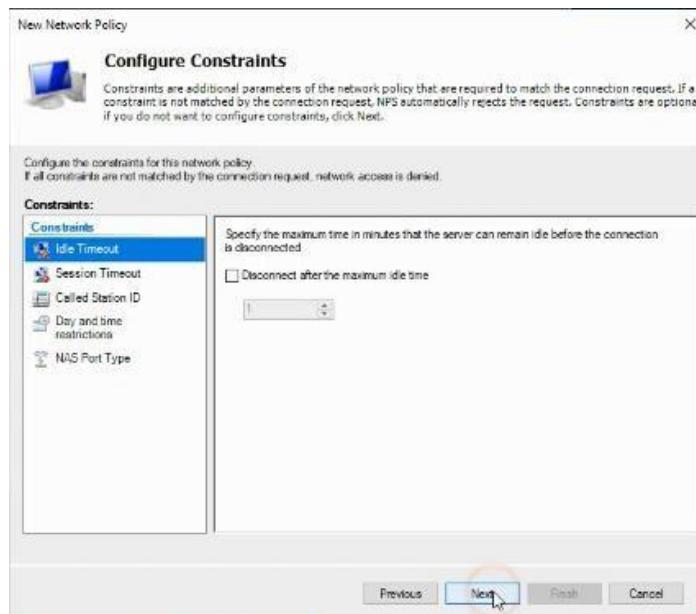


Figure 5.3.1.16: Configure Constraint

Step 17: In Standard, remove **Framed-Protocol** and edit Service Type attributes

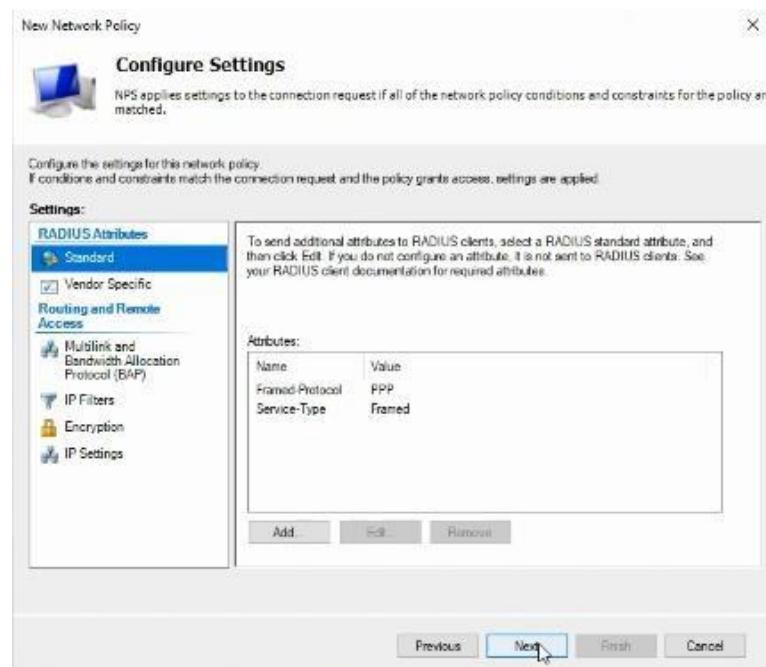


Figure 5.3.1.17: Configure Settings

Step 18: Then, select **others** > pick **Login**. After that, click **OK**.

Attribute name:	Service-Type
Attribute number:	6
Attribute format:	Enumerator
Attribute Value:	<input type="radio"/> Commonly used for Dial-Up or VPN <input type="radio"/> Commonly used for 802.1x <input checked="" type="radio"/> Others <input type="text" value="Login"/>

OK **Cancel**

Figure 5.3.1.18: Attribute Information

Step 19: In **Vendor Specific**, click **Add**. Vendor-Specific Attributes (VSA) is a method for communicating vendor-specific information between NASs and RADIUS servers. Attribute 26 encapsulates vendor specific attributes, thereby, allowing vendors to support their own extended attributes otherwise not suitable for general use.

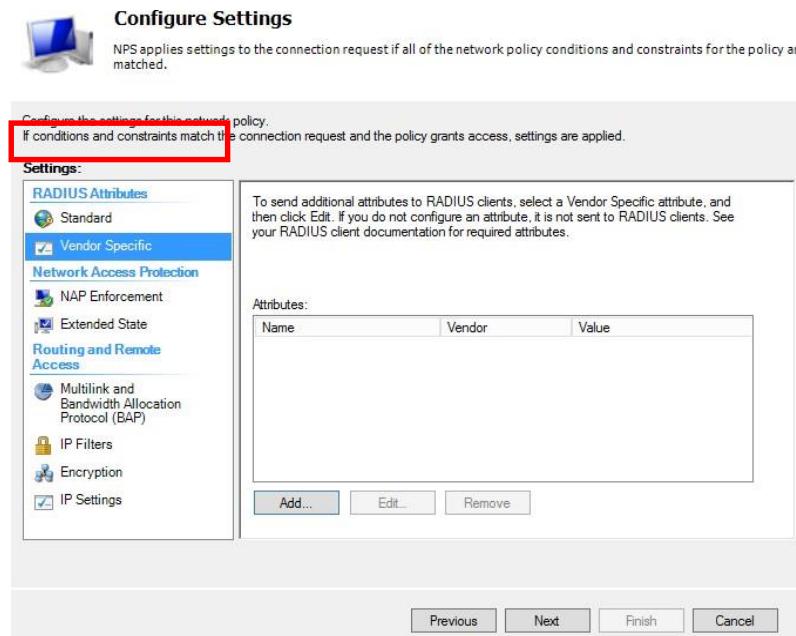


Figure 5.3.1.19 : Vendor Specific

Step 20: Add attributes name **Cisco-AV-Pair**, vendor Cisco and value **shell:priv-lvl=15**. By default, there are three privilege levels on the router.

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

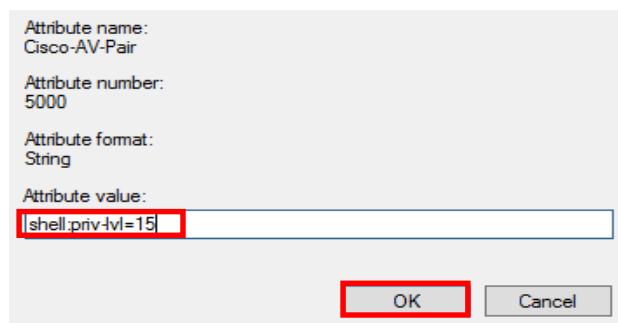


Figure 5.3.1.20: Attribute Value

Step 21: In **Completing New Network Policy**, it will display that successfully created the network policy, Click **Finish**. Then your network policy is created.

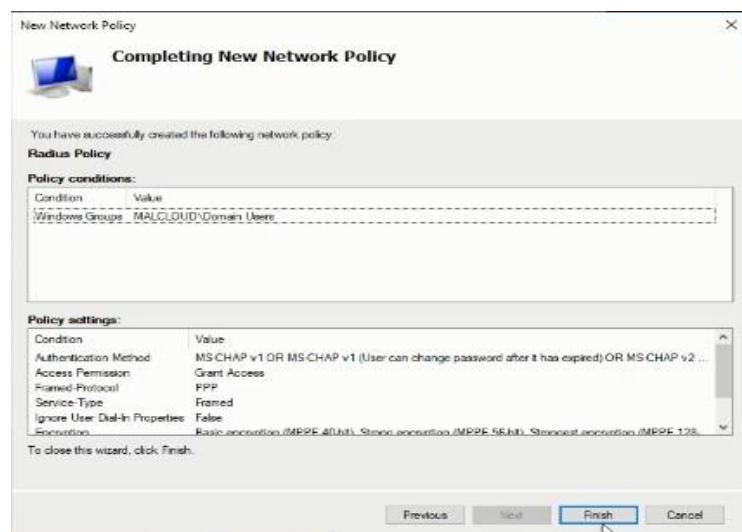


Figure 5.3.1.21: Successfully Creating Network Policy

Step 22: On the Accounting tab, click on Configure Accounting

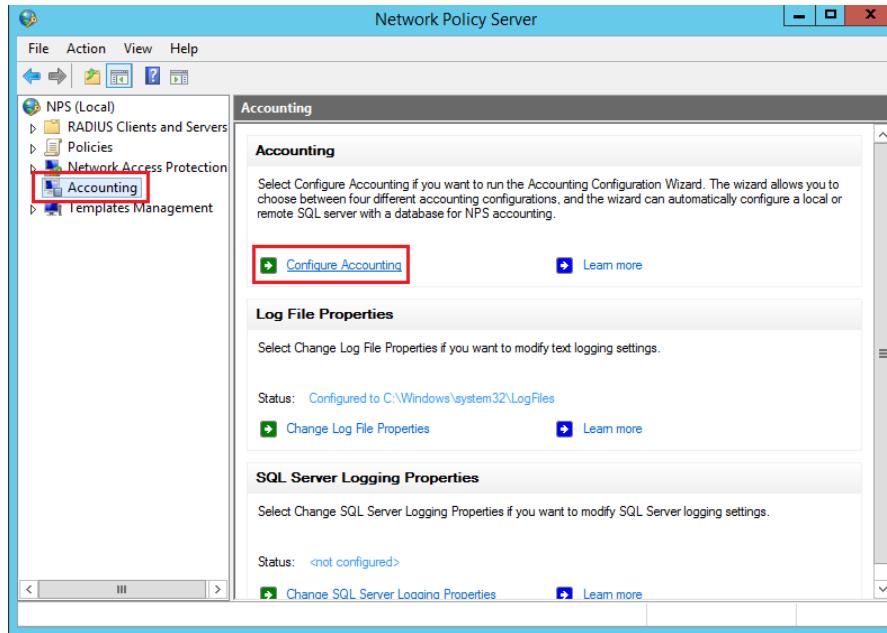


Figure 5.3.1.22: Accounting in Network Policy Server

Step 23: Click next on the Introduction page of the Accounting Configuration Wizard.

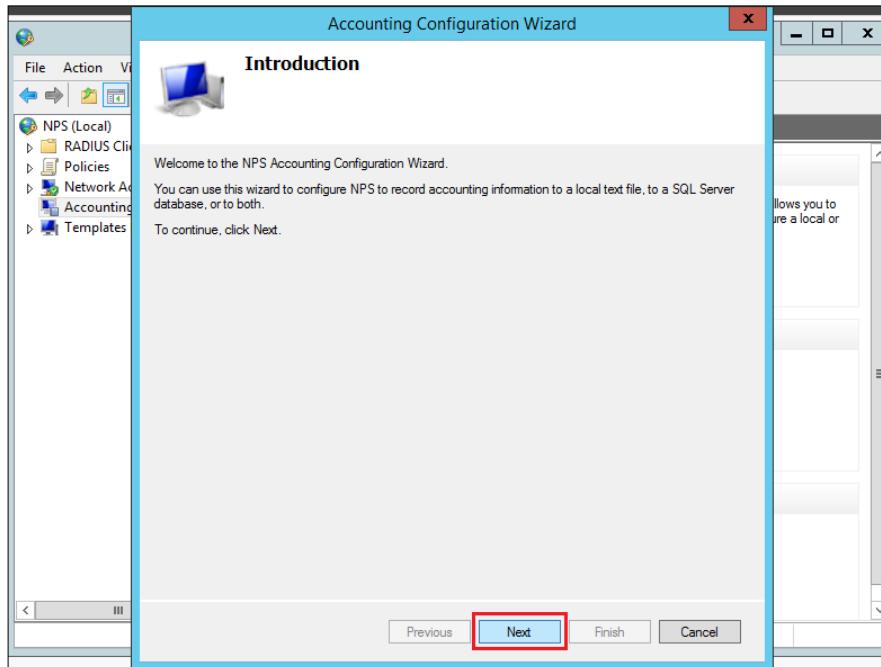


Figure 5.3.1.23: Introduction In Accounting Configuration

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

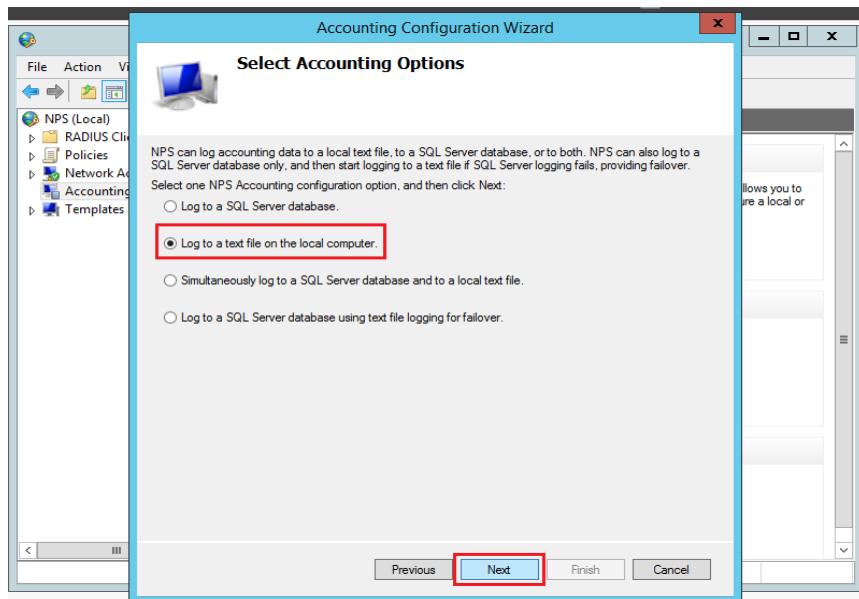


Figure 5.3.1.24: Select Accounting Option

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

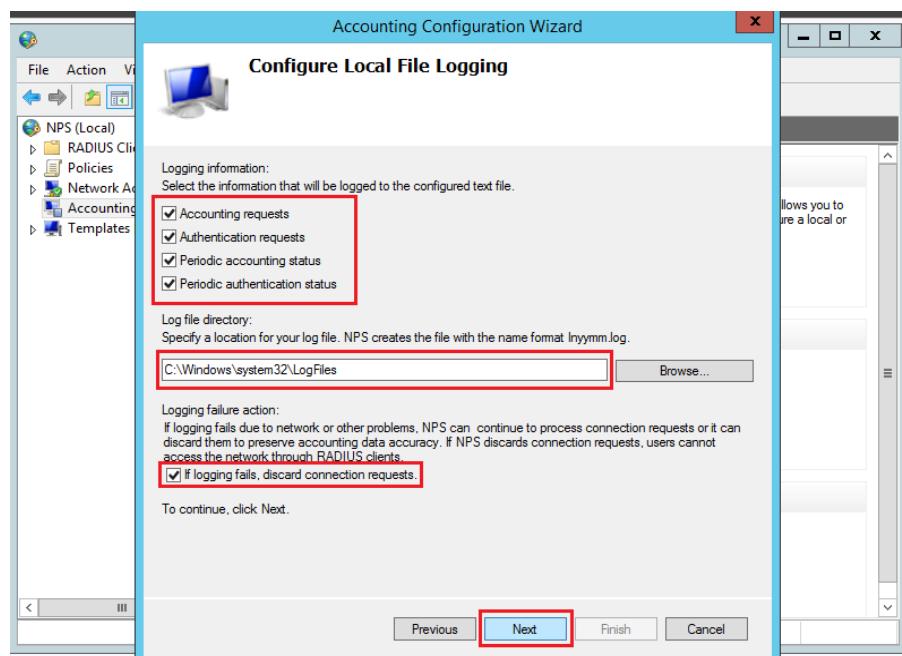


Figure 5.3.1.25: Configuring File Logging

Step 26: In the Conclusion page, click Close.

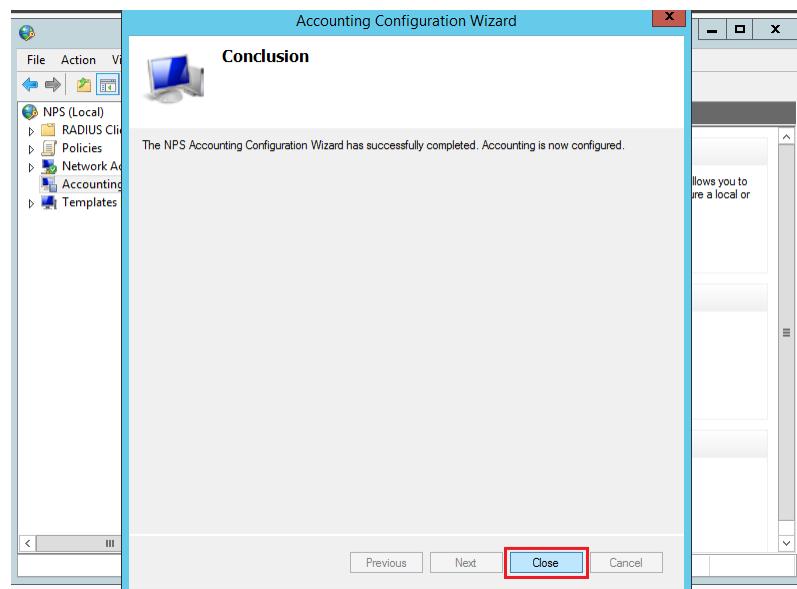


Figure 5.3.1.26: Conclusion

5.3.2 Server Virtualization

Step 1: Install Hyper-V in Windows Server by Click Manage > Add roles and features

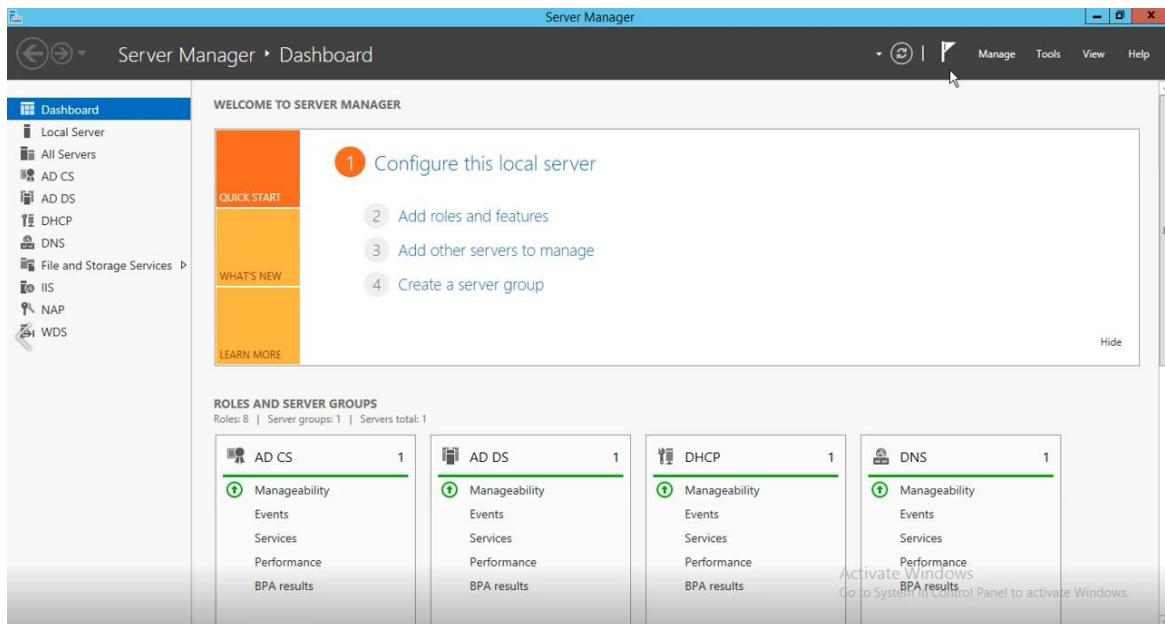


Figure 5.3.2.1 : Install Hyper-V

Step 2: Choose Role-based or feature –based installation for the installation type

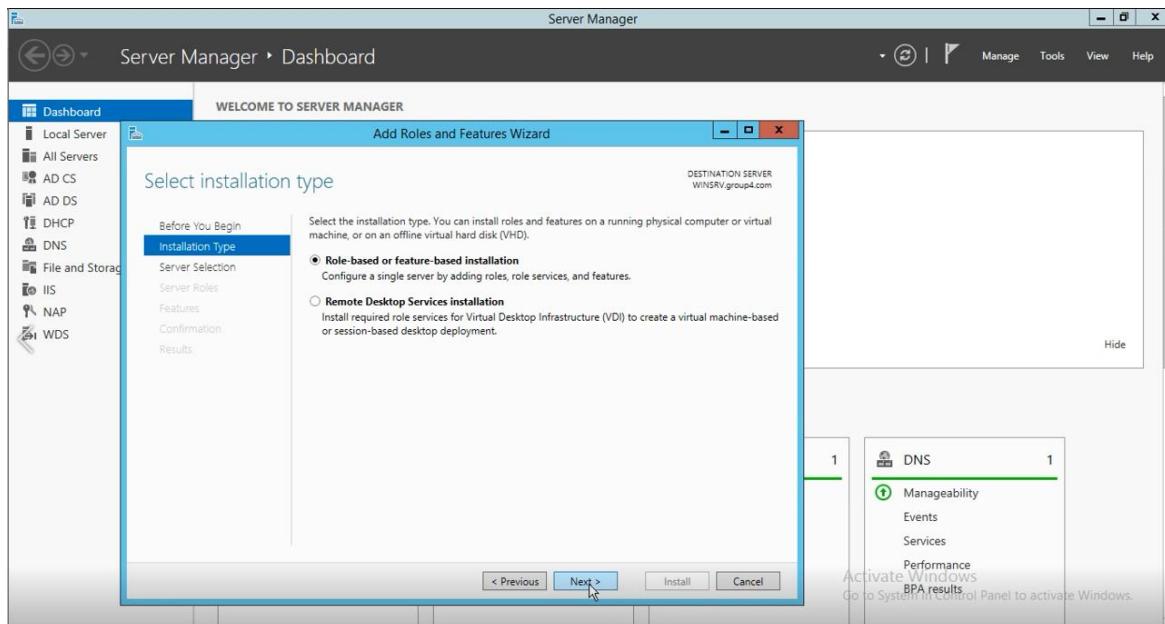


Figure 5.3.2.2: Installation type

Step 3: Choose the destination server

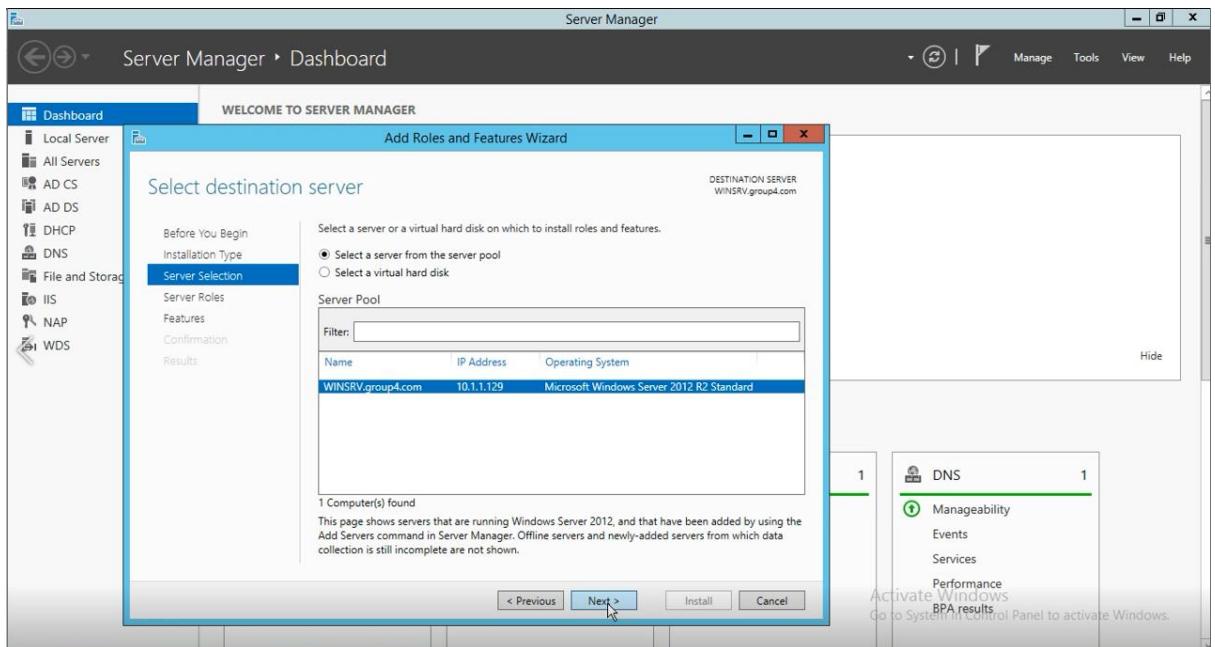


Figure 5.3.2.3: Select destination server

Step 4: Click Hyper-V to proceed the installation

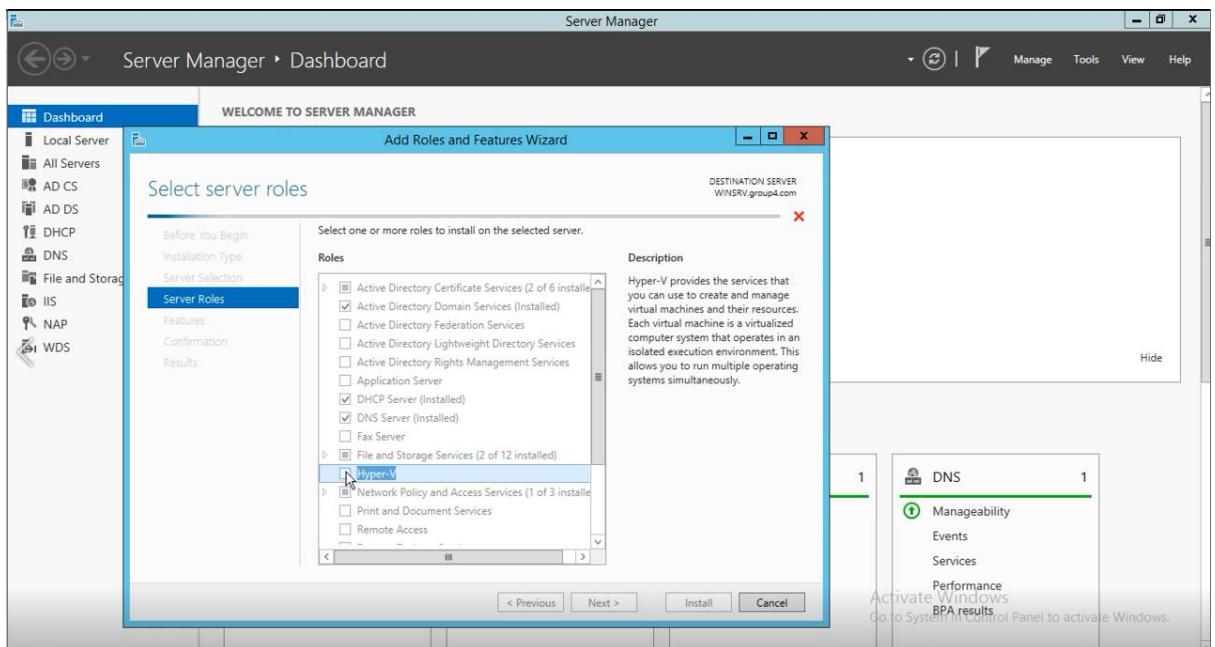


Figure 5.3.2.4 : Select Hyper-V

Step 5: Click next after Add Features

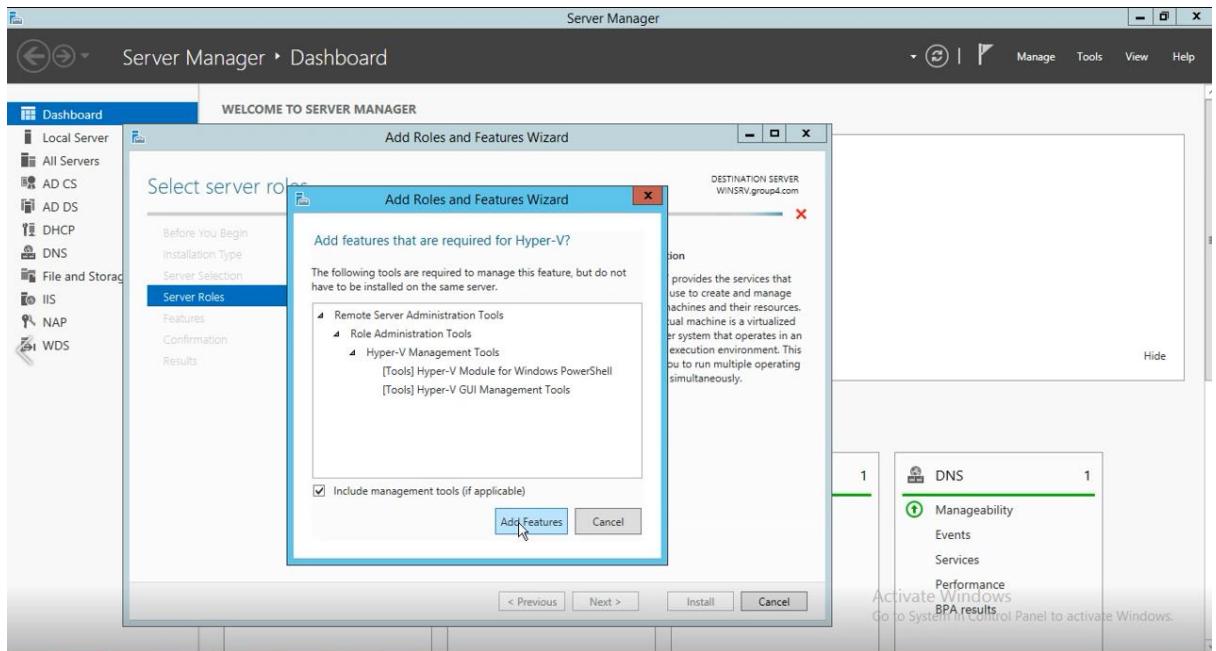


Figure 5.3.2.5: Add features

Step 6: Hyper-V was selected for installation

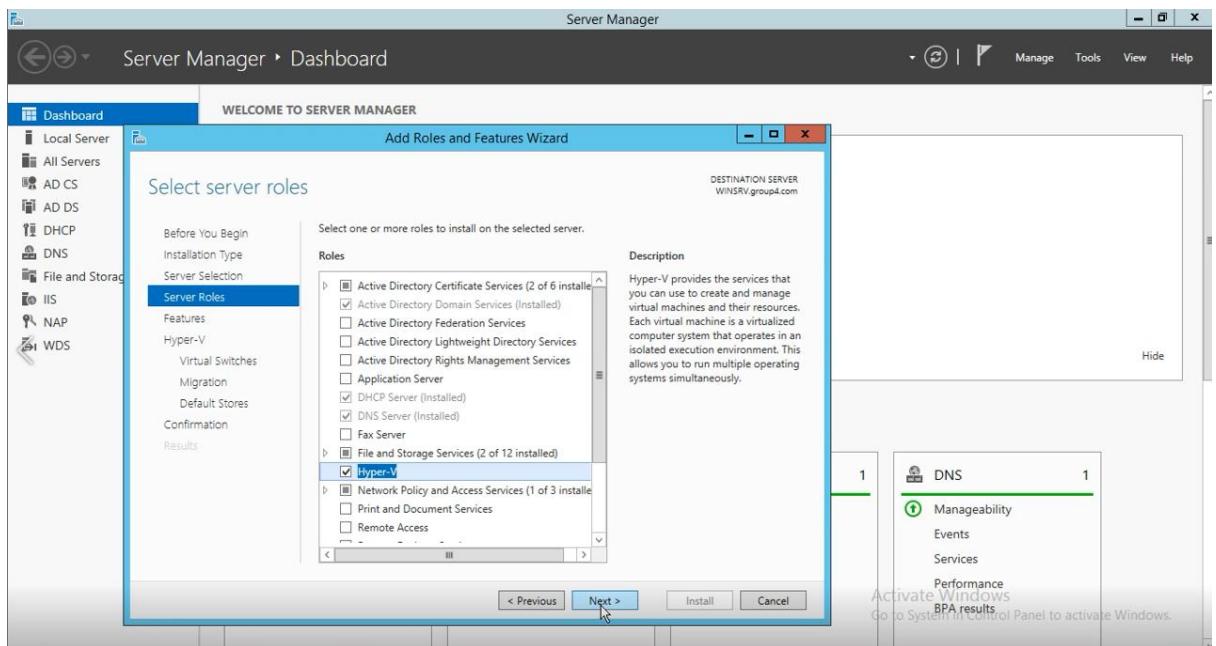


Figure 5.3.2.6 : Select server roles

Step 7: Just click Next for this step

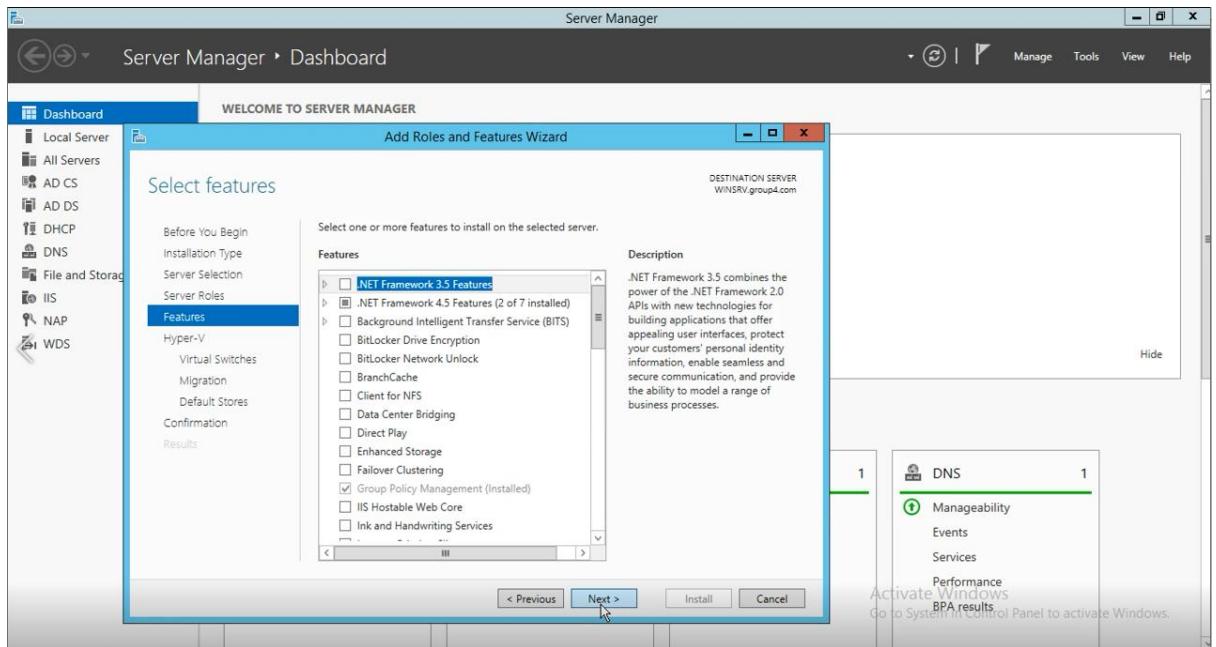


Figure 5.3.2.7: Select features

Step 8: The information about Hyper-V

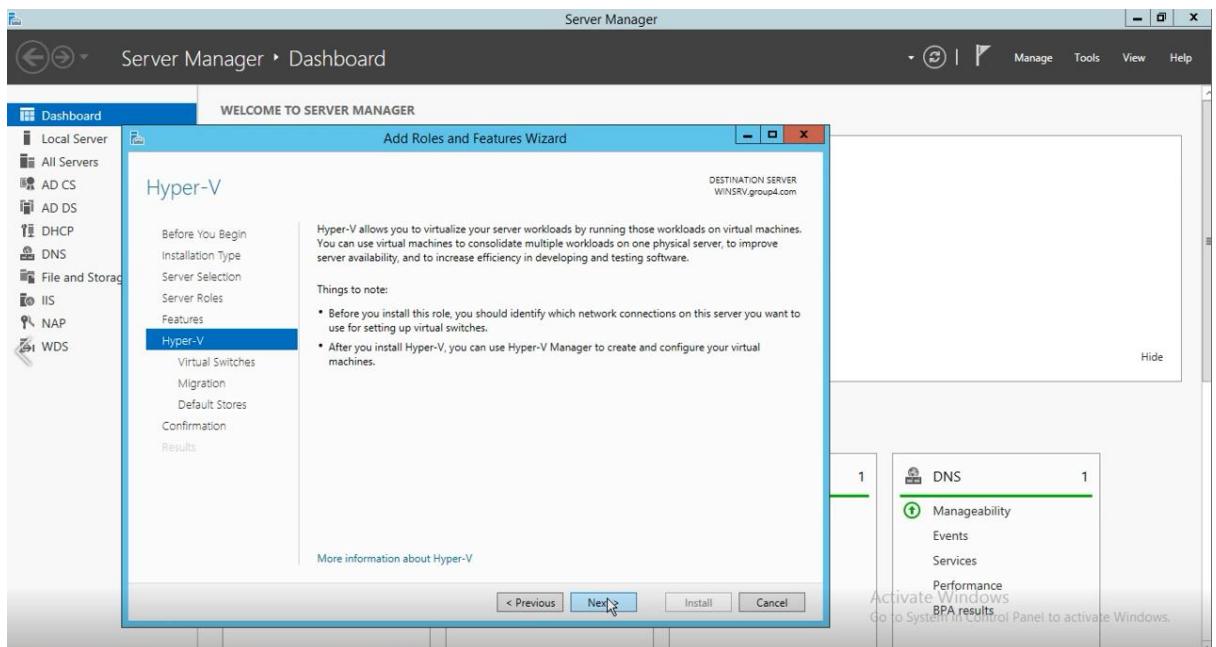


Figure 5.3.2.8 : Hyper-V information

Step 9: Choose network adapters to create virtual switches

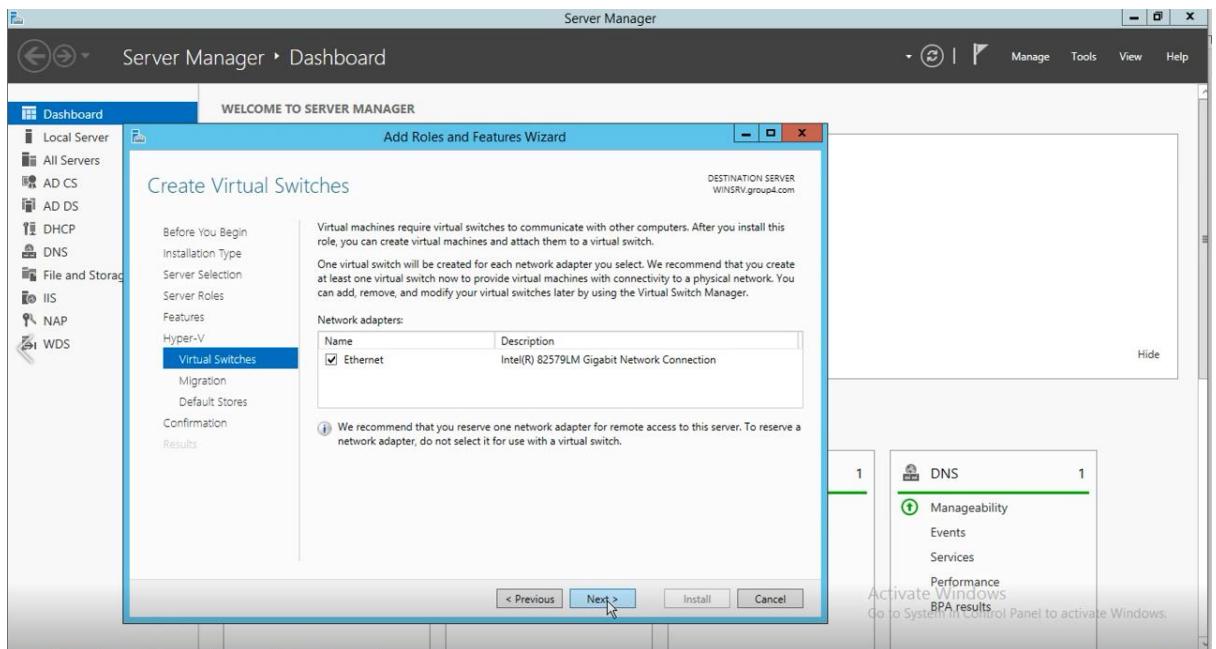


Figure 5.3.2.9 : Server roles

Step 10: Click Next for virtual machine migration

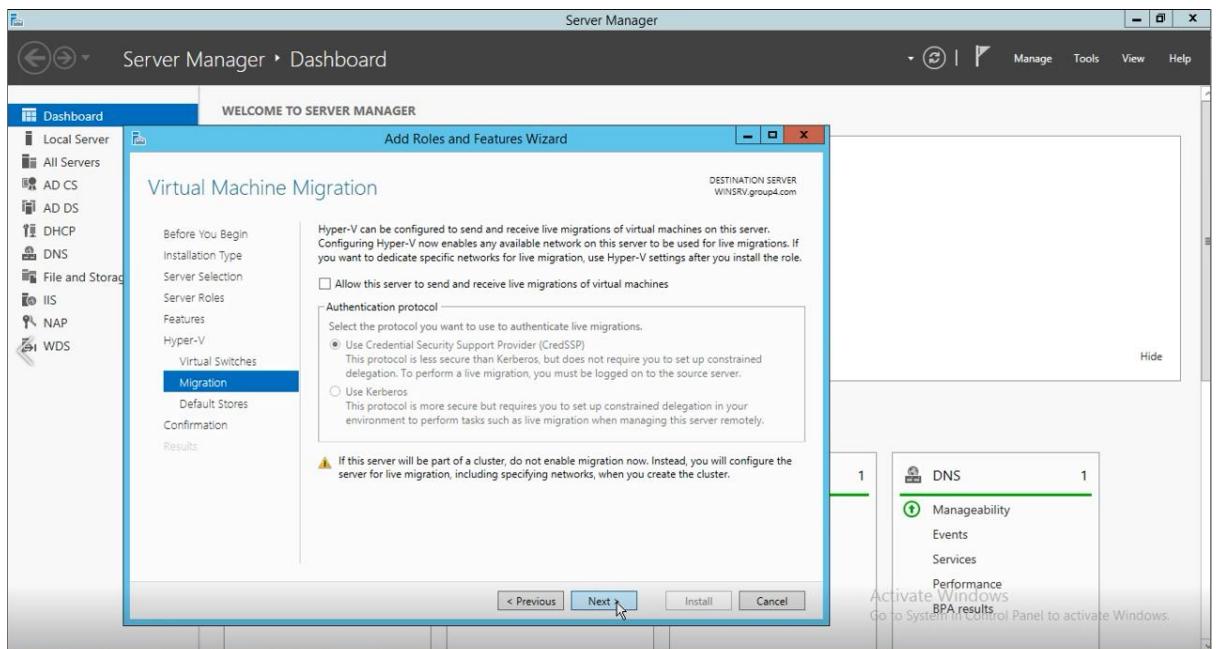


Figure 5.3.2.10: Virtual machine migration

Step 11: Click Next after choose the default locations to store virtual hard disk and virtual machine configuration files

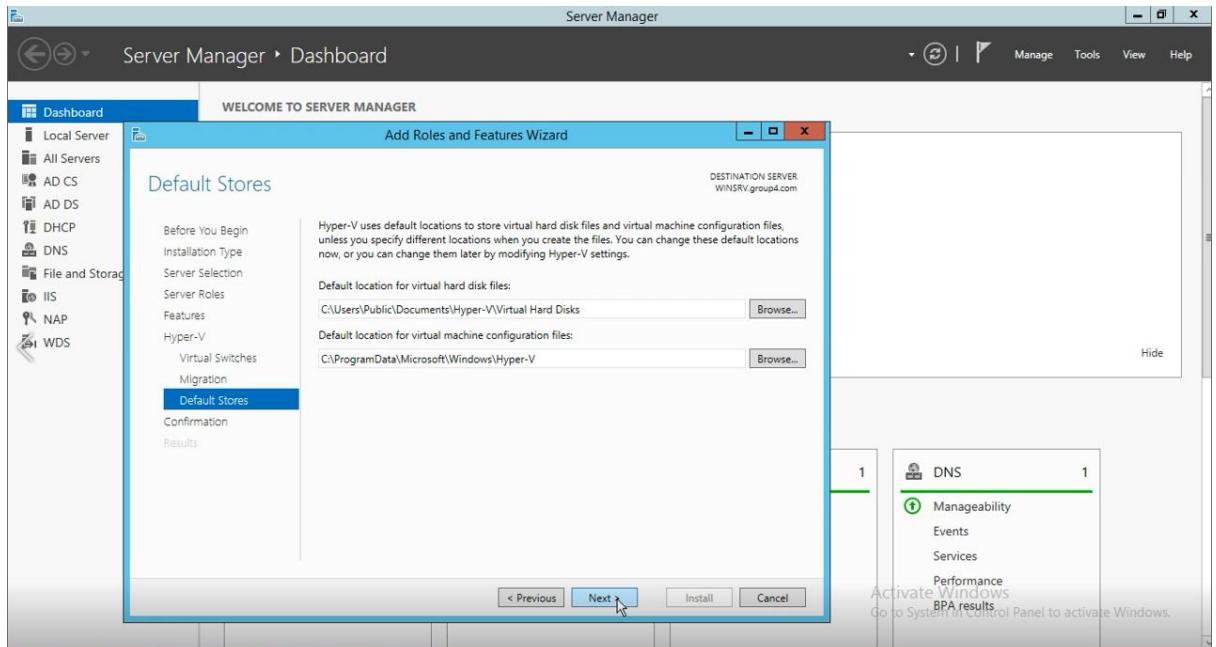


Figure 5.3.2.11 : Default stores

Step 12: Hyper-V installed after the installation progress end

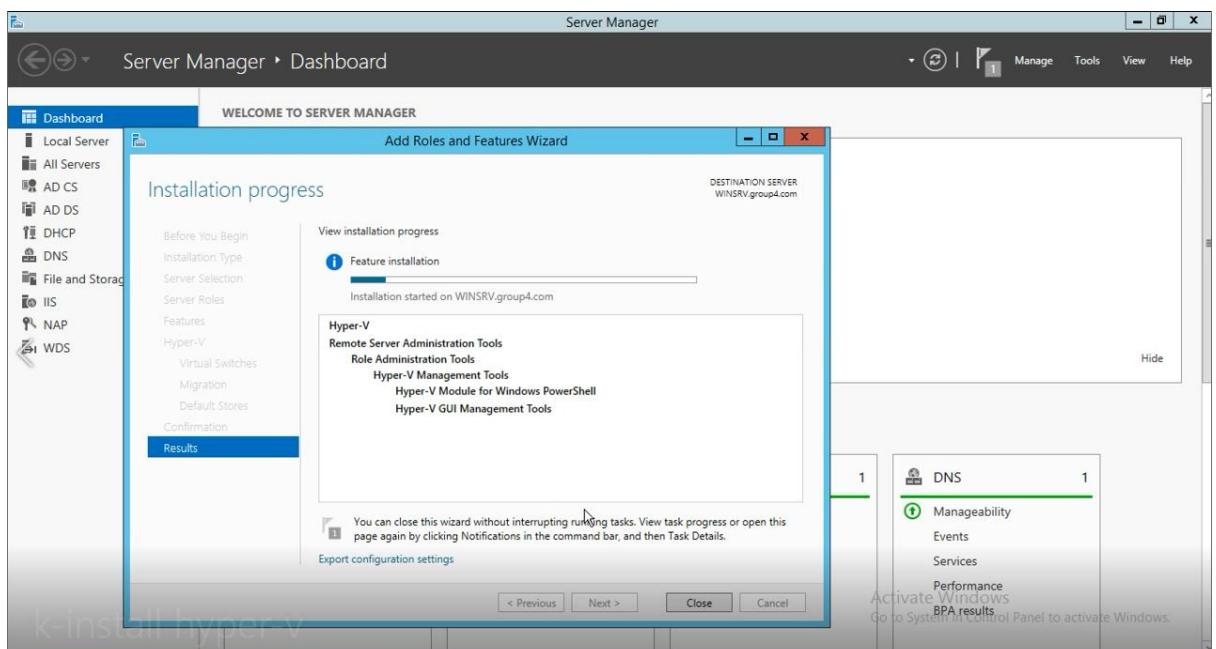


Figure 5.3.2.12 : Installation progress

Step 13: Create new virtual machine in the Hyper-V

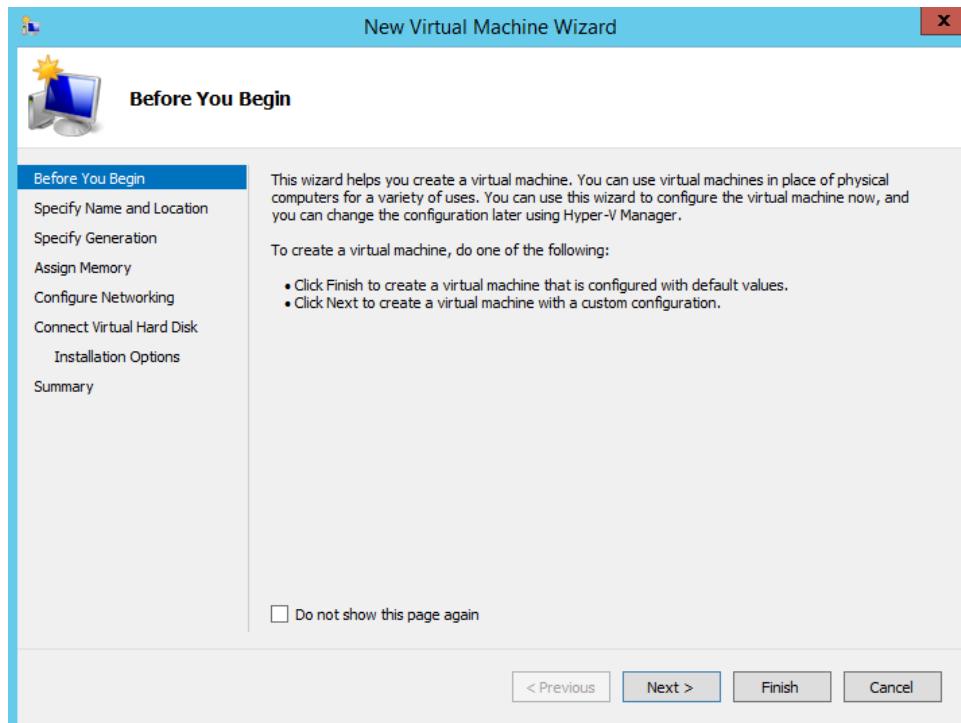


Figure 5.3.2.13: Add new virtual machine

Step 14: Name and specify location for new virtual machine

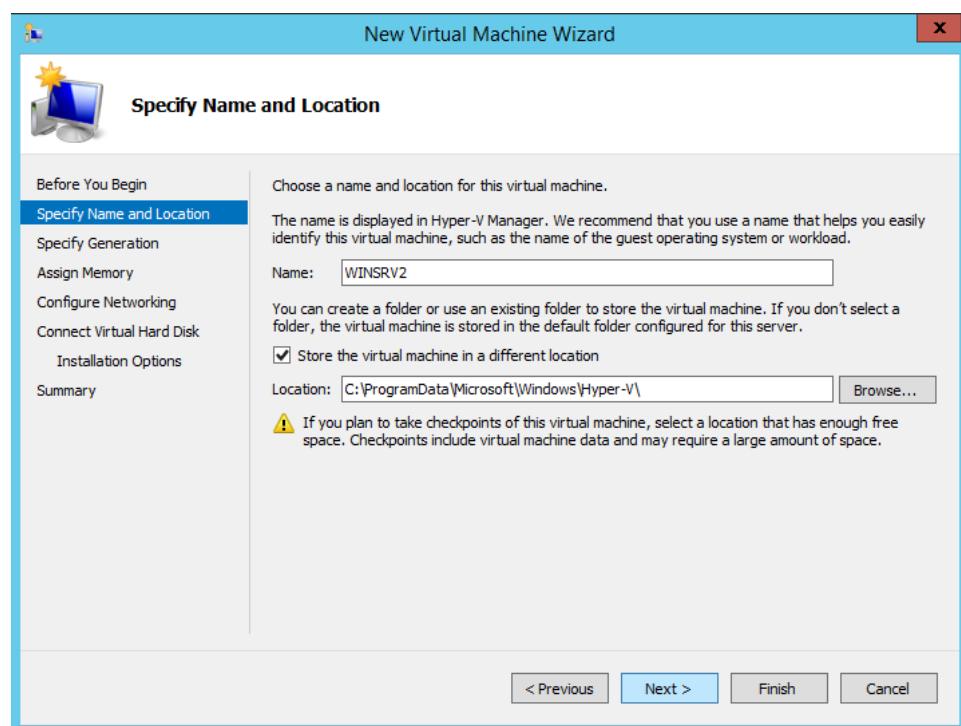


Figure 5.3.2.14 : Specify name and location

Step 15: Choose generation 1 and click Next

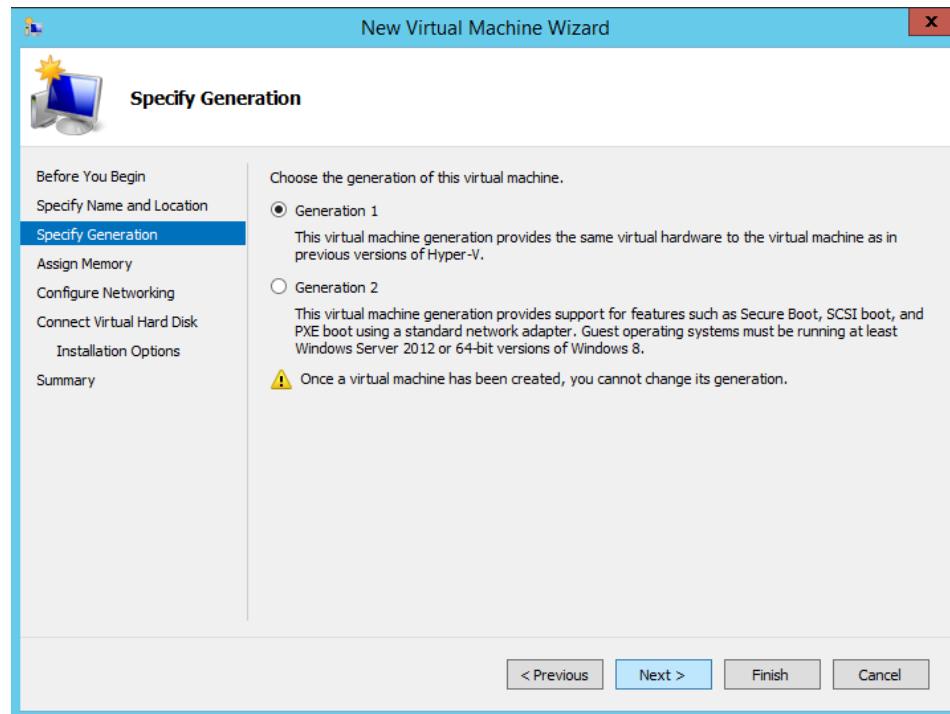


Figure 5.3.2.15: Specify generation

Step 16: Assign 4012mb for the memory

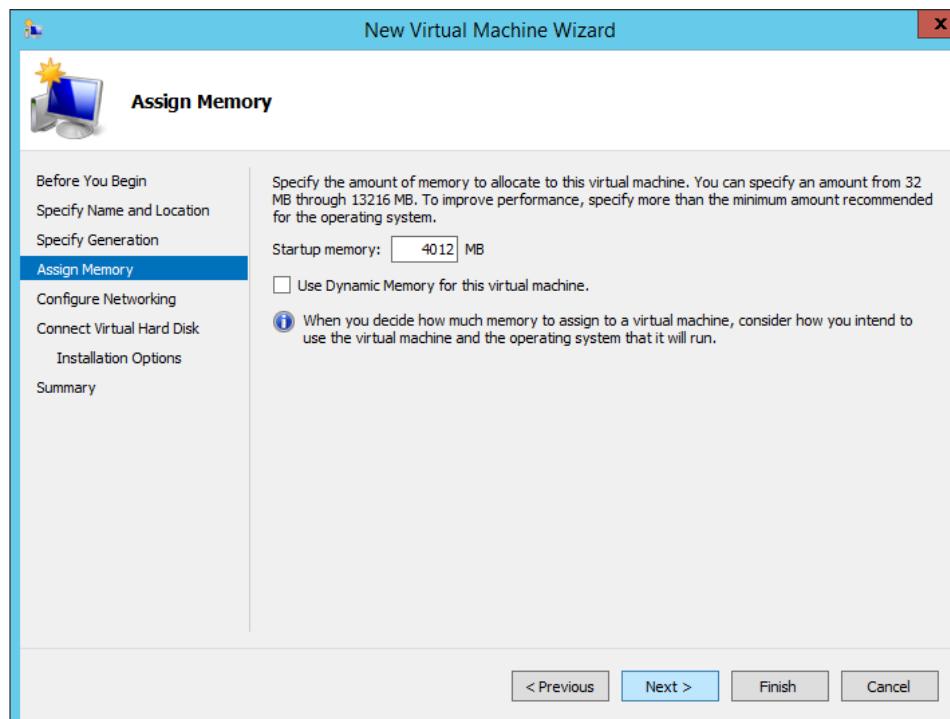


Figure 5.3.2.16: Assign memory

Step 17: Choose Host for configure networking

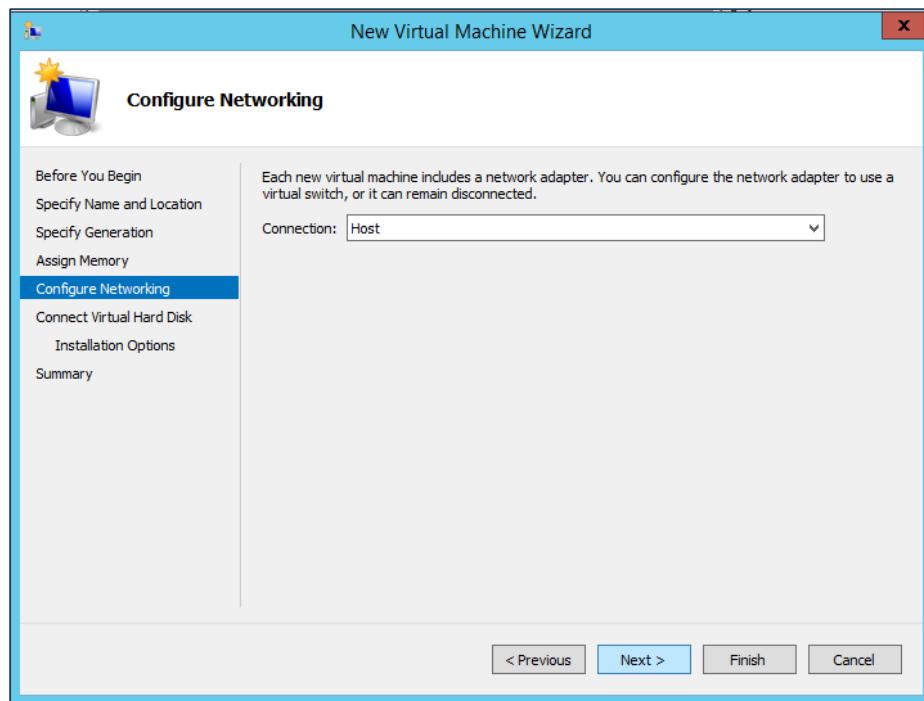


Figure 5.3.2.17: Configuring networking

Step 18: Create name, location and size for virtual hard disk

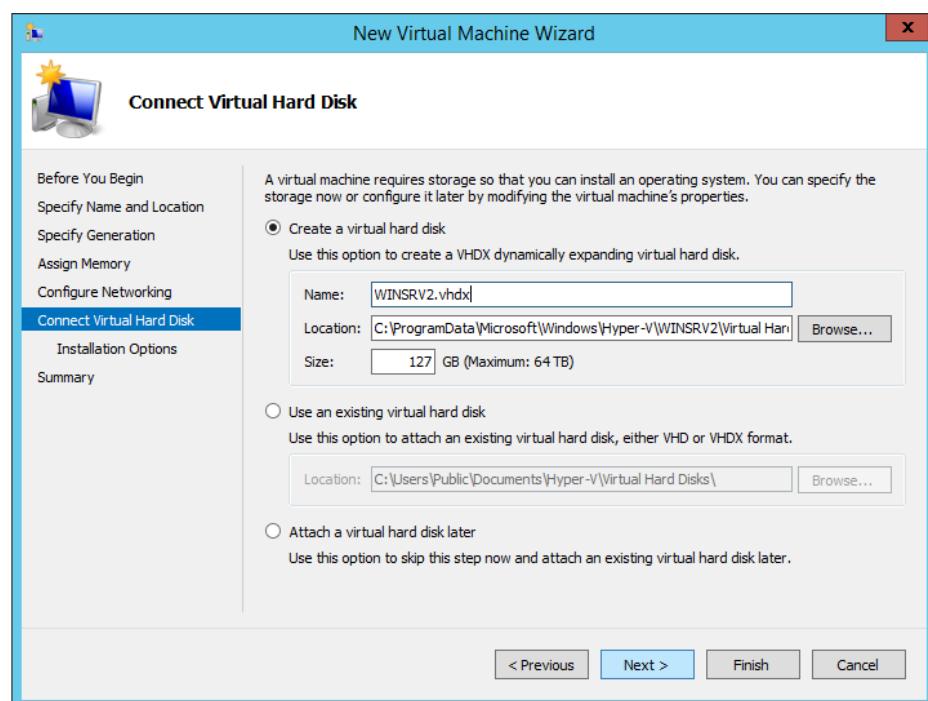


Figure 5.3.2.18 : Connect virtual hard disk

Step 19: Select the operating system for installation

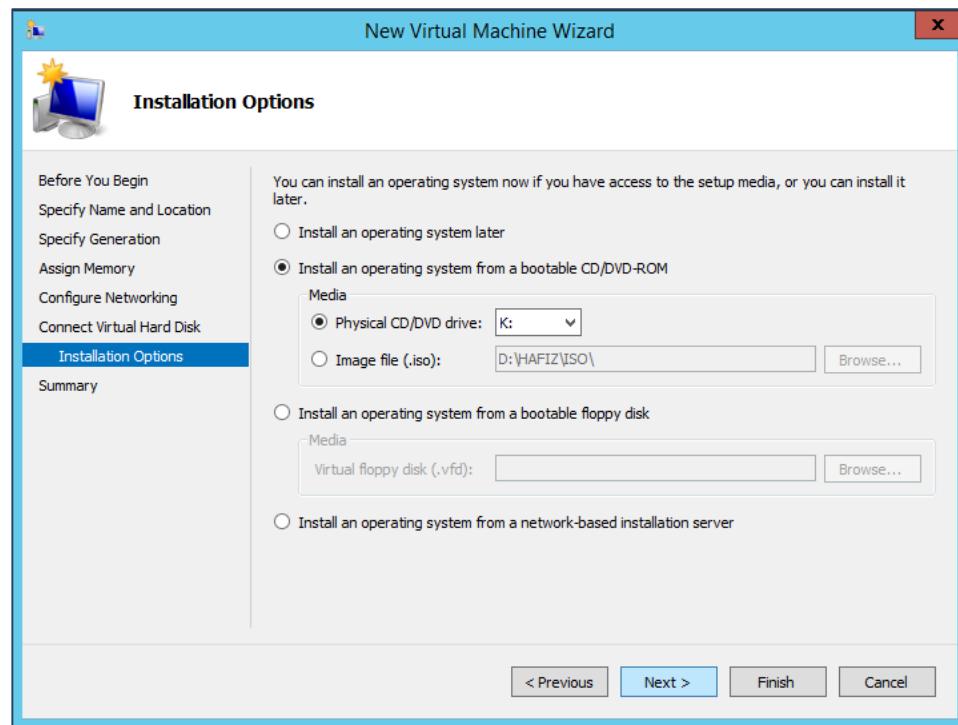


Figure 5.3.2.19: Installation options

Step 20: The selection is complete

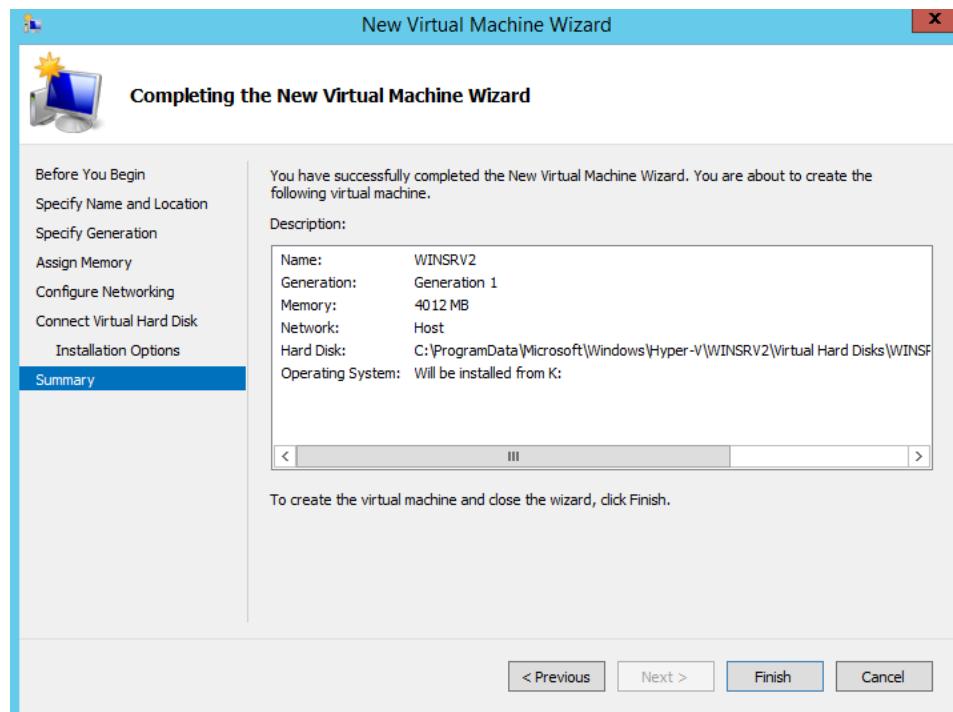


Figure 5.3.2.20: Summary of selection

Step 21: The operating system (Windows Server 2016) has been installed in Hyper-V

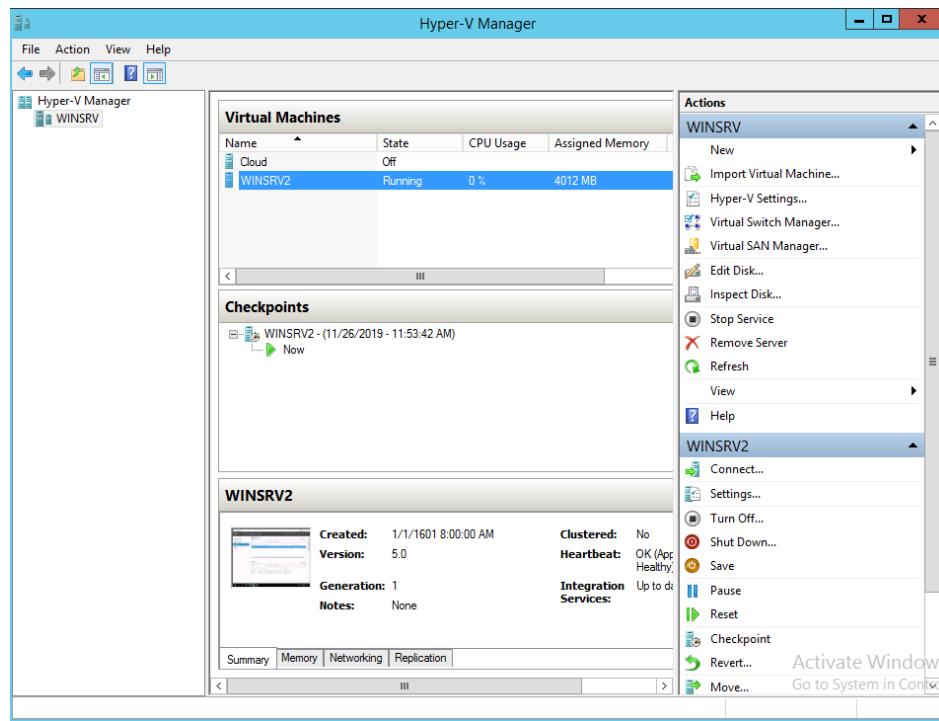


Figure 5.3.2.21: Virtual machine installed

Step 22: Connect to the new virtual machine

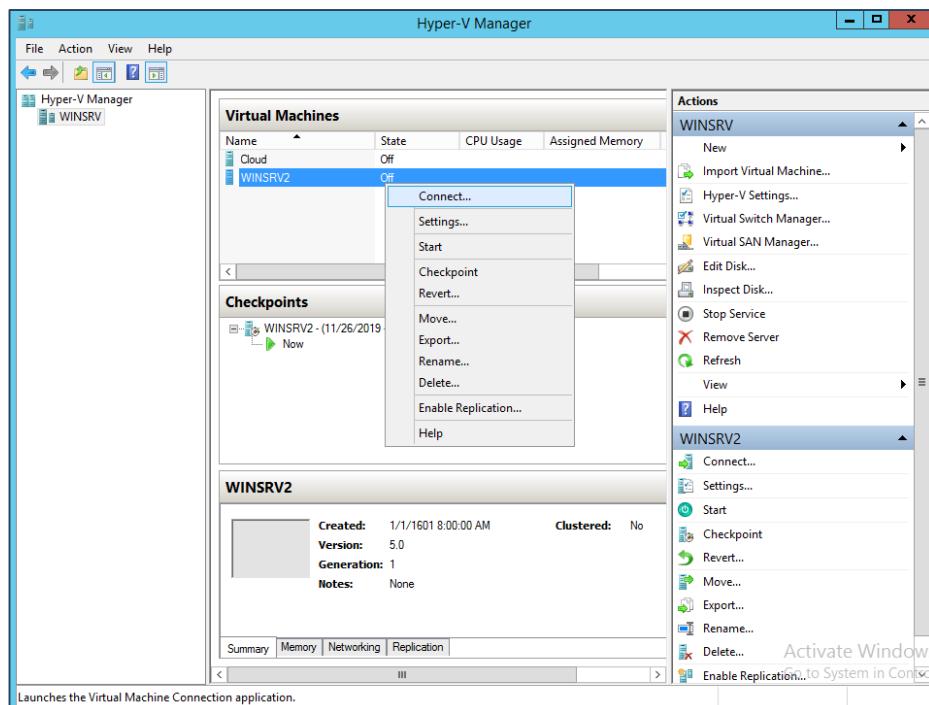


Figure 5.3.2.22: Connect virtual machine

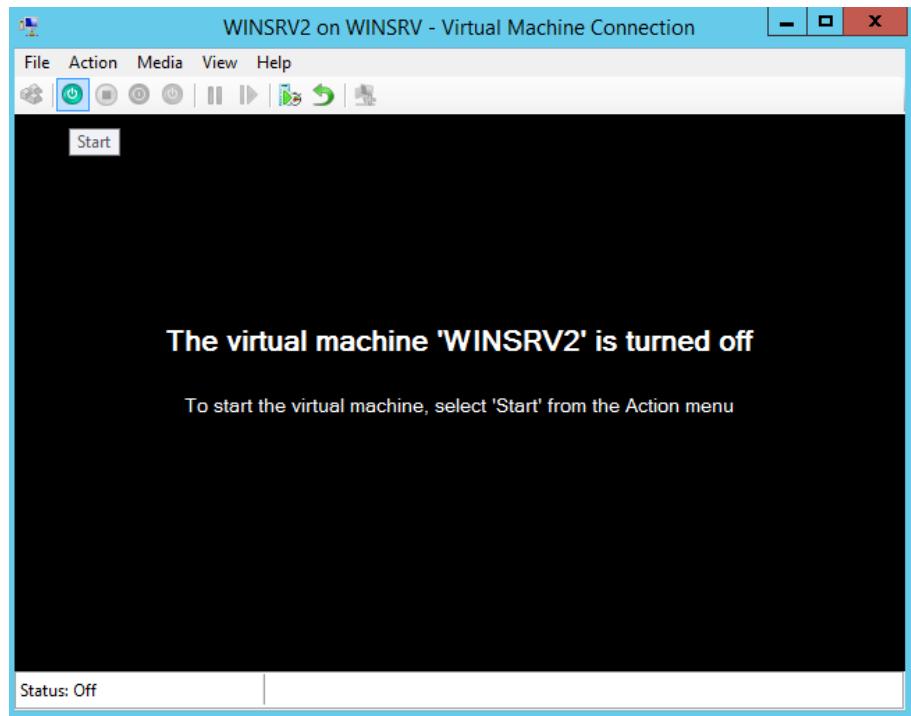
Step 23: Start the virtual machine

Figure 5.3.2.23: Start the virtual machine

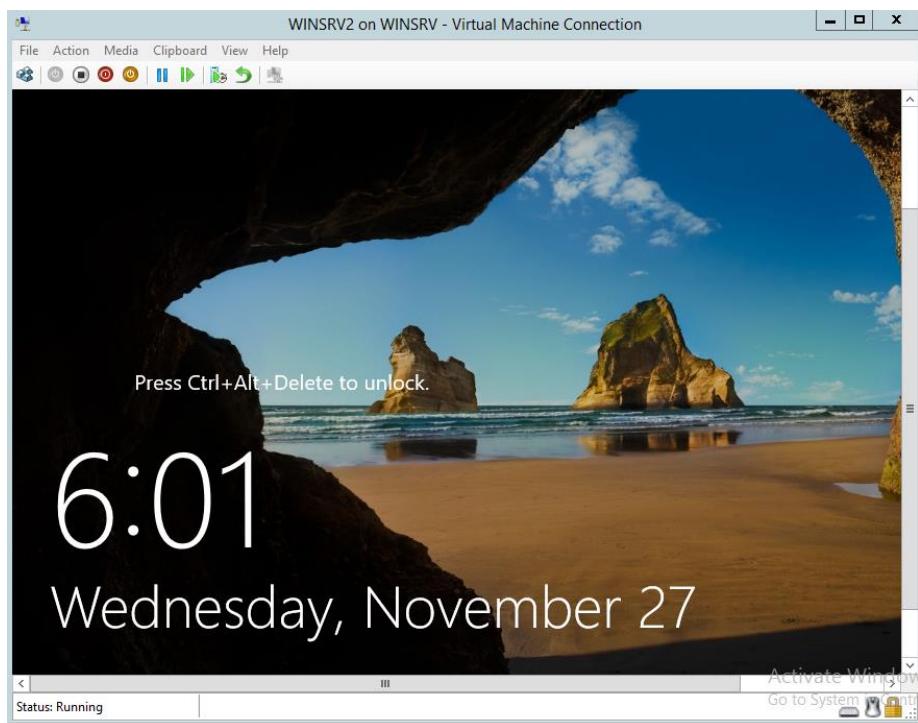
Step 24: Interface for the virtual machine

Figure 5.3.2.24: Front screen virtual machine

Step 25: Add roles and feature to install DHCP

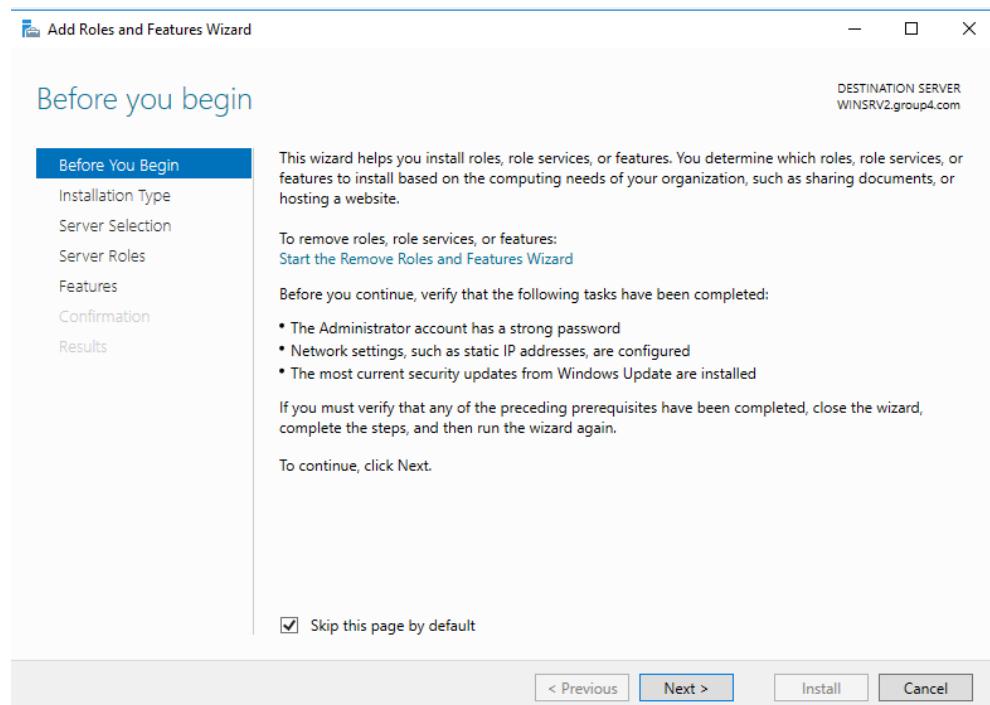


Figure 5.3.2.25: Install DHCP

Step 26: Choose role-based or feature-based installation

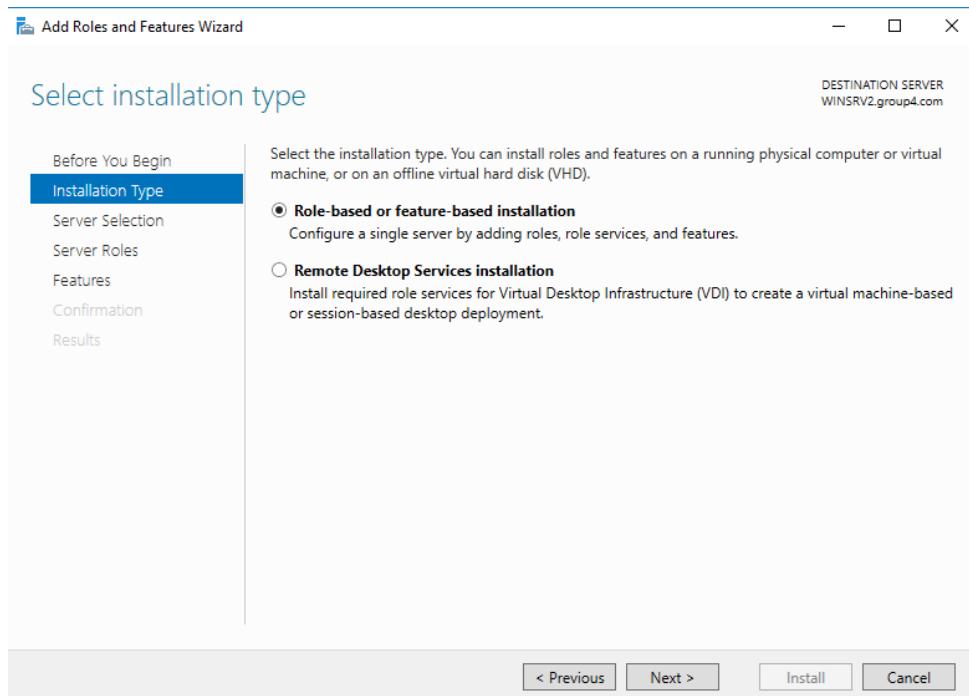


Figure 5.3.2.26: Installation type

Step 27: Select server destination

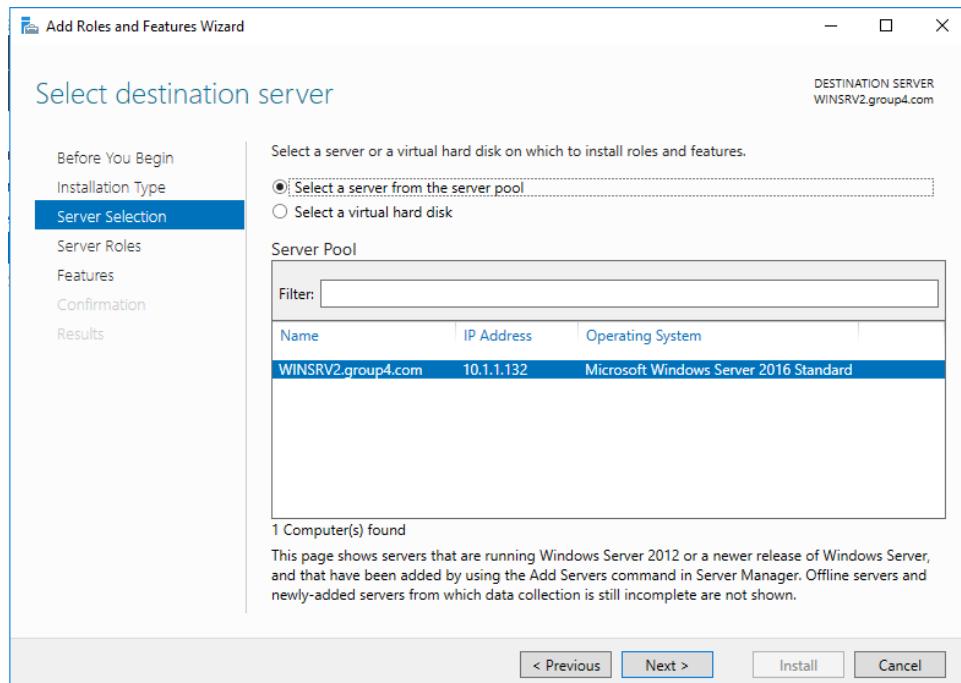


Figure 5.3.2.27: Destination server

Step 28: Tick for DHCP server installation

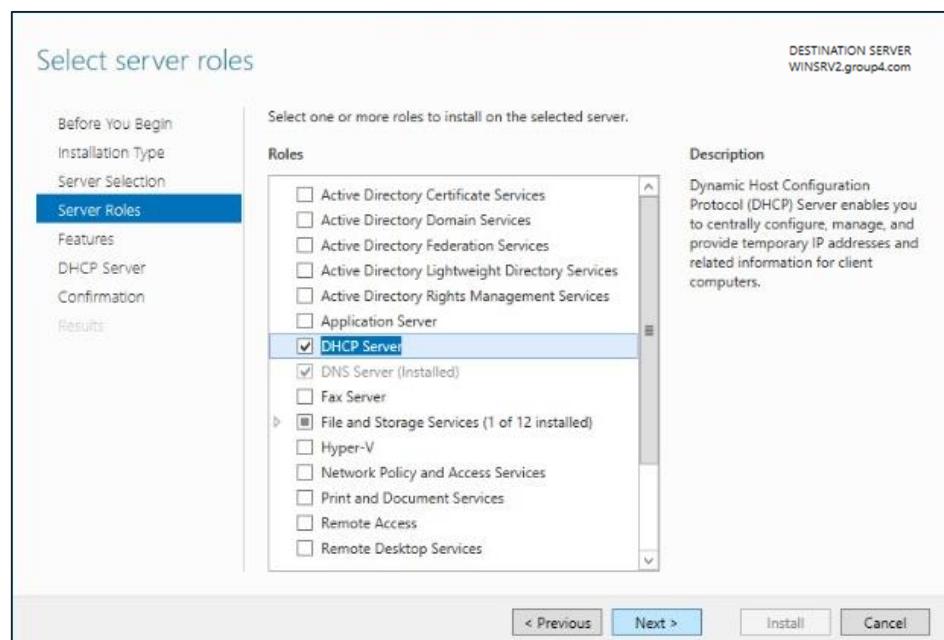


Figure 5.3.2.28: Select server roles

Step 29: Click Next for this features

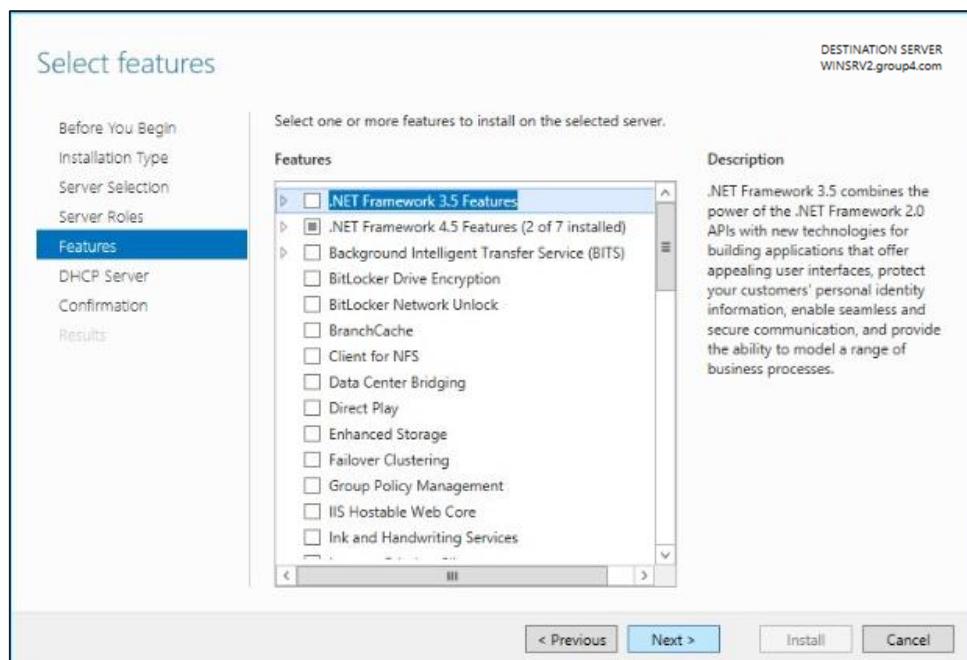


Figure 5.3.2.29: Select features

Step 30: Information about DHCP server

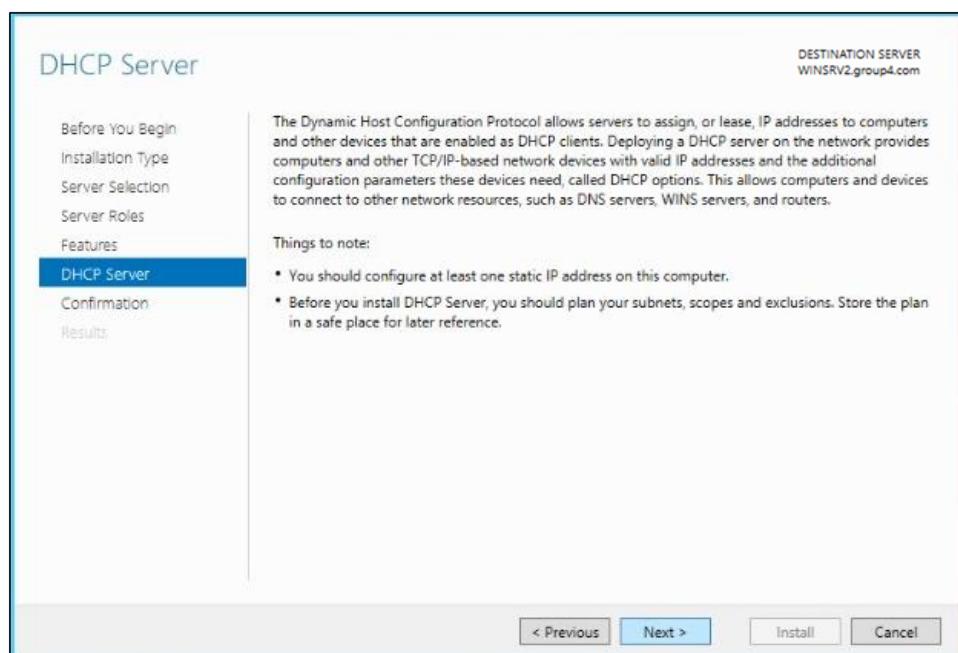


Figure 5.3.2.30 : DHCP information

Step 31: Tick restart and install the server

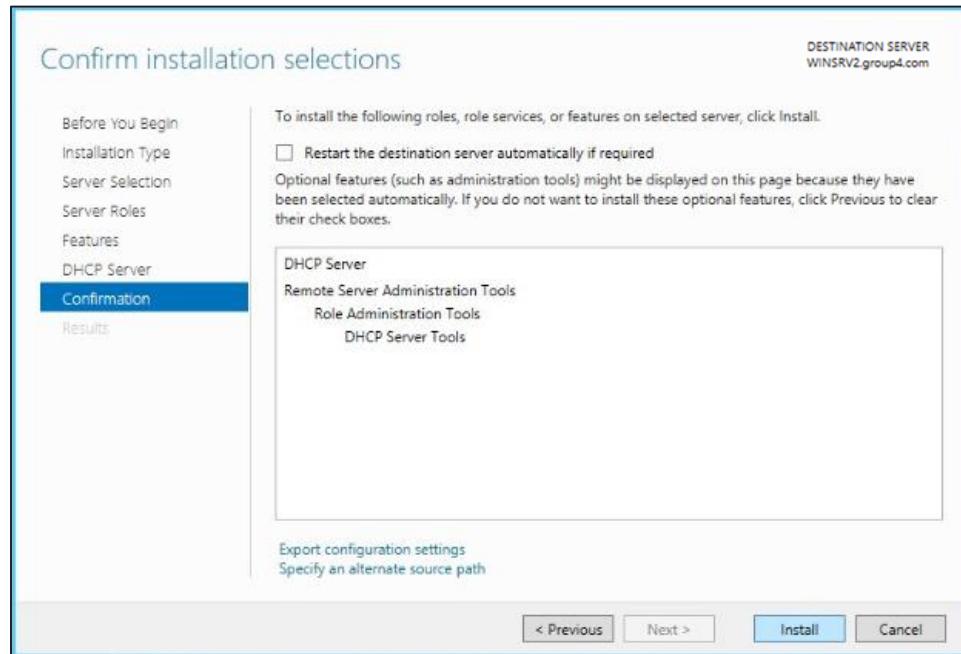


Figure 5.3.2.31: Confirmation installation

Step 32: Installation in progress. Wait until the progress finish

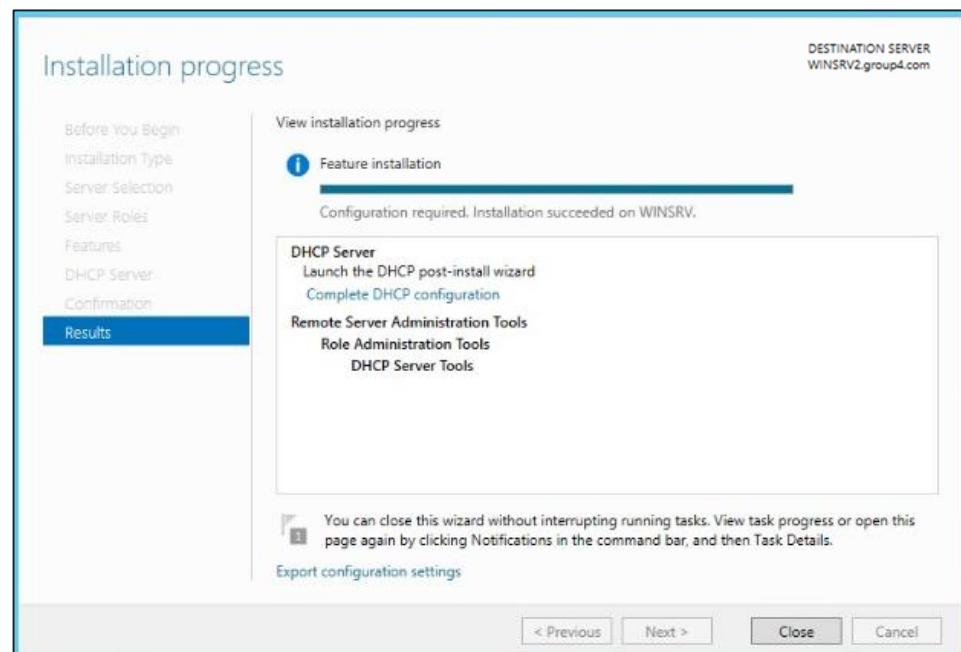


Figure 5.3.2.32 : Installation progress

Step 33: DHCP installed and can be view at the dashboard

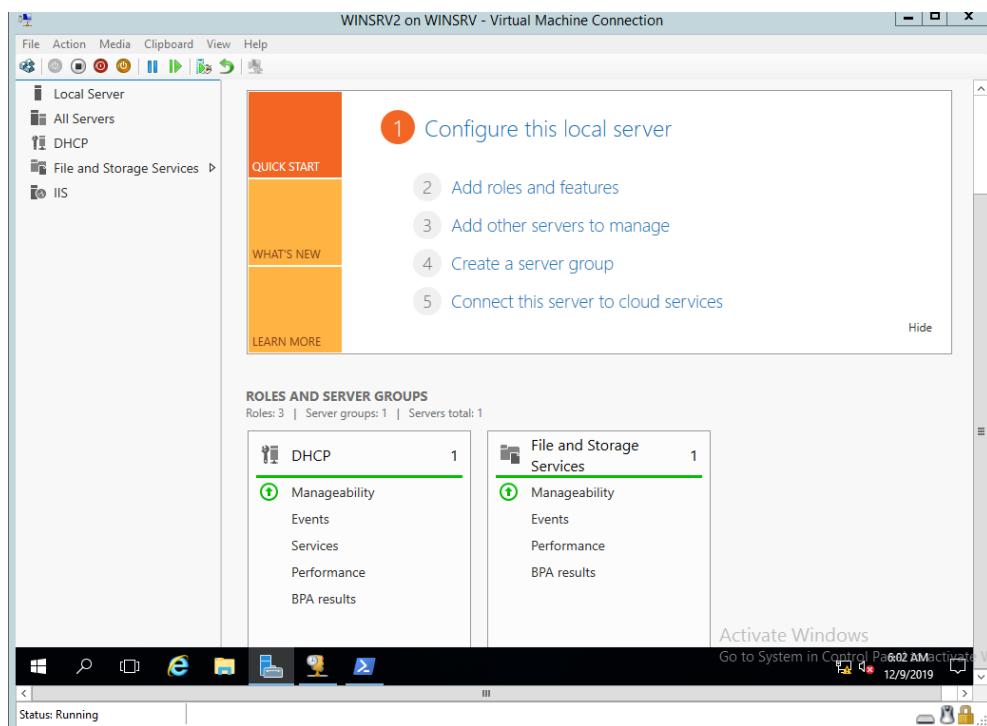


Figure 5.3.2.33 : DHCP installed

Step 34: Open DHCP management console. Click IPv4 and click “Configure Failover”

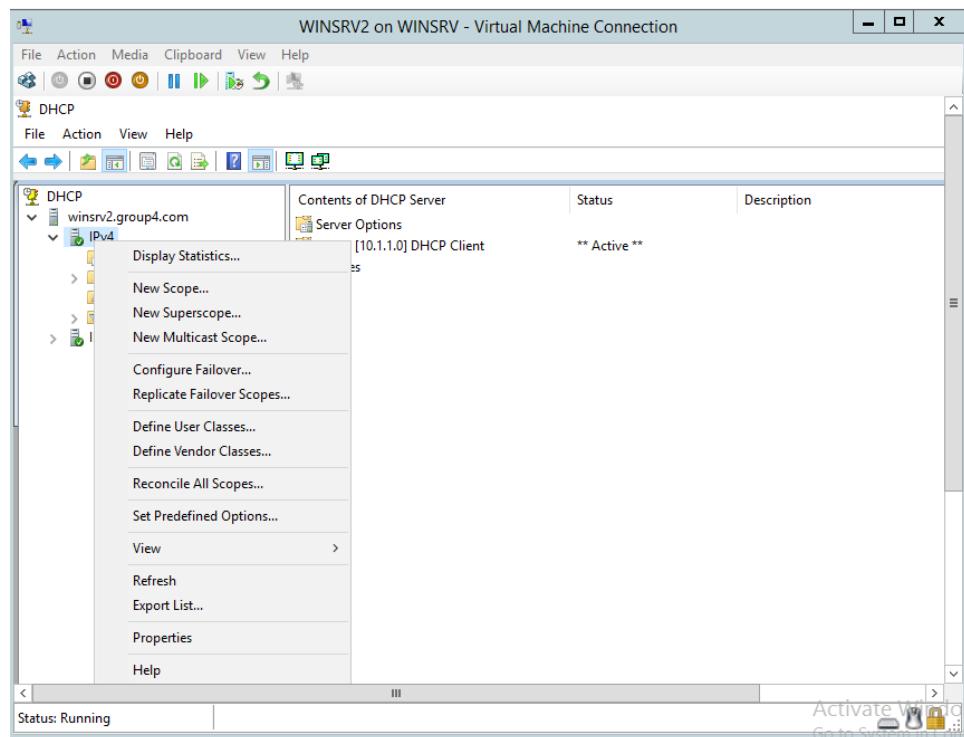


Figure 5.3.2.34 : Configure failover

Step 35: Create a new failover relationship by choosing mode load balance

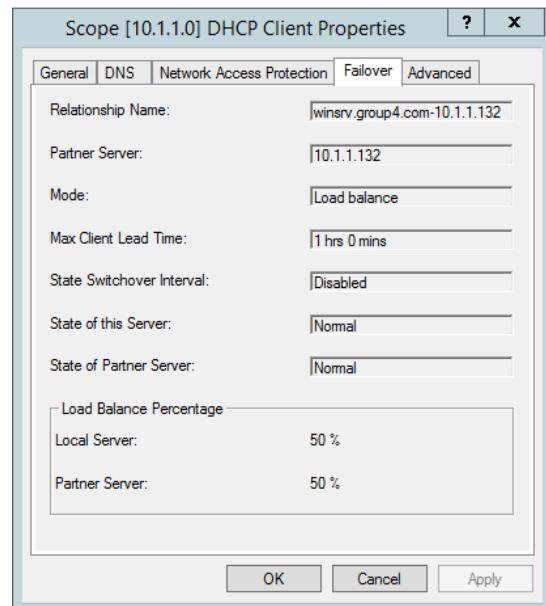


Figure 5.3.2.35 : New failover relationship

Step 36: Log of progress for configuring failover are successful

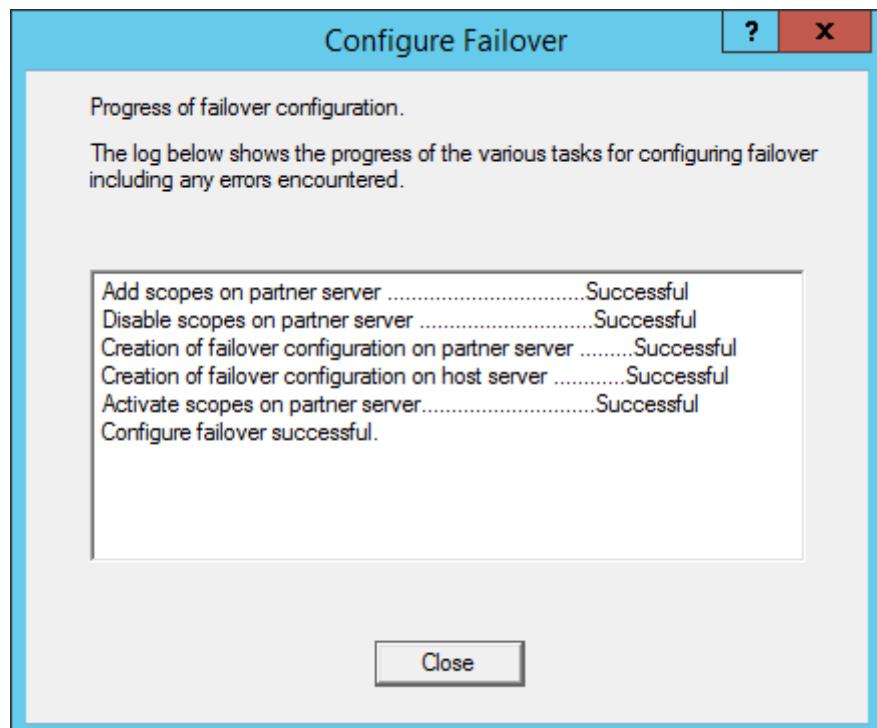


Figure 5.3.2.36 : Log of various task

5.3.3 Active Directory with UAC/GPO

Active Directory Domain Services

Install Active Directory Domain Services on Windows Server 2012 is using the server to become a domain controller.

Step 1: Add roles on server by select Active Directory Domain Services

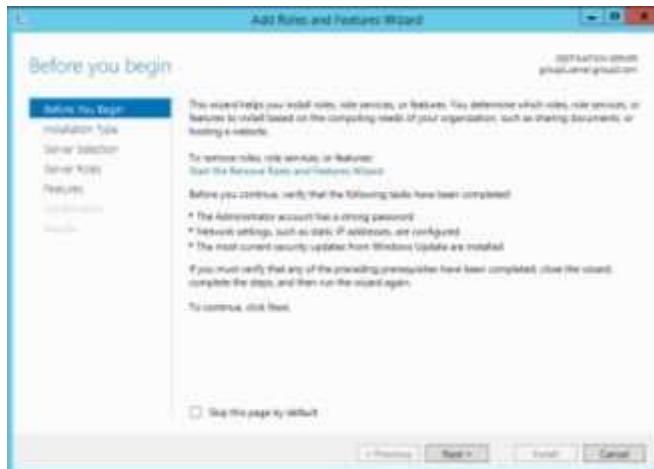


Figure 5.3.3 1: Add Roles and Features Active Directory

Step 2: Install Active Directory Domain Services by proceed Next

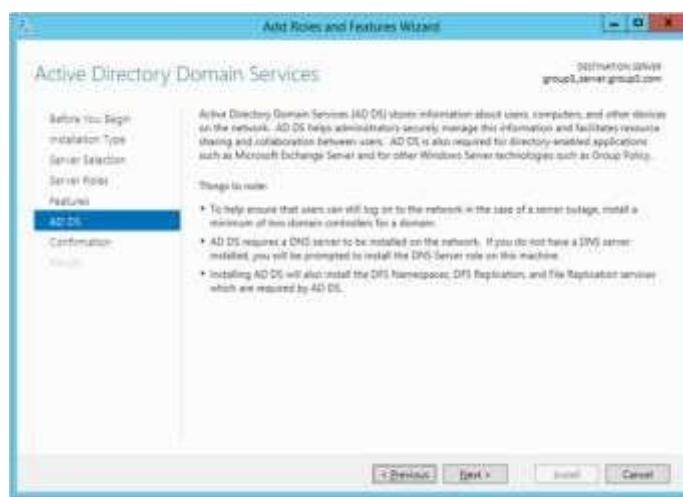


Figure 5.3.3.2: Install Active Directory Domain Services.

Step 3: Confirm the Installation of Active Directory Domain by clicking Install

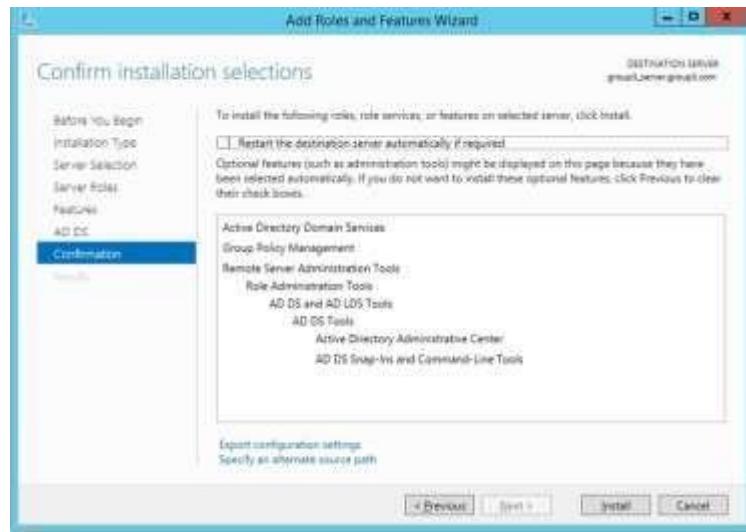


Figure 5.3.3.3: Confirmation Installation Active Directory.

Step 4: Finish the Installation finish of the Active Directory Domain Service.

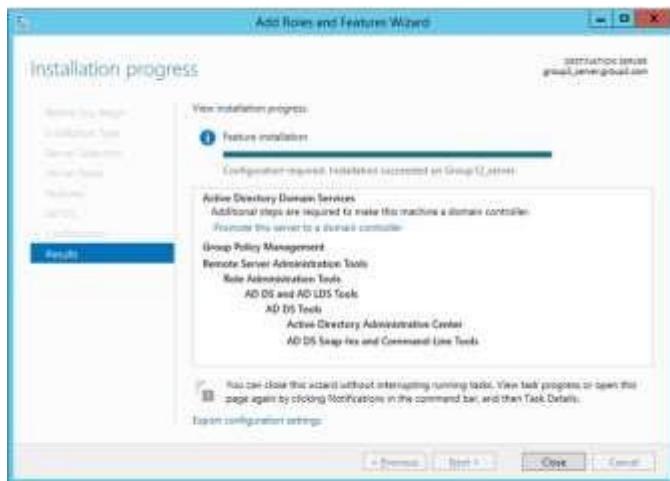


Figure 5.3.3.4 Installation Progress Active Directory Domain Services.

Step 5: Configure Active Directory Services by add a new forest and put the domain name group3.com

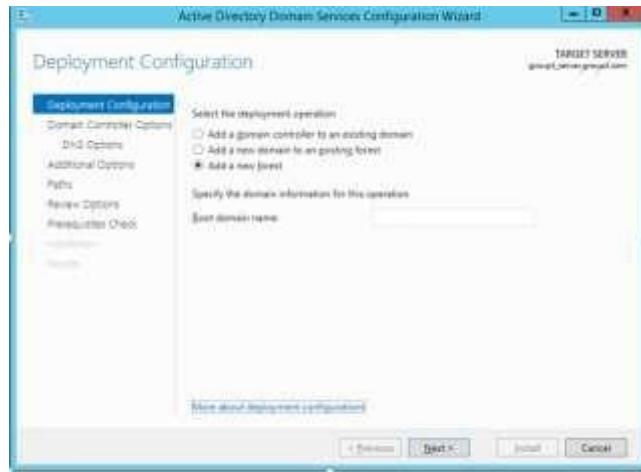


Figure 5.3.3.5: Deployment Configuration Active Directory Domain Services

Step 6: setting Domain Controller Option by set the password

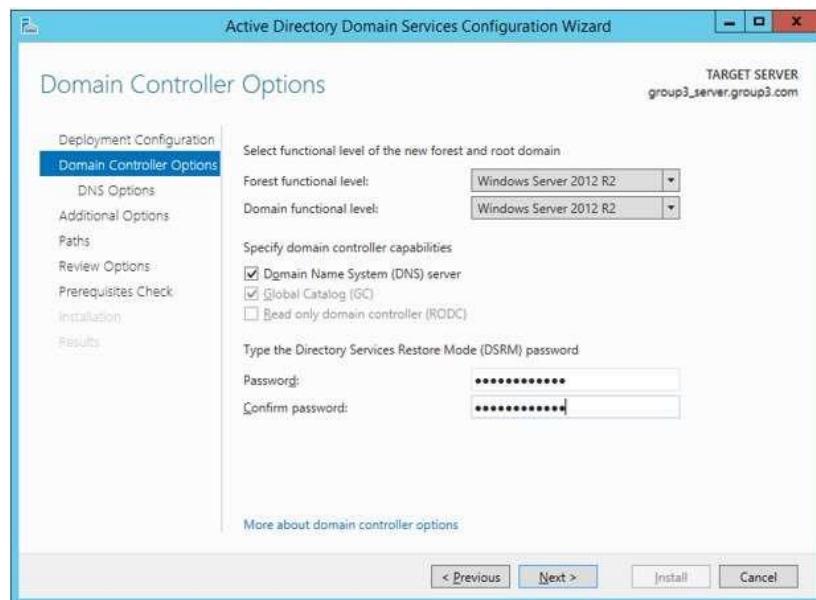


Figure 5.3.3.6: Setting Domain Controller Active Directory Services.

Step 7: Waiting for The NetBIOS domain name verify and click next.

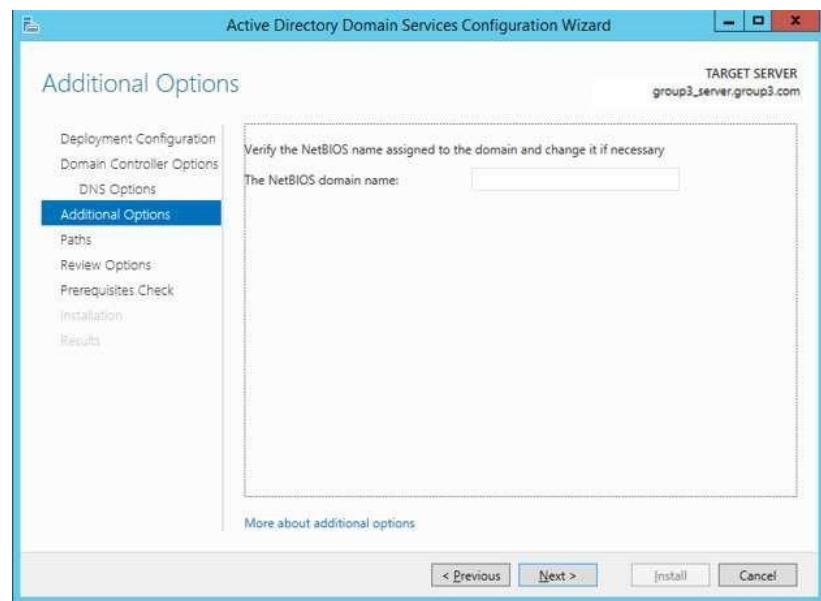


Figure 5.3.3.7: Additional Options Active Directory Services

Step 8: specify the location of AD DS Database, log file and SYSVOL

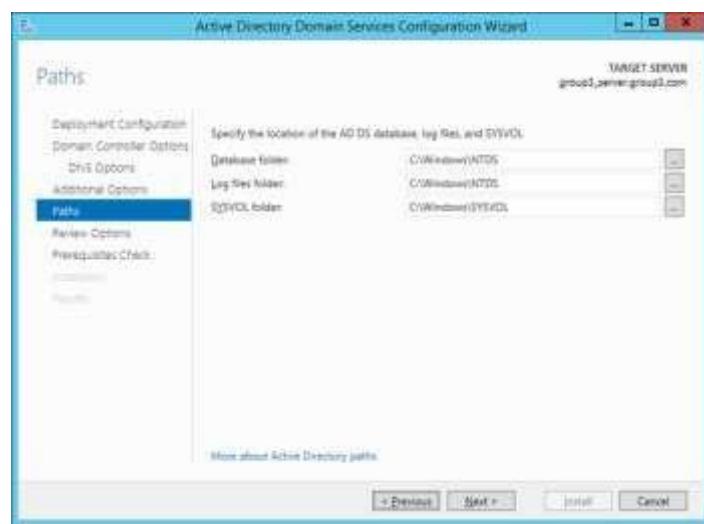


Figure 5.3.3.8: Configuration Paths Active Directory Domain Services

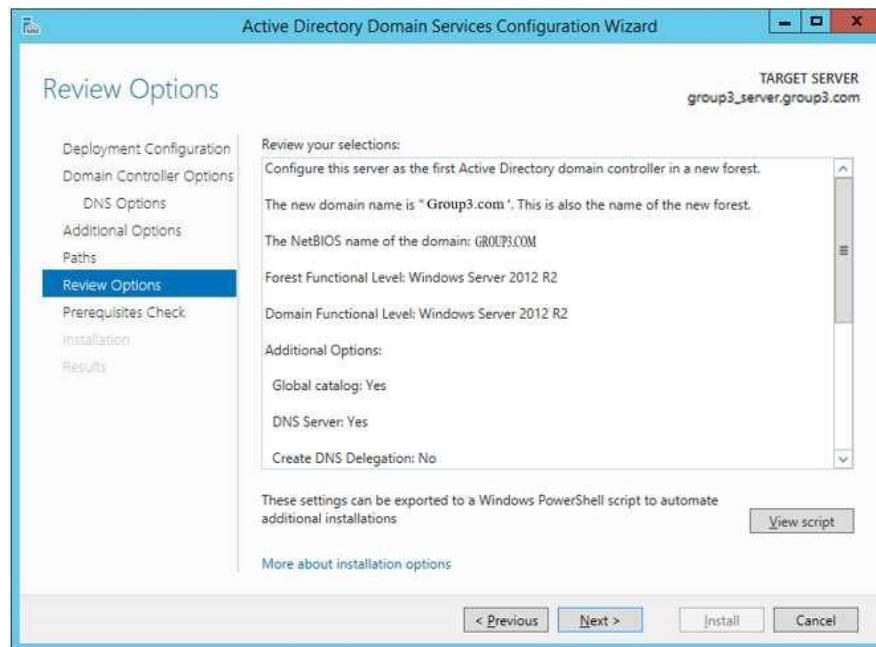
Step 9: Review the selection and success configure Active Directory

Figure 5.3.3.9: Review Options Active Directory.

Step 10: Restart the computer to complete the installation process Active Directory Domain.

Configuration Active Directory User and Computers UAC (New Account User)

Step 1: Click Tool on the dashboard windows server, then click Active Directory Users and Computers.

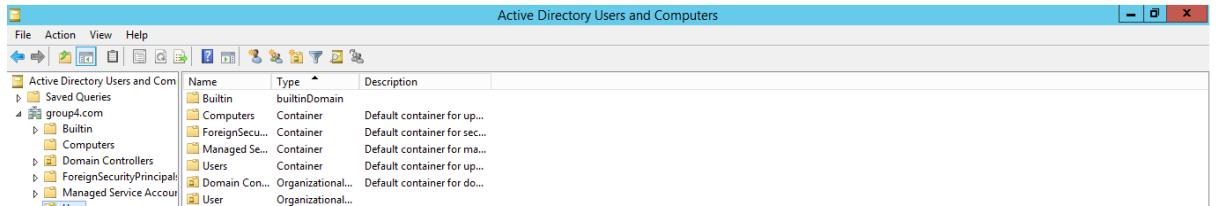


Figure 5.3.3.10: User and Computer Active Directory.

Step 2: Under group4.com on the user, right click then select new object user. Fill the form then click next.

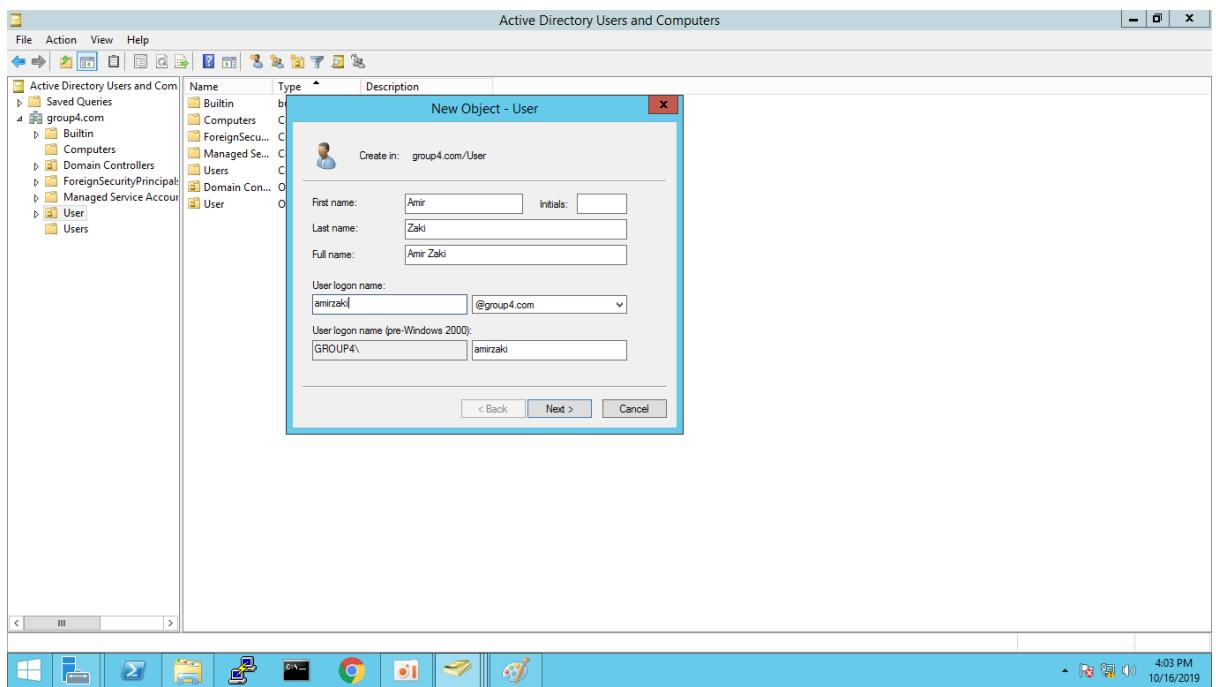


Figure 5.3.3.11: New Object – User.

Step 3: Insert the password of the new user, then tick the small box that determine “User must change password at next logon”. Click next and finish.

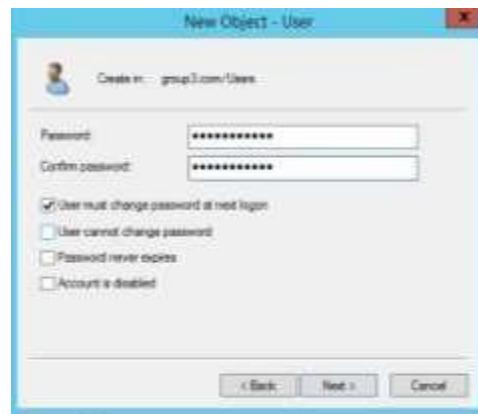


Figure 5.3.3.12: Insert default password the user.

Step 4: The new user already add on the domain controller.

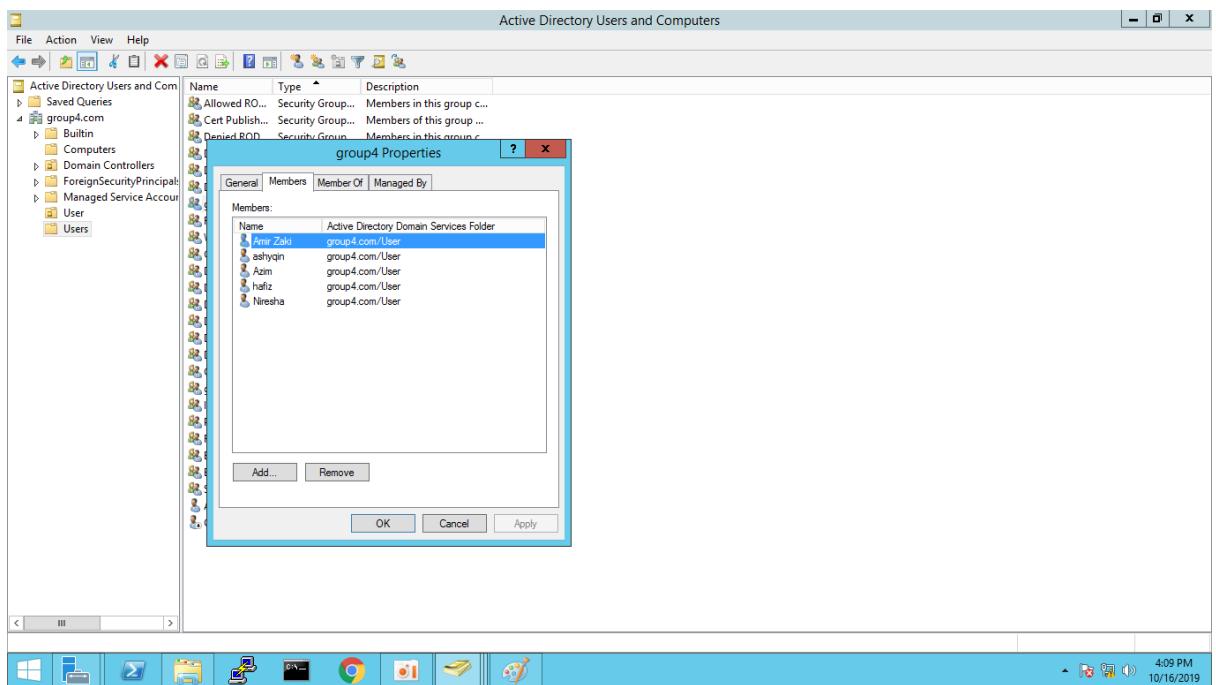


Figure 5.3.3.13: List User Active Directory

Group Policy Management (GPO)

Implementation group policy in active directory to controls the working environment of user accounts and computer accounts.

Step 1: Before go to group policy management. First create a new Organizational unit.

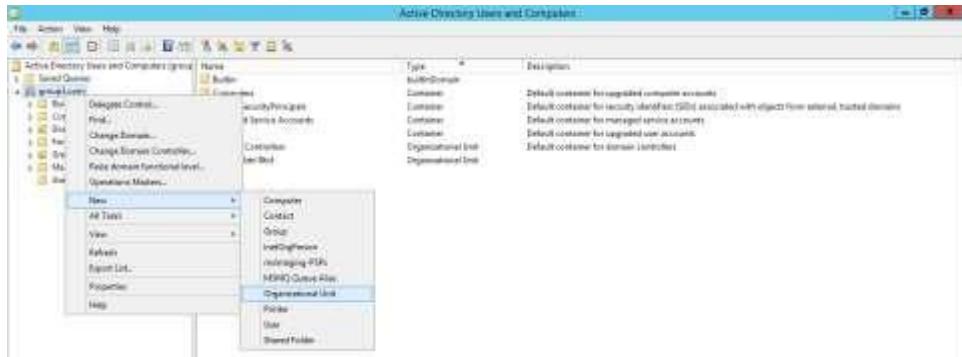


Figure 5.3.3.14: Create new Organizational Unit.

Step 2: Insert Group4 then click OK.

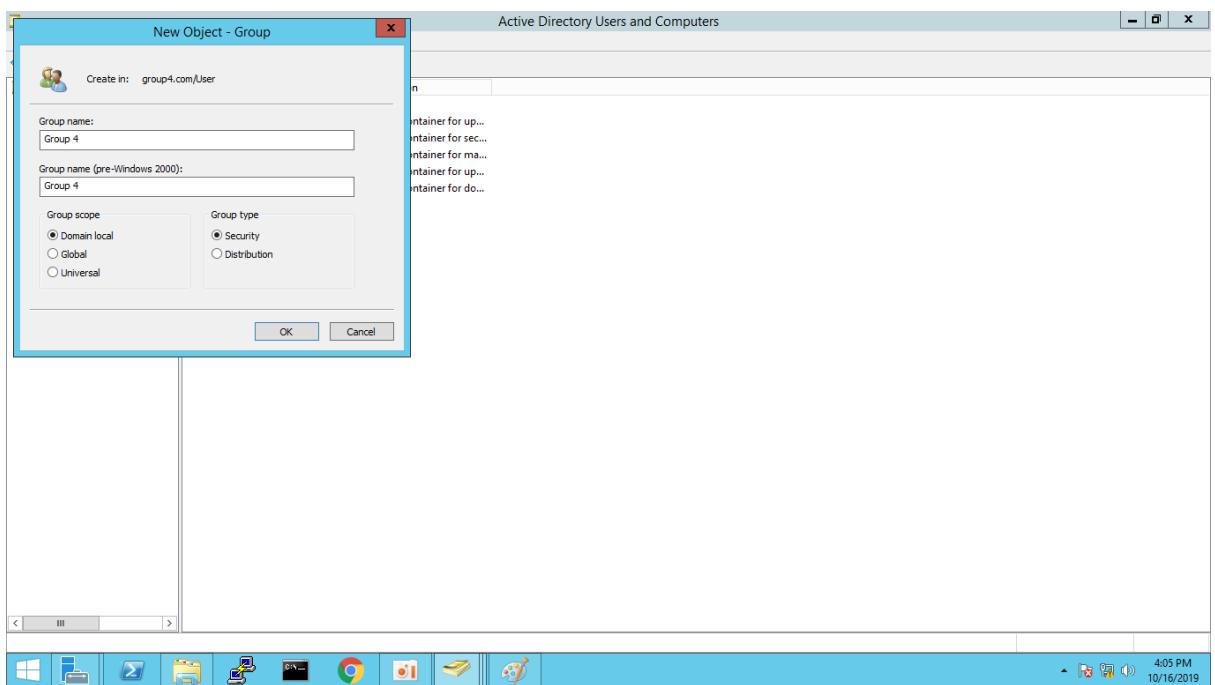


Figure 5.3.3.15: Insert the name Organizational Unit.

Step 3: Right click all the user, then click move.

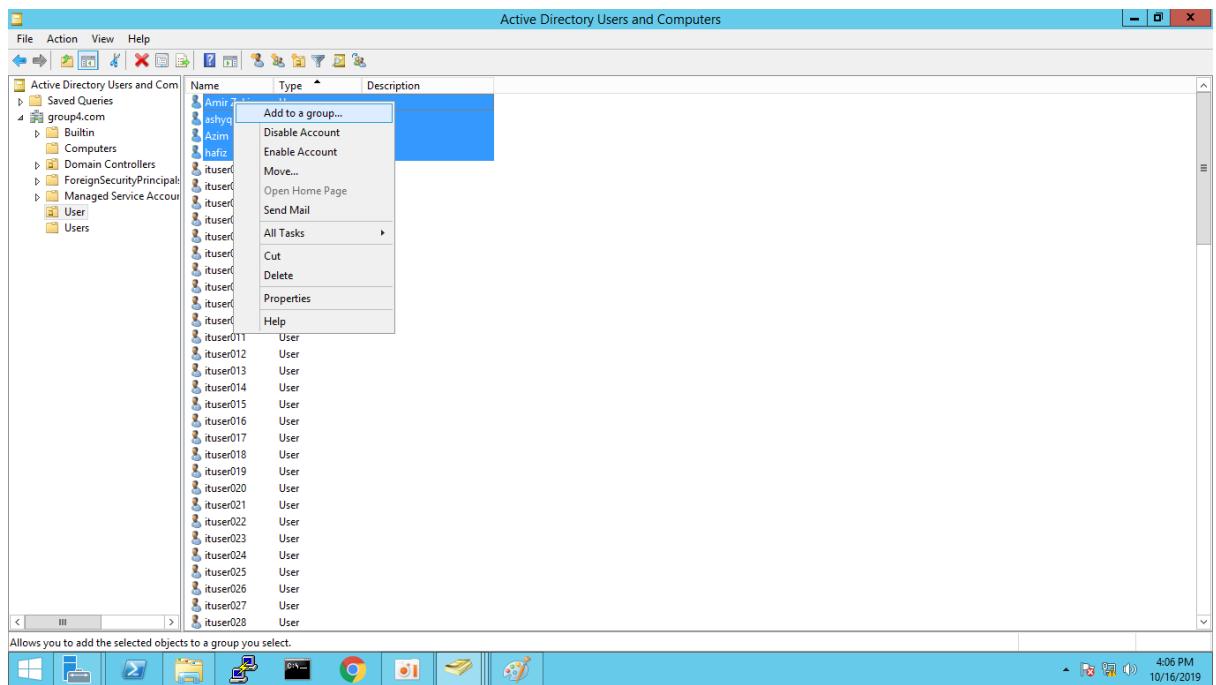


Figure 5.3.3.16: Move the user Active Directory.

Step 4: Move the user to Group4. Then click OK.

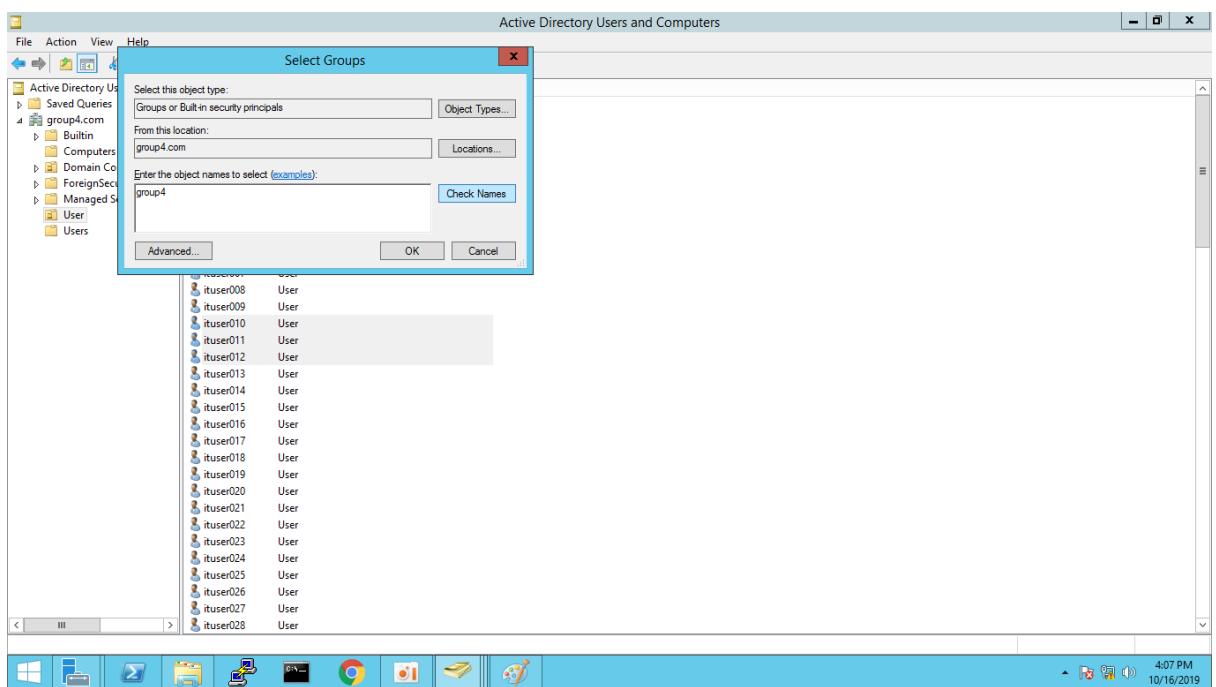


Figure 5.3.3.17: Move the user to the new Organizational Unit

Step 5: Open the dashboard in windows server, then click on tool. Open the Group Policy Management.



Figure 5.3.3.18 Group Policy Management Menu

Step 6: Under Forest: group4.com, click Group4. Then right click, select new GPO, insert the name Group4 policy.

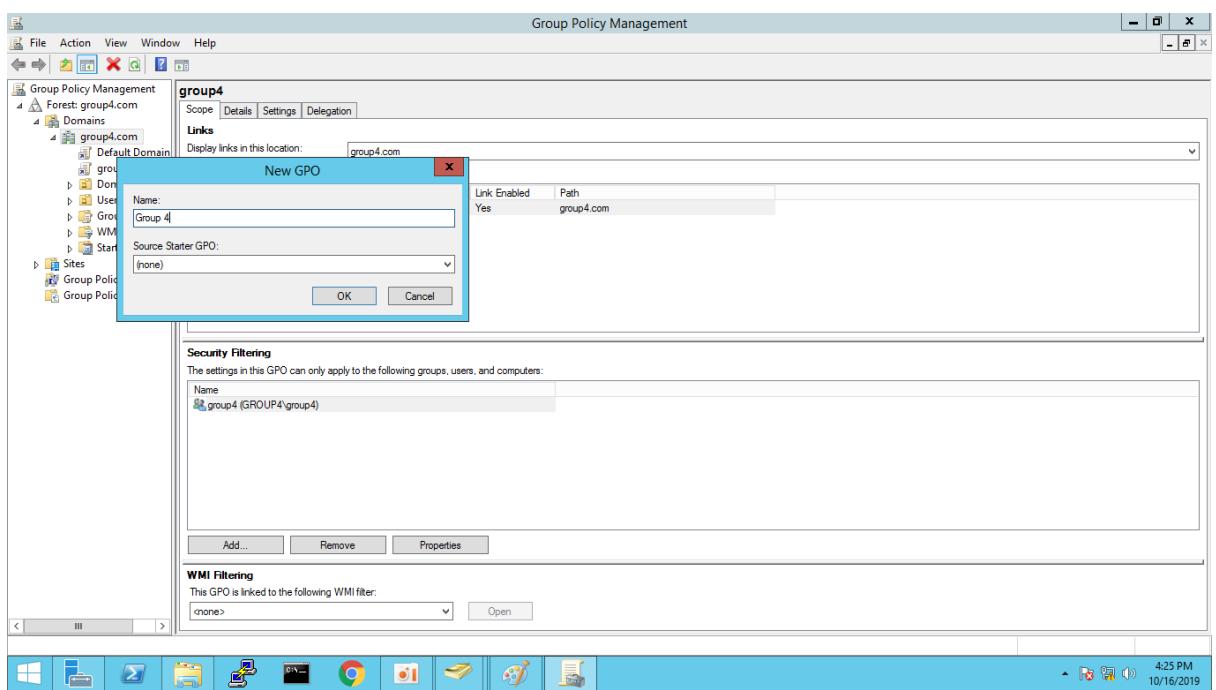


Figure 5.3.3.19 Create new GPO policy.

Step 7: After creating a new policy, right click Group4 policy then click edit.

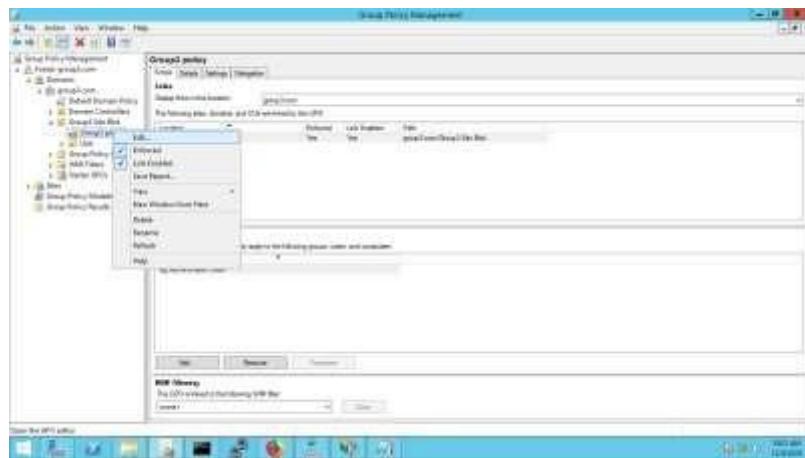


Figure 5.3.3.20: Edit the group policy.

Step 8: Inside the group policy management editor, click the user configuration after that click Policies then click Administrative Template.

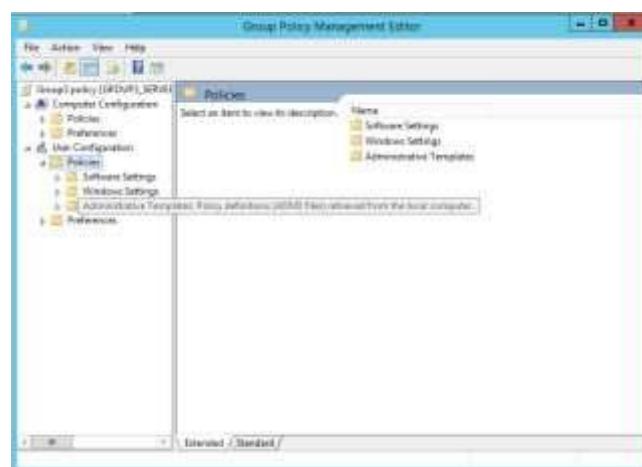


Figure 5.3.3.21: List policies in group policy management editor.

Step 9: Click System, select “Prevent access to the command prompt”

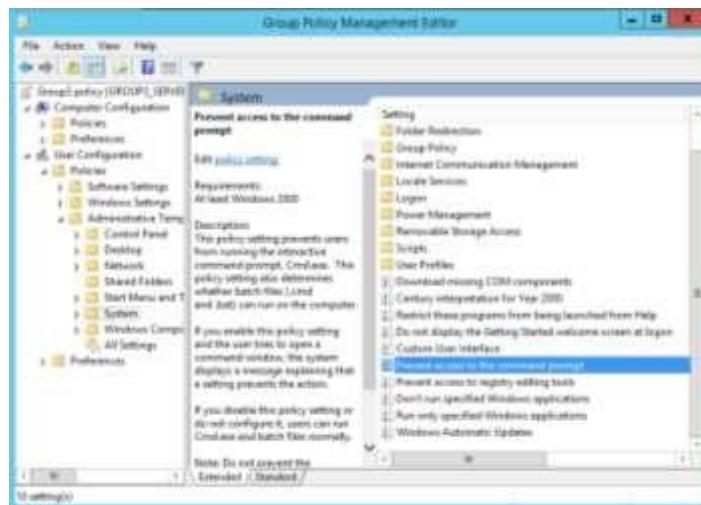


Figure 5.3.3.22: List of policy in System.

Step 10: Click enabled, then click OK.



Figure 5.3.3.23: Enable the policy command prompt.

Step 11: Under System, select “All Removable Storage classes: Deny all access”

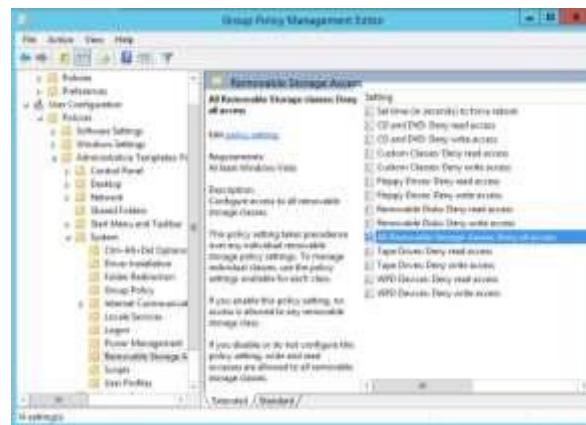


Figure 5.3.3.24 List of policy Removable Storage Access.

Step 12: Click enabled, then click OK.

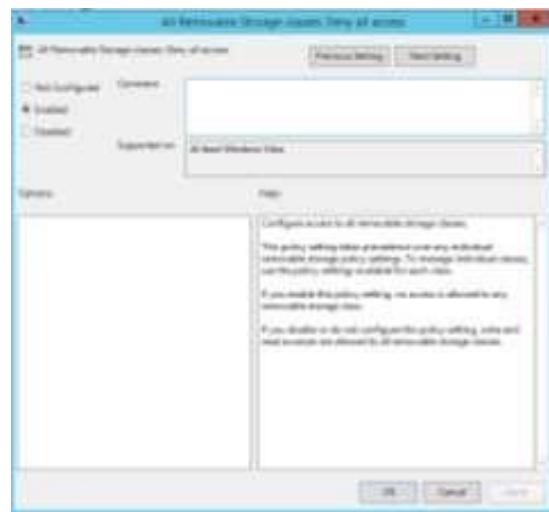


Figure 5.3.3.25 Enable the policy All Removable Storage Access.

Step 13: Click Group4.com, then click setting. It will show update policy on Group4.



Figure 5.3.3.26 Summary update policy.

Step 14: To active the policy, go to command prompt type “gpupdate /force”.

```
C:\>Administrator: Command Prompt
C:\>gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\>
```

Figure 5.3.3.27: Update policy on the command prompt.

5.3.4 Domain Name System

Domain Name System (IPv4 & IPv6)

Step 1: Add Roles and Features Wizard

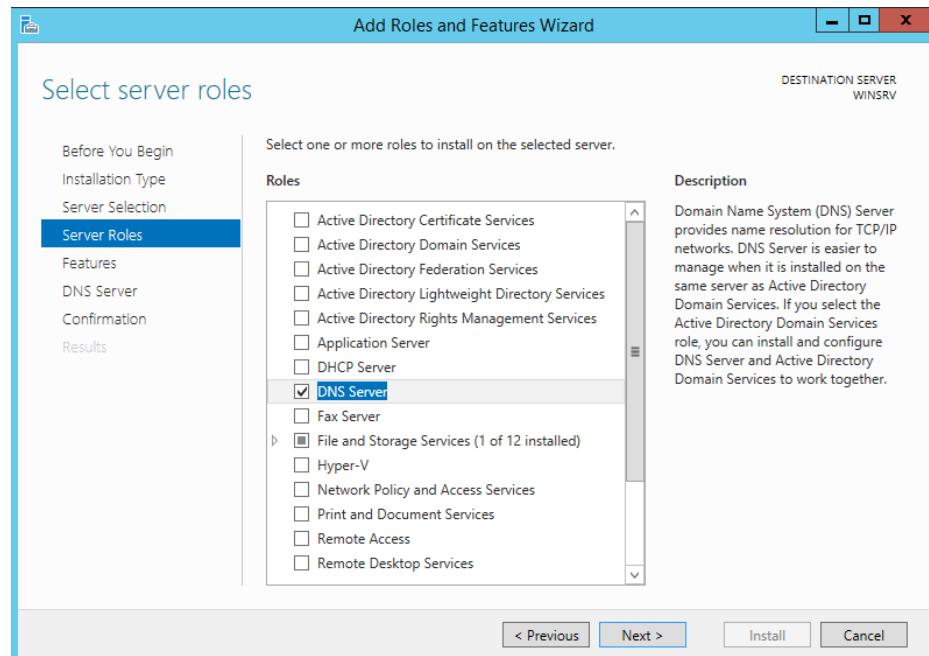


Figure 5.3.4.1: Add Roles for DNS Server

Step 2: Wait until installing DNS server complete.

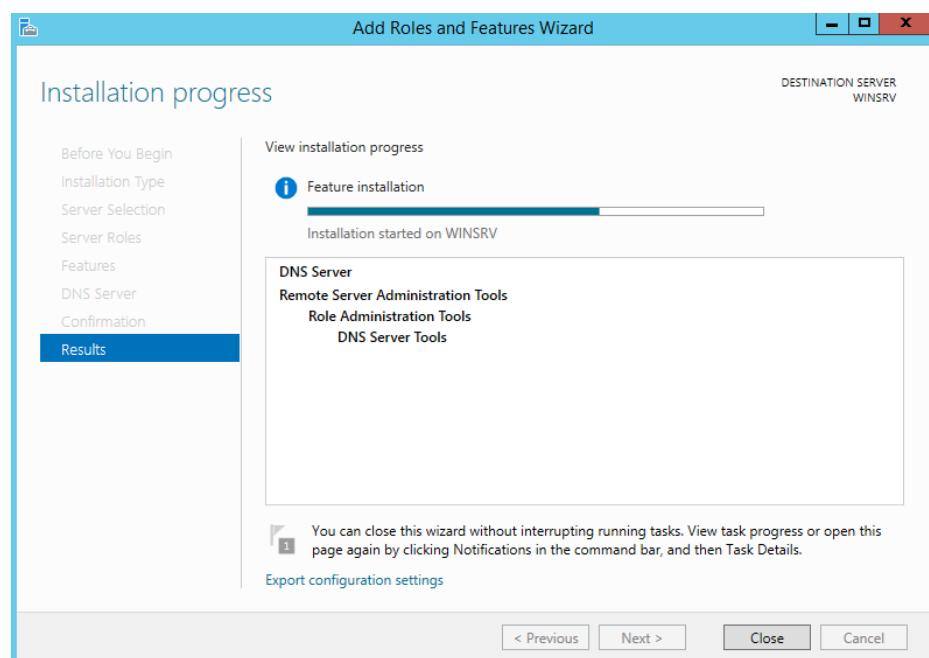


Figure 5.3.4.2: DNS Server Installation Progress

Step 3: Go to “tools” option and click on DNS to configure.

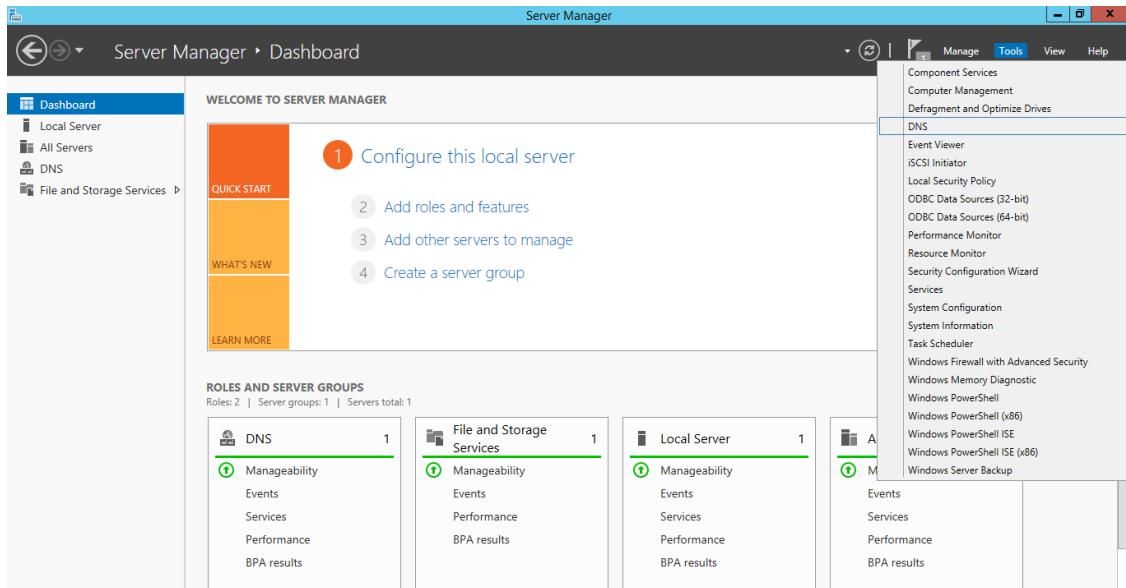


Figure 5.3.4.3: Option to Configure DNS

Step 4: In DNS manager, click on WINSRV to view list of zone. Then, right click on *Forward Lookup Zone* to add new zone.

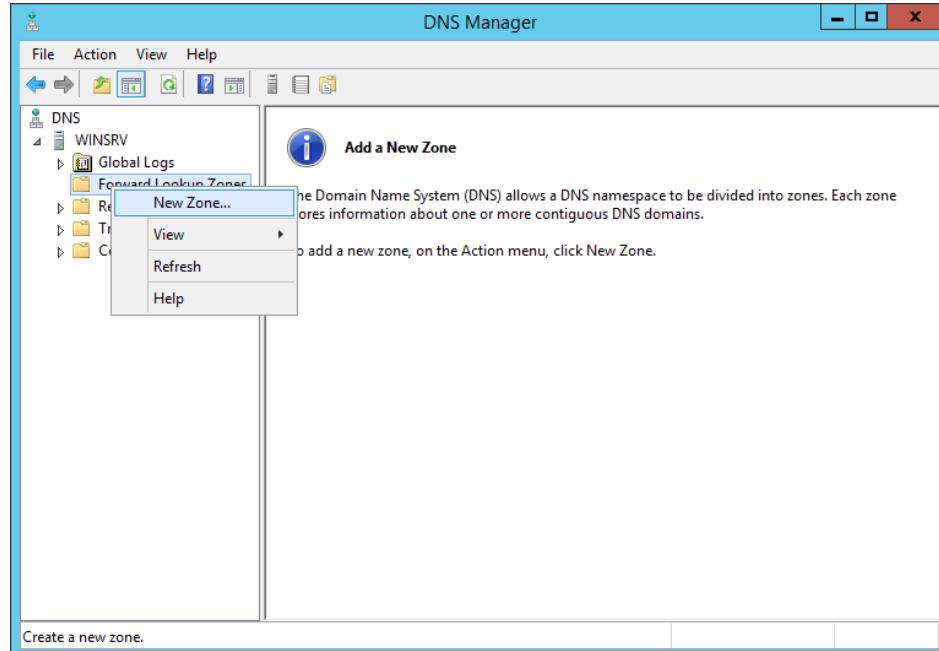


Figure 5.3.4.4: DNS Manager

Step 5: Configure DNS server wizard for Forward Lookup Zone.



Figure 5.3.4.5: New Zone Wizard

Step 6: Choose zone type as *primary zone* and then click next.

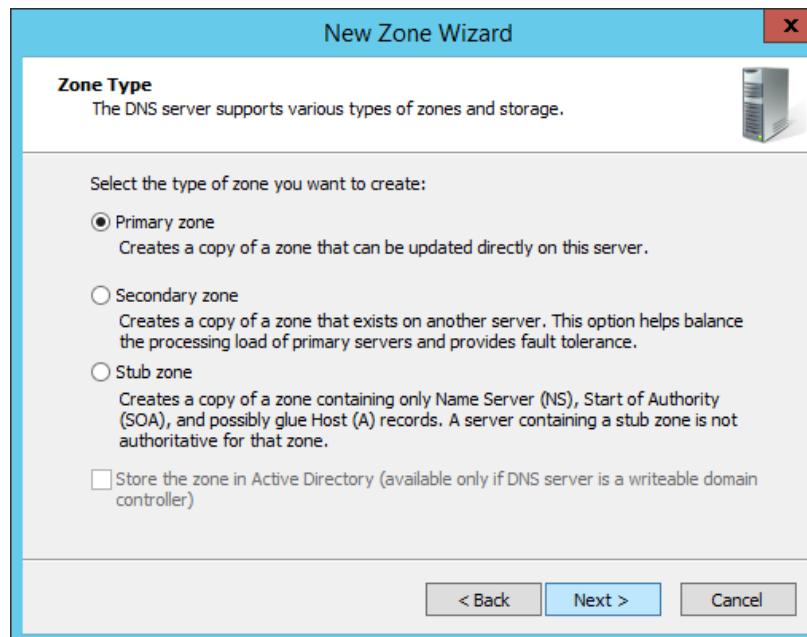


Figure 5.3.4.6: Select Zone Type

Step 7: Then, enter the zone name as “group4.com” to set zone name.

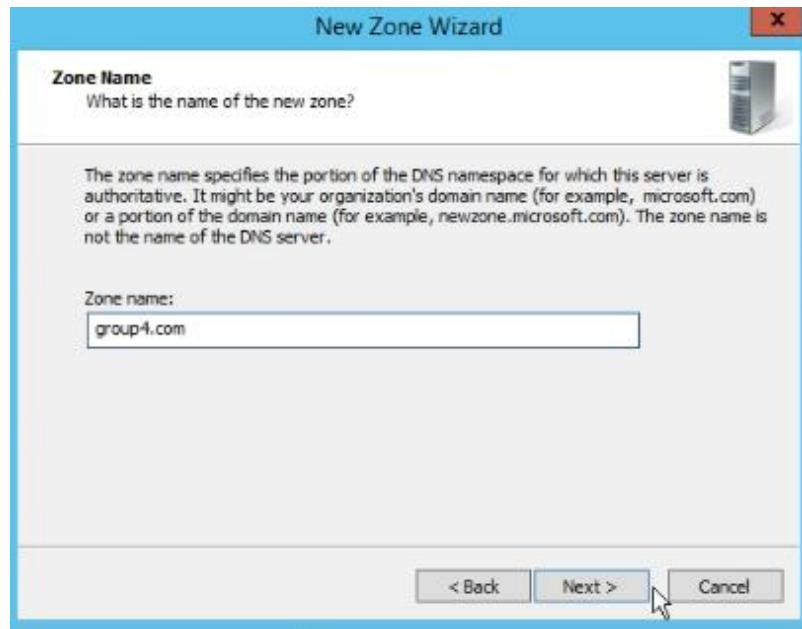


Figure 5.3.4.7: Set Zone Name

Step 8: Then, choose option Create a new file with this file name and click Next.



Figure 5.3.4.8: Set New File

Step 9: Successfully completed Forward Lookup DNS. Click Finish.



Figure 5.3.4.9: Completed Forward Lookup

Step 10: Next, right click on top of Reverse Lookup Zone and click New Zone. Click Next



Figure 5.3.4.10: New Zone Wizard for Reverse Lookup

Step 11: For Reverse Lookup Zone Name, select IPv4 Reverse Lookup Zone and click Next.

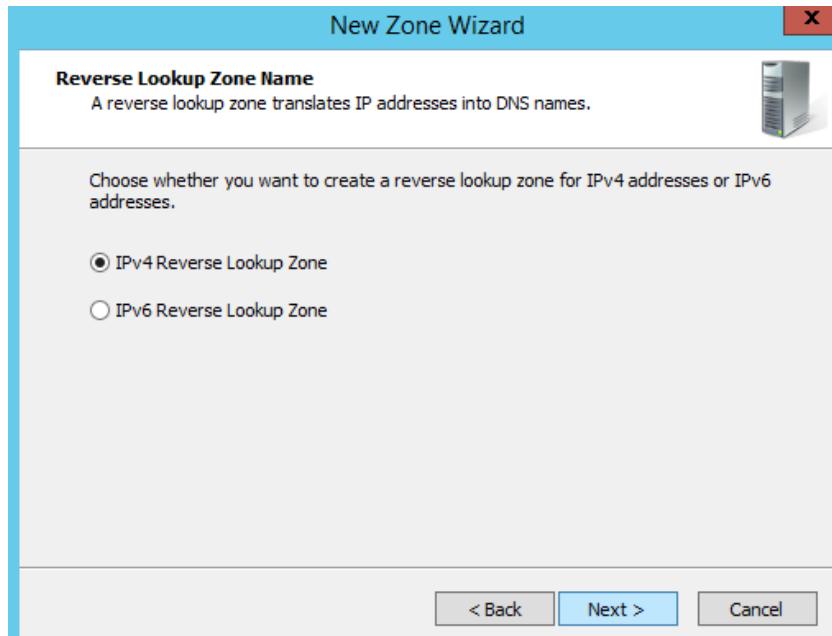


Figure 5.3.4.11: Reverse Lookup Zone Name

Step 12: Enter Network ID for the zone and click Next button.

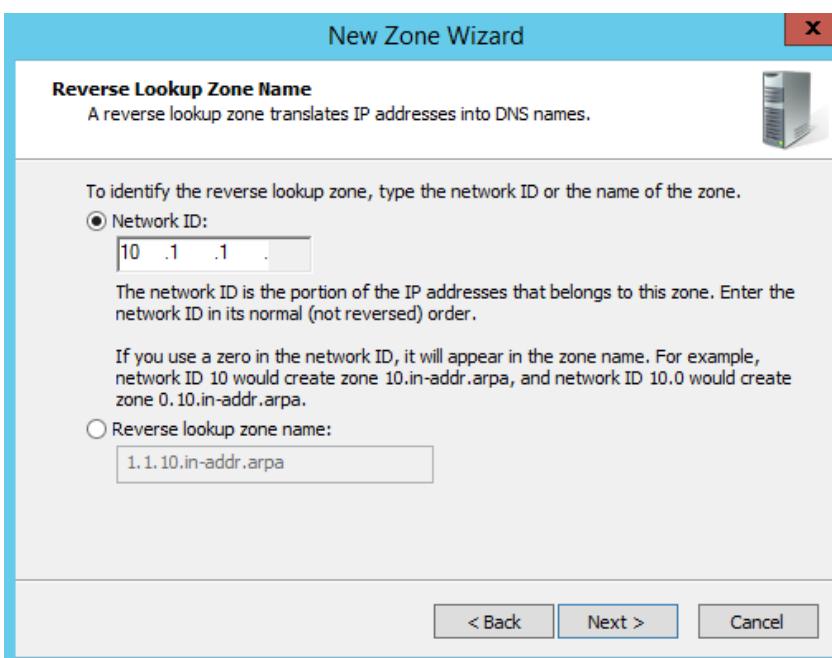


Figure 5.3.4.12: Enter Network ID

Step 13: Then, choose option Create a new file with this file name and click Next.

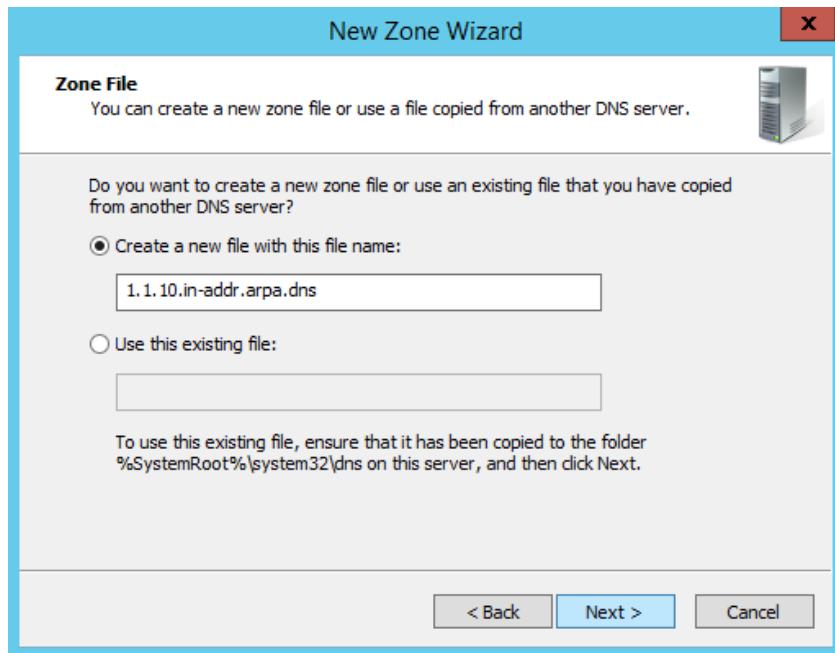


Figure 5.3.4.13: Create Zone File

Step 14: Choose Allow for dynamic update and click Next.

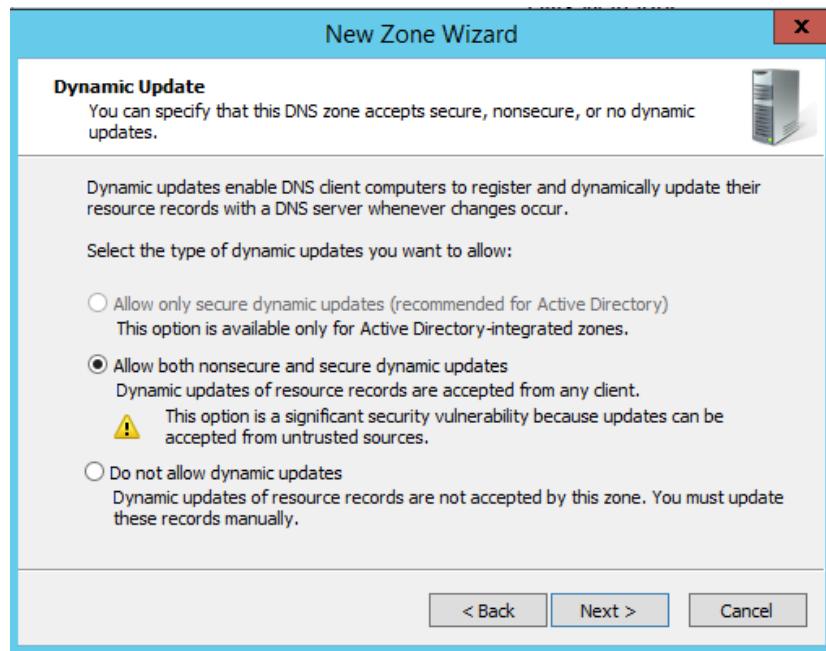


Figure 5.3.4.14: Enable Dynamic Updates

Step 15 Successfully completed IPv4 Reverse Lookup Configuration. Click Finish

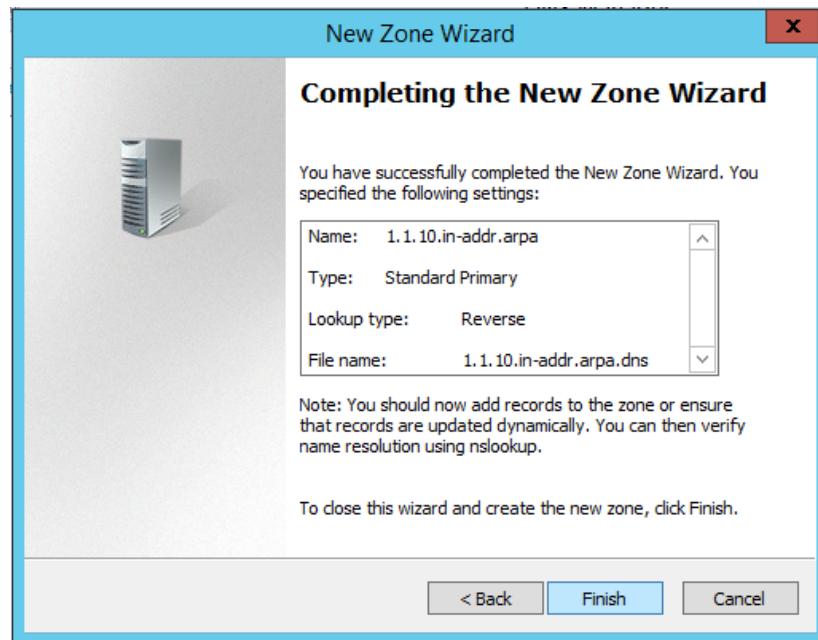


Figure 5.3.4.15: Completed IPv4 Reverse Lookup

Step 16: Go to DNS Manager, right click on top Reverse Lookup Zone and add New Zone.

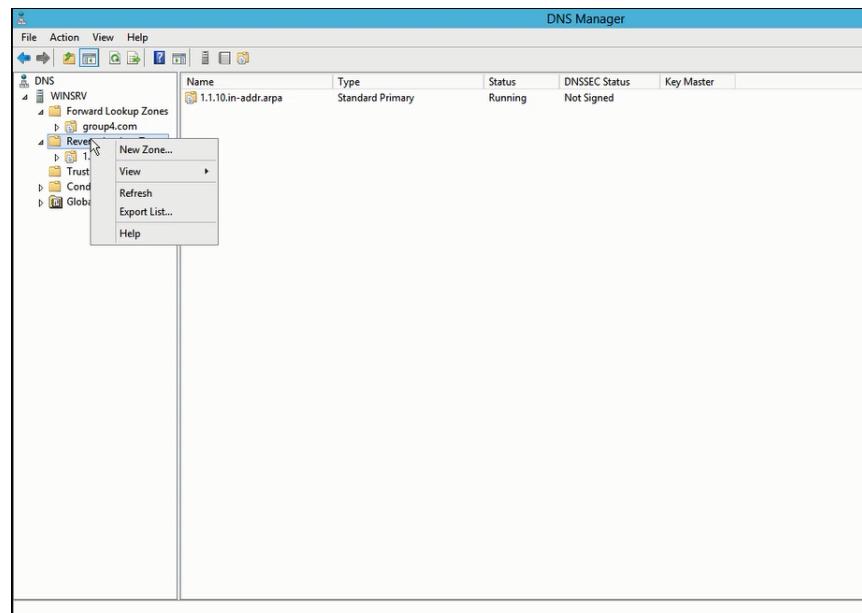


Figure 5.3.4.16: Add New Zone



Figure 5.3.4.17: New Zone for IPv6 Reverse Lookup

Step 17: Select IPv6 Reverse Lookup Zone and click Next.

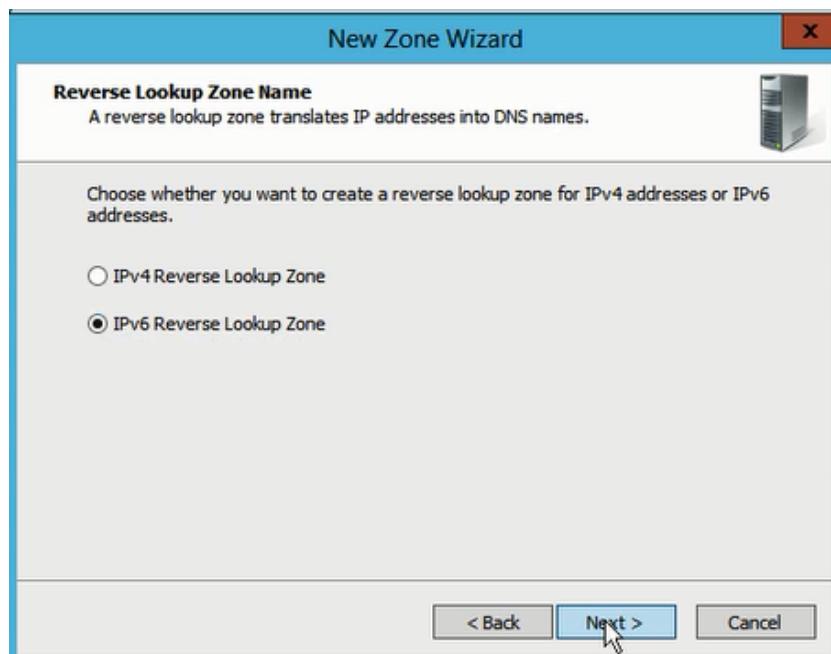


Figure 5.3.4.18: Select Reverse Lookup Zone Name

Step 18: Enter IPv6 Address Prefix and click Next.

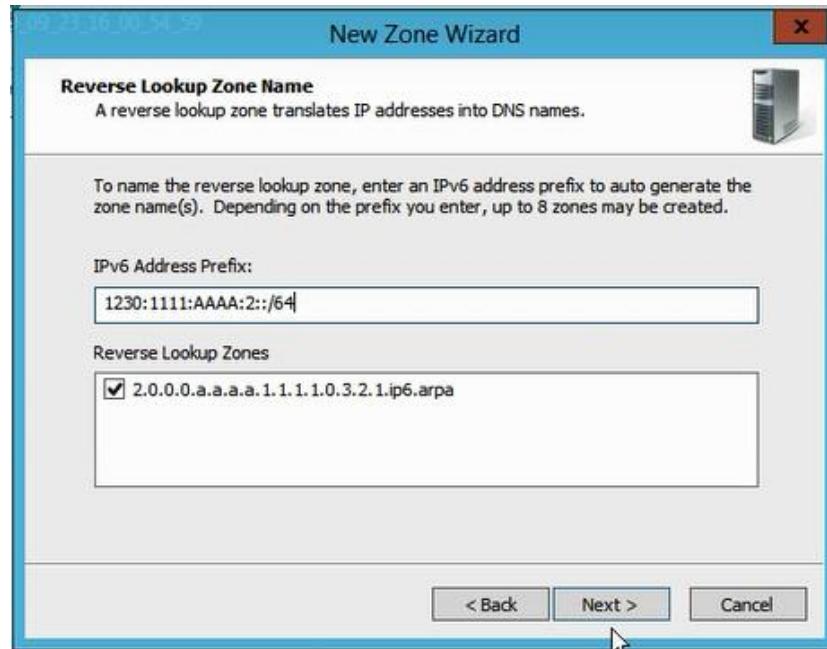


Figure 5.3.4.19: Set IPv6 Address Prefix

Step 19: Select option Create new file with this file name and then click Next.



Figure 5.3.4.20: Select Zone File

Step 20: Successfully completed IPv6 Reverse Lookup Configuration.

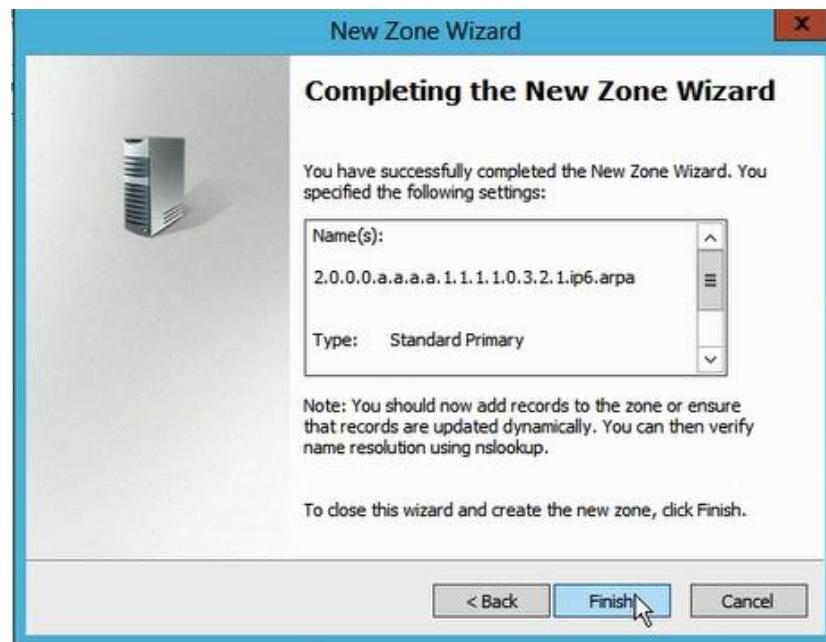


Figure 5.3.4.21: Completed IPv6 Reverse Lookup

Step 21: Go to DNS Manager, Verify DNS Resources

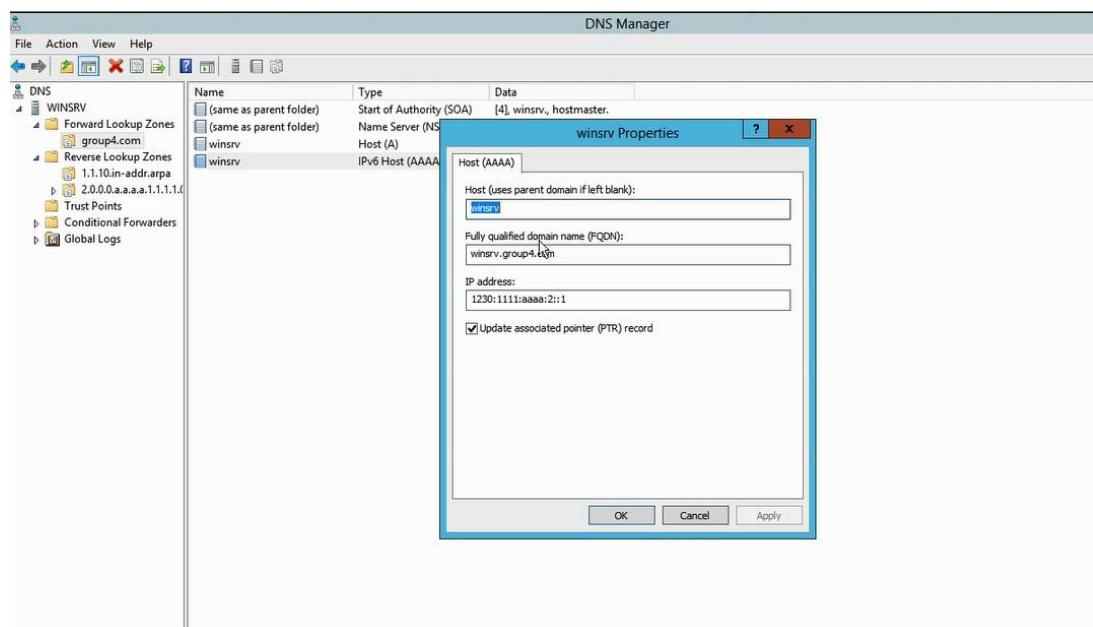


Figure 5.3.4.22: DNS Resources

Step 22: Click on parent folder properties to check server name that recorded.

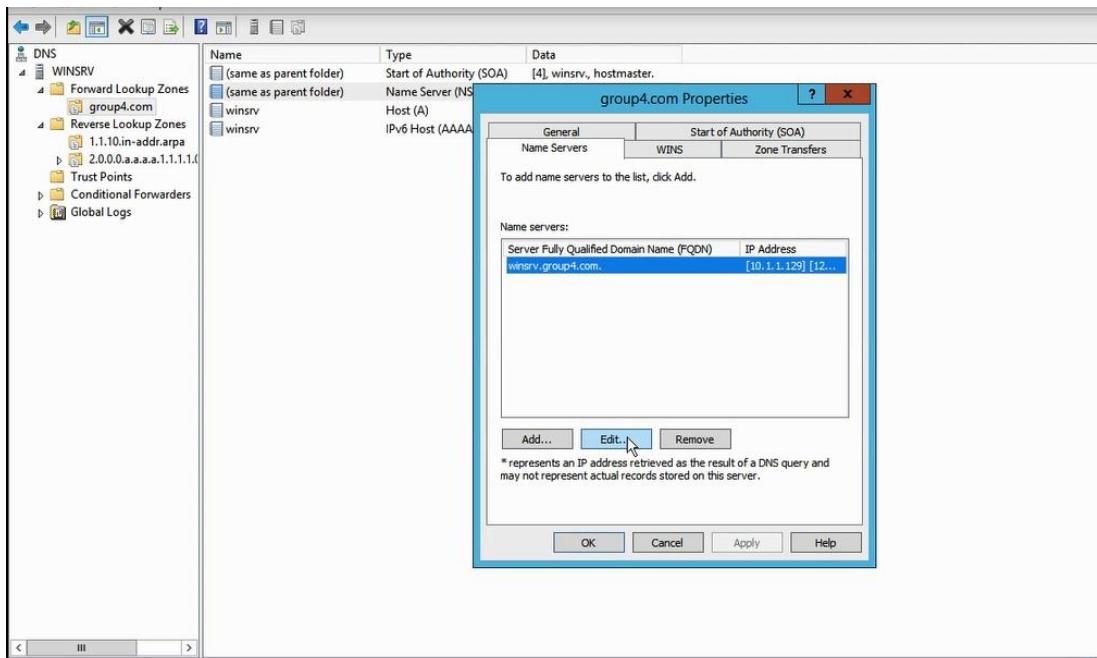


Figure 5.3.4.23: DNS Resources

Step 23: Verify Server Name, IPv4 and IPv6.

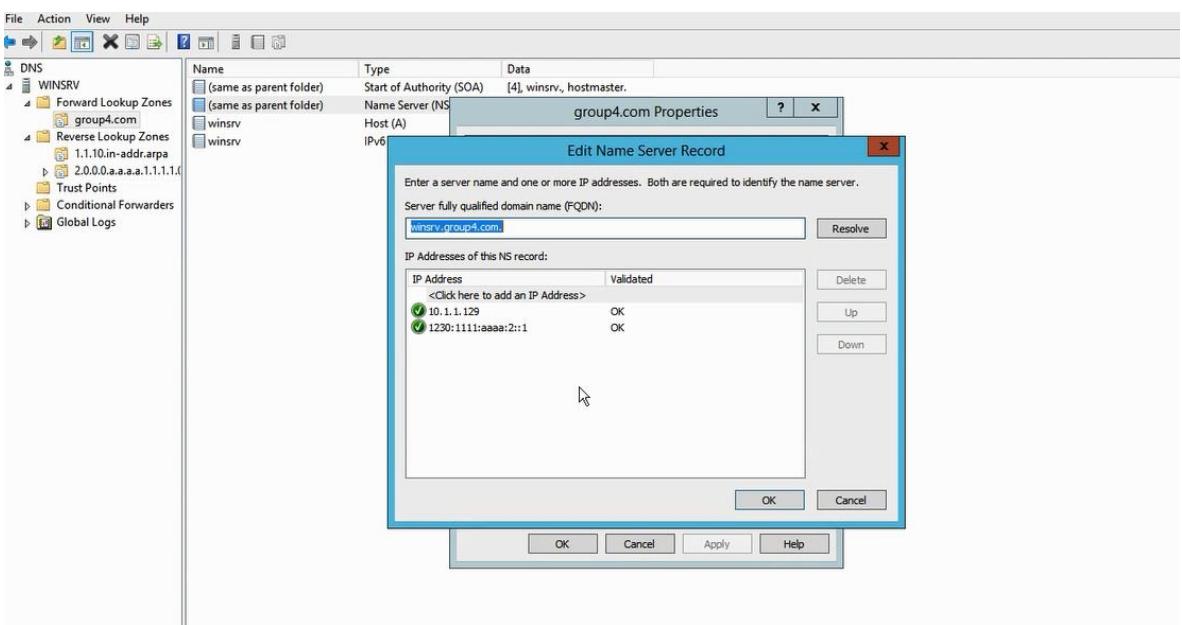


Figure 5.3.4.24: Server Record

Step 24: check at nslookup to verify the successfully created Domain Name for Windows, Debian, Ubuntu Server.



Figure 5.3.4.25: Terminal

5.3.5 Linux Email Server

Linux Mail Server

Step 1: Install postfix and dovecot for email service

```
root@debian:~# apt install postfix dovecot-imapd
Reading package lists... Done
Building dependency tree
Reading state information... Done
dovecot-imapd is already the newest version (1:2.2.27-3+deb9u5).
postfix is already the newest version (3.1.12-0+deb9u1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@debian:~#
```

Figure 5.3.5.1: Installing email services command.

Step 2: Select Internet Site for postfix configuration since the common email service will connect to internet.

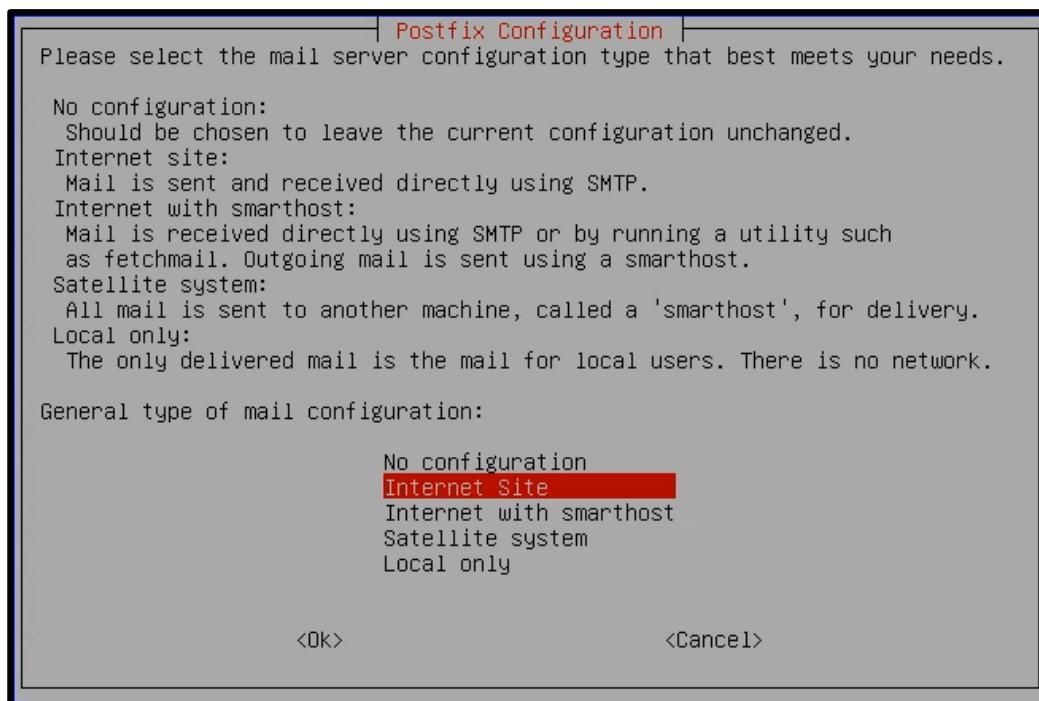


Figure 5.3.5.2: Select mail type for auto configuration by Postfix.

Step 3 : Enable encryption on smtp server by editing postfix configuration file in “/etc/postfix/main.cf” and locate your certificate for secure connection.

```
# TLS parameters
smtpd_tls_cert_file=/etc/certs/server.pem
smtpd_tls_key_file=/etc/certs/server.key
smtpd_use_tls=yes
```

Figure 5.3.5.3: Enable secure SMTP and locate the certificate.

Step 4: Disable port 25 and enable port 587 for email submission by client in “/etc/postfix/master.cf” file.

```
#dnsblog    unix  -      -      y      -      0      dnsblog
#tlsproxy   unix  -      -      y      -      0      tlsproxy
submission  inet n      -      y      -      -      -      smtpd
# -o syslog_name=postfix/submission
# -o smtpd_tls_security_level=encrypt
# -o smtpd_sasl_auth_enable=yes
# -o smtpd_reject_unlisted_recipient=no
# -o smtpd_client_restrictions=$mua_client_restrictions
# -o smtpd_helo_restrictions=$mua_helo_restrictions
# -o smtpd_sender_restrictions=$mua_sender_restrictions
# -o smtpd_recipient_restrictions=
# -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
# -o milter_macro_daemon_name=ORIGINATING
#smtps     inet n      -      y      -      -      -      smtpd
# -o syslog_name=postfix/smtps
# -o smtpd_tls_wrappermode=yes
# -o smtpd_sasl_auth_enable=yes
[ Read 124 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text^T To Spell  ^ Go To Line
```

Figure 5.3.5.4: Enable submission port and disable regular SMTP port 25.

Step 5: Configure dovecot for plain text login in “/etc/dovecot/conf.d/10-auth.conf” file.

```
# 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 = no
```

Figure 1.3.5.5: Enable plain login when connecting using telnet.

Step 6: Assign MAIL user in dovecot configuration file to create user email directory dynamically in “/etc/dovecot/conf.d/10-mail.conf” configuration file.

```
# Group to enable temporarily for privileged operations. Currently this is
# used only with INBOX when either its initial creation or dotlocking fails.
# Typically this is set to "mail" to give access to /var/mail.
mail_privileged_group = mail
```

Figure 5.3.5.2: Allow email spooling.

Step 7: Add DNS record for mail exchanger and host record in DNS server

Step 8: Enable port 143 for IMAP connections and disable port 993

```
service imap-login {
    inet_listener imap {
        port = 143
    }
    inet_listener imaps {
        port = 993
        #ssl = yes
    }
}
```

Figure 5.3.5.8: Disable other port except 143 for incoming email.

Step 9: Enable ssl connection for IMAP protocol and locate the certificate file in “/etc/dovecot/conf.d/10-ssl.conf”.

```
##  
## SSL settings  
##  
  
# SSL/TLS support: yes, no, required. <doc/wiki/SSL.txt>  
ssl = yes  
  
# 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/certs/server.pem  
ssl_key = </etc/certs/server.key
```

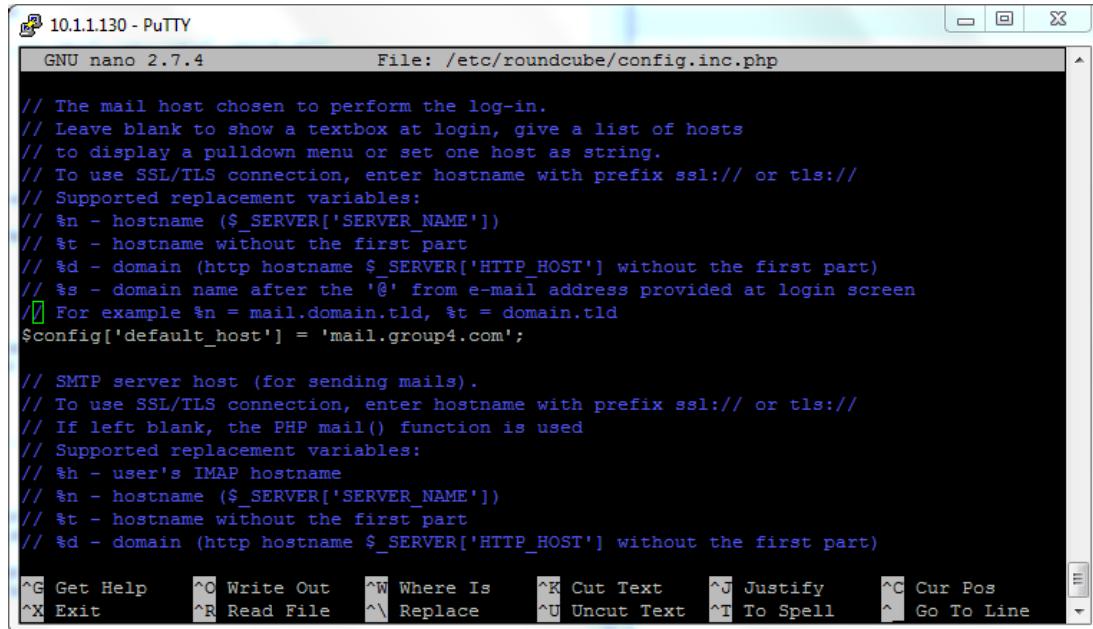
Figure 5.3.5.9: Enable secure IMAP and locate the certificate.

Step 10: Install Roundcube for web mail service.

```
root@debian:~# apt install roundcube roundcube-core roundcube-mysql roundcube-plugins  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
roundcube-core is already the newest version (1.2.3+dfsg.1-4+deb9u3).  
roundcube-mysql is already the newest version (1.2.3+dfsg.1-4+deb9u3).  
roundcube-plugins is already the newest version (1.2.3+dfsg.1-4+deb9u3).  
The following NEW packages will be installed:  
  roundcube  
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.  
Need to get 1,376 B of archives.  
After this operation, 13.3 kB of additional disk space will be used.  
Do you want to continue? [Y/n] [
```

Figure 5.3.5.10: Roundcube webmail installation command.

Step 11: Set the Roundcube setting for default mail server.



```
GNU nano 2.7.4          File: /etc/roundcube/config.inc.php

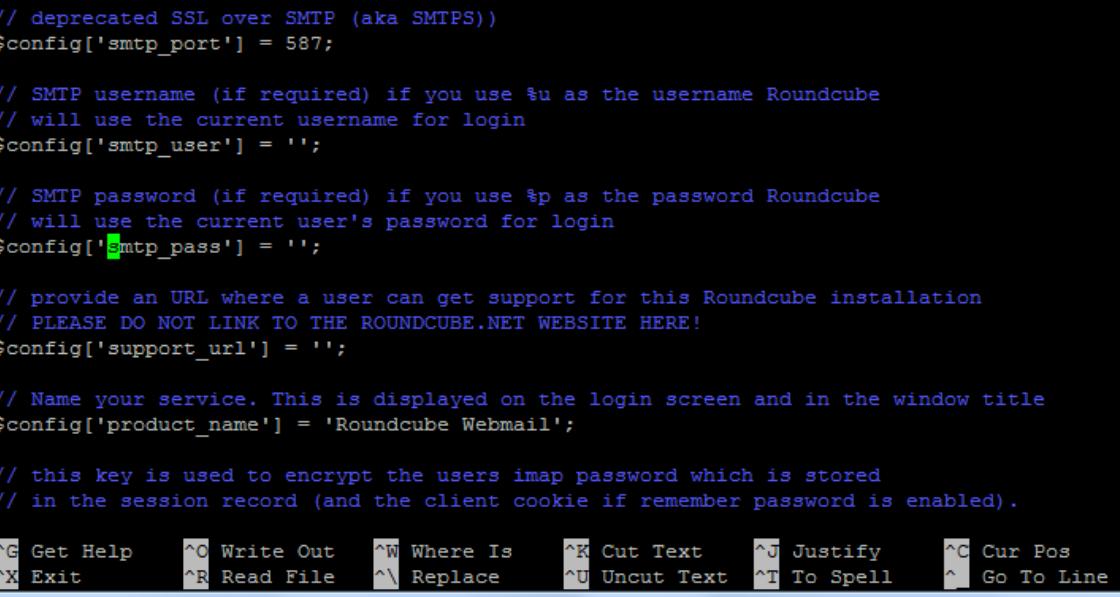
// The mail host chosen to perform the log-in.
// Leave blank to show a textbox at login, give a list of hosts
// to display a pulldown menu or set one host as string.
// To use SSL/TLS connection, enter hostname with prefix ssl:// or tls://
// Supported replacement variables:
// %n - hostname ($_SERVER['SERVER_NAME'])
// %t - hostname without the first part
// %d - domain (http hostname $_SERVER['HTTP_HOST'] without the first part)
// %s - domain name after the '@' from e-mail address provided at login screen
// For example %n = mail.domain.tld, %t = domain.tld
$config['default_host'] = 'mail.group4.com';

// SMTP server host (for sending mails).
// To use SSL/TLS connection, enter hostname with prefix ssl:// or tls://
// If left blank, the PHP mail() function is used
// Supported replacement variables:
// %h - user's IMAP hostname
// %n - hostname ($_SERVER['SERVER_NAME'])
// %t - hostname without the first part
// %d - domain (http hostname $_SERVER['HTTP_HOST'] without the first part)

^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   ^
^V Go To Line
```

Figure 5.3.5.31: Specifies the host for Roundcube connection to email server.

Step 12: Set the SMTP server which roundcube will be use.



```
// deprecated SSL over SMTP (aka SMTPS)
$config['smtp_port'] = 587;

// SMTP username (if required) if you use %u as the username Roundcube
// will use the current username for login
$config['smtp_user'] = '';

// SMTP password (if required) if you use %p as the password Roundcube
// will use the current user's password for login
$config['smtp_pass'] = '';

// provide an URL where a user can get support for this Roundcube installation
// PLEASE DO NOT LINK TO THE ROUNDCUBE.NET WEBSITE HERE!
$config['support_url'] = '';

// Name your service. This is displayed on the login screen and in the window title
$config['product_name'] = 'Roundcube Webmail';

// this key is used to encrypt the users imap password which is stored
// in the session record (and the client cookie if remember password is enabled).

^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   ^
^V Go To Line
```

Figure 5.3.5.12: Specifies the SMTP server for Roundcube connection.

Step 13: Enable virtual hosting for mail service in web server by editing the “/etc/apache2/site-available/000-default.conf”



```
----->
<VirtualHost *:443>
    ServerName mail.group4.com

    DocumentRoot /var/lib/roundcube

    SSLEngine      on
    SSLCertificateFile    /etc/certs/server.pem
    SSLCertificateKeyFile   /etc/certs/server.key

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

</VirtualHost>

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

Figure 5.3.5.13: Enable virtual hosting for Roundcube webmail.

Step 14: Restart postfix, dovecot and apache2 service.

5.3.6 IDS with Port Mirror

Installation of Snort as IDS

Step 1: Install the required libraries with the following command

```
group4@ubuntu:~$ sudo apt install -y gcc libpcre3-dev zlib1g-dev libluajit-5.1-dev libpcap-dev openssl libssl-dev libnnghttp2-dev libdumbnet-dev bison flex libdn
et
Reading package lists... Done
Building dependency tree
Reading state information... Done
bison is already the newest version (2:3.0.4.dfsg-1build1).
flex is already the newest version (2.6.4-6).
libdumbnet-dev is already the newest version (1.12-7build1).
libnnghttp2-dev is already the newest version (1.30.0-1ubuntu1).
libpcap-dev is already the newest version (1.8.1-6ubuntu1).
libpcre3-dev is already the newest version (2:8.39-9).
zlib1g-dev is already the newest version (1:1.2.11.dfsg-0ubuntu2).
libdnet is already the newest version (2.65).
libluajit-5.1-dev is already the newest version (2.1.0~beta3+dfsg-5.1).
gcc is already the newest version (4:7.4.0-1ubuntu2.3).
libssl-dev is already the newest version (1.1.1-1ubuntu2.1~18.04.4).
openssl is already the newest version (1.1.1-1ubuntu2.1~18.04.4).
0 upgraded, 0 newly installed, 0 to remove and 21 not upgraded.
group4@ubuntu:~$ █
```

Figure 5.3.6.1: Install prerequisite snort

Step 2: Download the latest DAQ source package from the Snort website with the wget command underneath

```
group4@ubuntu:~$ wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
--2019-11-20 12:35:09-- https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
Resolving www.snort.org (www.snort.org)... 2606:4700::6812:8a09, 2606:4700::6812:8b09, 104.18.138.9, ...
Connecting to www.snort.org (www.snort.org)|2606:4700::6812:8a09|:443... failed:
Network is unreachable.
Connecting to www.snort.org (www.snort.org)|2606:4700::6812:8b09|:443... failed:
Network is unreachable.
Connecting to www.snort.org (www.snort.org)|104.18.138.9|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/011/803/original/daq-2.0.6.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20191120%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20191120T043449Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=0478c1758e42268d434a4fa7cabbd8696e00036e5d1e4fb9ad7e7b3d7bcc1973 [following]
--2019-11-20 12:35:09-- https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/011/803/original/daq-2.0.6.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20191120%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20191120T043449Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=0478c1758e42268d434a4fa7cabbd8696e00036e5d1e4fb9ad7e7b3d7bcc1973
Resolving snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)... 5
```

Figure 5.3.6.2: Download DAQ packages

Step 3: Unzip the file and install DAQ

```
group4@ubuntu:~$ cd daq-2.0.6/
group4@ubuntu:~/daq-2.0.6$ ./configure && make && make install
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
checking for gawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
checking for style of include used by make... GNU
checking dependency style of gcc... gcc3
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking how to print strings... printf
checking for a sed that does not truncate output... /bin/sed
```

Figure 5.3.6.3: Install DAQ

Step 4: Next, download the Snort source code with wget

```
group4@ubuntu:~$ wget https://www.snort.org/downloads/snort/snort-2.9.15.tar.gz
--2019-11-20 12:33:58-- https://www.snort.org/downloads/snort/snort-2.9.15.tar.gz
Resolving www.snort.org (www.snort.org)... 2606:4700::6812:8a09, 2606:4700::6812:8b09, 104.18.138.9, ...
Connecting to www.snort.org (www.snort.org)|2606:4700::6812:8a09|:443... failed:
Network is unreachable.
Connecting to www.snort.org (www.snort.org)|2606:4700::6812:8b09|:443... failed:
Network is unreachable.
Connecting to www.snort.org (www.snort.org)|104.18.138.9|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/011/796/original/snort-2.9.15.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20191120%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20191120T043340Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=62dfa4c1e745255c9293ebda5eaba3e56c378fc1e13ae36d33ea041b6162654c [following]
--2019-11-20 12:34:00-- https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/011/796/original/snort-2.9.15.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20191120%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20191120T043340Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=62dfa4c1e745255c9293ebda5eaba3e56c378fc1e13ae36d33ea041b6162654c
```

Figure 5.3.6.4: Download Snort Package

Step 5: Then configure the installation of Snort with sourcefire enabled

Step 6: Start with updating the shared libraries using the command underneath. Next, create a symlink to the Snort binary

```
group4@ubuntu:~/snort-2.9.15$ sudo ldconfig
[sudo] password for group4:
group4@ubuntu:~/snort-2.9.15$ ln -s /usr/local/bin/snort /usr/sbin/snort
ln: failed to create symbolic link '/usr/sbin/snort': File exists
```

Figure 5.3.6.5: Create Symlink

Step 7: Create the folder structure to house the Snort configuration

```
group4@ubuntu:~$ sudo mkdir /etc/snort
group4@ubuntu:~$ sudo mkdir /etc/snort/preproc_rules
group4@ubuntu:~$ sudo mkdir /etc/snort/rules
group4@ubuntu:~$ mkdir /var/log/snort
mkdir: cannot create directory '/var/log/snort': File exists
group4@ubuntu:~$ sudo mkdir /var/log/snort
mkdir: cannot create directory '/var/log/snort': File exists
group4@ubuntu:~$ sudo mkdir /usr/local/lib/snort_dynamicrules
mkdir: cannot create directory '/usr/local/lib/snort_dynamicrules': File exists
group4@ubuntu:~$ touch /etc/snort/rules/white_list.rules
touch: cannot touch '/etc/snort/rules/white_list.rules': Permission denied
group4@ubuntu:~$ sudo touch /etc/snort/rules/white_list.rules
group4@ubuntu:~$ sudo touch /etc/snort/rules/black_list.rules
group4@ubuntu:~$ sudo touch /etc/snort/rules/local.rules
group4@ubuntu:~$ █
```

Figure 5.3.6.6: Create directory and file

Step 8: Now set proper permission to the following directories

```
group4@ubuntu:~$ sudo chmod -R 5775 /etc/snort/
group4@ubuntu:~$ sudo chmod -R 5775 /var/log/snort/
group4@ubuntu:~$ sudo chmod -R 5775 /usr/local/lib/snort
group4@ubuntu:~$ sudo chmod -R 5775 /usr/local/lib/snort_dy
namicrules/ █
```

Figure 5.3.6.7: Change file permission

Step 9: Copy .conf, .map and .dtd files to the /etc/snort/ directory from snort file we have extracted and also need to copy the dynamic preprocessors files

```
group4@ubuntu:~/snort-2.9.15/etc$ sudo cp -avr *.conf *.map *.dtd /etc/snort/
'file_magic.conf' -> '/etc/snort/file_magic.conf'
'snort.conf' -> '/etc/snort/snort.conf'
'threshold.conf' -> '/etc/snort/threshold.conf'
'gen-msg.map' -> '/etc/snort/gen-msg.map'
'unicode.map' -> '/etc/snort/unicode.map'
'attribute_table.dtd' -> '/etc/snort/attribute_table.dtd'

group4@ubuntu:~/snort-2.9.15$ sudo cp -avr src/dynamic preprocessors/build/usr/local/lib/snort_dynamicpreprocessor/* /usr/local/lib/snort_dynamicpreprocessor/
'src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicpreprocessor/libsf_appid_preproc.a' -> '/usr/local/lib/snort_dynamicpreprocessor/libsf_appid_preproc.a'
'src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicpreprocessor/libsf_appid_preproc.la' -> '/usr/local/lib/snort_dynamicpreprocessor/libsf_appid_preproc.la'
removed '/usr/local/lib/snort_dynamicpreprocessor/libsf_appid_preproc.so'
'src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicpreprocessor/libsf_appid_preproc.so' -> '/usr/local/lib/snort_dynamicpreprocessor/libsf_appid_preproc.so'
removed '/usr/local/lib/snort_dynamicpreprocessor/libsf_appid_preproc.so.0'
'src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicpreprocessor/libsf_appid_preproc.so.0' -> '/usr/local/lib/snort_dynamicpreprocessor/libsf_appid_preproc.so.0'
'src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicpreprocessor/libsf_appid_preproc.so.0.0.0' -> '/usr/local/lib/snort_dynamicpreprocessor/libsf_appid_preproc.so.0.0.0'
```

Figure 5.3.6.8: Copy necessary file

Step 10: Now open /etc/snort/snort.conf and change the file as shown below

```
GNU nano 2.9.3                               /etc/snort/snort.conf

# Step #1: Set the network variables. For more information, see README.variables
#####
# Setup the network addresses you are protecting
ipvar HOME_NET 10.1.1.0/28

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

# List of DNS servers on your network
ipvar DNS_SERVERS 10.1.1.129/28
#
# List of SMTP servers on your network
ipvar SMTP_SERVERS 10.1.1.130/28

# List of web servers on your network
ipvar HTTP_SERVERS 10.1.1.130/28

# List of sql servers on your network
ipvar SQL_SERVERS $HOME_NET

# List of telnet servers on your network
```

Figure 5.3.6.9: Snort configuration file

Step 11: Next, validate the configuration file with the following command

```
group4@ubuntu:~$ sudo snort -T -c /etc/snort/snort.conf
Running in Test mode

      --= Initializing Snort =--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined : [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2
809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 80
28 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 909
0:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined : [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined : [ 1024:65535 ]
PortVar 'SSH_PORTS' defined : [ 22 ]
PortVar 'FTP_PORTS' defined : [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined : [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined : [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 183
0 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000
8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000
9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined : [ 2123 2152 3386 ]
Detection:
  Search-Method = AC-Full-Q
  Split Any/Any group = enabled
  Search-Method-Optimizations = enabled
```

Figure 5.3.6.10: Validate Snort

Configure Port Mirror.**Step 1:** Configure monitor session 1

```
SW4#config t
Enter configuration commands, one per line. End with CNTL/Z.
SW4(config)#monitor session 1 source interface fa0/3, fa0/22, fa0/23, fa0/24
SW4(config)#monitor session 1 destination interface fa0/13
SW4(config)#exit
SW4#
*May 14 11:15:56.945: %SYS-5-CONFIG_I: Configured from console by AzimGroup4 on
console
SW4#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

Figure 5.3.6.11: Setup port mirror configuration

Step 2: Verify the monitor session has created.

```
SW4#
SW4#show monitor session 1
Session 1
-----
Type          : Local Session
Source Ports  :
    Both      : Fa0/3,Fa0/22-24
Destination Ports   : Fa0/13
    Encapsulation : Native
    Ingress      : Disabled
```

Figure 5.3.6.12: Validate port mirror

5.3.7 Wireless User Authentication user Radius Server.

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

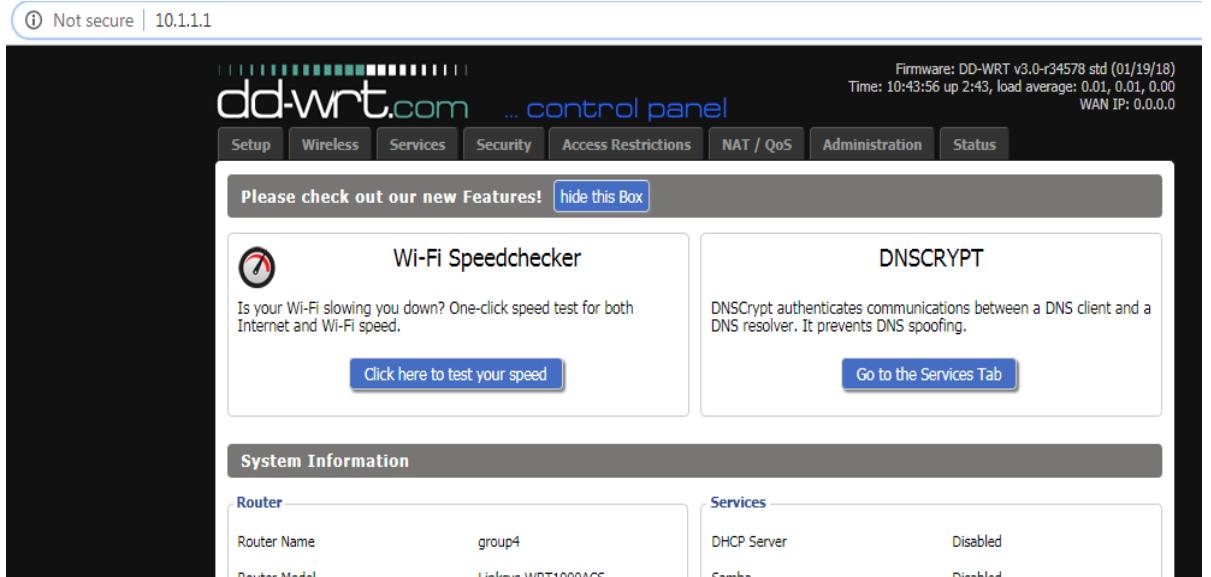


Figure 5.3.7.1: Access Point Web

Step 2: Select Setup > Basic Setup and fill all the requirements to set IP for Access Point (AP) and Click OK.

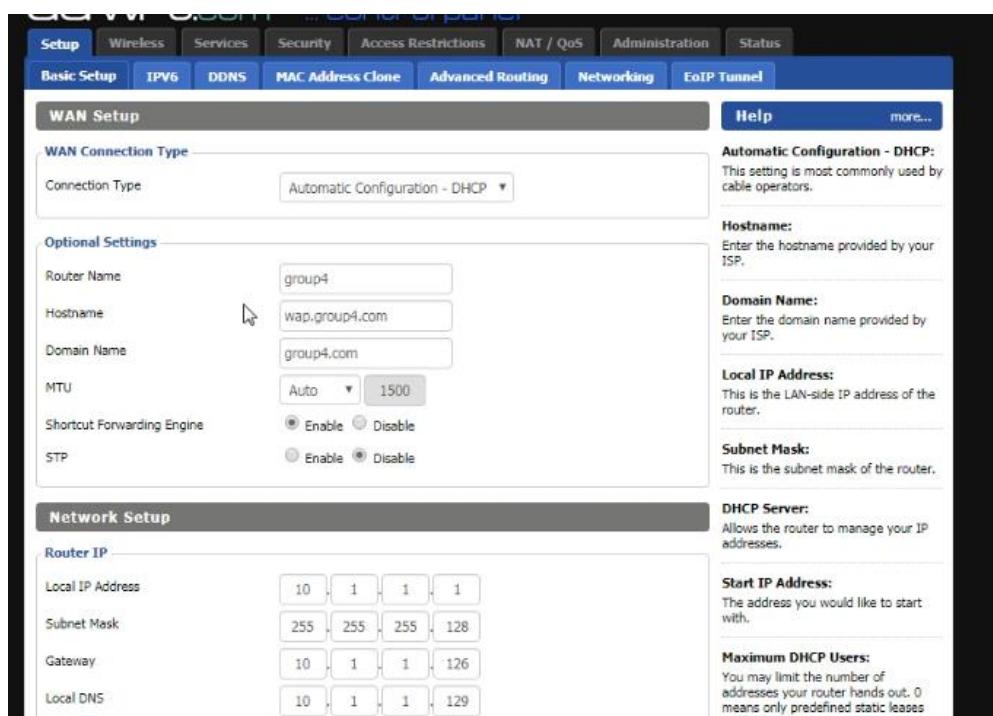


Figure 5.3.7.2: Basic Setup for Access Point

Step 3: After that select Wireless, set all wireless requirements for 5GHz and 2.4GHz.

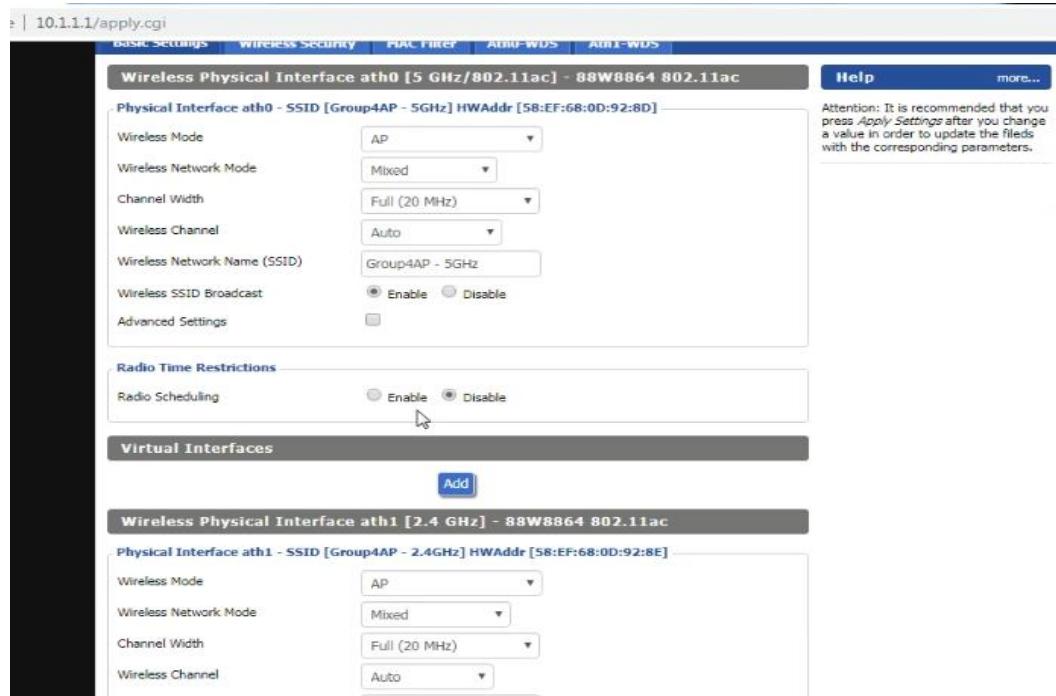


Figure 5.3.7.3: Wireless Physical Interface info of AP

Step 4: After that select Wireless > Wireless Security mode set WPA2/WPA Mixed Enterprise, Server Address and Port Number of the Radius Server for the network 5GHz and 2.4GHz.

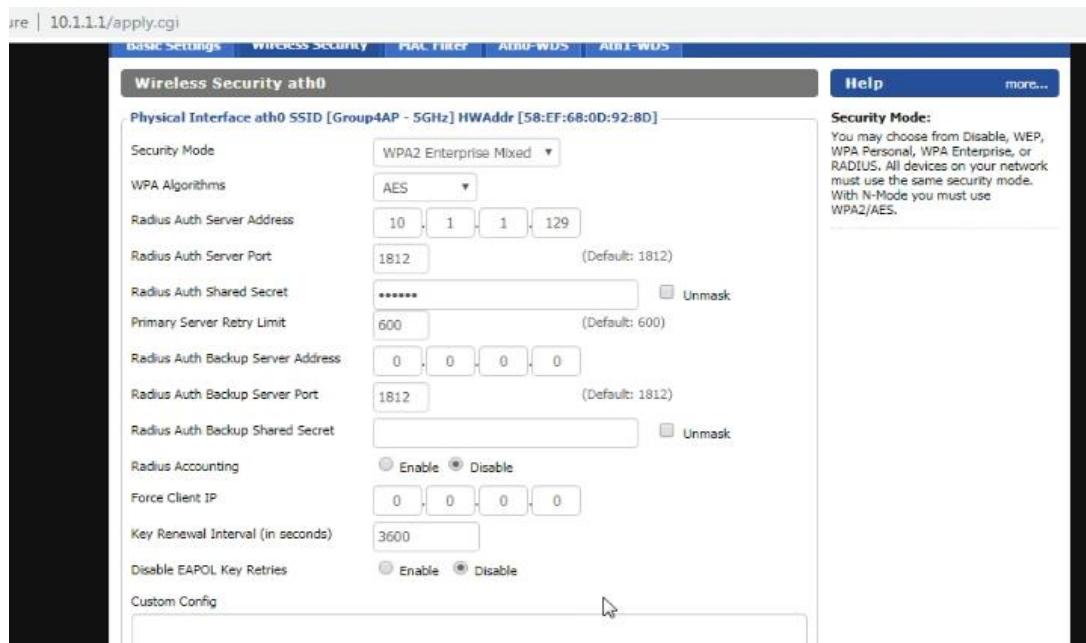


Figure 5.3.7.4: Wireless Security Information of AP

Step 5: Open Server Manager at 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 Users.

Step 6: Create New Object – Group.

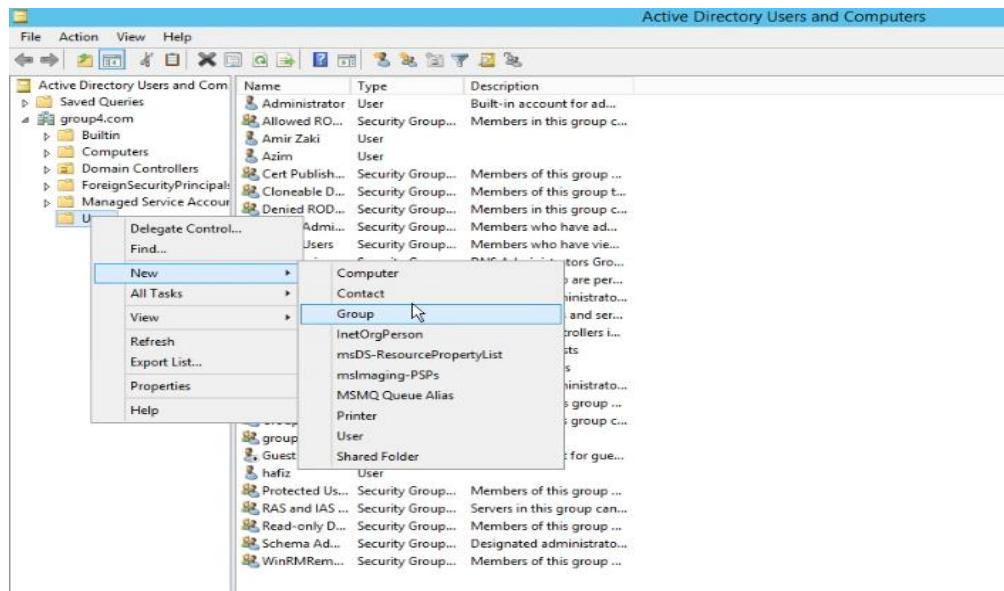


Figure 5.3.7.5: Create New Object - Group

Step 7: Then, fill in the Group Name (group4). Then, click OK.

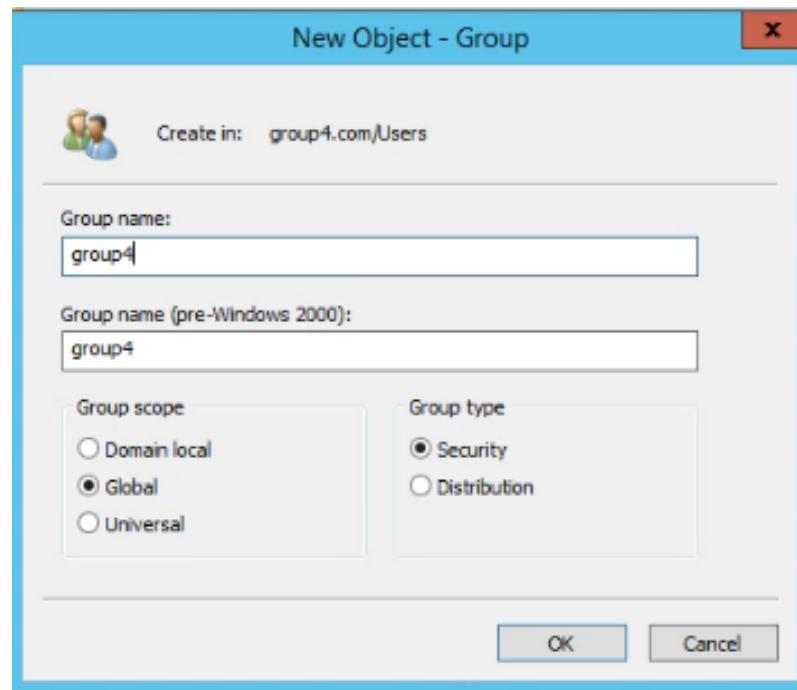


Figure 5.3.7.6: Information of New Group

Step 8: Create New Object – User.

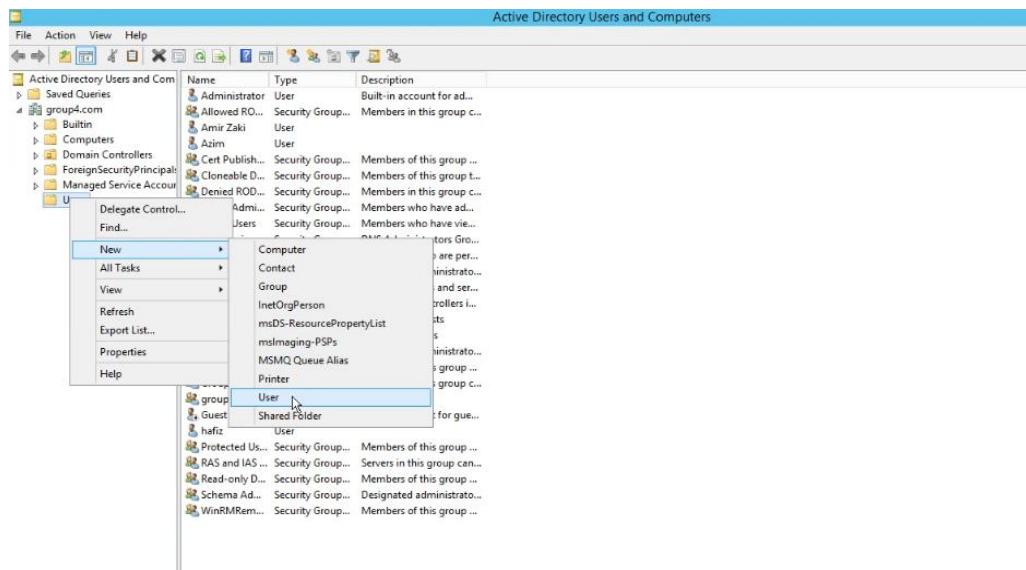


Figure 5.3.7.7: Create New Object - User

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

Then, click Next.

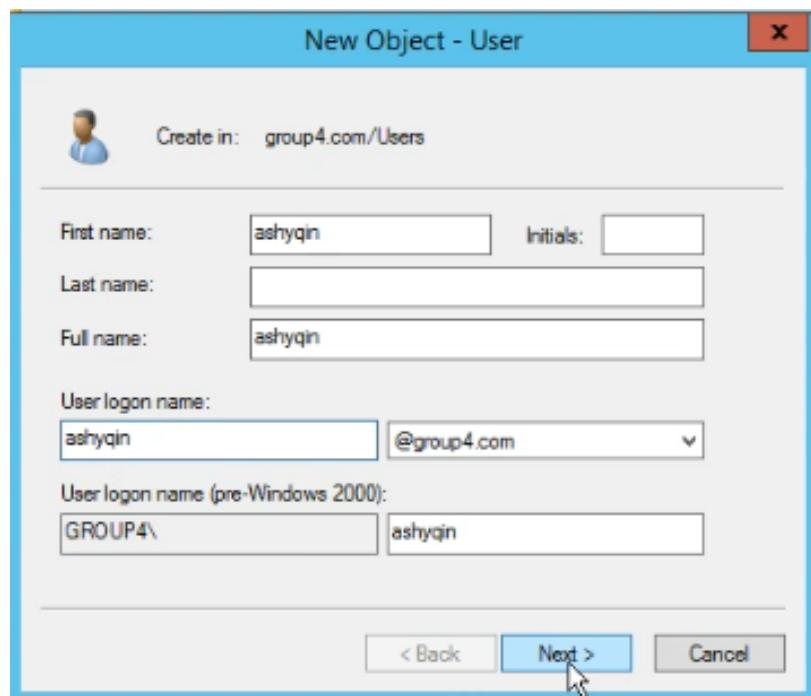


Figure 5.3.7.8: Information of New User

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.

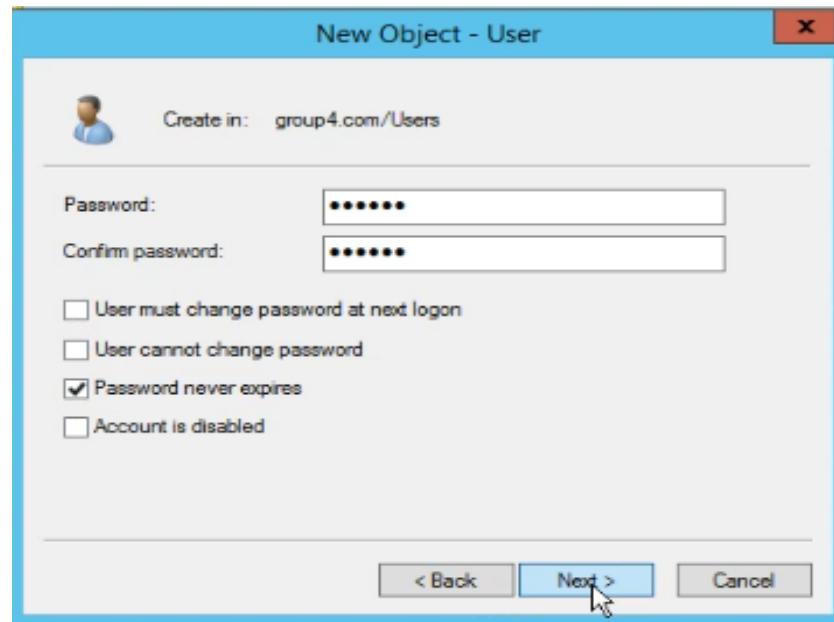


Figure 5.3.7.9: Creating password to the user

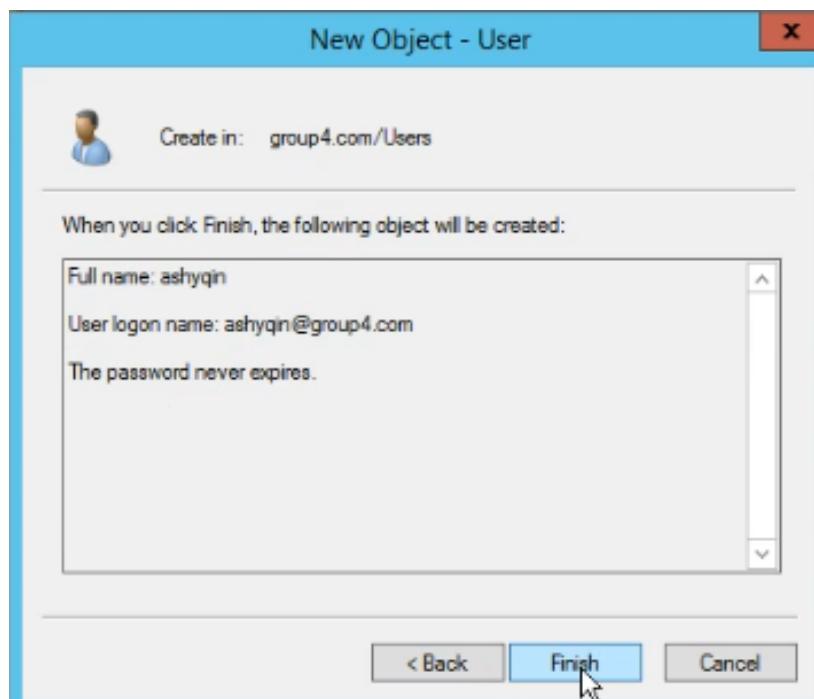


Figure 5.3.7.10: Confirmation of User

Step 11: To check the members of group4, right click on group4 and select Properties.

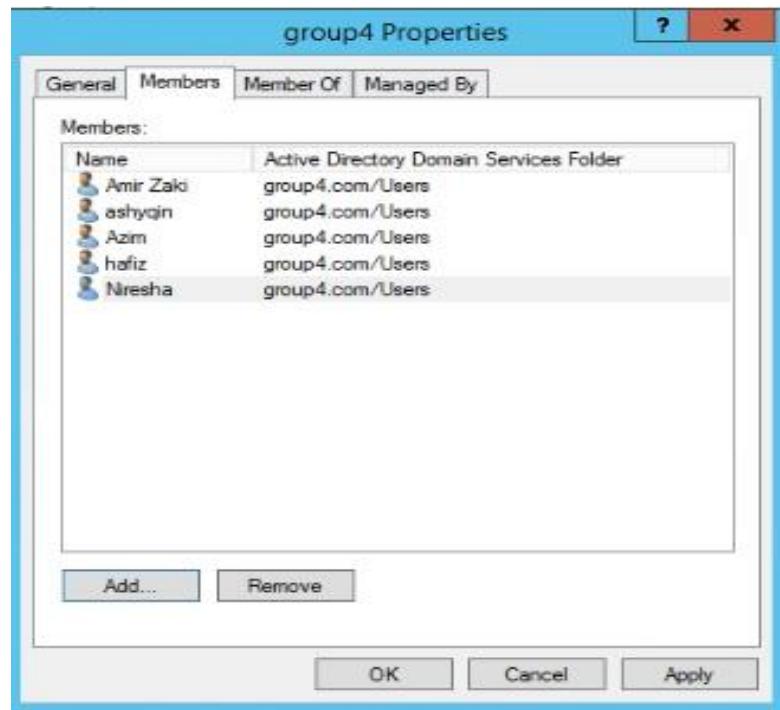


Figure 5.3.7.11: Members of group4

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

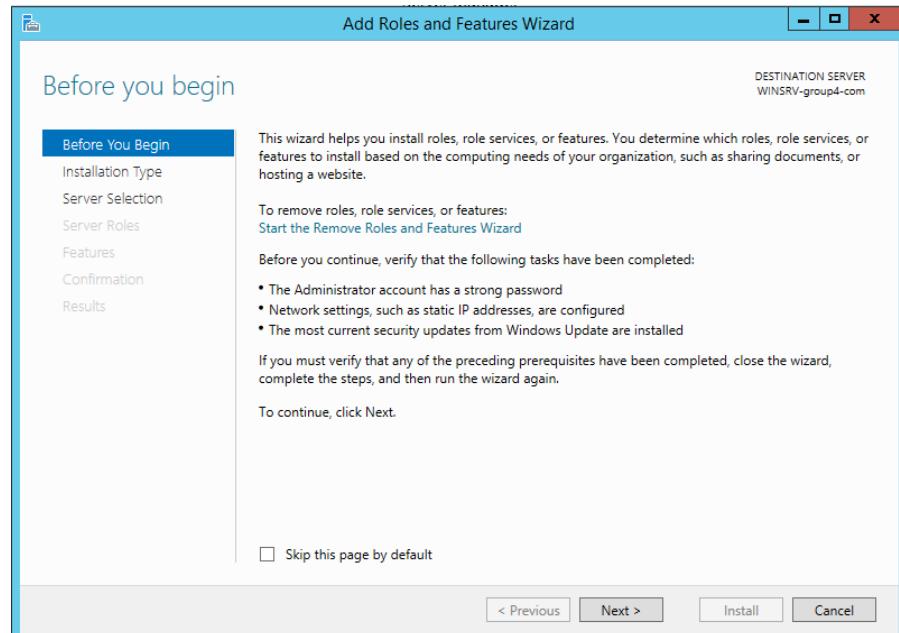


Figure 5.3.7.12: Add Roles and Features Wizard

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

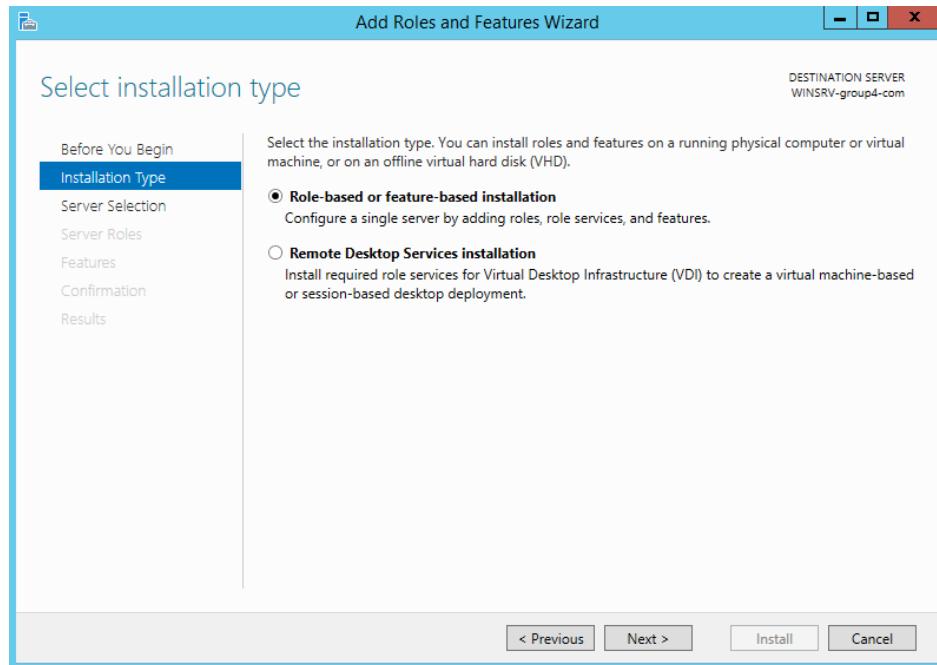


Figure 5.3.7.13: Select Installation Type

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

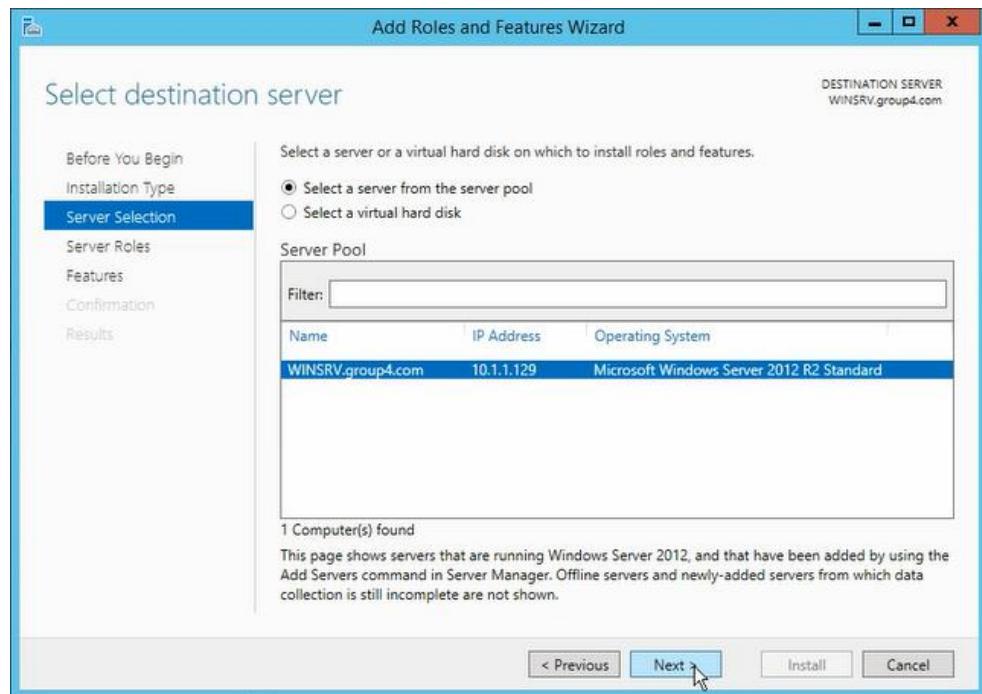


Figure 5.3.7.14: Select Destination Server

Step 15: 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.

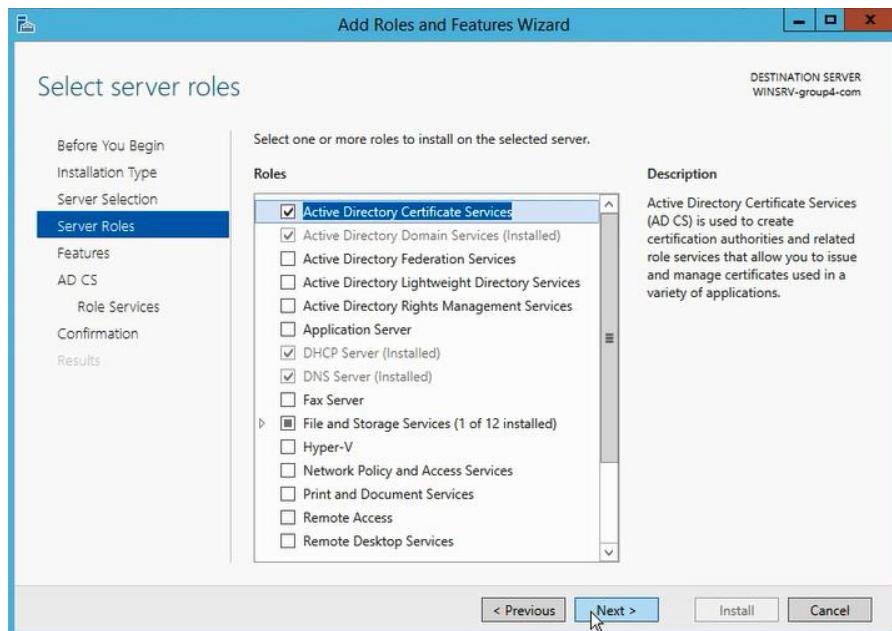


Figure 5.3.7.15: Select Server Roles

Step 16: This window will pop up, select, [Tools] Certification Authority Management Tools and click Add Features.

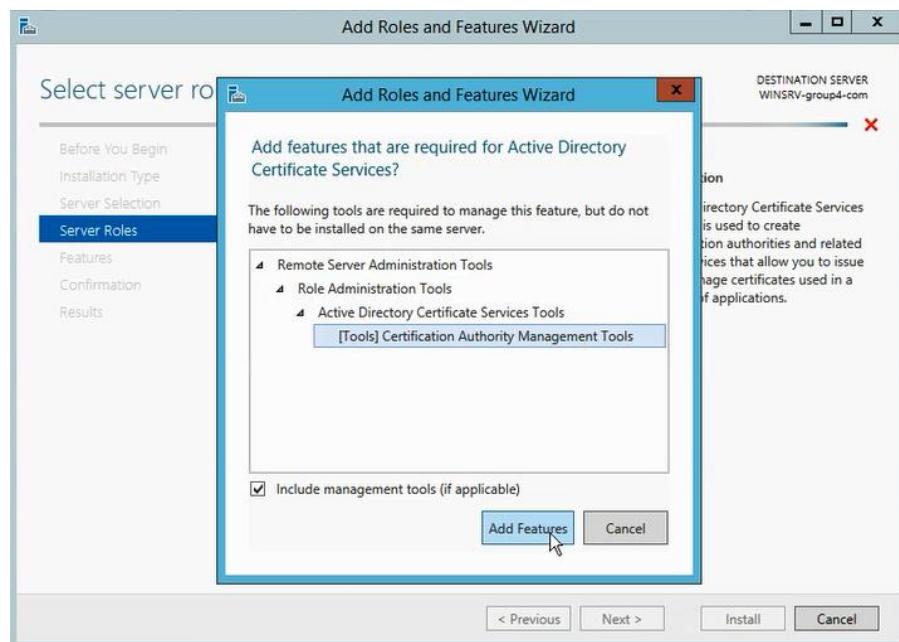


Figure 5.3.7.16: Adding Features for AD CS

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.

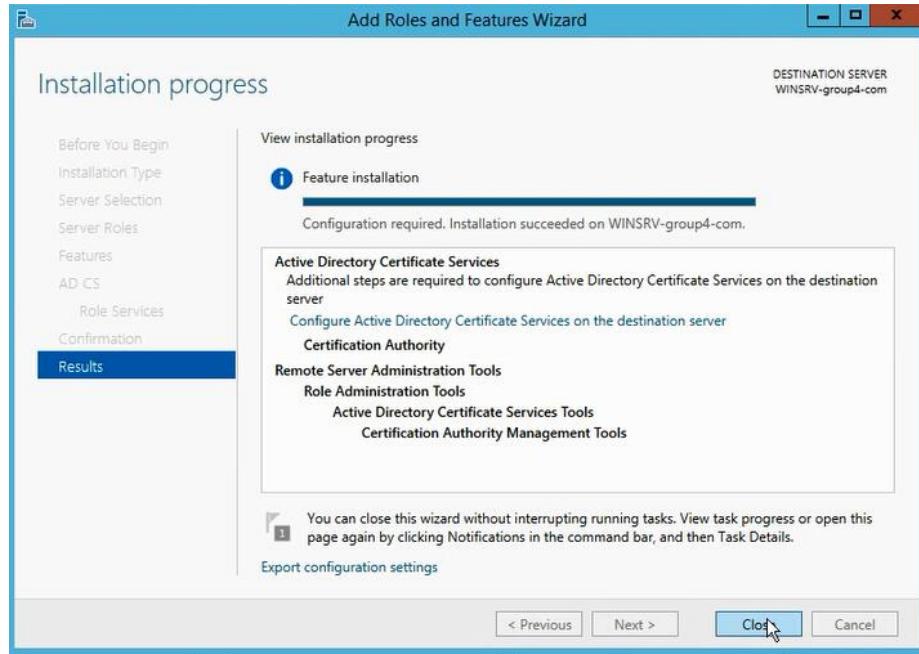


Figure 5.3.7.17: Installation Progress

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

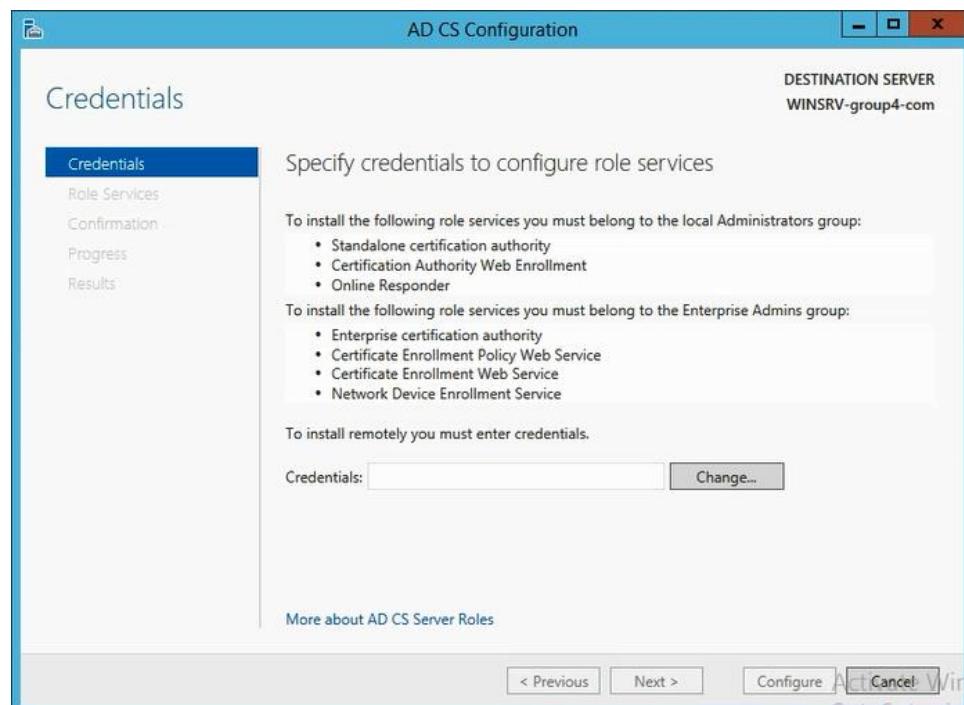


Figure 5.3.7.18: Role Services Configuration

Step 19: For Roles Service, make sure to tick on Certificate Authority. Then, click Next.

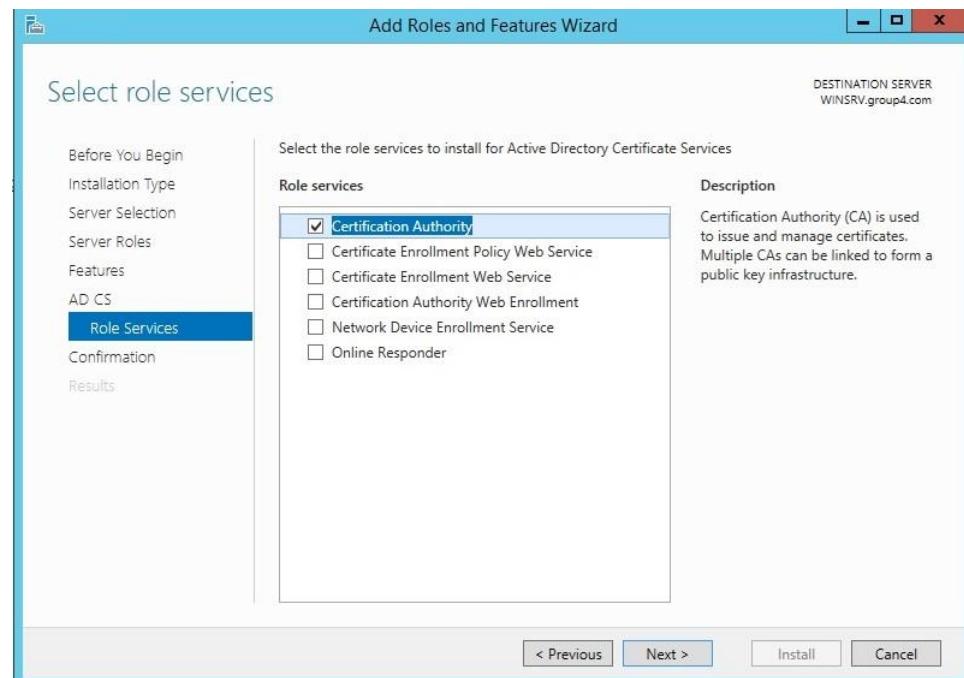


Figure 5.3.7.19: Select Role Services for AD CS

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

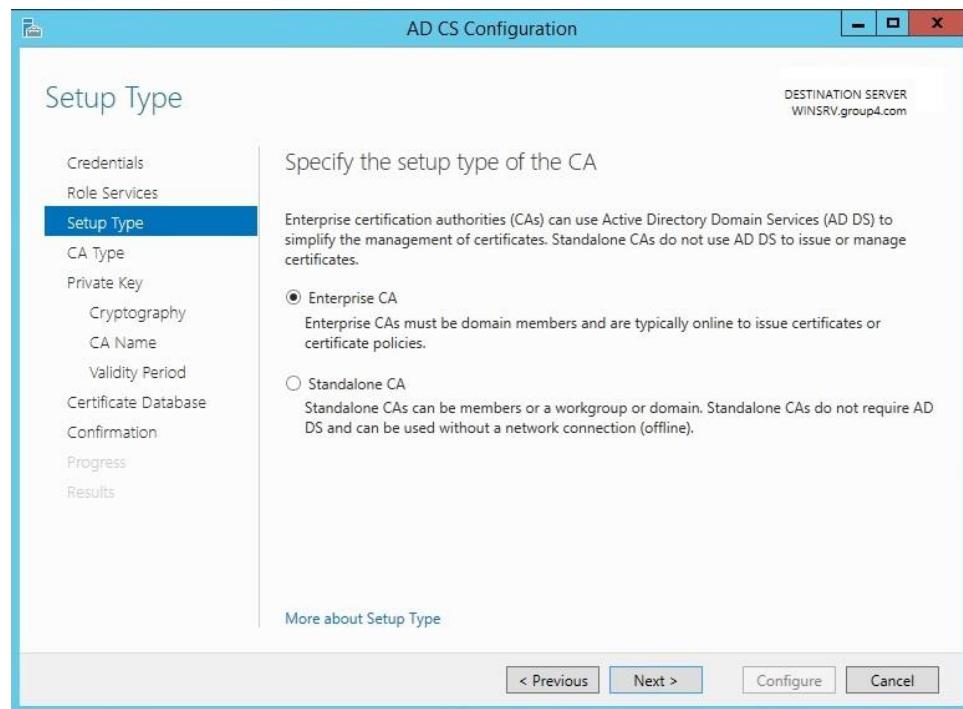


Figure 5.3.7.20: Setup Type of CA

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



Figure 5.3.7.21: CA Type Specification

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



Figure 5.3.7.22: Choosing the Private Key

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

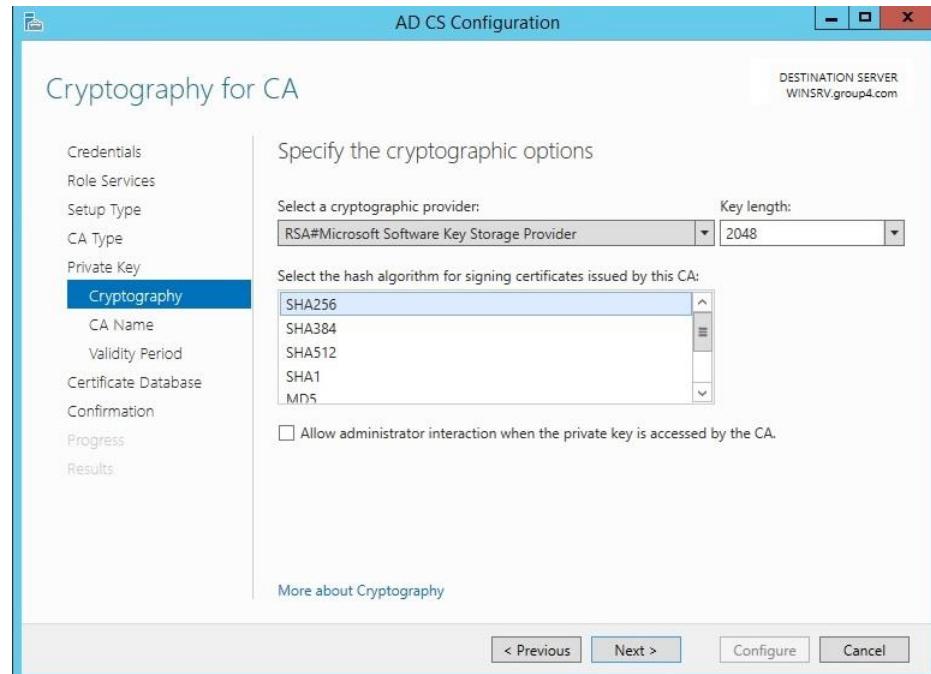


Figure 5.3.7.23: Selecting Cryptography for CA

Step 24: Then, specify the validity period. In our case, we choose 5 Years. After that, click Next.

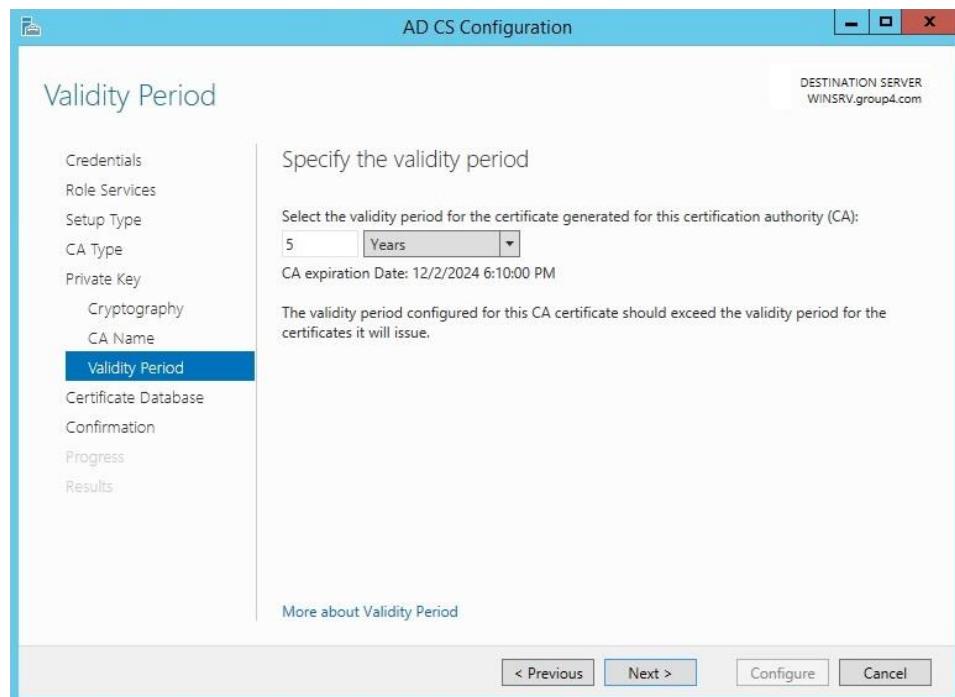


Figure 5.3.7.24: Specify Validity Period

Step 25: For Certificate database, specify the database locations and click Next.

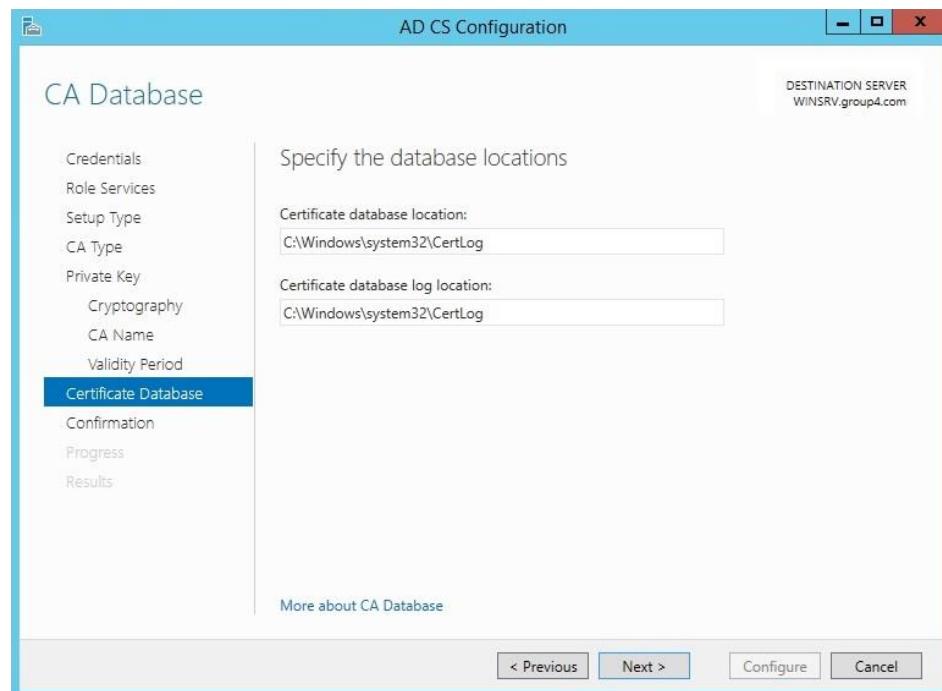


Figure 5.3.7.25: Specify Database Location

Step 26: After looking for the confirmation, click on Configure. Click close after the configuration succeeded.

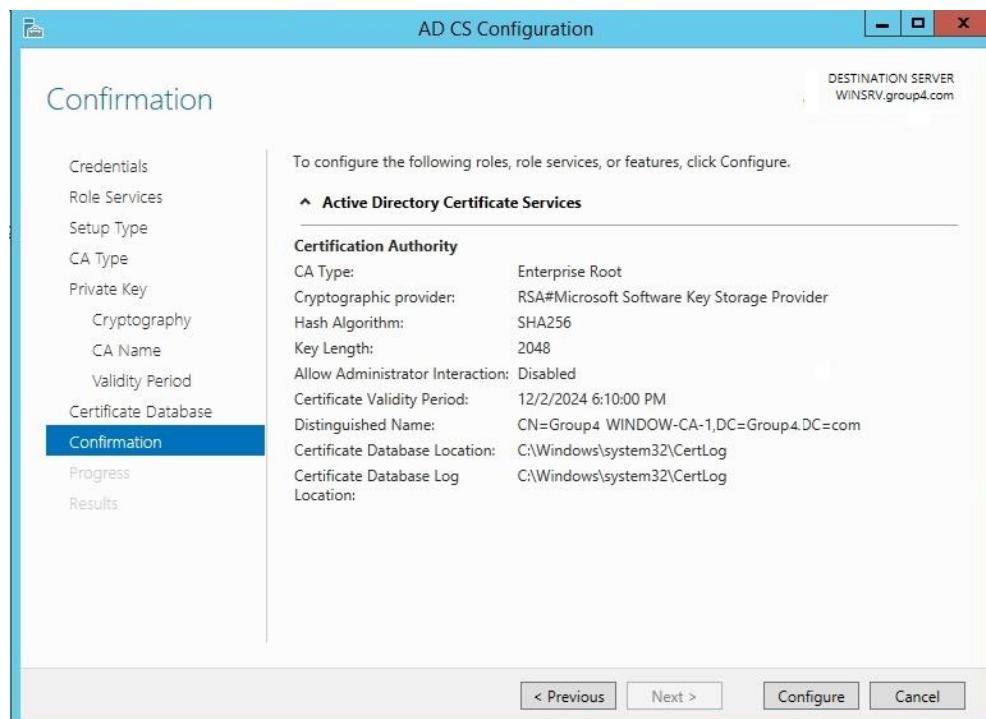


Figure 5.3.7.26: Confirmation of AD CS Configuration

Step 27: Active Directory Certificate Services configuration is successful.

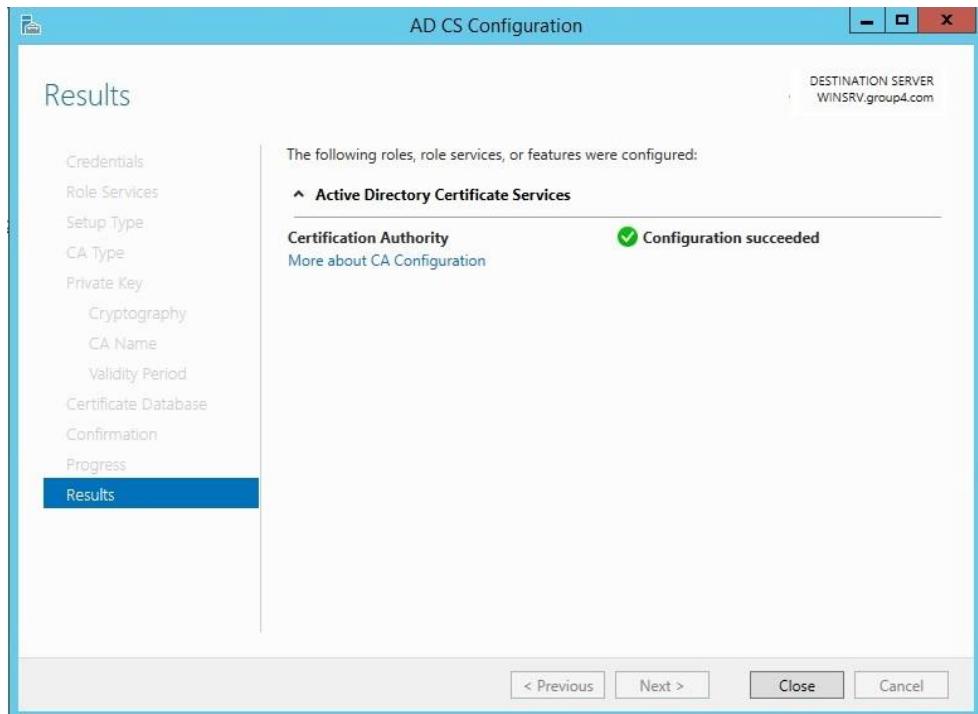


Figure 5.3.7.27: Results of AD CS Configuration

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 Certificate and Add it, then click OK.

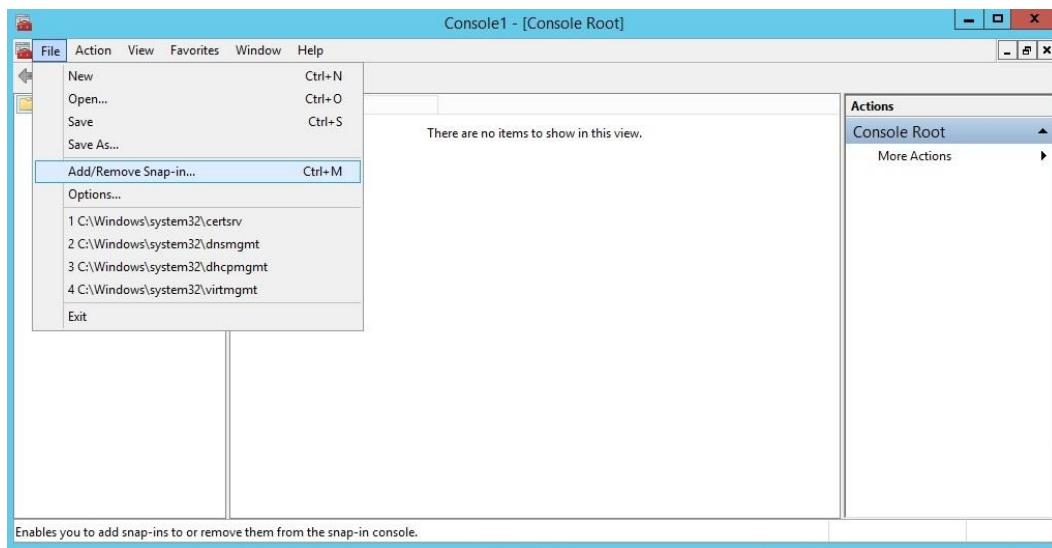


Figure 5.3.7.28: Console Root Page

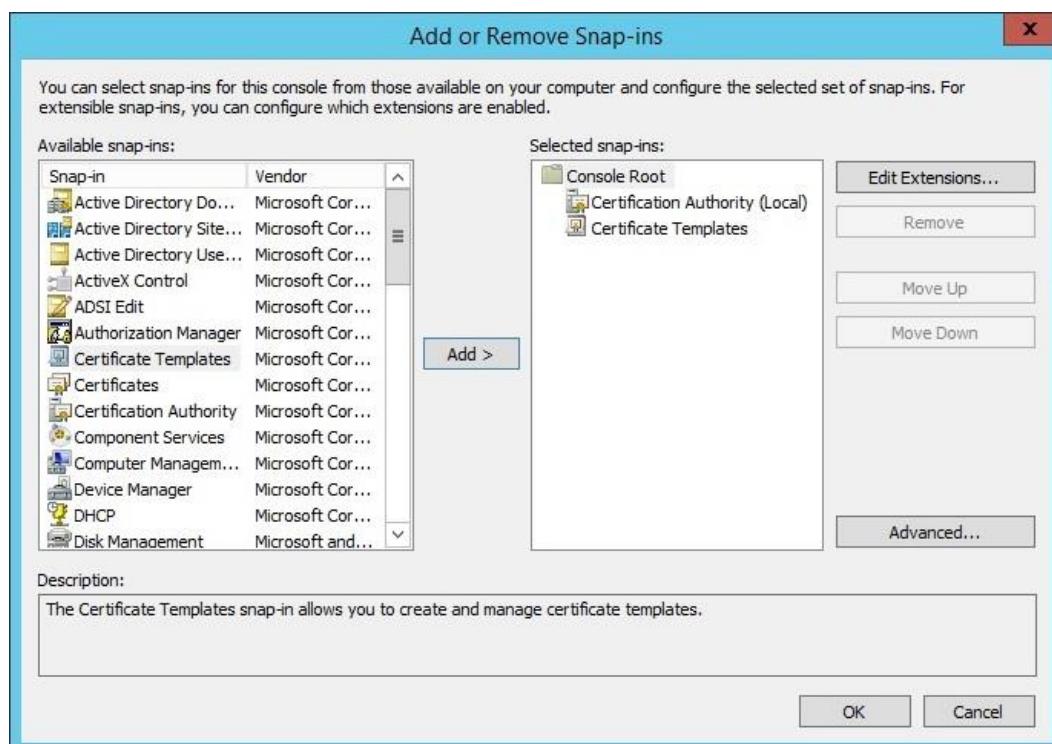


Figure 5.3.7.29: Adding or Remove snap-ins

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

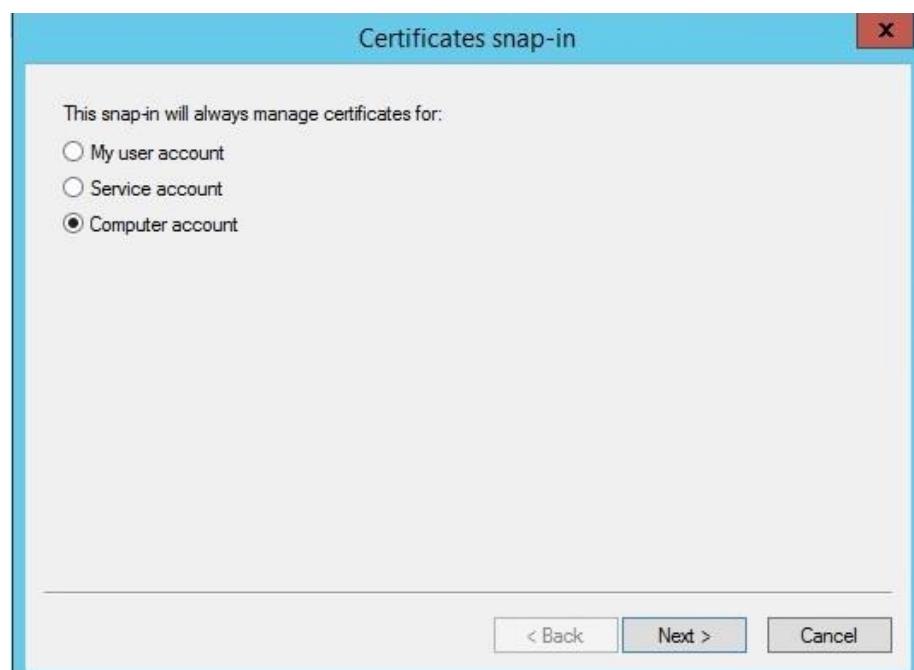


Figure 5.3.7.30: Choosing Certificates Snap In

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

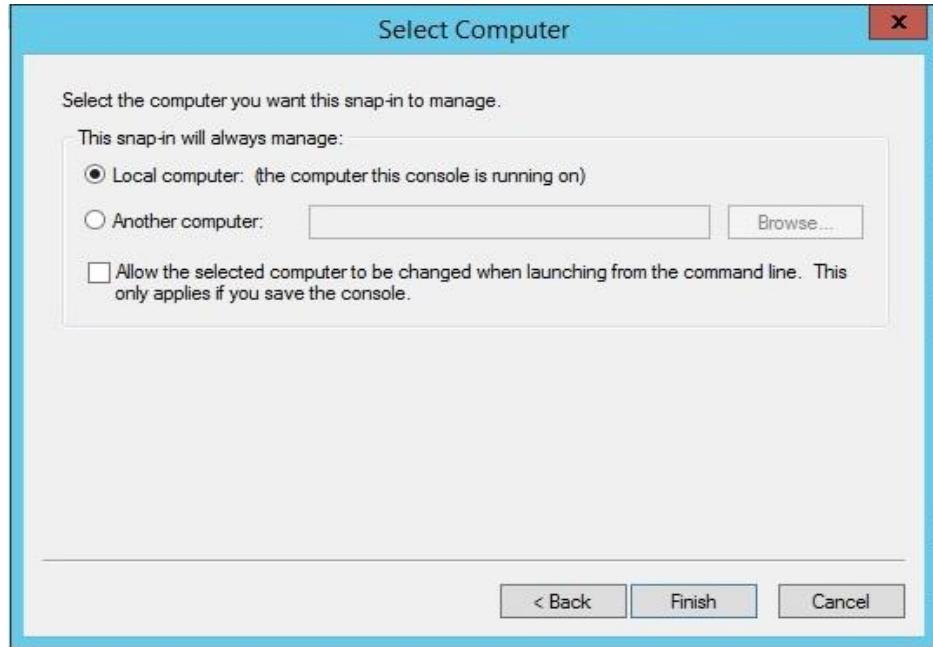


Figure 5.3.7.31: Select Local Computer to manage snap-in

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 the computer is connected to the network and you have credential that can be used to verify your right to obtain the certificate. After making sure of the following, click Next.

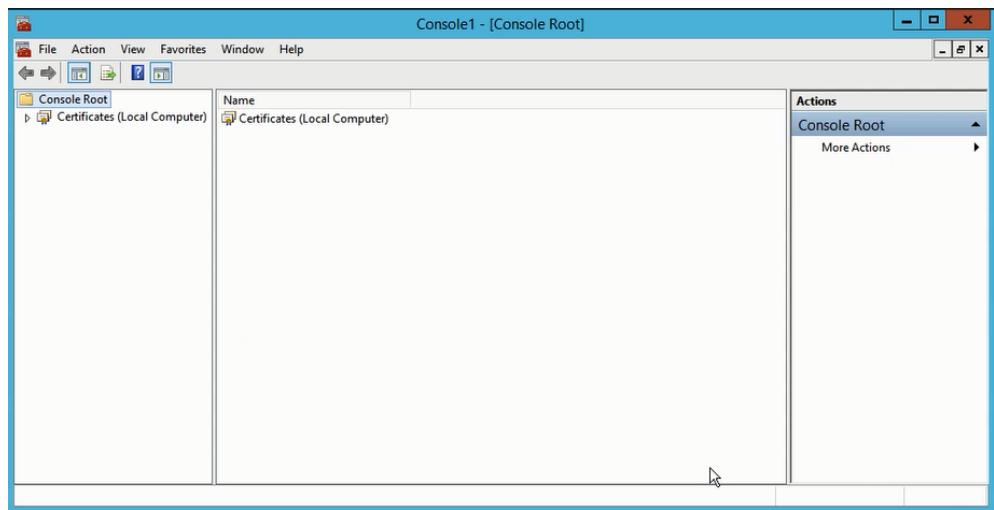


Figure 5.3.7.32: Loading the Certificate into Consolz

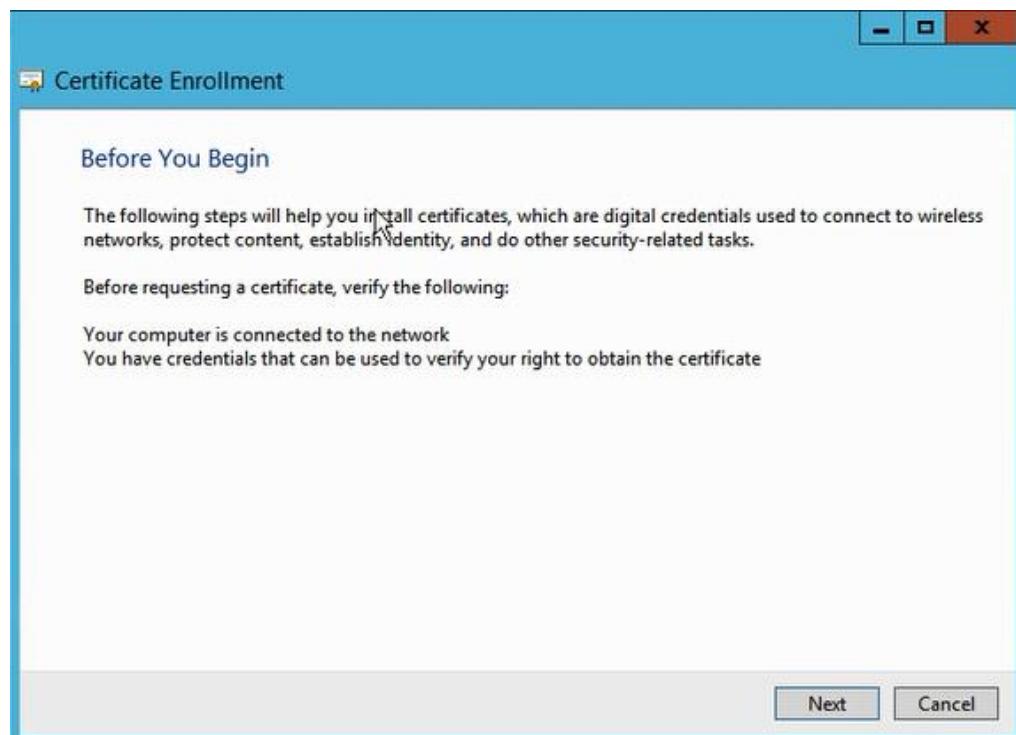


Figure 5.3.7.33: Beginning of Certificate Enrollment

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

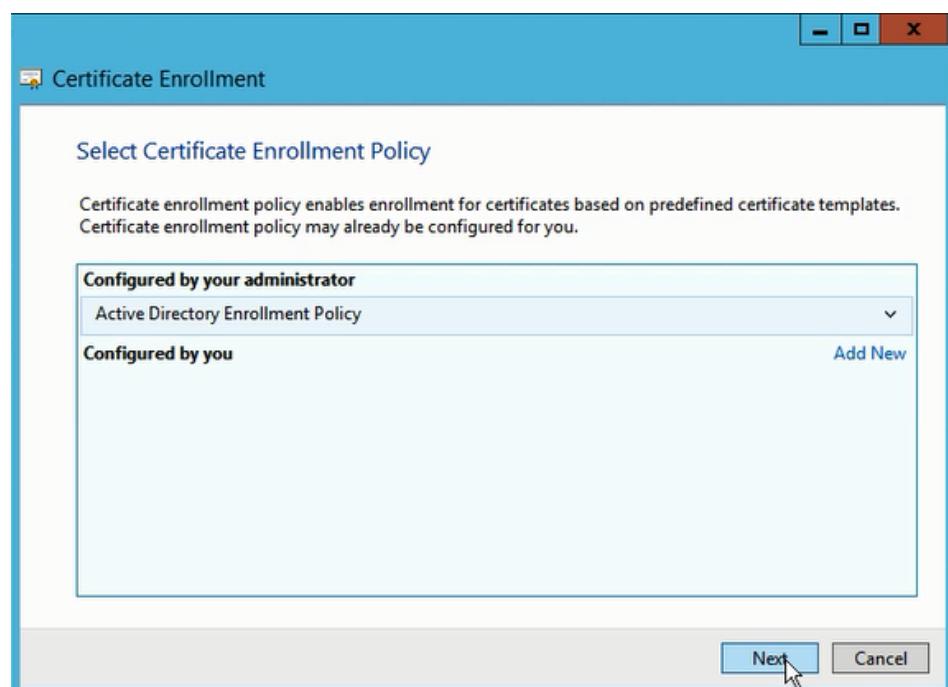


Figure 5.3.7.34: Selecting Certificate Enrollment Policy

Step 33: For Request Certificate, tick on Domain Controller and then, click Enroll.

After that, the enrolment will be installed and then, click Finish.

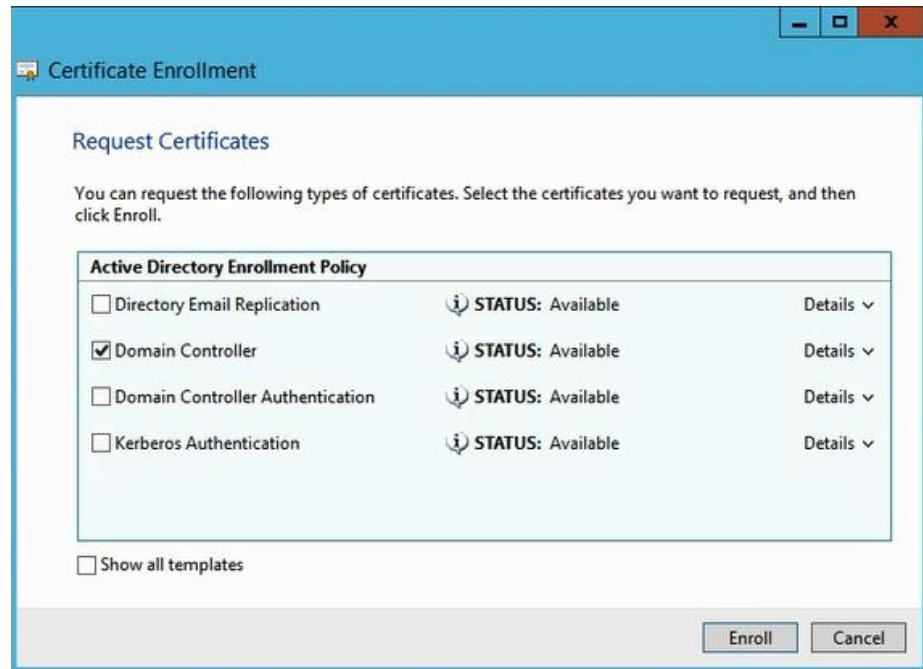


Figure 5.3.7.35: Requesting Certificates

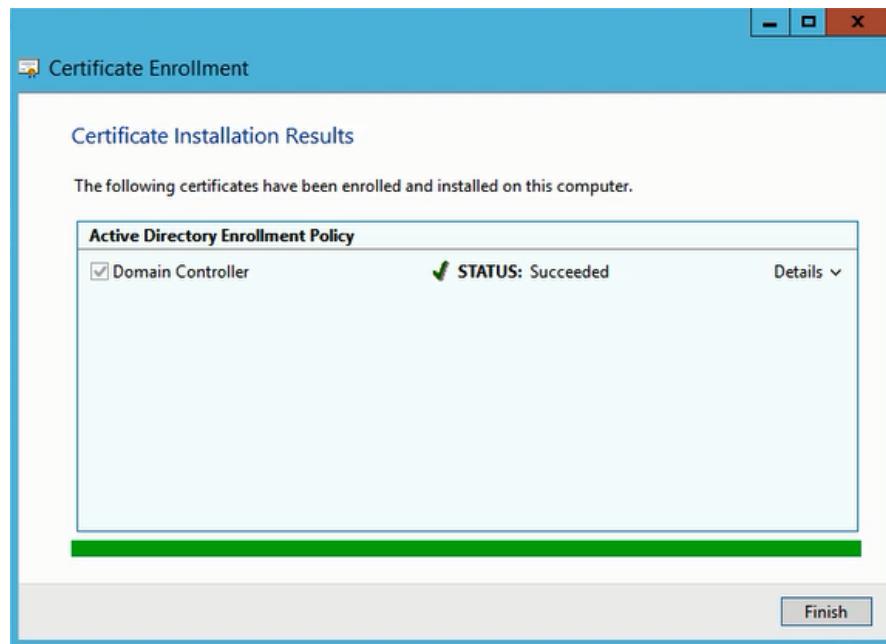


Figure 5.3.7.36: Installation of Certificate

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

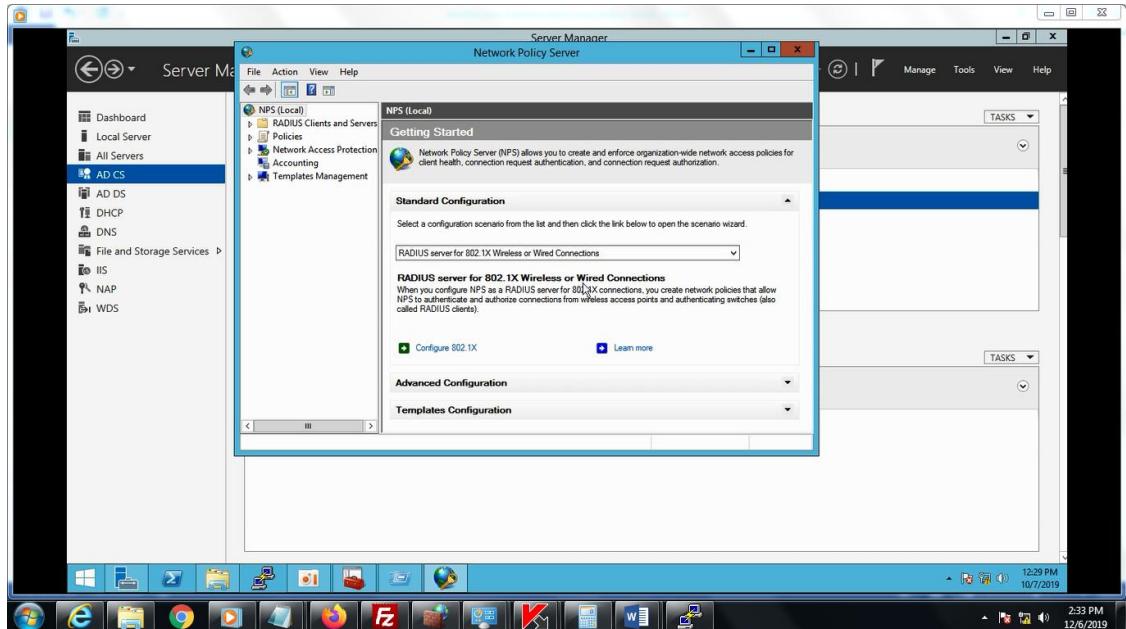


Figure 5.3.7.37: Network Policy server page

Step 35: Then, select Secure Wireless Connection for 802.1X Connection Type and click Next > Add.

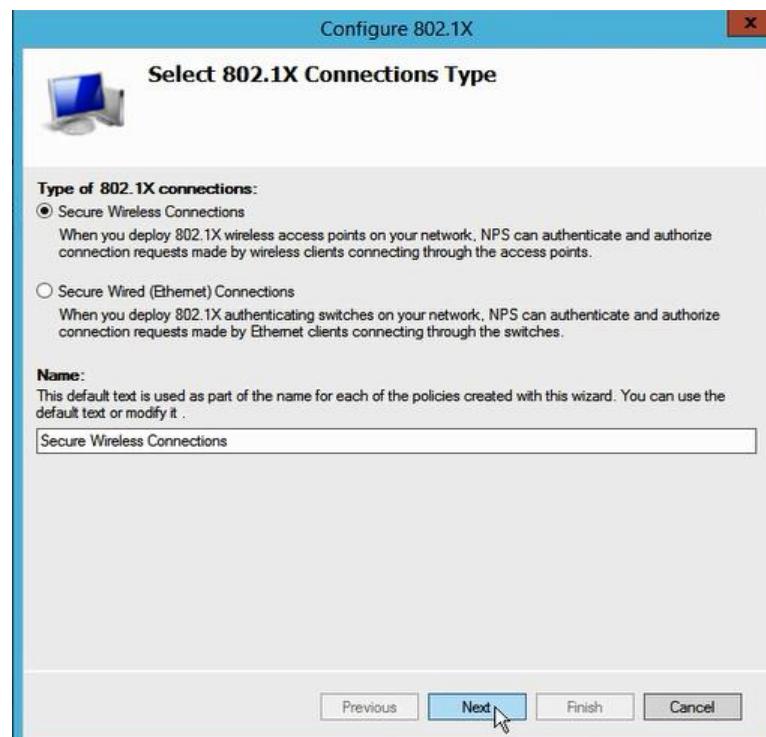


Figure 5.3.7.38: Select 802.1X Connection Type

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.

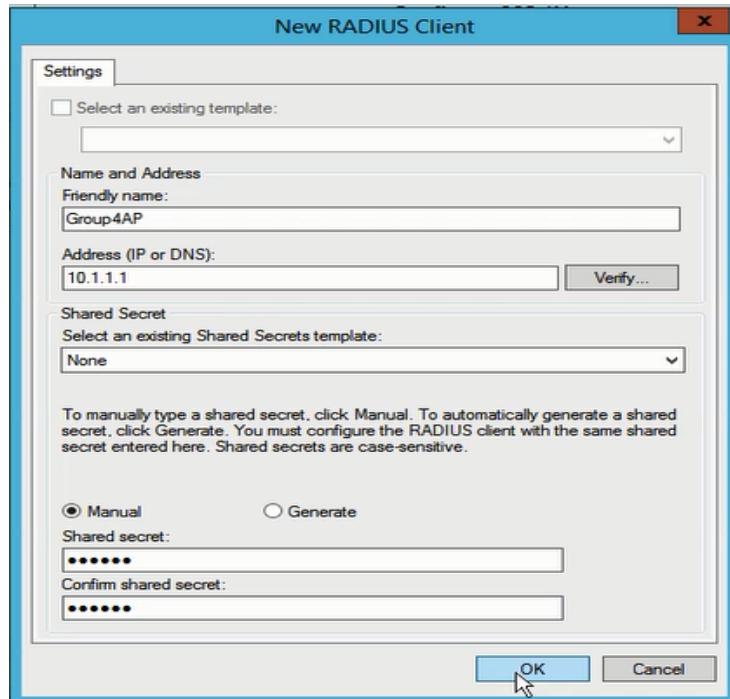


Figure 5.3.7.39: Setting up new RADIUS Client

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

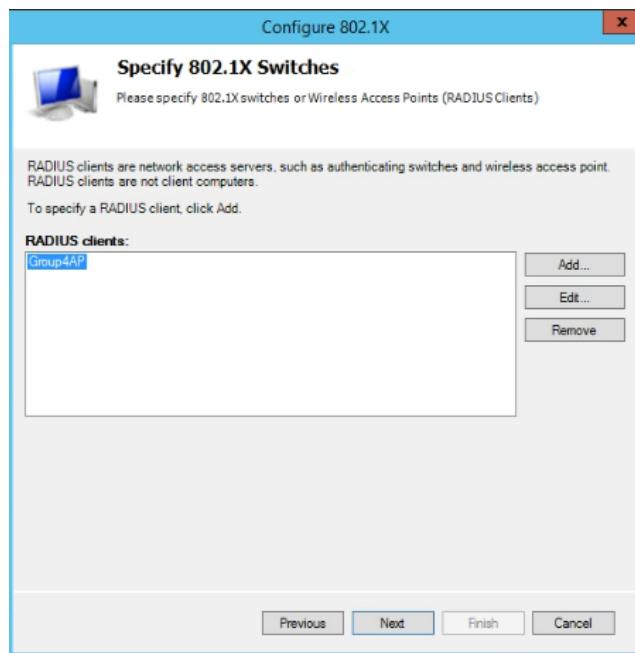


Figure 5.3.7.40: Add RADIUS Client

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

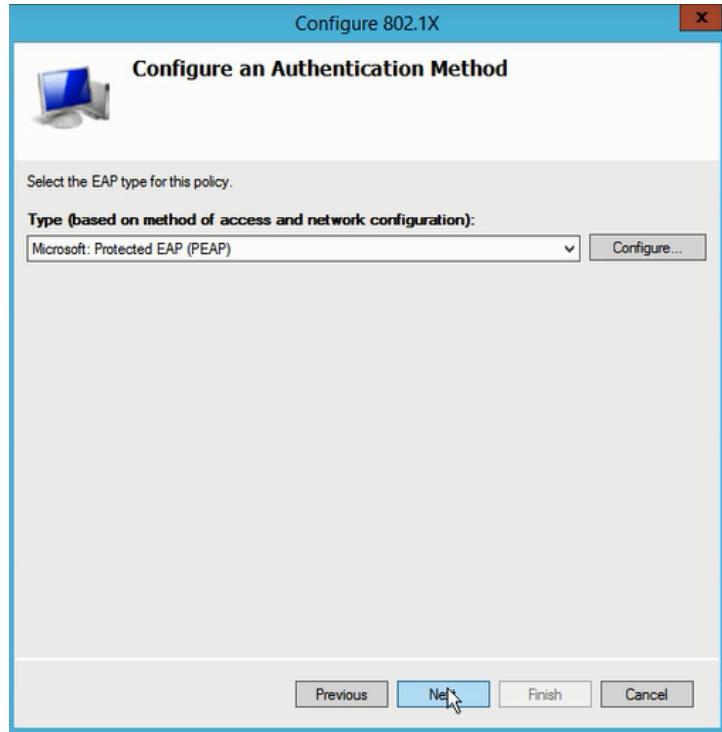


Figure 5.3.7.41: Select the PEAP type for the policy

Step 39: Then, specify the user groups for the group that have been created and add it (group4.com). After that, click Next > Next.



Figure 5.3.7.42: Specify user Group

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



Figure 5.3.7.43: 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 5.3.7.44: Certificate Export Wizard

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



Figure 5.3.7.45: Choose to not export private key

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.

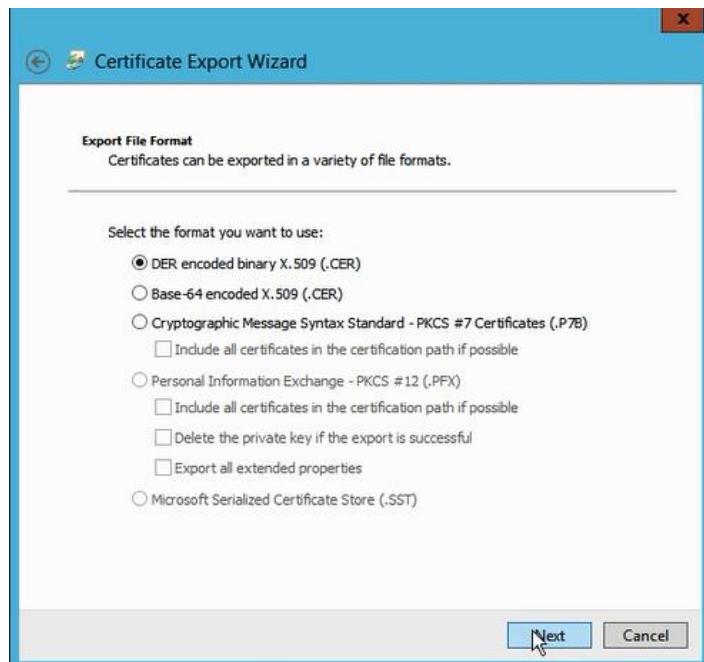


Figure 5.3.7.46: Selecting export file format

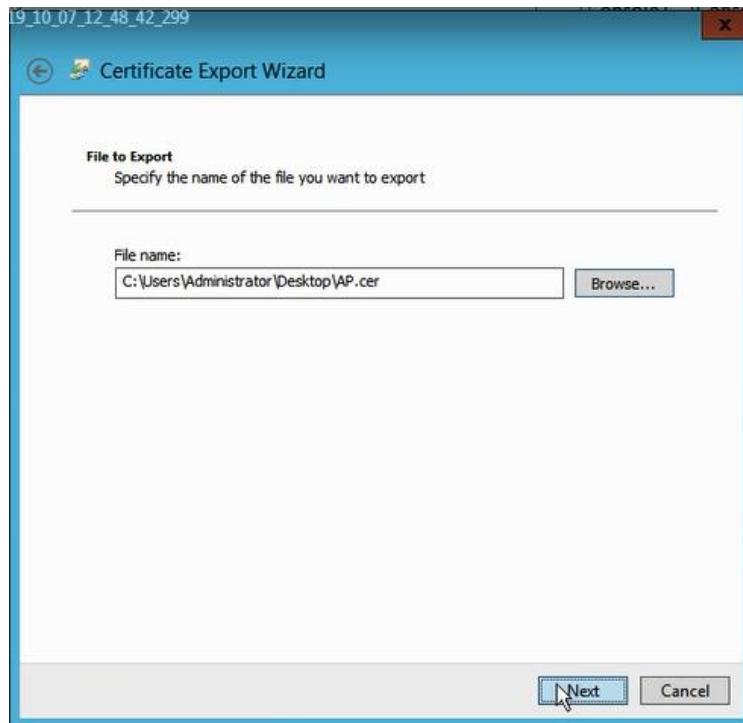


Figure 5.3.7.46: Select File Name to export Certificate

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

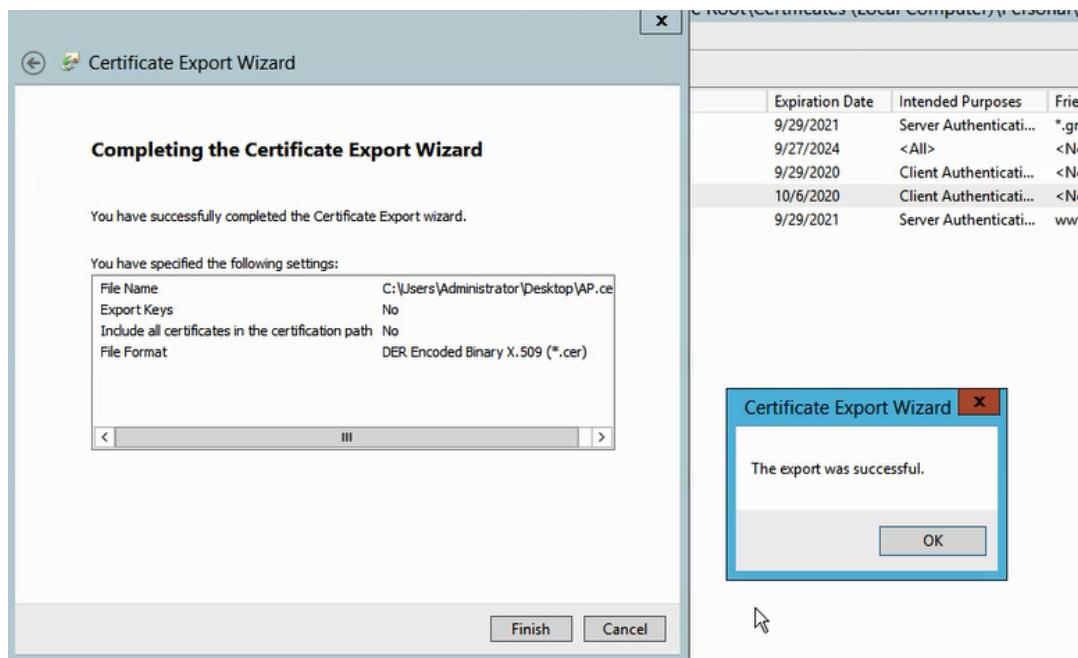


Figure 5.3.7.47: Completing the Certificate export wizard

5.3.8 Network Management System

Network Management System is for administrators manage a network a network's independent component inside a bigger network management framework.

Installation of Zabbix NMS

Step 1: Connect debian PC to the internet and then install the apache2, mysql and php.

```
#apt-get update
#apt-get install apache2
#apt-get install mysql-server
#apt-get install php php-mbstring php-gd php-xml php-bcmath php-ldap php-mysql
```

Figure 5.3.8.1: Show the installation of apache2, mysql and php.

Step 2: Then, open the php.ini file and change the time zone into ‘Asia/Kuala Lumpur’ for Zabbix server can detect and run well because of the synchronize of time.

```
#nano /etc/php/7.0/apache2/php.ini

[Date]
; http://php.net/date.timezone
date.timezone = 'Asia/Kuala_Lumpur'
```

Figure 5.3.8.2: Show the opening file and change the time zone in the php.ini file.

Step 3: Download from the repo Zabbix. Then, depackage the downloaded file.

```
#wget https://repo.zabbix.com/zabbix/4.0/debian/pool/main/z/zabbix-release/zabbix-release_4.0-3+stretch_all.deb
#dpkg -i zabbix-release_4.0-3+stretch_all.deb
```

Figure 5.3.8.3: Show the download from the repo and depackage the downloaded file.

Step 4: Install the Zabbix agent, mysql and the Zabbix frontend.

```
#apt-get update
#apt-get install zabbix-server-mysql zabbix-frontend-php zabbix-agent
```

Figure 5.3.8.4: Show the installation of Zabbix agent, mysql and the frontend.

Step 5: Then, enter to the mysql. Firstly, create the database and name it as ‘Zabbixdb’. After that, create the user as ‘Zabbix’ and set the password into ‘Abc123’. Then, grant all the privilege of the ‘Zabbixdb’ to the ‘Zabbix’ user.

```
#mysql -u root -p
mysql> CREATE DATABASE zabbixdb character set utf8 collate utf8_bin;
mysql> CREATE USER 'zabbix'@'localhost' IDENTIFIED BY 'Abc123';
mysql> GRANT ALL PRIVILEGES ON zabbixdb.* TO 'zabbix'@'localhost' WITH GRANT OPTION;
mysql> FLUSH PRIVILEGES;
```

Figure 5.3.8.5: Show the database and the user is created.

Step 6: Go to the ‘Zabbix-server-mysql’ directory. Then, open the file ‘Zabbix_server.conf’ to configure. Change the database hostname into ‘localhost’, database name into ‘Zabbixdb’, database user into ‘Zabbix’ and database password set to ‘Abc123’ to gain access databse to the Zabbix.

```
#cd /usr/share/doc/zabbix-server-mysql
#zcat create.sql.gz | mysql -u zabbix -p zabbixdb

#nano /etc/zabbix/zabbix_server.conf
DBHost=localhost
DBName=zabbixdb
DBUser=zabbix
DBPassword=Abc123
```

Figure 5.3.8.6: Show the open file of ‘Zabbix_server.conf’ and change database name,host,user and the password.

Step 7: Restart the ‘apache2.service’, ‘Zabbix-server’ and the ‘Zabbix-agent’. The purpose for restarting is to apply change after we setup all the configuration that been made by us.

```
#systemctl restart apache2.service
#systemctl restart zabbix-server
#systemctl restart zabbix-agent
```

Figure 5.3.8.7: Show the restart of all Zabbix service.

Step 8: Copy the ‘apache.conf’ to site-available and name it as ‘v-host-Zabbix.conf’

```
#cp /etc/zabbix/apache.conf /etc/apache2/site-available/vhost-zabbix.conf
```

Figure 5.3.8.8: Show the copy file.

Step 9: Open the Mozilla Firefox and put ‘nms.group4.com/setup.php’ at the URL to setup Zabbix. The setup page will be displayed. Click ‘Next Step’.

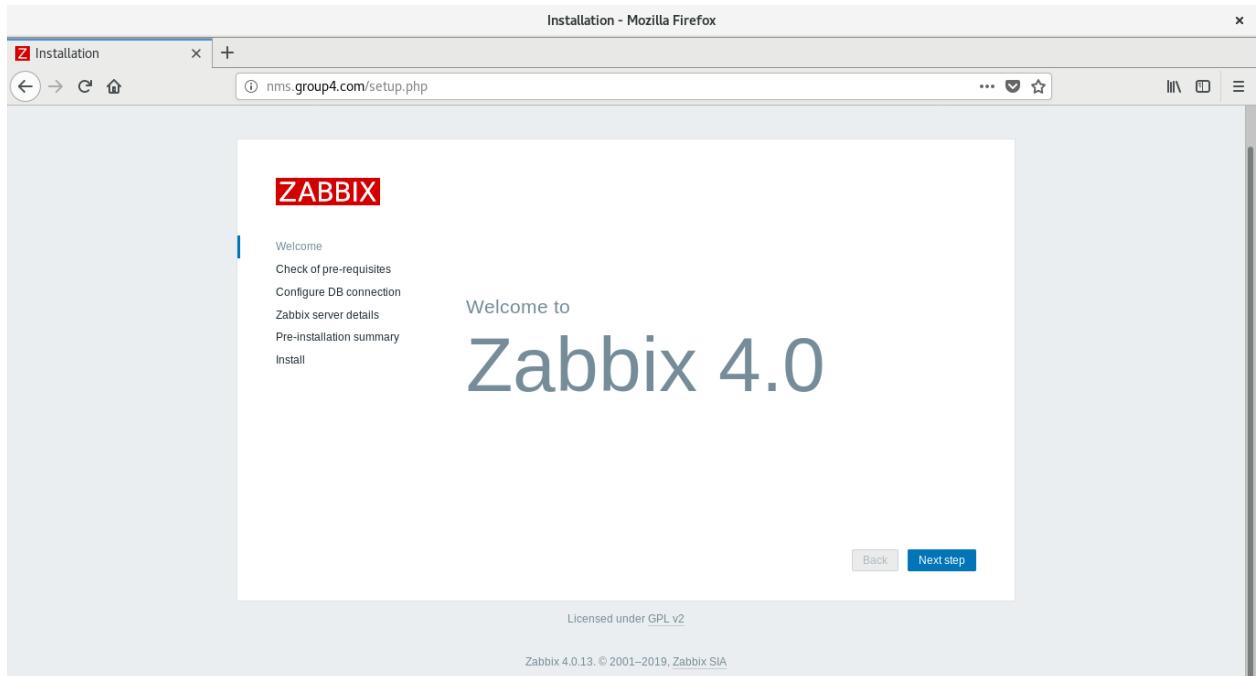


Figure 5.3.8.9: Show the opening setup page for Zabbix.

Step 10: The next page is for check of pre requisites before finish setup of the Zabbix server. Check all the pre-requisites and make sure the all the pre-requisites are ‘OK’ and green.

	Current value	Required	
PHP version	7.0.33-0+deb9u5	5.4.0	OK
PHP option "memory_limit"	128M	128M	OK
PHP option "post_max_size"	16M	16M	OK
PHP option "upload_max_filesize"	2M	2M	OK
PHP option "max_execution_time"	300	300	OK
PHP option "max_input_time"	300	300	OK
PHP option "date.timezone"	Asia/Kuala_Lumpur		OK
PHP databases support	MySQL		OK
PHP bcmath	on		OK
PHP mbstring	on		OK

Figure 5.3.8.10: Show the check for pre-requisites.

Step 11: Then, configure the connection for database. Select database type to ‘MySQL’, enter database host as ‘localhost’, use default database port, enter database name as ‘Zabbix’, set user as ‘Zabbix’ and set password as ‘Abc123’.

Configure DB connection

Please create database manually, and set the configuration parameters for connection to this database. Press “Next step” button when done.

Database type: MySQL

Database host: localhost

Database port: 0 - use default port

Database name: zabbix

User: zabbix

Password: *****

Figure 5.3.8.11: Show the configure of database connection.

Step 12: Set the Zabbix server details. Don't change the host and the port or use the port 10051. Change the name only. Set the name into 'NMS'. NMS is the Zabbix server name.

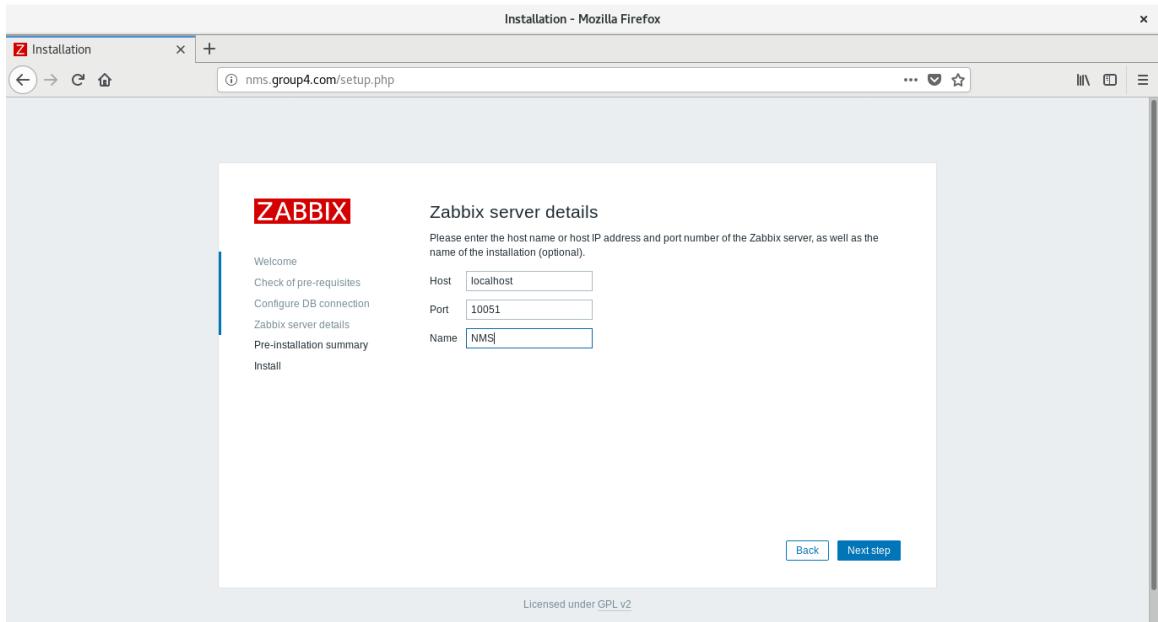


Figure 5.3.8.12: Show the Zabbix server details.

Step 13: Check all the pre-installation summary and make sure it all same like we enter. This is the most important because if there is any error, the Zabbix server cannot run or work properly.

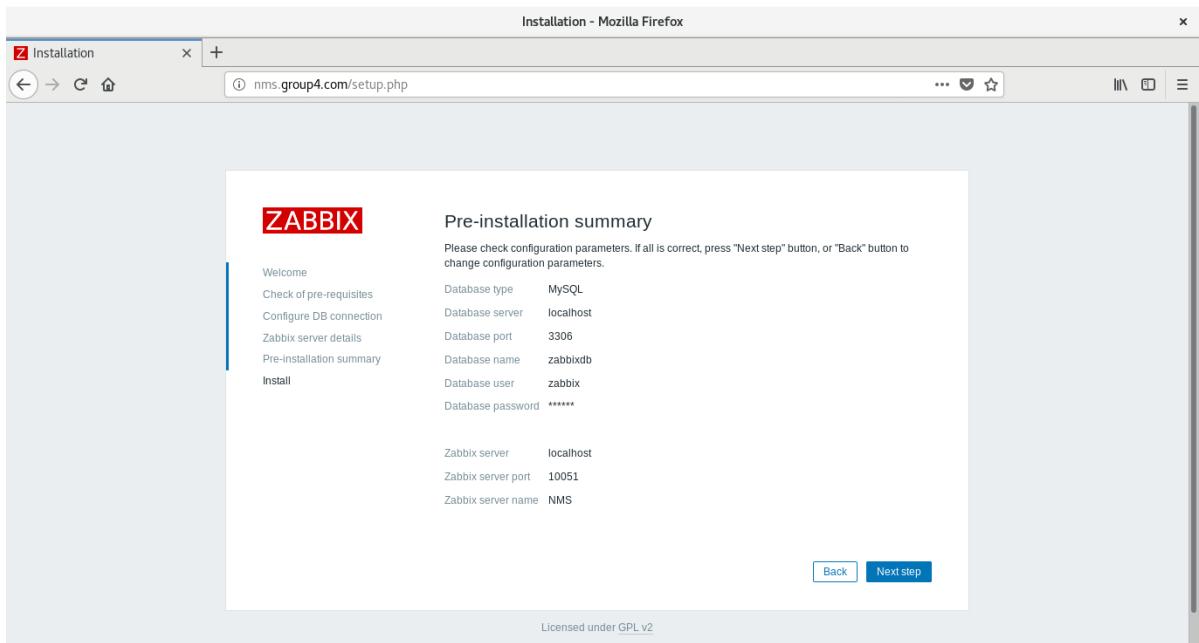


Figure 5.3.8.13: Show the pre-installation summary.

Step 14: Then, go to the login page and enter ‘Admin’ at the username and enter ‘Zabbix’ as the password.

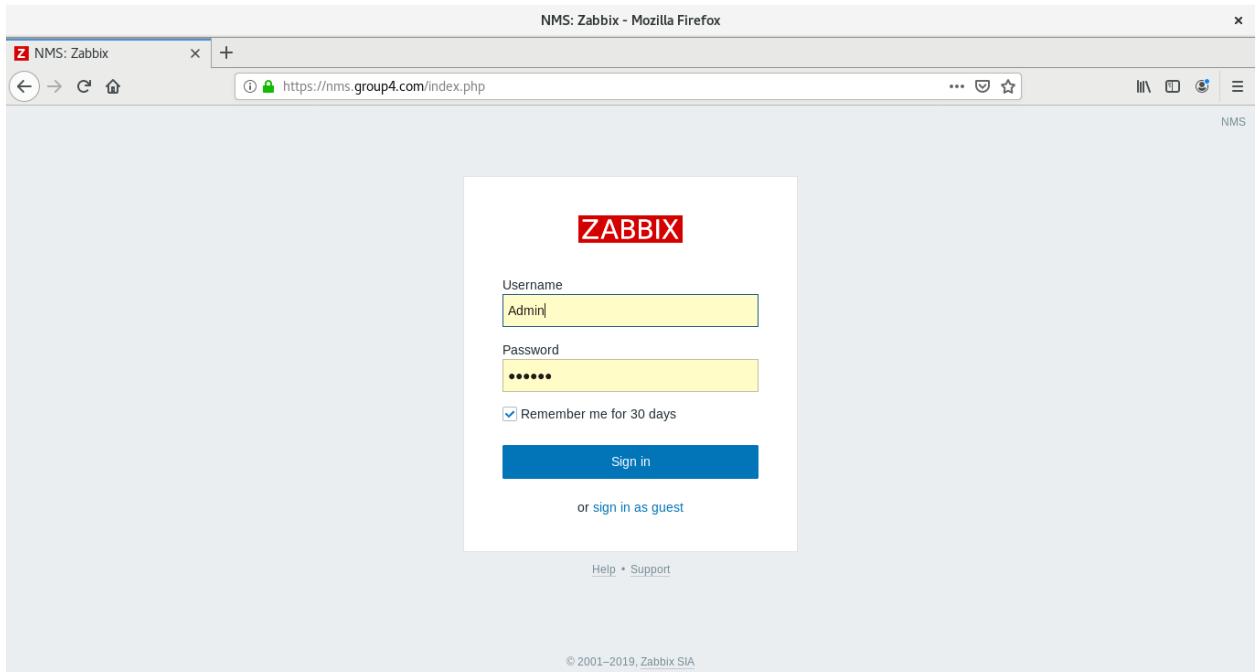


Figure 5.3.8.3.14: Show the login page for Zabbix.

Step 15: After that, it is successfully login and the dashboard for monitoring will be displayed.

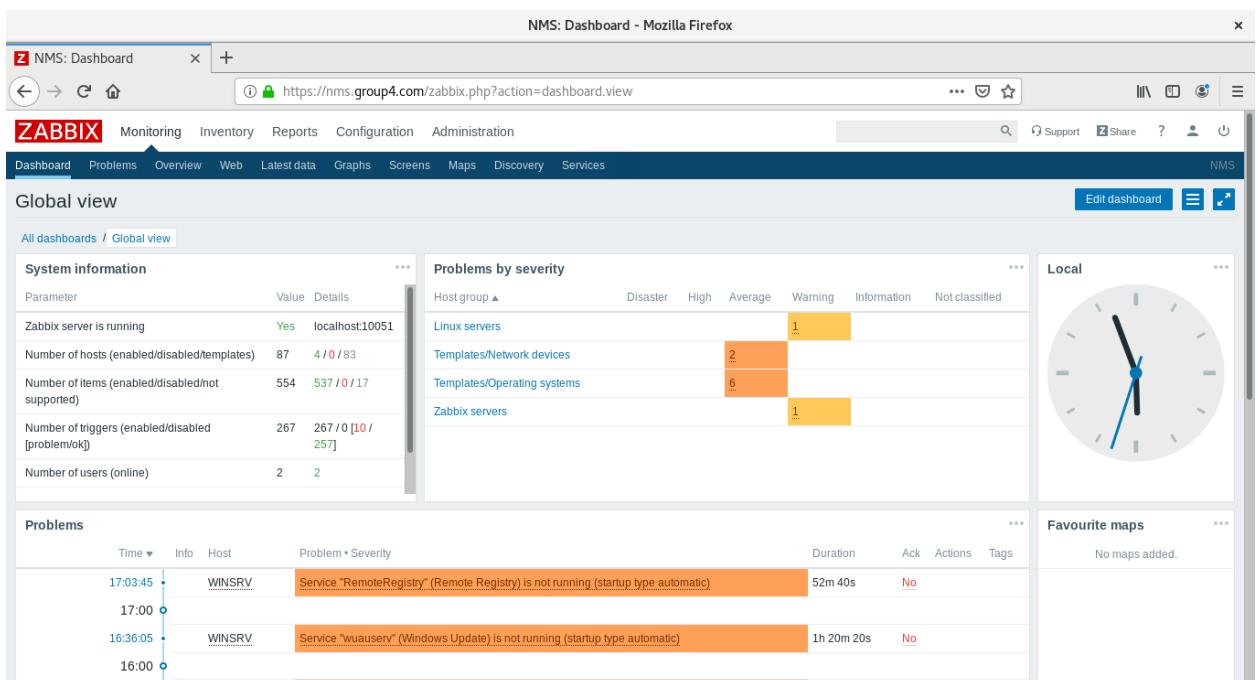


Figure 5.3.8.15. Show Zabbix dashboard

Installation of Zabbix agent at Windows server.

Step 1: Open the Windows server PC. Install the Zabbix-agent for Windows. Unzip it. Make a new folder at ‘C:’ and name the folder as ‘Zabbix’. Unzip the Zabbix agent and put the content into the ‘Zabbix folder’ that we just created.



Figure 5.3.8.16: Show the Zabbix agent for Windows.

Step 2: Now edit the configuration and update the server and hostname value. Set server into Zabbix IP, ’10.1.1.130’ and set the hostname to the hostname of the client system, ‘WINSRV’ for Windows server.

```
#Server=[zabbix server ip]
#Hostname=[Hostname of client system ]

Server=10.1.1.130
Hostname=WINSRV
```

Figure 5.3.8.17: Show the update of configuration.

Step 3: Install Zabbix agent as Windows service. Install Zabbix agent as Windows server by executing following command into the command line.

```
c:\zabbix\bin\win64> zabbix_agentd.exe -c c:\zabbix\conf\zabbix_agentd.conf --install
```

Figure 5.3.8.7.18: Show the installation of the Zabbix agent

Step 4: Start and stop the agent service. It is for apply change to the service after we made the changes in the setup. It can be restart using command line or restart at the task manager -> service.

```
c:\zabbix\bin\win64> zabbix_agentd.exe --start
zabbix_agentd.exe [5048]: service [Zabbix Agent] started successfully
c:\zabbix\bin\win64> zabbix_agentd.exe --stop
zabbix_agentd.exe [7608]: service [Zabbix Agent] stopped successfully
```

Figure 5.3.8.19: Show to stop and start Zabbix agent service using command line.

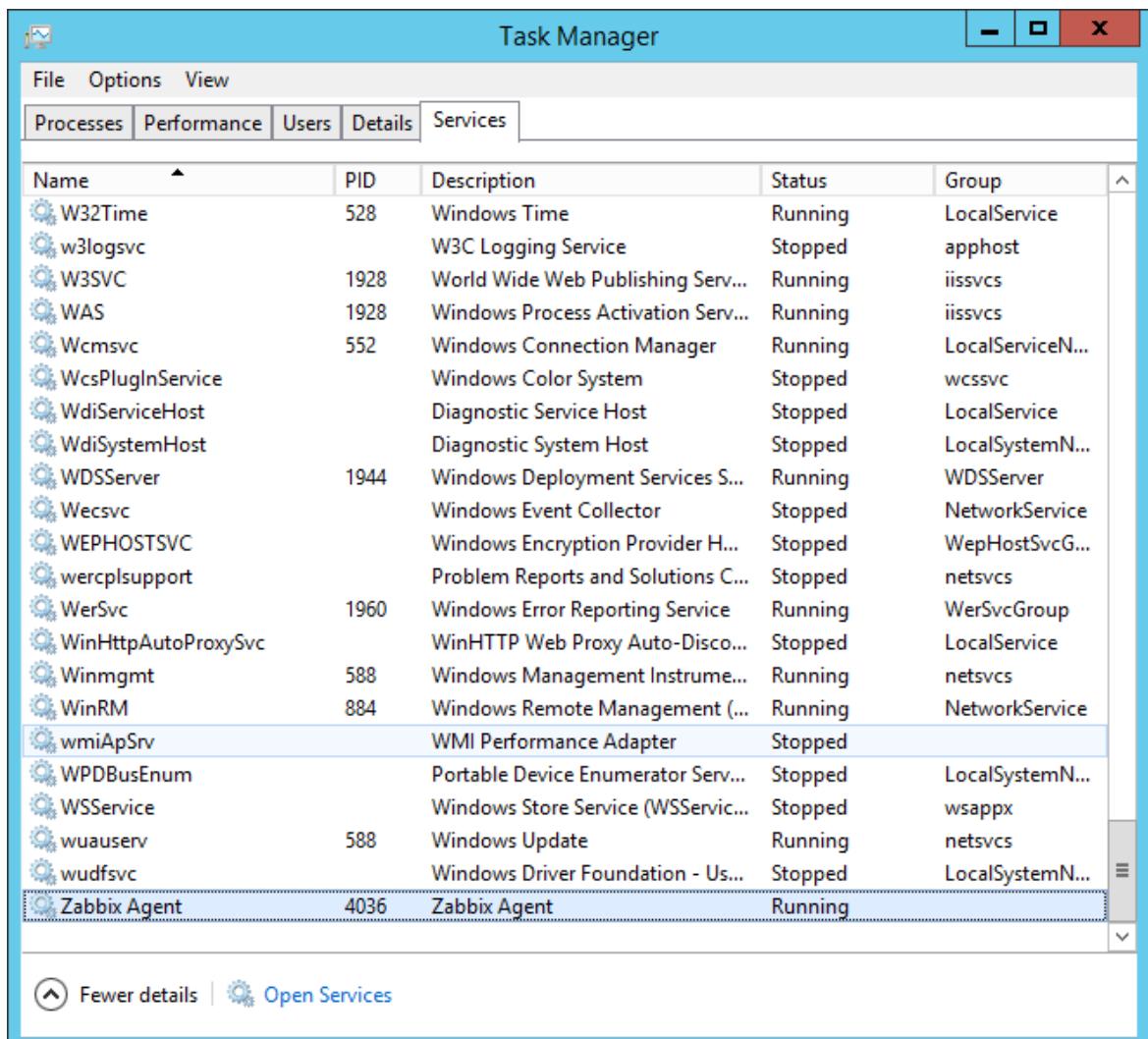
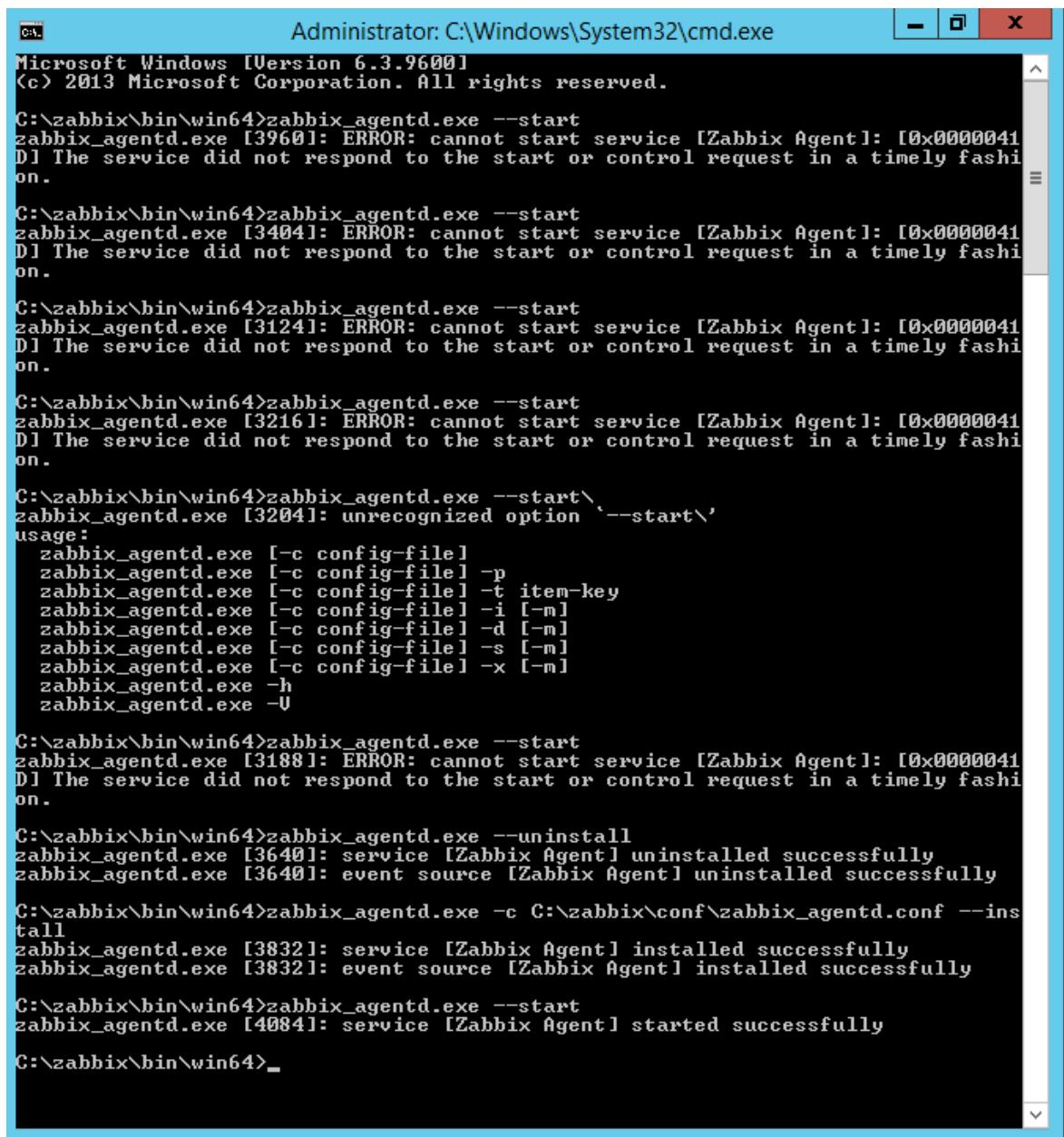


Figure 5.3.8.20: Show to stop and start Zabbix agent using task manager.



The screenshot shows a Windows Command Prompt window titled "Administrator: C:\Windows\System32\cmd.exe". The window contains the following text output:

```

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

C:\zabbix\bin\win64>zabbix_agentd.exe --start
zabbix_agentd.exe [3960]: ERROR: cannot start service [Zabbix Agent]: [0x0000041
D] The service did not respond to the start or control request in a timely fashi
on.

C:\zabbix\bin\win64>zabbix_agentd.exe --start
zabbix_agentd.exe [3404]: ERROR: cannot start service [Zabbix Agent]: [0x0000041
D] The service did not respond to the start or control request in a timely fashi
on.

C:\zabbix\bin\win64>zabbix_agentd.exe --start
zabbix_agentd.exe [3124]: ERROR: cannot start service [Zabbix Agent]: [0x0000041
D] The service did not respond to the start or control request in a timely fashi
on.

C:\zabbix\bin\win64>zabbix_agentd.exe --start
zabbix_agentd.exe [3216]: ERROR: cannot start service [Zabbix Agent]: [0x0000041
D] The service did not respond to the start or control request in a timely fashi
on.

C:\zabbix\bin\win64>zabbix_agentd.exe --start\
zabbix_agentd.exe [3204]: unrecognized option '--start\
usage:
zabbix_agentd.exe [-c config-file]
zabbix_agentd.exe [-c config-file] -p
zabbix_agentd.exe [-c config-file] -t item-key
zabbix_agentd.exe [-c config-file] -i [-m]
zabbix_agentd.exe [-c config-file] -d [-m]
zabbix_agentd.exe [-c config-file] -s [-m]
zabbix_agentd.exe [-c config-file] -x [-m]
zabbix_agentd.exe -h
zabbix_agentd.exe -V

C:\zabbix\bin\win64>zabbix_agentd.exe --start
zabbix_agentd.exe [3188]: ERROR: cannot start service [Zabbix Agent]: [0x0000041
D] The service did not respond to the start or control request in a timely fashi
on.

C:\zabbix\bin\win64>zabbix_agentd.exe --uninstall
zabbix_agentd.exe [3640]: service [Zabbix Agent] uninstalled successfully
zabbix_agentd.exe [3640]: event source [Zabbix Agent] uninstalled successfully

C:\zabbix\bin\win64>zabbix_agentd.exe -c C:\zabbix\conf\zabbix_agentd.conf --ins
tall
zabbix_agentd.exe [3832]: service [Zabbix Agent] installed successfully
zabbix_agentd.exe [3832]: event source [Zabbix Agent] installed successfully

C:\zabbix\bin\win64>zabbix_agentd.exe --start
zabbix_agentd.exe [4084]: service [Zabbix Agent] started successfully

C:\zabbix\bin\win64>_

```

Figure 5.3.8.21: Show the full coding of the installation, stop and start of the Zabbix agent.

Installation Zabbix agent at Ubuntu.

Step 1: Open the Ubuntu server PC. Add repository to install required packages for Zabbix agent using the following command. Install Zabbix agent for Ubuntu 18.04 (Bionic).

```
root@ubuntu:/home/group4# wget https://repo.zabbix.com/zabbix/4.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_4.0-3+bionic_all.deb
--2019-11-16 21:12:00-- https://repo.zabbix.com/zabbix/4.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_4.0-3+bionic_all.deb
Resolving repo.zabbix.com (repo.zabbix.com)... 162.243.159.138, 2604:a880:1:20::b82:1001
Connecting to repo.zabbix.com (repo.zabbix.com)|162.243.159.138|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4068 (4.0K) [application/octet-stream]
Saving to: 'zabbix-release_4.0-3+bionic_all.deb'

zabbix-release_4.0- 100%[=====] 3.97K ---KB/s   in 0s

2019-11-16 21:12:01 (315 MB/s) - 'zabbix-release_4.0-3+bionic_all.deb' saved [4068/4068]
```

Figure 5.3.8.22: Show the installation of zabbix agent for Ubuntu from repositories.

Step 2: After install the zabbix agent, depackage the installed file.

```
root@ubuntu:/home/group4# sudo dpkg -i zabbix-release_4.0-3+bionic_all.deb
Selecting previously unselected package zabbix-release.
(Reading database ... 176327 files and directories currently installed.)
```

Figure 5.3.8.23: Show the depackage downloaded file.

Step 3: As we have successfully added Zabbix apt repositories in our system, then install the Zabbix agent.

```
root@ubuntu:/home/group4# sudo apt-get install zabbix-agent
Reading package lists...
Building dependency tree...
Reading state information...
The following NEW packages will be installed:
  zabbix-agent
```

Figure 5.3.8.24: Show the installation of Zabbix agent.

Step 4: After installation is successful, edit the Zabbix agent configuration file /etc/zabbix/zabbix_agentd.conf and update Zabbix server IP.

```
root@ubuntu:/home/group4# nano /etc/zabbix/zabbix_agentd.conf
```

Figure 5.3.8.25: Show the way to open the zabbix_agentd.conf file.

Step 5: Then, change the server into Zabbix agent ip, '10.1.1.130' and change the hostname to the hostname of the client system, 'UBUNTU'.

```

root@ubuntu:/home/group4
File Edit View Search Terminal Help
GNU nano 2.9.3                               /etc/zabbix/zabbix_agentd.conf

### Option: Server
#      List of comma delimited IP addresses, optionally in CIDR notation, or DNS names of Zabbix servers and Zabbix proxies.
#      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:127.0.0.1' are treated equally
#      and '::/0' will allow any IPv4 or IPv6 address.
#      '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.example.com

# Mandatory: yes, if StartAgents is not explicitly set to 0
# Default:
# Server=

Server=10.1.1.130

### 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 list of active checks.
#
# Mandatory: no
# Default:
# ListenIP=0.0.0.0

### Option: StartAgents
#      Number of pre-forked instances of zabbix_agentd that process passive checks.
#      If set to 0, disables passive checks and the agent will not listen on any TCP port.

^G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify   ^C Cur Pos   M-U Undo
^X Exit       ^R Read File    ^L Replace    ^U Uncut Text  ^T To Spell   ^G Go To Line M-E Redo
                                         M-A Mark Text M-J To Bracket
                                         M-G Copy Text M-W WhereIs Next

```

Figure 5.3.8.26: Show the server is set into Zabbix server ip.

```

root@ubuntu:/home/group4
File Edit View Search Terminal Help
GNU nano 2.9.3                               /etc/zabbix/zabbix_agentd.conf

# Mandatory: no
# Range: 0-100
# Default:
# StartAgents=3

##### Active checks related

### Option: ServerActive
#      List of comma delimited IP:port (or DNS name:port) pairs of Zabbix servers and Zabbix proxies for active checks.
#      If port is not specified, default port is used.
#      IPv6 addresses must be enclosed in square brackets if port for that host is specified.
#      If port is not specified, square brackets for IPv6 addresses are optional.
#      If this parameter is not specified, active checks are disabled.
#      Example: ServerActive=127.0.0.1:20051,zabbix.domain,[::1]:30051,::1,[12Fc::1]

# Mandatory: no
# Default:
# ServerActive=

ServerActive=10.1.1.130

### Option: Hostname
#      Unique, case sensitive hostname.
#      Required for active checks and must match hostname as configured on the server.
#      Value is acquired from HostnameItem if undefined.

# Mandatory: no
# Default:
# Hostname=

Hostname=UBUNTU

### Option: HostnameItem

^G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify   ^C Cur Pos   M-U Undo
^X Exit       ^R Read File    ^L Replace    ^U Uncut Text  ^T To Spell   ^G Go To Line M-E Redo
                                         M-A Mark Text M-J To Bracket
                                         M-G Copy Text M-W WhereIs Next

```

Figure 5.3.8.27: Show the hostname is set to hostname of the client.

Step 6: After adding Zabbix server IP in configuration file, restart the agent service.

```
root@ubuntu:/home/group4# systemctl enable zabbix-agent
Synchronizing state of zabbix-agent.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-agent
root@ubuntu:/home/group4# systemctl start zabbix-agent
root@ubuntu:/home/group4# systemctl status zabbix-agent
● zabbix-agent.service - Zabbix Agent
    Loaded: loaded (/lib/systemd/system/zabbix-agent.service; enabled; vendor pre
    Active: active (running) since Sat 2019-11-16 21:13:54 +08; 2min 40s ago
```

Figure 5.3.8.28: Show the enable, start, stop and status of the Zabbix agent.

5.3.9 Secure FTP

Installing the Secure FTP via vsftpd

Step 1: Install VSFTPD, and enable the VSFTPD service.

A screenshot of a terminal window titled "group4@ubuntu: ~". The window has standard window controls (minimize, maximize, close) in the top right corner. The menu bar at the top includes "File", "Edit", "View", "Search", "Terminal", and "Help". The main area of the terminal shows the command "group4@ubuntu:~\$ sudo apt-get install vsftpd" being typed. The text is white on a dark background, and the cursor is positioned after the "d" in "vsftpd".

A screenshot of a terminal window titled "group4@ubuntu: ~". The window has a dark background with light-colored text. At the top, there's a menu bar with options: File, Edit, View, Search, Terminal, Help. Below the menu is a command line input field where the user is typing the command "sudo systemctl start vsftpd.service". The text is in white, and the cursor is positioned at the end of the command.

Figure 5.3.9.1: The command to install and enable service.

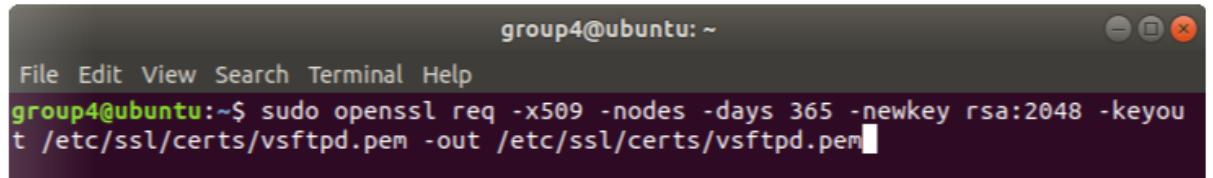
Step 2: Open the configuration file and make some change & save the file.

```
group4@ubuntu: ~
File Edit View Search Terminal Help
GNU nano 2.9.3           /etc/vsftpd.conf          Modified

# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
#
# Run standalone?  vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
#pasv_enable = YES
#pasv_min_port = 40000
#pasv_max_port = 40100
#
# This directive enables listening on IPv6 sockets. By default, listening
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text ^T To Spell ^_ Go To Line
```

Figure 5.3.9.2: The configuration file of vsftpd

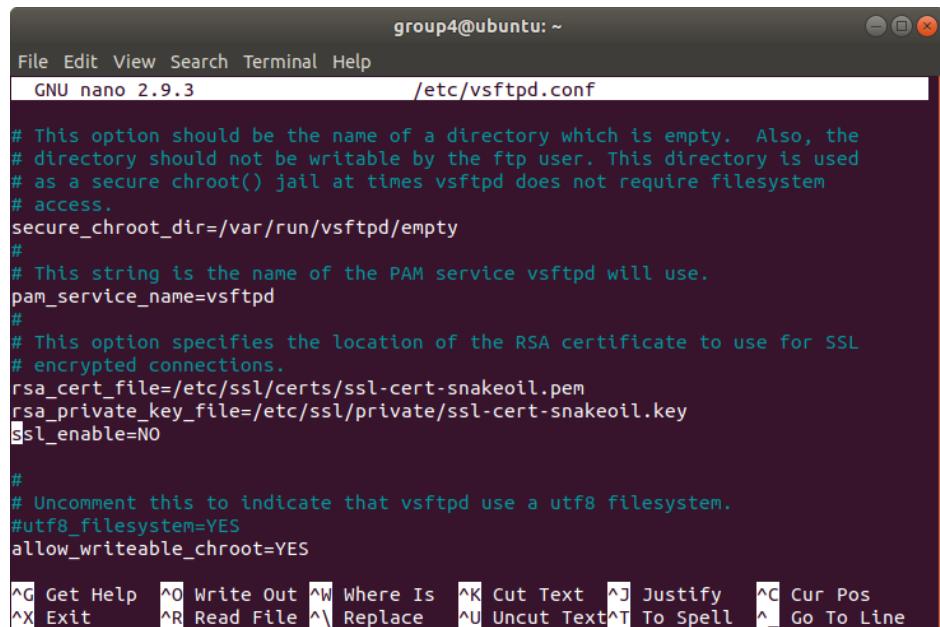
Step 3: Run the command as below to create folder to store certificates.



```
group4@ubuntu: ~
File Edit View Search Terminal Help
group4@ubuntu:~$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/certs/vsftpd.pem -out /etc/ssl/certs/vsftpd.pem
```

Figure 5.3.9.3: The command to store certificate.

Step 4: After generating the certificate, open the vsftpd conf.file and add the lines below.



```
group4@ubuntu: ~
File Edit View Search Terminal Help
GNU nano 2.9.3          /etc/vsftpd.conf

# This option should be the name of a directory which is empty. Also, the
# directory should not be writable by the ftp user. This directory is used
# as a secure chroot() jail at times vsftpd does not require filesystem
# access.
secure_chroot_dir=/var/run/vsftpd/empty
#
# This string is the name of the PAM service vsftpd will use.
pam_service_name=vsftpd
#
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
SSL_enable=NO
#
# Uncomment this to indicate that vsftpd use a utf8 filesystem.
#utf8_filesystem=YES
allow_writeable_chroot=YES

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

Figure 5.3.9.4: The vsftpd configuration file

Step 5: Open an FTP client and connect, and you should be prompted to allow to confirm the certificate presented to client.

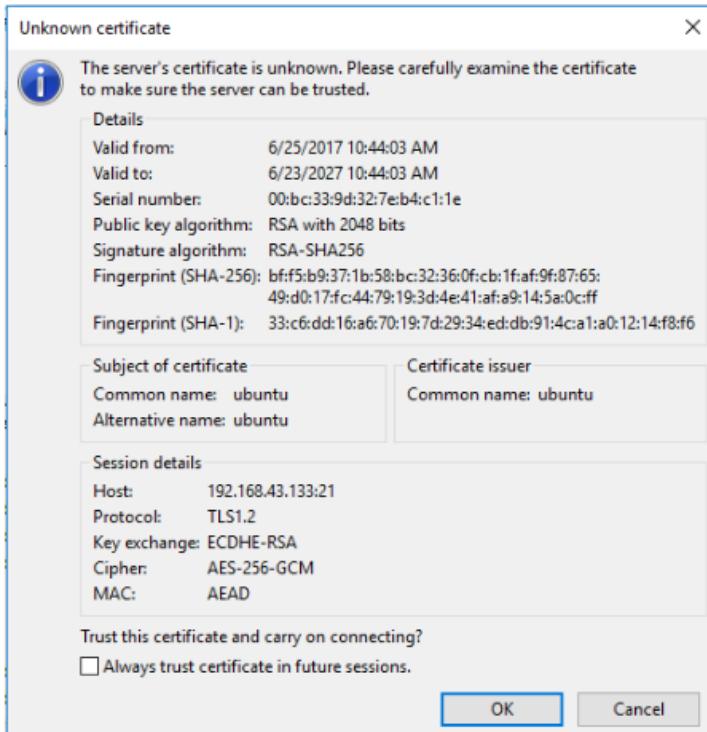


Figure 5.3.9.5: The certificate prompted.

5.3.10 Dynamic Host Configuration Protocol (IPv4 and IPv6)

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.

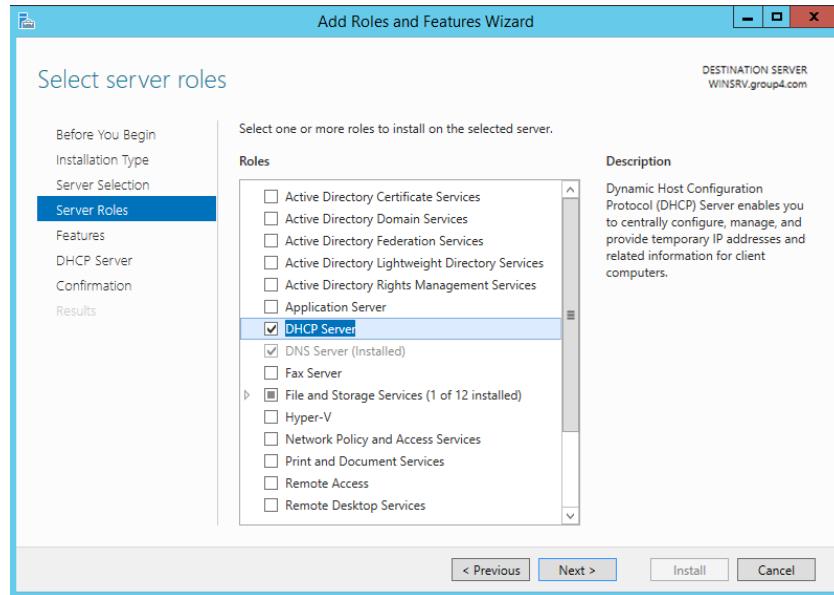


Figure 5.3.10.1: Adding role for DHCP

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

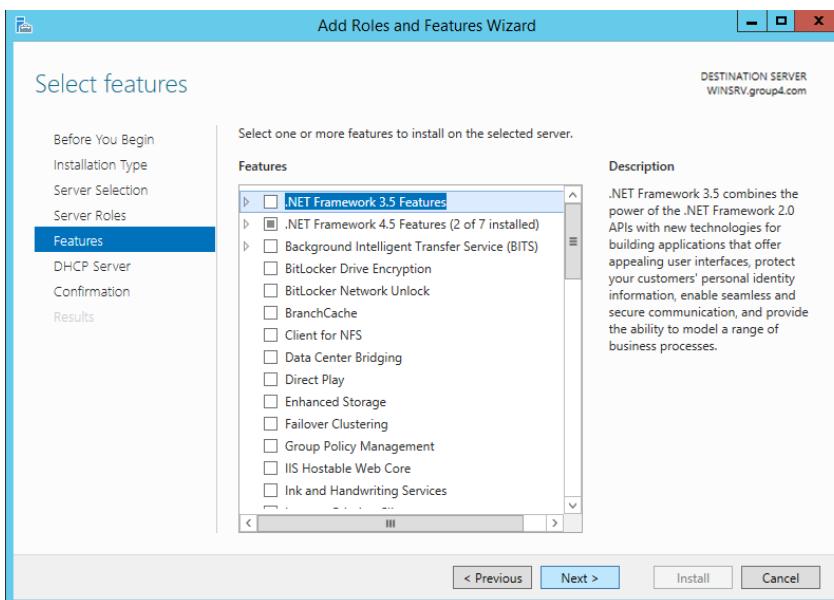


Figure 5.3.10.2: Select features for DHCP

Step 4: Then, wait till the installation completed.

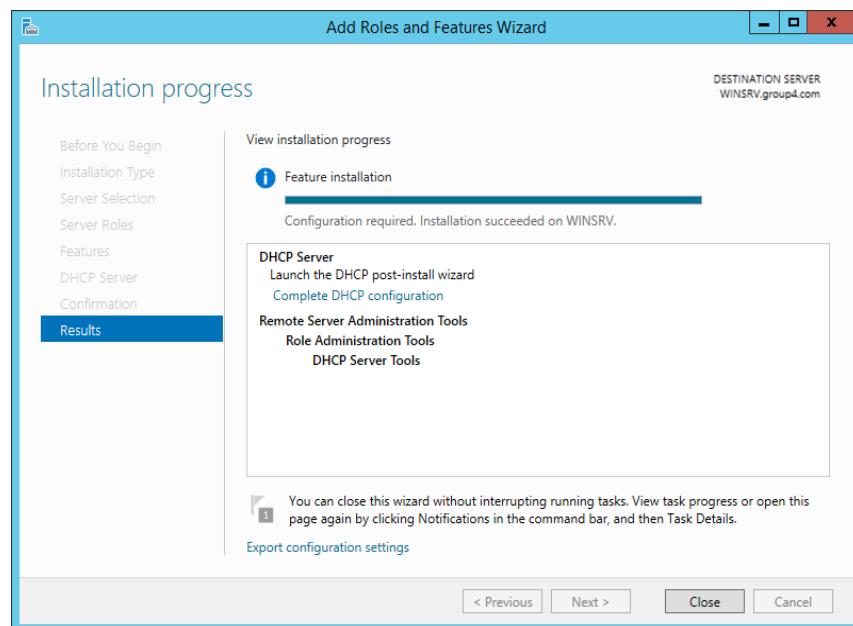


Figure 5.3.10.3: DHCP role to be completed

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

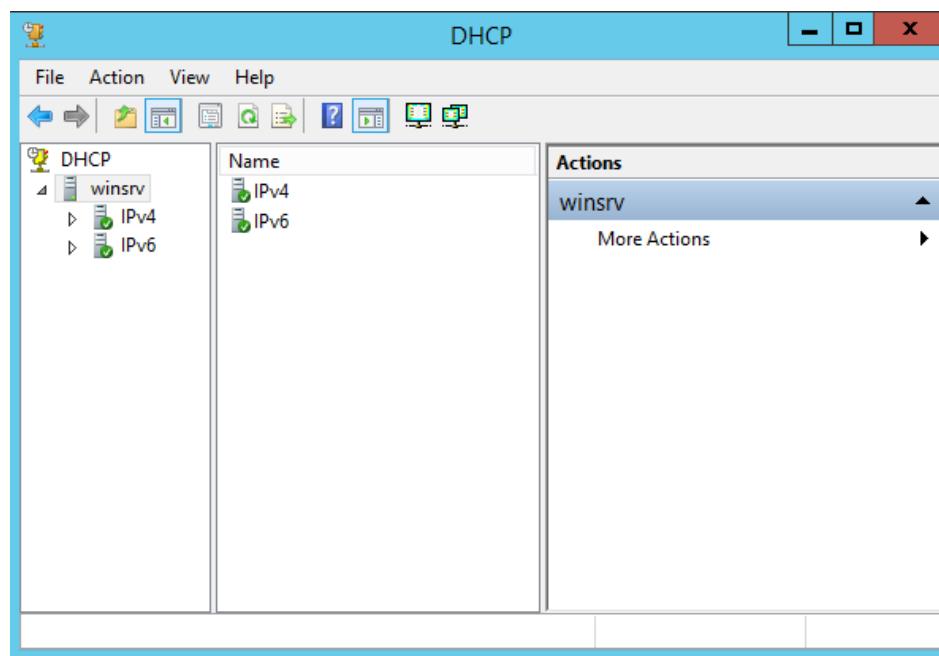


Figure 5.3.10.4: DHCP configuration page

Step 6: Add New Scope Wizard and click Next.



Figure 5.3.10.5: Create scope name for New Scope Wizard

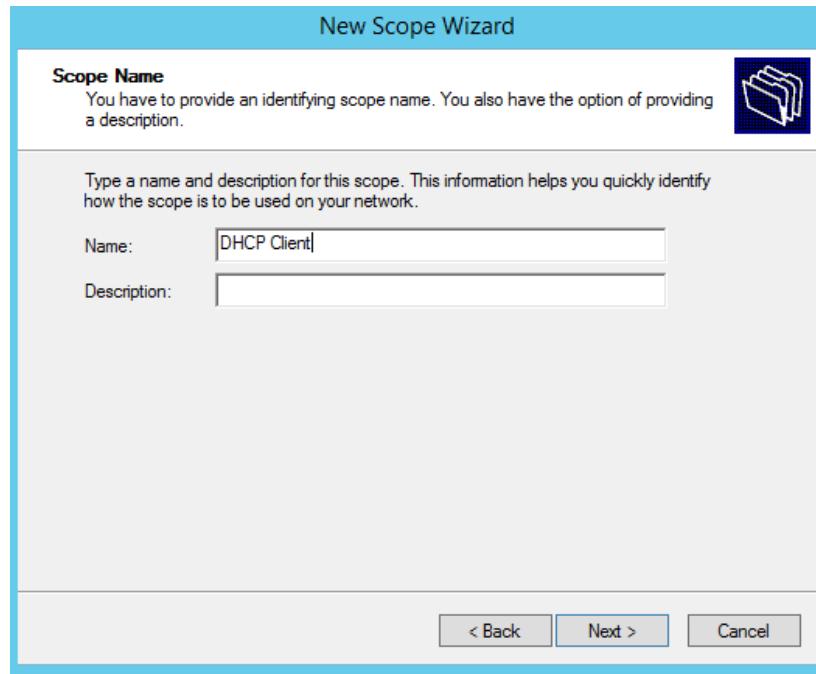


Figure 5.3.10.6: Create scope name for New Scope Wizard

Step 7: Set IP Address Range to distribute the IP for server.

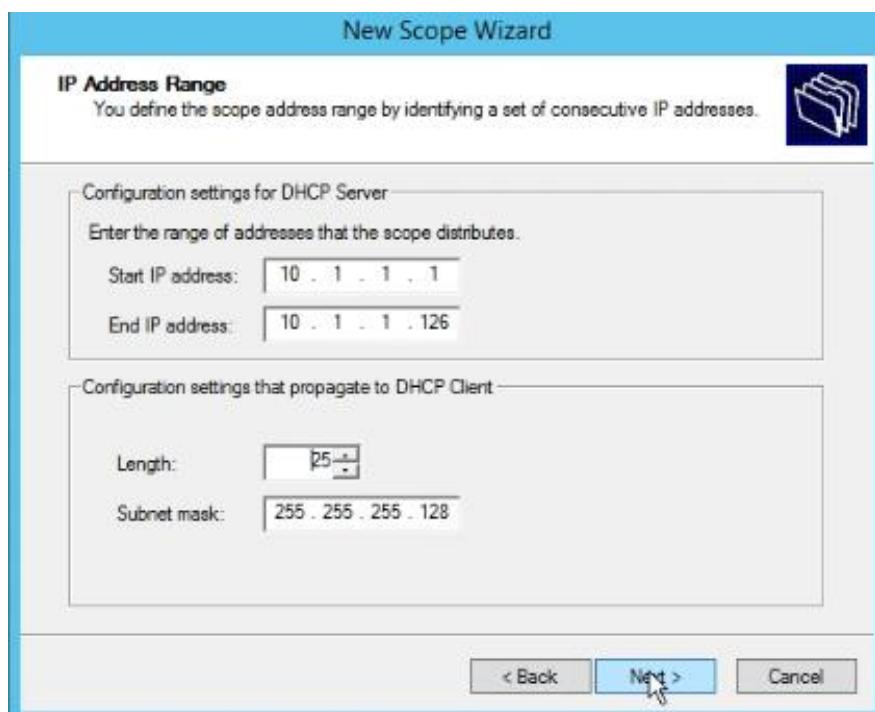


Figure 5.3.10.7: Set IP Address Range

Step 8: Then, set the lease duration. It is to specifies how long client can use and IP Address from this scope. After that, click Next.

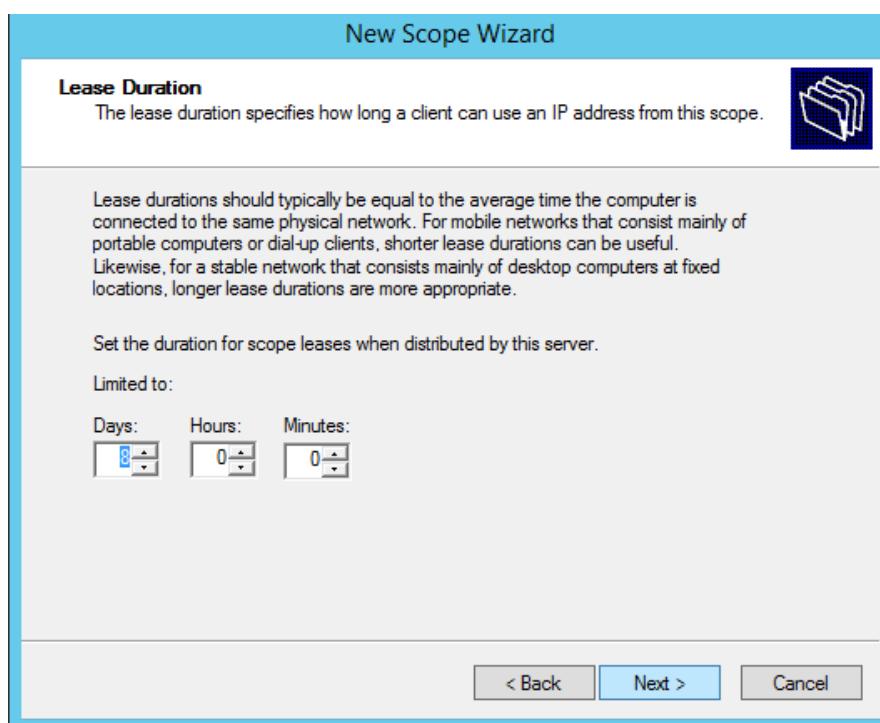


Figure 5.3.10.8: Set the lease duration

Step 9: Then, choose Yes, I want to configure these option now and click Next.

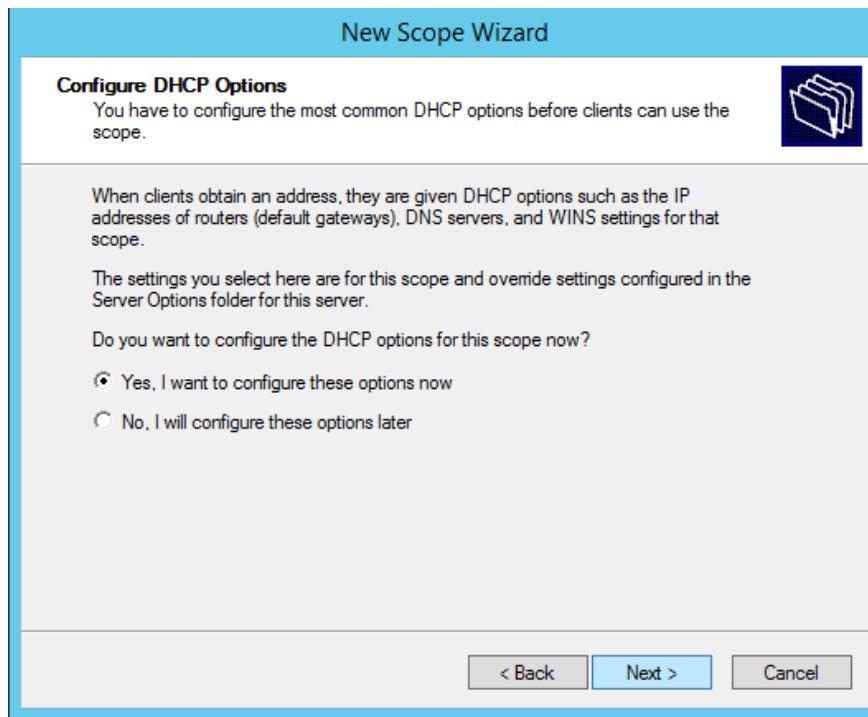


Figure 5.3.10.9: Configure DHCP options

Step 10: Insert Router's IP Address add in and click Next.

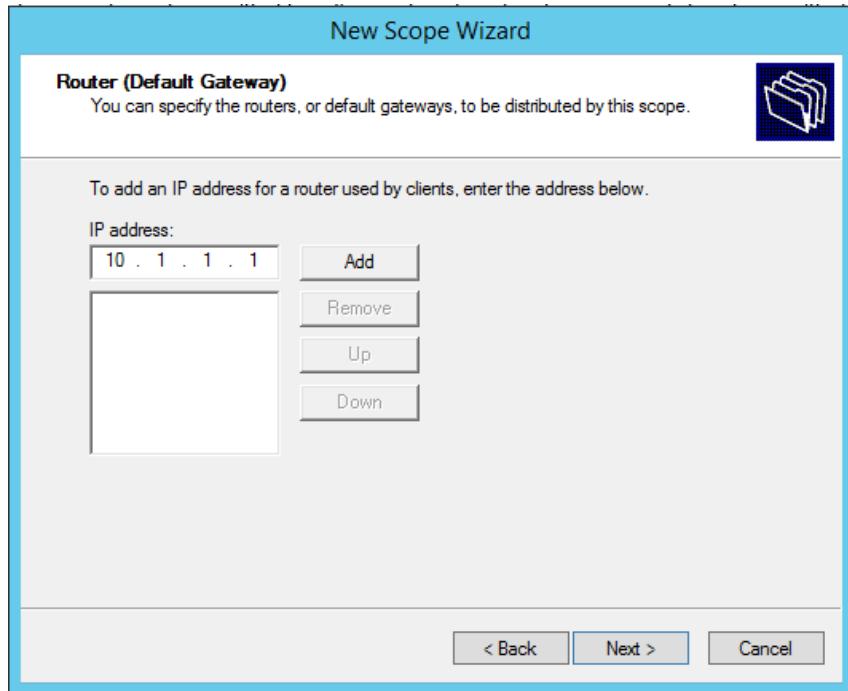


Figure 5.3.10.10: Add IP for Router

Step 11: Then, set parent domain name and also IP address for DNS Server. Click Next.

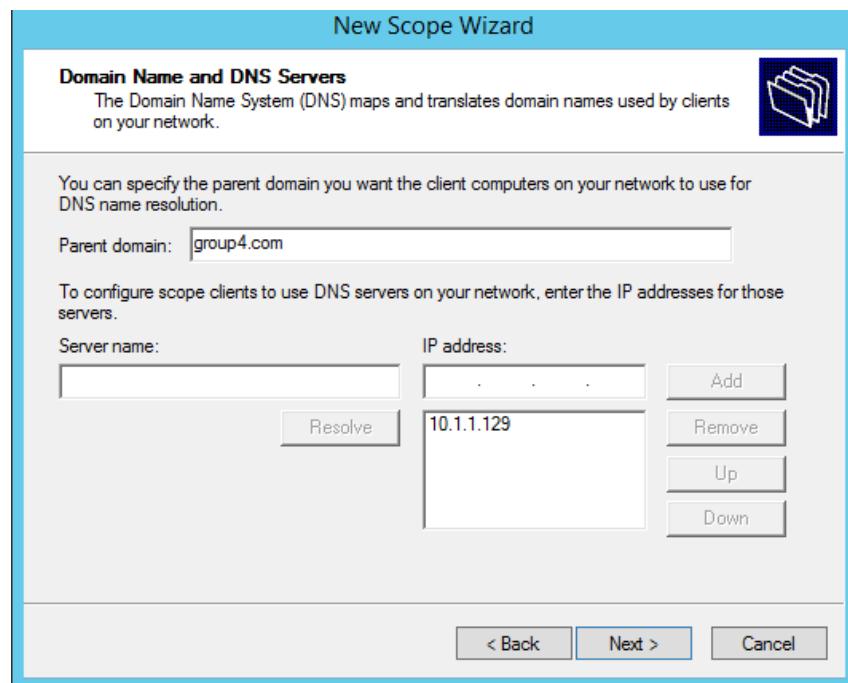


Figure 5.3.10.11: Set Domain Name and DNS Server

Step 12: Activate the scope, then click Finish. New Scope Wizard successfully completed.

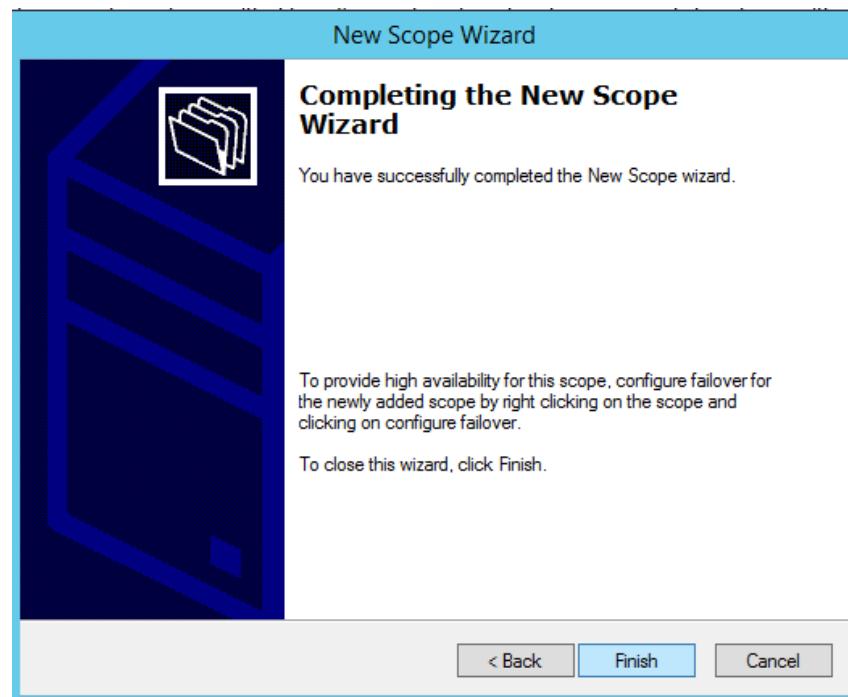


Figure 5.3.10.12: Completed New Scope Wizard

Dynamic Host Configuration Protocol (DHCP) IPv6

Step 1: Right click on IPv6 and choose New Scope and click Next.

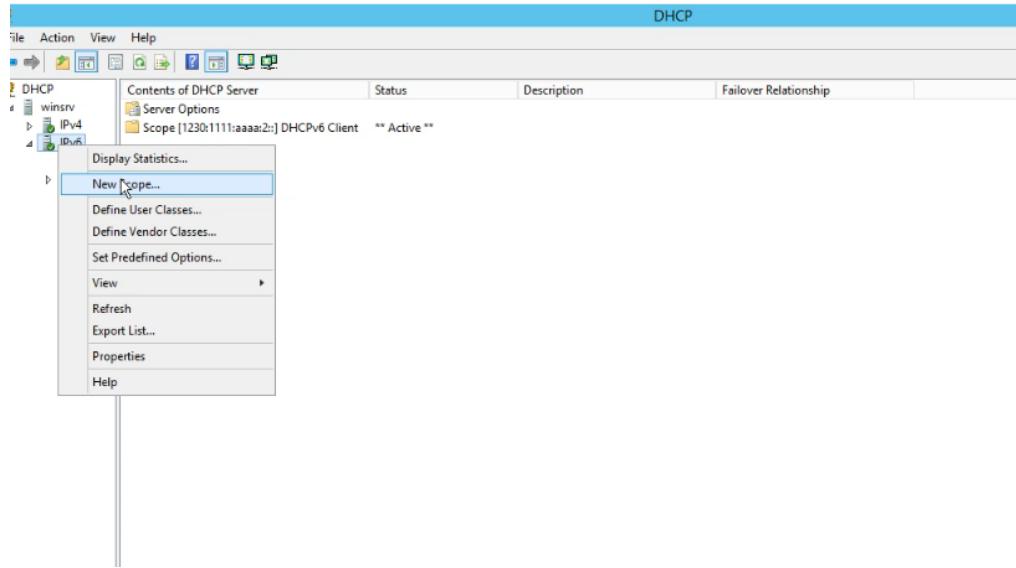


Figure 5.3.10.13: Add New Scope

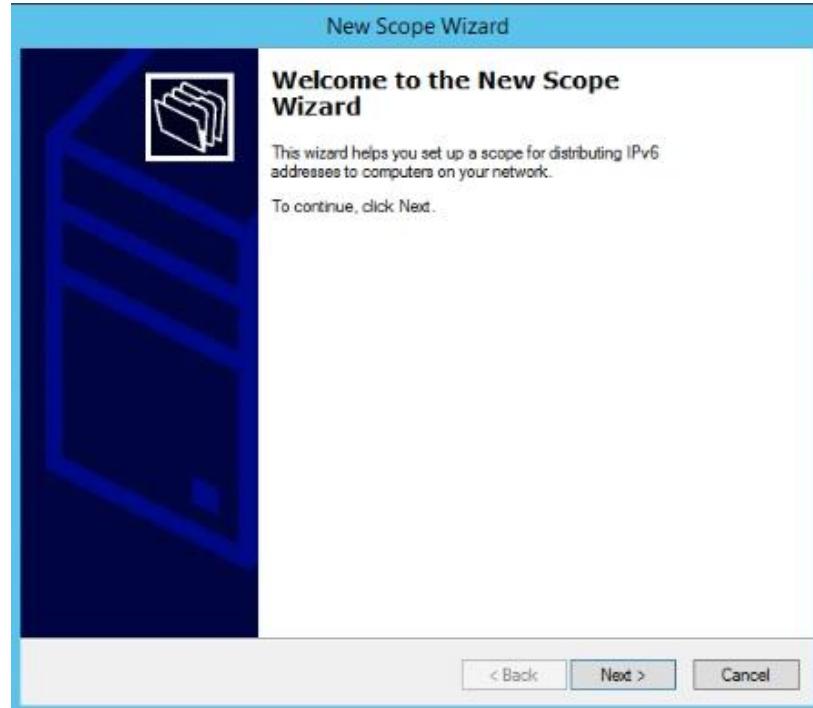


Figure 5.3.10.14: New Scope Wizard

Step 2: Insert name as “**DHCPv6 Client**” then click Next.

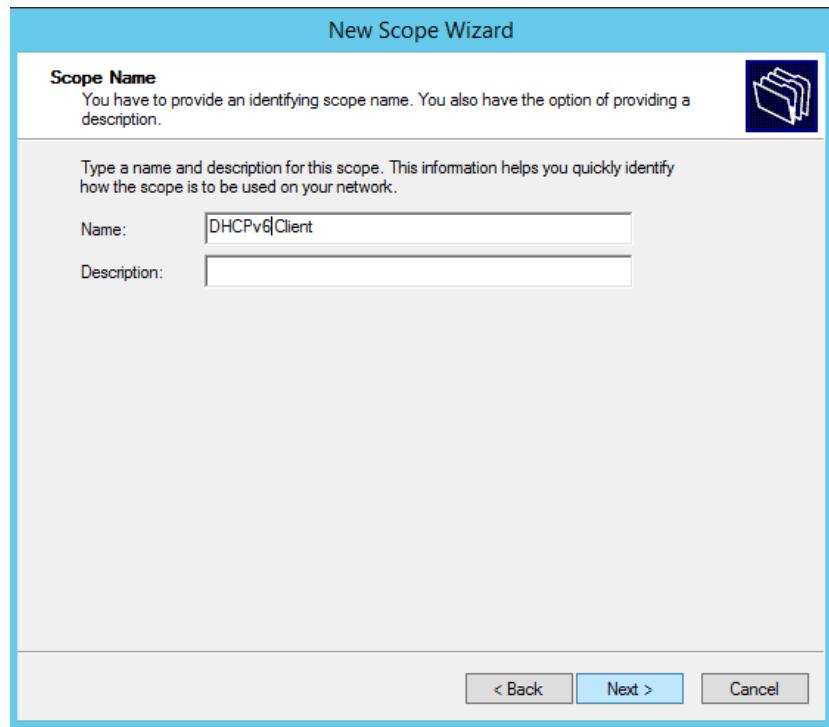


Figure 5.3.10.15: Set Scope Name

Step 3: After that, insert prefix with (1230:1111:AAAA:2::) then click Next.

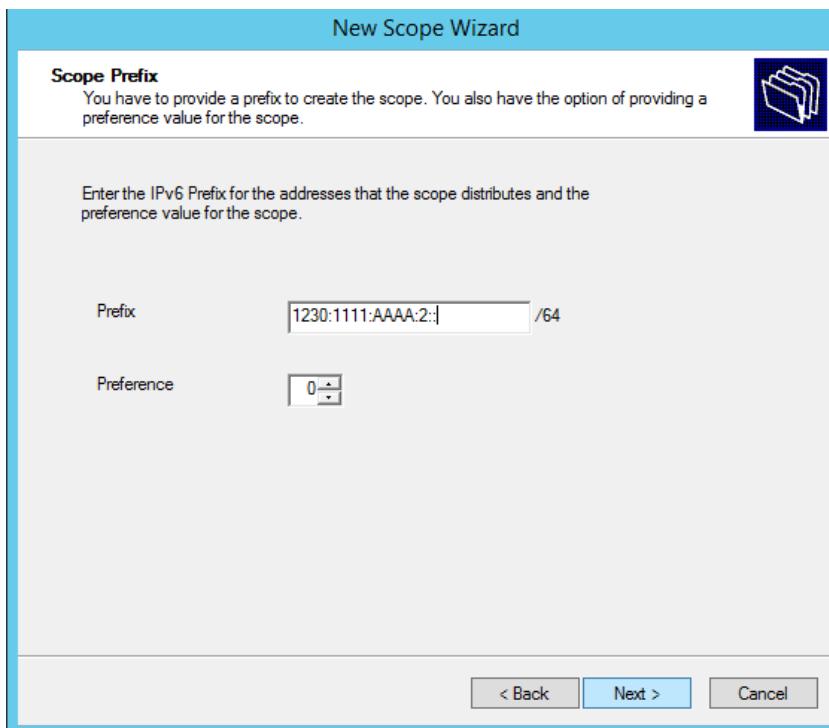


Figure 5.3.10.16: Set Prefix

Step 4: Then, set scope lease by preferred & valid life time for IPv6 used by client and click Next.

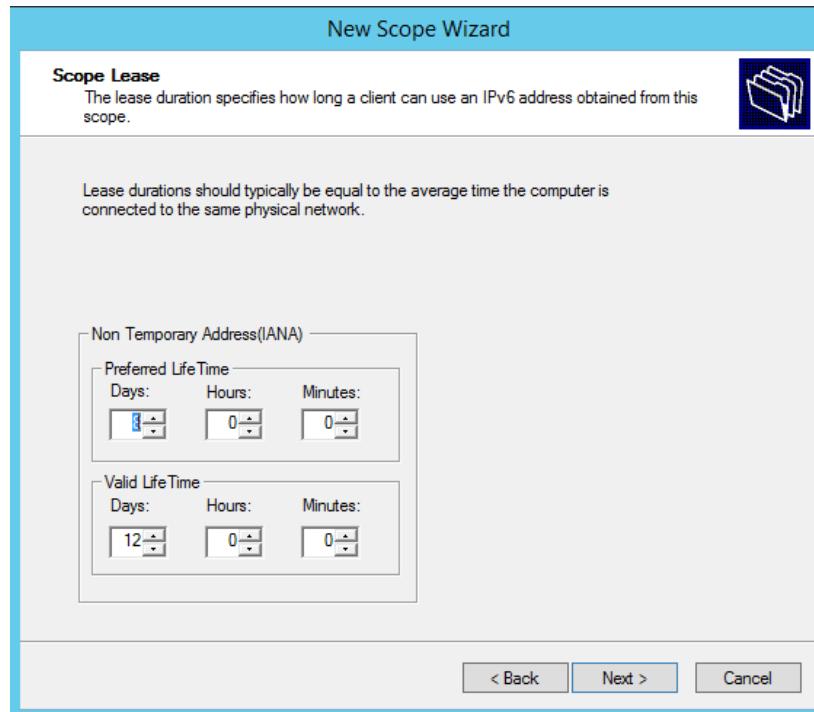


Figure 5.3.10.17: Set Scope Lease for IPv6

Step 5: New Scope Wizard successfully completed for IPv6. Click Finish

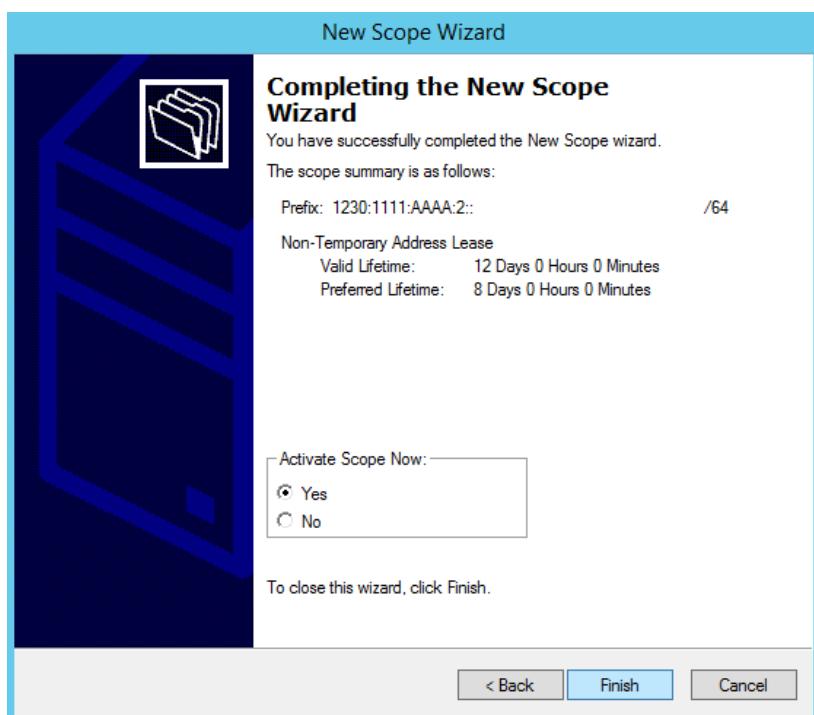


Figure 5.3.10.18: Completed New Scope Wizard

5.3.11 Web, SSL and Virtual Hosting

Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network.

Step 1: As the Internet Information Services (IIS) Manager is already been downloaded, proceed to open the IIS Manager to request certificate at Windows server.

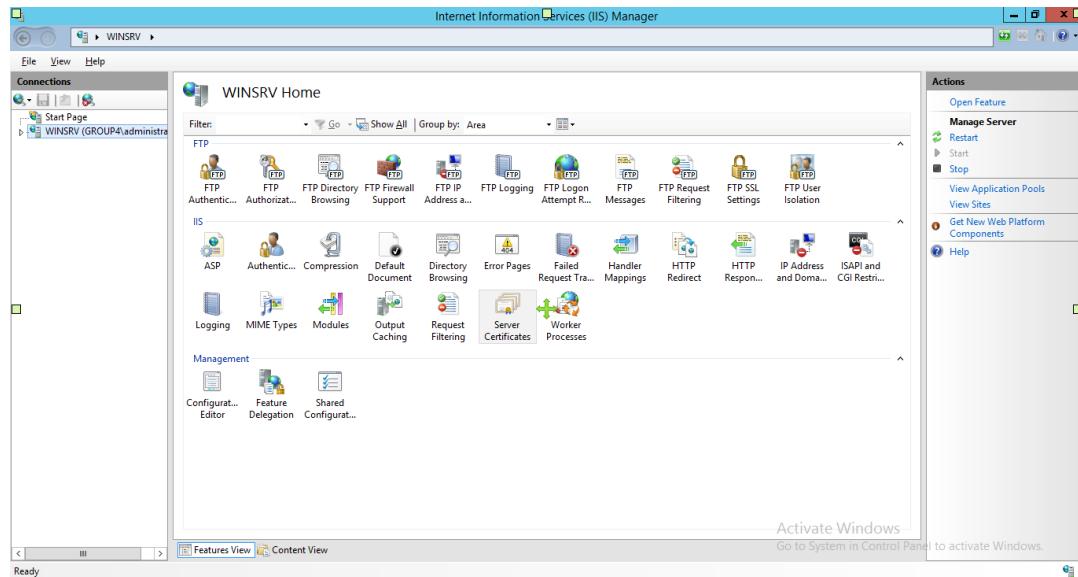


Figure 5.3.11.1: Show the IIS Manager.

Step 2: After that, open server certificate.

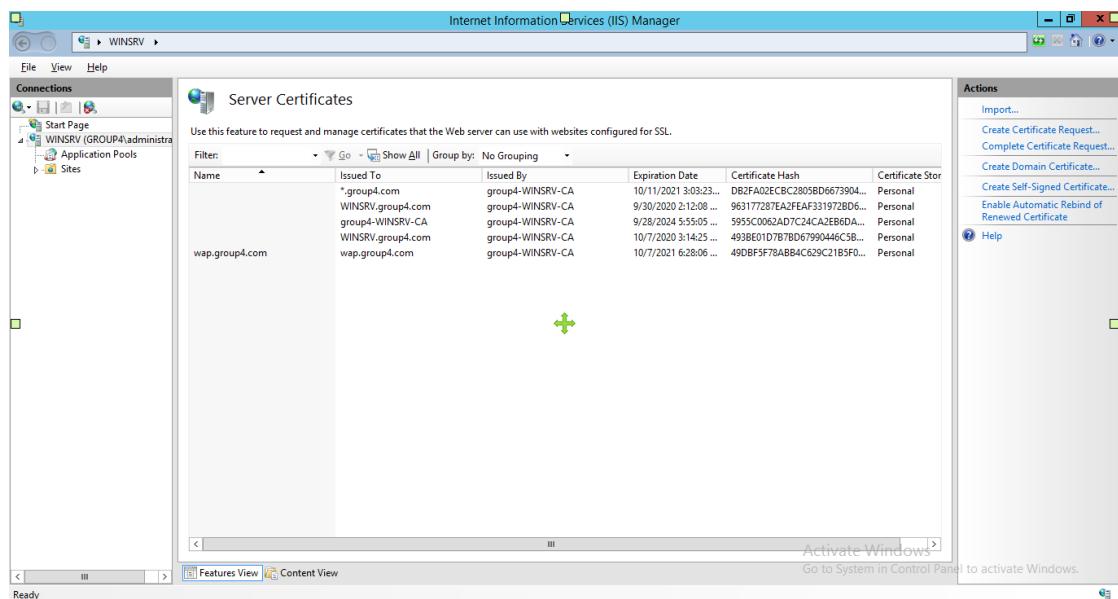


Figure 5..3.11.2: Show the server certificate.

Step 3: Then, create the domain certificate by click on the right panel ‘Create Domain Certificate...’. Enter the same at common name, organization, organizational unit, city/locality, state/province as ‘group4’ and select ‘MY’ for the country/region to synchronize with our time.

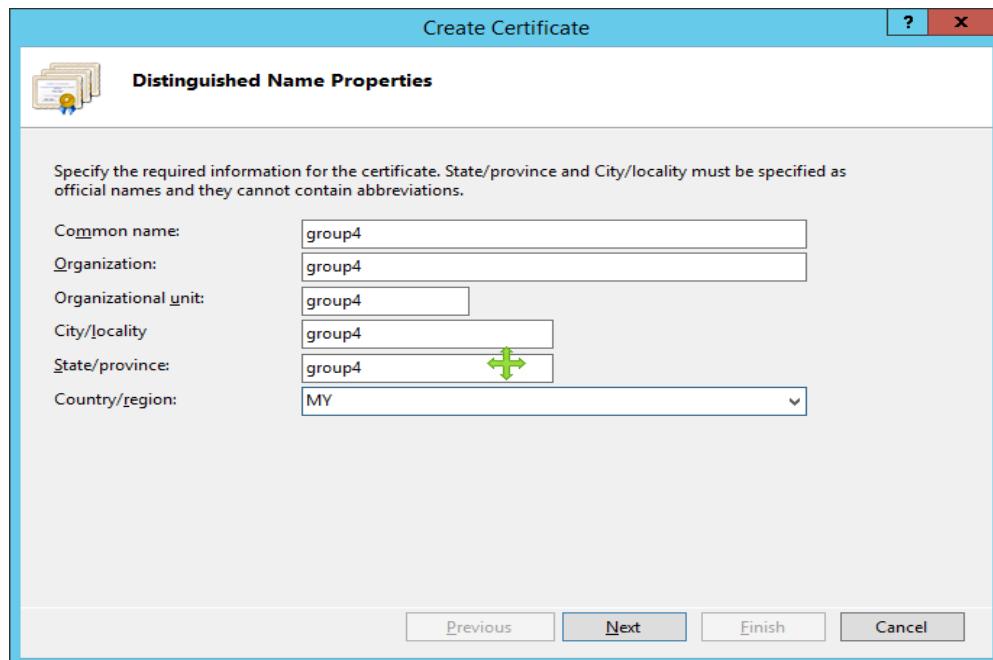


Figure 5.3.11.3: Show the create certificate.

Step 4: At the next page, in the specify online certification authority, select the certificate.

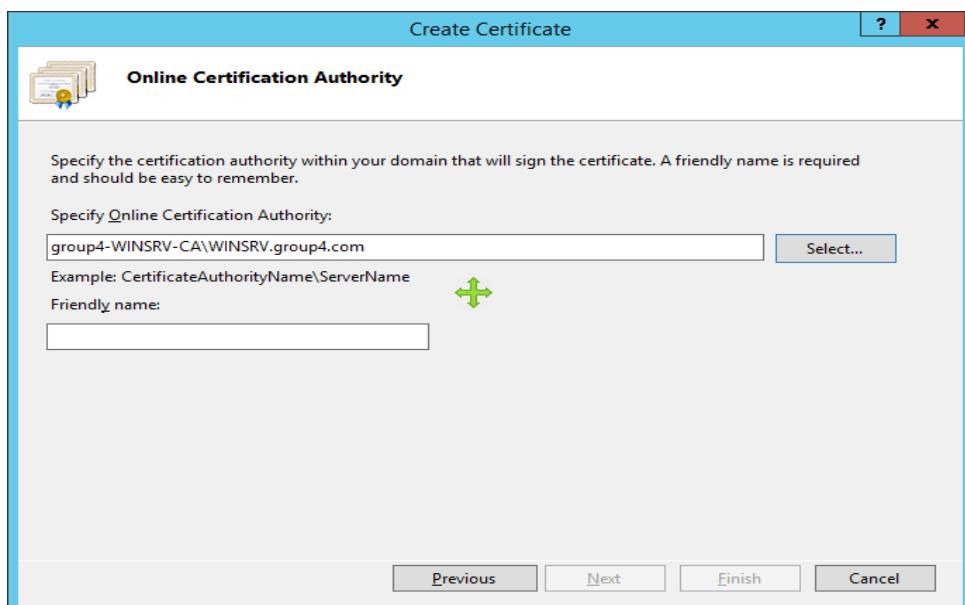


Figure 5.3.11.4: Show the select of certificate.

Step 5: The SSL certificate, it will be use in Linux, Debian. Open the Debian server and integrated the certificate from Windows server. Convert the pfx format and get private key from pfx.

```
#openssl pkcs12 -in www.pfx -out www.pem -nodes -nokeys
#openssl pkcs12 -in www.pfx -out www.key -nodes -nocerts
```

Figure 5.3.11.5: Show the integrated SSL on Debian.

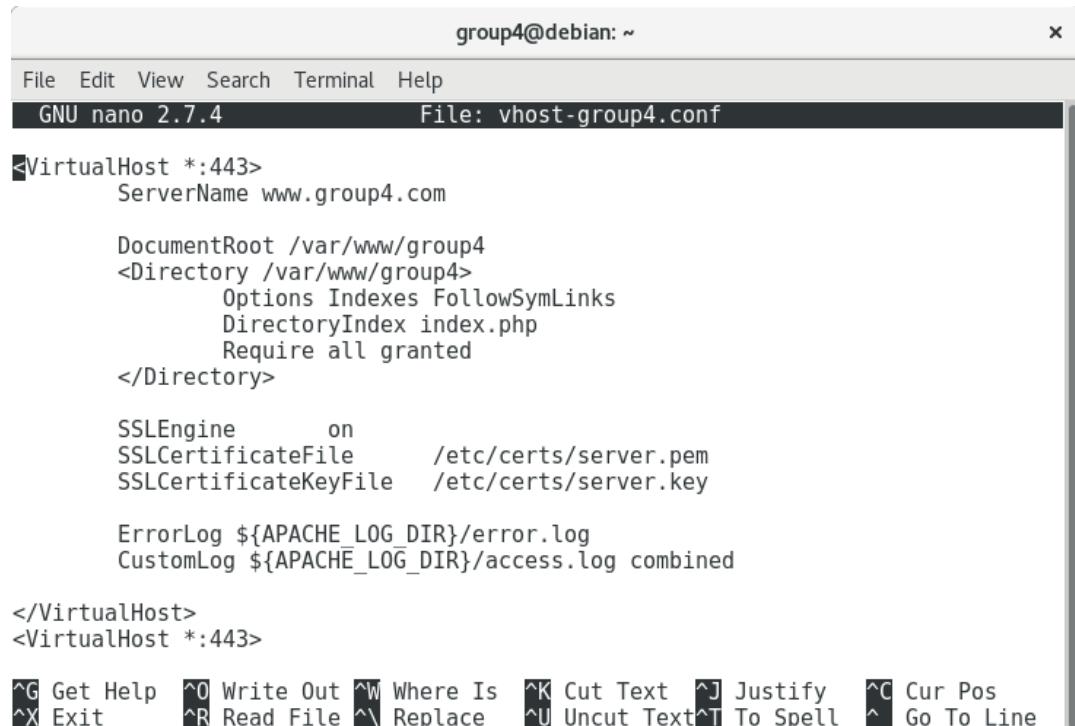
Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server (or pool of servers).

Step 6: Firstly, create the virtual host. Enter to the directory of /etc/apache2/sites-available/ and copy the 000-default.conf as vhost-group4.conf.

```
root@debian:/home/group4# cd /etc/apache2/sites-available/
root@debian:/etc/apache2/sites-available# nano vhost-group4.conf
```

Figure 5.3.11.6: Show the directory and copy the file.

Step 7: Then, open the file that just copy, ‘vhost-group.conf’. Enter the following code into that file.



```
<VirtualHost *:443>
    ServerName www.group4.com

    DocumentRoot /var/www/group4
    <Directory /var/www/group4>
        Options Indexes FollowSymLinks
        DirectoryIndex index.php
        Require all granted
    </Directory>

    SSLEngine on
    SSLCertificateFile /etc/certs/server.pem
    SSLCertificateKeyFile /etc/certs/server.key

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

</VirtualHost>
<VirtualHost *:443>
```

The terminal window title is "group4@debian: ~". The menu bar includes File, Edit, View, Search, Terminal, Help. The nano status bar shows "GNU nano 2.7.4" and "File: vhost-group4.conf". The bottom status bar shows various keyboard shortcuts for nano.

Figure 5.3.11.7: Show the coding put into the vhost-group4.conf file.

Step 8: After that, deactivate and activate the virtual host.

```
a2dissite vhost-group4.conf
a2ensite vhost-group4.conf
```

Figure 5.3.11.8: Show the deactivate and activate the virtual host.

Step 9: After done with virtual host, then proceed to web server. The file for web server is already been made while setup the virtual hosting. Then, open the ‘index.php’ from the path /var/www/group4/ to setup the web server page.

```
root@debian:/home/group4# nano /var/www/group4/index.php
root@debian:/home/group4# █
```

Figure 5.3.11.9: Show the open for index.php

Step 10: Then, setup the web server as we wish. Enter the html or php command to view the output on the page.



The screenshot shows a terminal window titled "group4@debian: ~". The menu bar includes File, Edit, View, Search, Terminal, and Help. The title bar shows "GNU nano 2.7.4" and "File: /var/www/group4/index.php". The main area contains the following PHP code:

```
<?php
    echo "Welcome To Group 4";
?>
```

At the bottom, there is a status bar with various keyboard shortcuts:

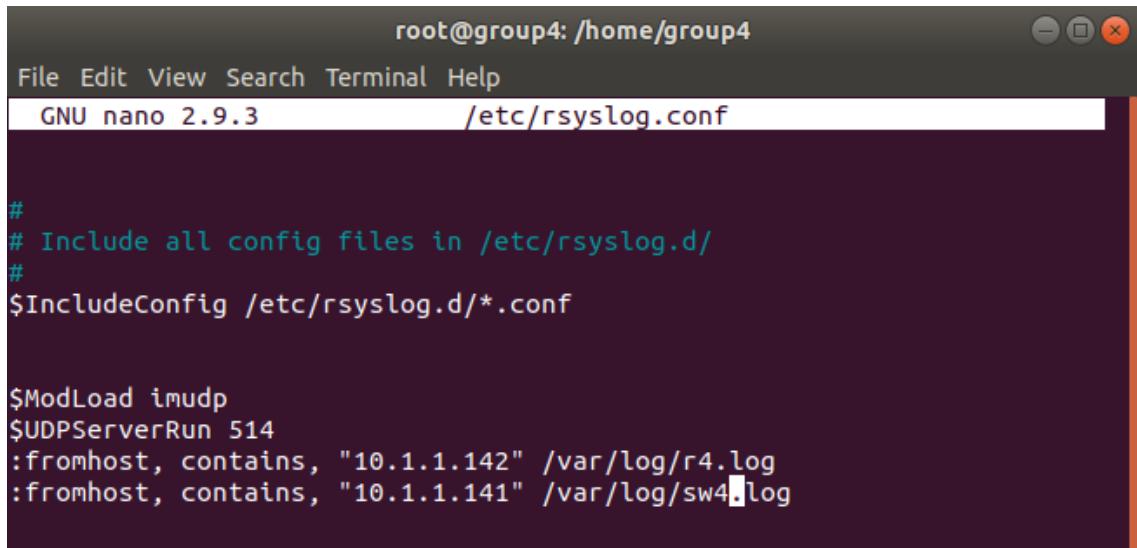
- [Read 3 lines]
- ^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
- ^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^ Go To Line

Figure 5.3.11.10: Show the setup of index.php.

5.3.12 Syslog

Syslog stands for System Logging Protocol and is a standard protocol used to send system log or event messages to a specific server, called a syslog server. It is primarily used to collect various device logs from several different machines in a central location for monitoring and review.

Step 1: Firstly, open the “rsyslog.conf” file to configure. The path is /etc/rsyslog.conf. Open it and put the following command. Create the log for switch and router to keep their log. For switch, name it as ‘sw4.log’ and the router name it as, ‘r4.log’ and put at the path /var/log/.



```

root@group4: /home/group4
File Edit View Search Terminal Help
GNU nano 2.9.3          /etc/rsyslog.conf

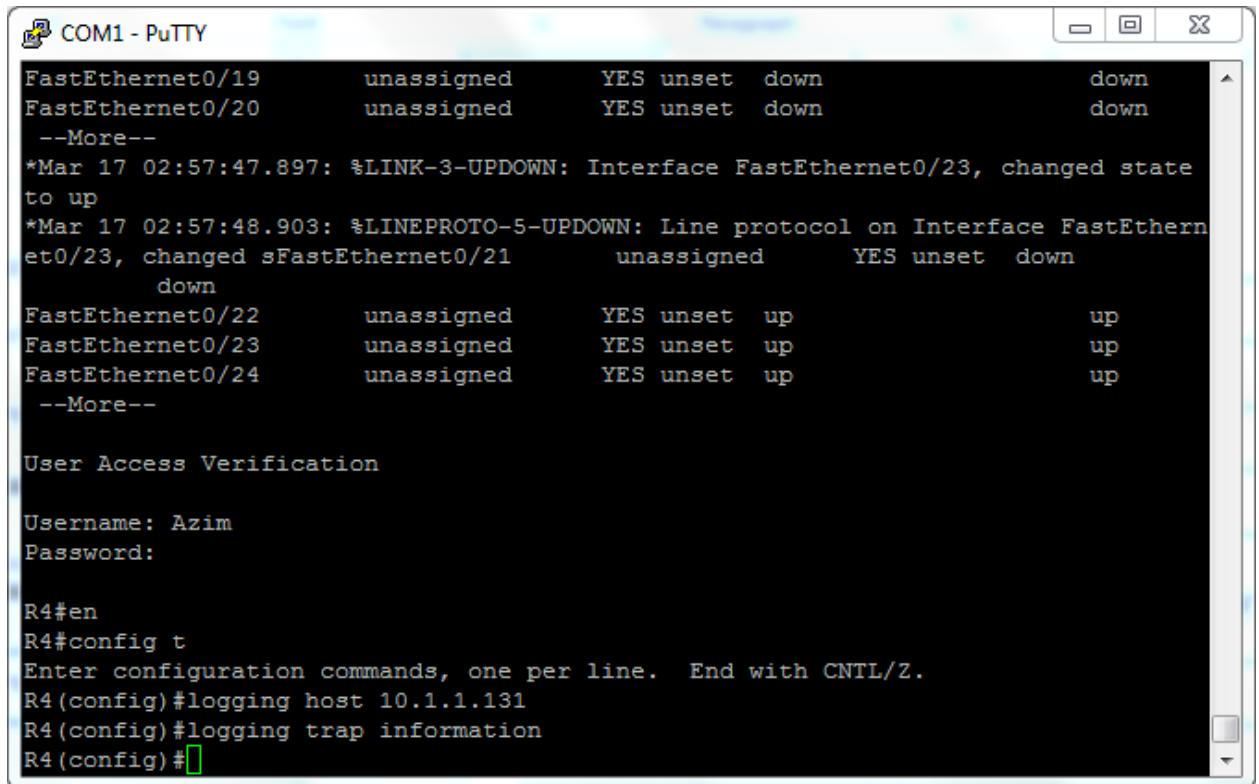
#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf

$ModLoad imudp
$UDPServerRun 514
:fromhost, contains, "10.1.1.142" /var/log/r4.log
:fromhost, contains, "10.1.1.141" /var/log/sw4.log

```

Figure 5.3.12.1: Show the configure rsyslog.conf.

Step 2: Connect putty to the router. Type enable. Then, config t. After that, enter logging host into Ubuntu server ip. Then, make the logging trap information for store the information happen.



The screenshot shows a PuTTY terminal window titled "COM1 - PuTTY". The session displays the following output:

```
FastEthernet0/19      unassigned      YES unset  down          down
FastEthernet0/20      unassigned      YES unset  down          down
--More--
*Mar 17 02:57:47.897: %LINK-3-UPDOWN: Interface FastEthernet0/23, changed state
to up
*Mar 17 02:57:48.903: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/23, changed state
FastEthernet0/21      unassigned      YES unset  down          down
FastEthernet0/22      unassigned      YES unset  up           up
FastEthernet0/23      unassigned      YES unset  up           up
FastEthernet0/24      unassigned      YES unset  up           up
--More--

User Access Verification

Username: Azim
Password:

R4#en
R4#config t
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#logging host 10.1.1.131
R4(config)#logging trap information
R4(config)#[
```

Figure 5.3.12.2: Show the trap information for router.

5.3.13 Dynamic Routing and Network Address Translation

Step 1: Create OSPF process “4” in the router and advertised the interface using “network” command under the router configuration mode for IPv4 network.

```
router ospf 4
  router-id 4.4.4.4
  log adjacency-changes
  network 10.1.1.0 0.0.0.127 area 0
  network 10.1.1.128 0.0.0.15 area 0
  network 113.114.115.0 0.0.0.7 area 0
```

Figure 5.3.13.1: OSPFv2 running configuration with created process and advertised network.

Step 2: Create OSPF process 4 and add the router ID under the router configuration mode for IPv6 network.

```
ipv6 router ospf 4
  router-id 4.4.4.4
  log adjacency-changes
!
```

Figure 5.3.13.2: OSPFv3 running configuration with created process and router-id.

Step 3: Advertise IPv6 interfaces into OSPF process on each interface.

```

interface FastEthernet0/1.10
encapsulation dot1Q 10
ip address 10.1.1.126 255.255.255.128
ip access-group 101 in
ip helper-address 10.1.1.129
ipv6 address 1230:1111:AAAA:1::FFFE/64
ipv6 dhcp relay destination 1230:1111:AAAA:2::1
ipv6 ospf 4 area 0
!
interface FastEthernet0/1.20
encapsulation dot1Q 20
ip address 10.1.1.142 255.255.255.240
ip nat inside
ip virtual-reassembly
ipv6 address 1230:1111:AAAA:2::FFFE/64
ipv6 ospf 4 area 0
!
interface Loopback1
ip address 1.1.1.1 255.255.255.255
ip ospf 4 area 0
!
interface Tunnel0
ip address 2.2.2.1 255.255.255.252
ip ospf 4 area 0
ipv6 address 1230:1111:AAAA:3::1/64
ipv6 ospf 4 area 0
tunnel source Serial0/2/1
tunnel destination 113.114.115.2
!
```

Figure 5.3.13.3: Advertised interfaces.

Step 4: Create an access list to match our internal network.

```

ip access-list extended NAT
permit ip 10.1.1.128 0.0.0.15 any
permit ip 10.1.1.0 0.0.0.127 any
!
```

Figure 5.3.13.4: The highlighted statement matched internal network.

Step 5: Configure PAT to translate the internal network to outside IP address of interface s0/2/0

```

ip nat inside source list NAT interface Serial0/2/1 overload
ip nat inside source static 10.1.1.131 113.114.115.3
```

Figure 5.3.13.5: Translate all the internal network to public IP address on interface serial0/2/0.

Step 6: Configure static NAT for proxy server to access from outside network.

```
| ip nat inside source list NAT interface Serial0/2/1 overload  
| ip nat inside source static 10.1.1.131 113.114.115.3
```

Figure 5.3.13.6: MAP the proxy server to a single public IP address.

Step 7: Specify the correct interface for public and internal network.

```
| interface FastEthernet0/1.20  
|   encapsulation dot1Q 20  
|   ip address 10.1.1.142 255.255.255.240  
|   ip nat inside  
|   ip virtual-reassembly  
|   ipv6 address 1230:1111:AAAA:2::FFFE/64  
|   ipv6 ospf 4 area 0  
!
```

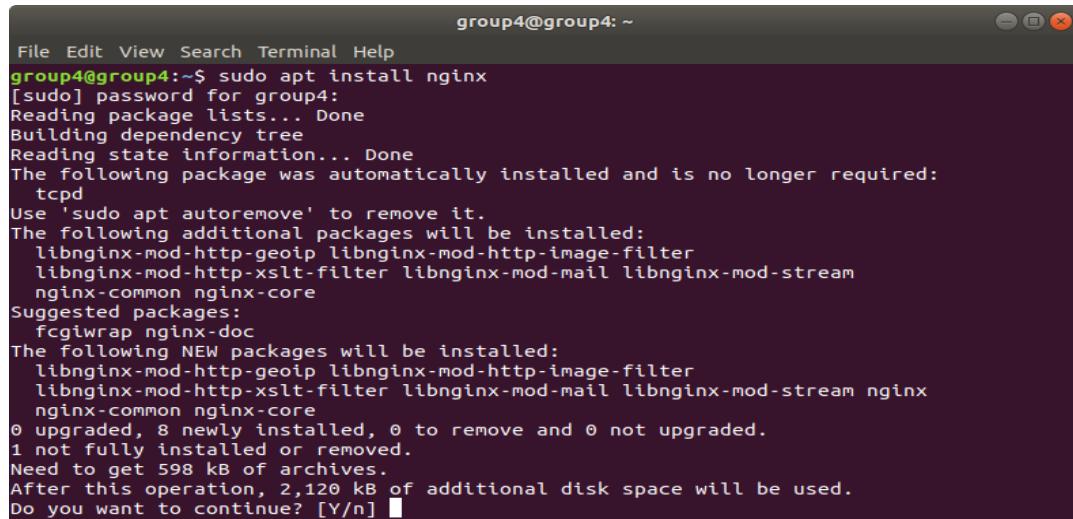
Figure 5.3.13.7: Set interface serial0/2/0 as an outside interface.

5.3.14 Proxy Server

Installing nginx server

Step 1: Open terminal in Ubuntu.

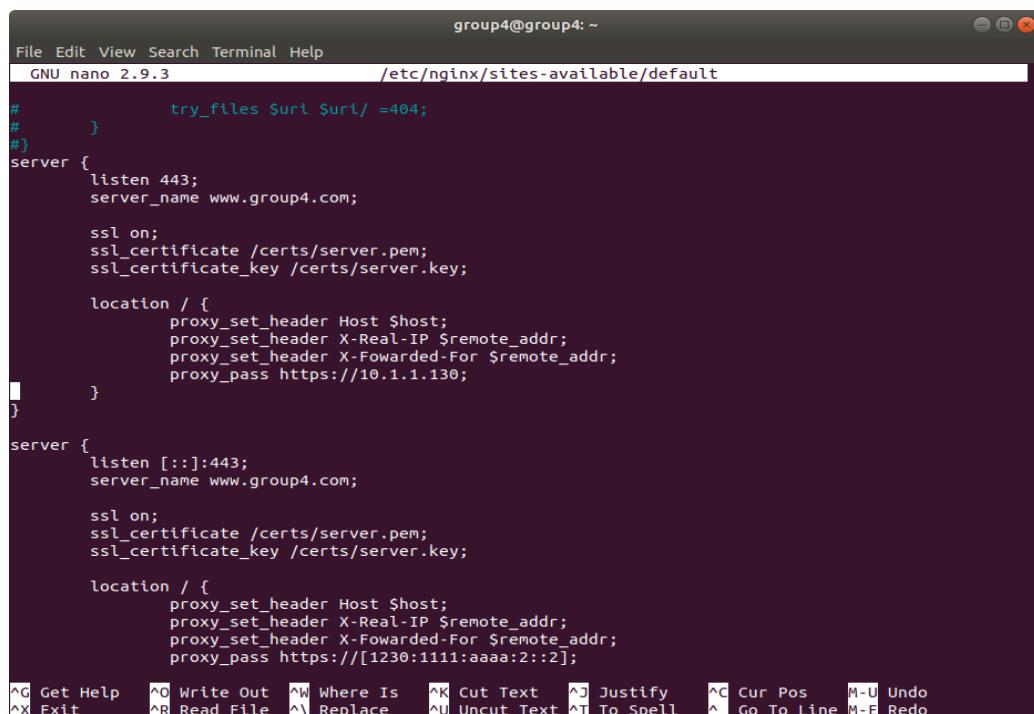
Step 2: Enter command `sudo apt install nginx` to install nginx server into Ubuntu.



```
group4@group4: ~
File Edit View Search Terminal Help
group4@group4:~$ sudo apt install nginx
[sudo] password for group4:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  tcpd
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  libnginx-mod-http-geoip libnginx-mod-http-image-filter
  libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream
  nginx-common nginx-core
Suggested packages:
  fcgiwrap nginx-doc
The following NEW packages will be installed:
  libnginx-mod-http-geoip libnginx-mod-http-image-filter
  libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream nginx
  nginx-common nginx-core
0 upgraded, 8 newly installed, 0 to remove and 0 not upgraded.
1 not fully installed or removed.
Need to get 598 kB of archives.
After this operation, 2,120 kB of additional disk space will be used.
Do you want to continue? [Y/n] ■
```

Figure 5.4.14.1: shows installation of nginx.

Step 3: Enter command `nano /etc/nginx/sites-available/default` to add and write the configuration.



```
group4@group4: ~
File Edit View Search Terminal Help
GNU nano 2.9.3          /etc/nginx/sites-available/default
#
#           try_files $uri $uri/ =404;
#}
server {
  listen 443;
  server_name www.group4.com;

  ssl on;
  ssl_certificate /certs/server.pem;
  ssl_certificate_key /certs/server.key;

  location / {
    proxy_set_header Host $host;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Fowarded-For $remote_addr;
    proxy_pass https://10.1.1.130;
  }
}

server {
  listen [::]:443;
  server_name www.group4.com;

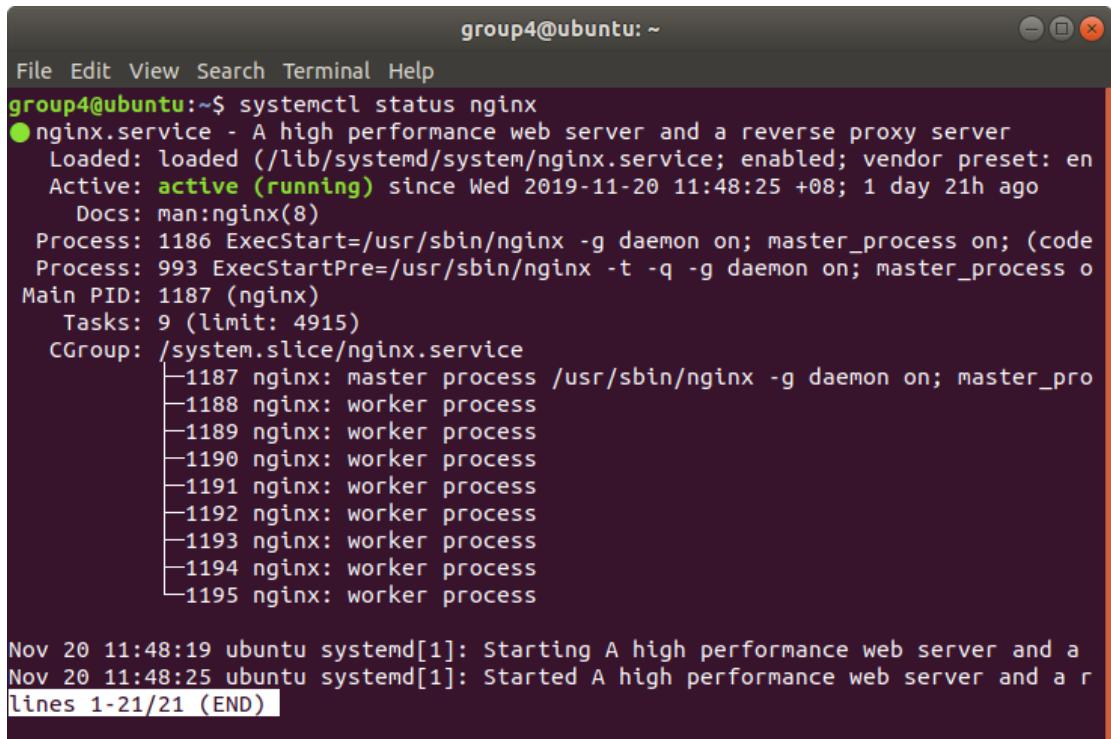
  ssl on;
  ssl_certificate /certs/server.pem;
  ssl_certificate_key /certs/server.key;

  location / {
    proxy_set_header Host $host;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Fowarded-For $remote_addr;
    proxy_pass https://[1230:1111:aaaa:2::2];
  }
}
```

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

Figure 5.3.14.2: shows the configuration of the nginx.

Step 4: Enter command `systemctl nginx` status to check the active(running) status of nginx.



The screenshot shows a terminal window titled "group4@ubuntu: ~". The window contains the following text output from the `systemctl status nginx` command:

```
File Edit View Search Terminal Help
group4@ubuntu:~$ systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
  Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: en
  Active: active (running) since Wed 2019-11-20 11:48:25 +08; 1 day 21h ago
    Docs: man:nginx(8)
 Process: 1186 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code
 Process: 993 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process o
 Main PID: 1187 (nginx)
   Tasks: 9 (limit: 4915)
  CGroup: /system.slice/nginx.service
          ├─1187 nginx: master process /usr/sbin/nginx -g daemon on; master_pro
          ├─1188 nginx: worker process
          ├─1189 nginx: worker process
          ├─1190 nginx: worker process
          ├─1191 nginx: worker process
          ├─1192 nginx: worker process
          ├─1193 nginx: worker process
          ├─1194 nginx: worker process
          └─1195 nginx: worker process

Nov 20 11:48:19 ubuntu systemd[1]: Starting A high performance web server and a
Nov 20 11:48:25 ubuntu systemd[1]: Started A high performance web server and a
lines 1-21/21 (END)
```

Figure 5.3.14.3: shows the active (running) of the nginx.

5.3.15 Access Control List

Step 1: Show ip interface brief on neighbor router to check their VLAN for client network address. ACL do at neighbor VLAN to avoid them to remote our server

Interface	IP-Address	OK?	Method	Status	Prot
FastEthernet0/0	unassigned	YES	NVRAM	administratively down	down
FastEthernet0/1	192.168.3.217	YES	NVRAM	up	up
FastEthernet0/1.10	192.168.3.209	YES	NVRAM	up	up
FastEthernet0/1.20	192.168.3.193	YES	NVRAM	up	up
FastEthernet0/1.30	192.168.3.201	YES	NVRAM	up	up
FastEthernet0/1.40	192.168.3.1	YES	NVRAM	up	up
FastEthernet0/1.50	192.168.3.129	YES	NVRAM	up	up
Serial0/2/0	unassigned	YES	NVRAM	down	down
Serial0/2/1	113.114.115.2	YES	NVRAM	up	up
NVIO	3.3.3.3	YES	unset	up	up
Loopback1	3.3.3.3	YES	NVRAM	up	up

Figure 5.3.15.1: list of VLAN on neighbor router

Step 2: Do ip access-group ACL-GROUP6 in to apply the access list to an interface

```
RtGroup3(config-ext-nacl)#int fa0/1.40
RtGroup3(config-subif)#ip access-gr
RtGroup3(config-subif)#ip access-group
RtGroup3(config-subif)#ip access-group
RtGroup3(config-subif)#ip access-group ?
  <1-199>      IP access list (standard or extended)
  <1300-2699>  IP expanded access list (standard or extended)
  WORD          Access-list name

RtGroup3(config-subif)#ip access-group ACL-GROUP4 in
```

Figure 5.3.15.2: ip access-group

Step 3: Apply command for deny the our server

```
RtGroup3(config)# IP access-list ext ACL-GROUP4
RtGroup3(config-ext-nacl)#$cp 192.168.3.0 0.0.0.127 10.1.1.128 0.0.0.15 eq 22
RtGroup3(config-ext-nacl)#$192.168.3.0 0.0.0.127 host 10.1.1.130 echo
RtGroup3(config-ext-nacl)#$cp 192.168.3.0 0.0.0.127 host 10.1.1.129 eq telnet
RtGroup3(config-ext-nacl)#$cp 192.168.3.0 0.0.0.127 host 10.1.1.131 eq ftp
RtGroup3(config-ext-nacl)#
RtGroup3(config-ext-nacl)#          permit ip any any
```

Figure 5.3.15.3: ACL command

Step 4: Show this command to see the ACL configuration

```
RtGroup3(config-ext-nacl)#do sh access-list
Standard IP access list NAT
 10 permit 192.168.3.192, wildcard bits 0.0.0.7 (14 matches)
 20 permit 192.168.3.200, wildcard bits 0.0.0.7 (14 matches)
 30 permit 192.168.3.208, wildcard bits 0.0.0.7 (80 matches)
 40 permit 192.168.3.0, wildcard bits 0.0.0.127 (251 matches)
 50 permit 192.168.3.128, wildcard bits 0.0.0.63
Extended IP access list ACL-GROUP4
 10 deny tcp 192.168.3.0 0.0.0.127 10.1.1.128 0.0.0.15 eq 22 (15 matches)
 30 deny tcp 192.168.3.0 0.0.0.127 host 10.1.1.129 eq telnet (7 matches)
 40 deny tcp 192.168.3.0 0.0.0.127 host 10.1.1.131 eq ftp (77 matches)
 60 deny icmp 192.168.3.0 0.0.0.127 host 10.1.1.130 echo (4 matches)
 70 permit ip any any (44 matches)
Extended IP access list IPSEC-ACL
 10 permit gre host 113.114.115.2 host 113.114.115.1 (559796 matches)
```

Figure 5.3.15.4: show access-list

5.3.16 Trivial File Transfer Protocol

Installing TFTP

Step 1: Open terminal in Debian 9 and enter as a root user.

Step 2: Enter command *apt install tftpd-hpa* to install the tftp.

```
File Edit View Search Terminal Help
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  pxelinux
The following NEW packages will be installed:
  tftpd-hpa
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 50.2 kB of archives.
After this operation, 121 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian buster/main amd64 tftpd-hpa amd64 5.2+20150808-8-1+b1 [50.2 kB]
Fetched 50.2 kB in 6s (8,739 B/s)
Preconfiguring packages ...
Selecting previously unselected package tftpd-hpa.
(Reading database ... 129190 files and directories currently installed.)
Preparing to unpack .../tftpd-hpa_5.2+20150808-1+b1_amd64.deb ...
Unpacking tftpd-hpa (5.2+20150808-1+b1) ...
Setting up tftpd-hpa (5.2+20150808-1+b1) ...
tftpd user (tftp) already exists, doing nothing.
Processing triggers for man-db (2.8.5-2) ...
Processing triggers for systemd (241-7~deb10u2) ...
```

Figure 5.3.16.1: installed tftpd-hpa

Step 3: Enter command *nano /etc/default/tftpd-hpa* to configure the tftp.

```
File Edit View Search Terminal Help
GNU nano 3.2          /etc/default/tftpd-hpa          Modified

# /etc/default/tftpd-hpa

TFTP_USERNAME="tftp"
TFTP_DIRECTORY="/srv/tftp"
TFTP_ADDRESS="0.0.0.0:69"
TFTP_OPTIONS="--secure -c"

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

Figure 5.3.16.2: show configuration of tftp

Step 4: check the status running of tftp using command *service tftpd-hpa status*.

```
root@debian:/home/group4# service tftpd-hpa status
● tftpd-hpa.service - LSB: HPA's tftp server
  Loaded: loaded (/etc/init.d/tftpd-hpa; generated; vendor preset: enabled)
  Active: active (running) since Sat 2019-11-16 18:28:38 +08; 3min 46s ago
    Docs: man:systemd-sysv-generator(8)
 Process: 9977 ExecStop=/etc/init.d/tftpd-hpa stop (code=exited, status=0/SUCCESS)
 Process: 10014 ExecStart=/etc/init.d/tftpd-hpa start (code=exited, status=0/SUCCESS)
   Tasks: 1 (limit: 4915)
  CGroup: /system.slice/tftpd-hpa.service
          └─10021 /usr/sbin/in.tftpd --listen --user tftp --address 0.0.0.0:69 --secure -c /srv/tftp

Nov 16 18:28:38 debian systemd[1]: Starting LSB: HPA's tftp server...
Nov 16 18:28:38 debian tftpd-hpa[10014]: Starting HPA's tftpd: in.tftpd.
Nov 16 18:28:38 debian svstemd[1]: Started LSB: HPA's tftpd server.
```

Figure 5.3.16.3: show active (running) tftp.

5.3.17 Quota Screening

Step 1: Add Roles and Features to install file server resource manager

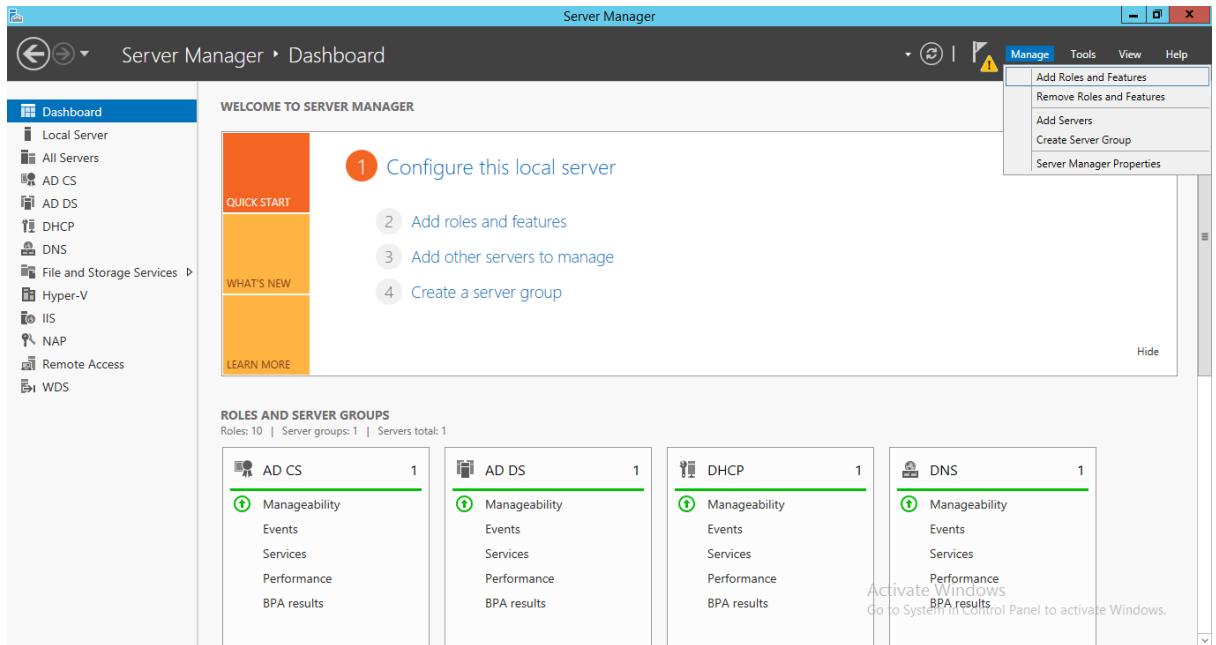


Figure 5.3.17.1: Add roles and features

Step 2: Click Role-based or featured-based installation

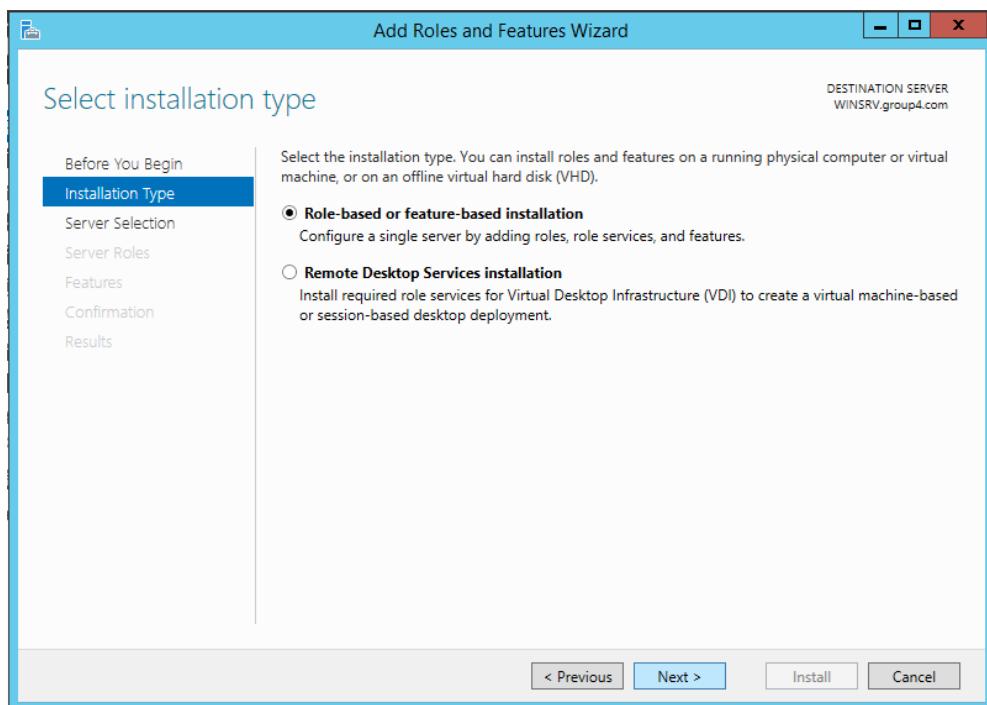


Figure 5.3.17.2: Installation type

Step 3: Select the server from the server pool and click Next

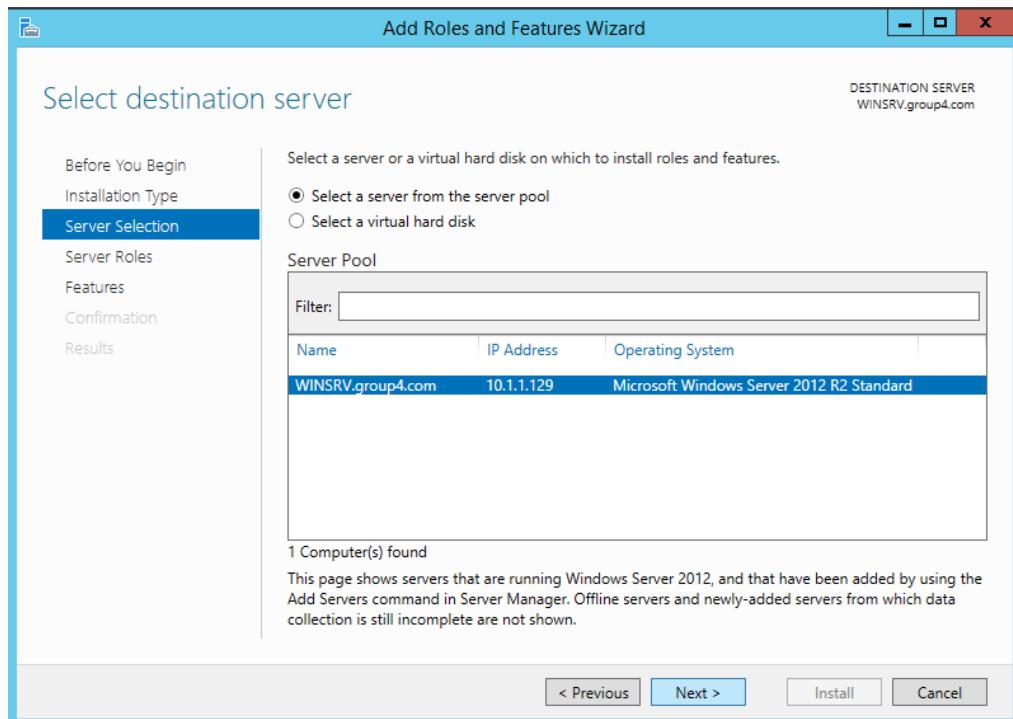


Figure 5.3.17.3: Select destination server

Step 4: Click Next after tick to the File and Storage Service

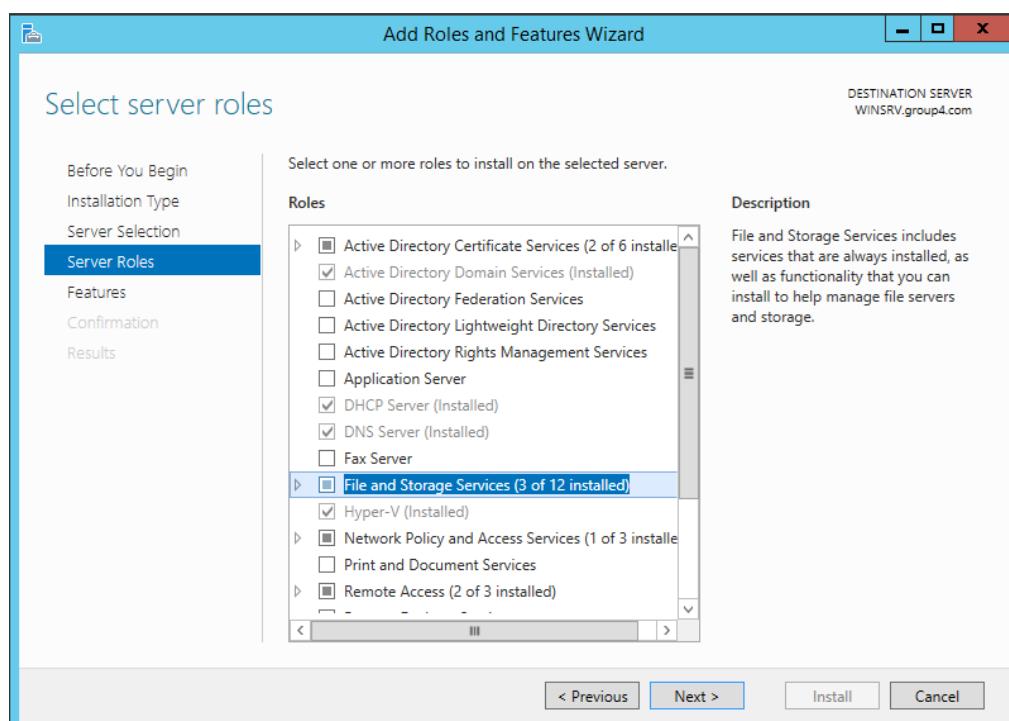


Figure 5.3.17.4: Server roles

Step 5: Click Next after tick for File Server and File Server Resource Manager

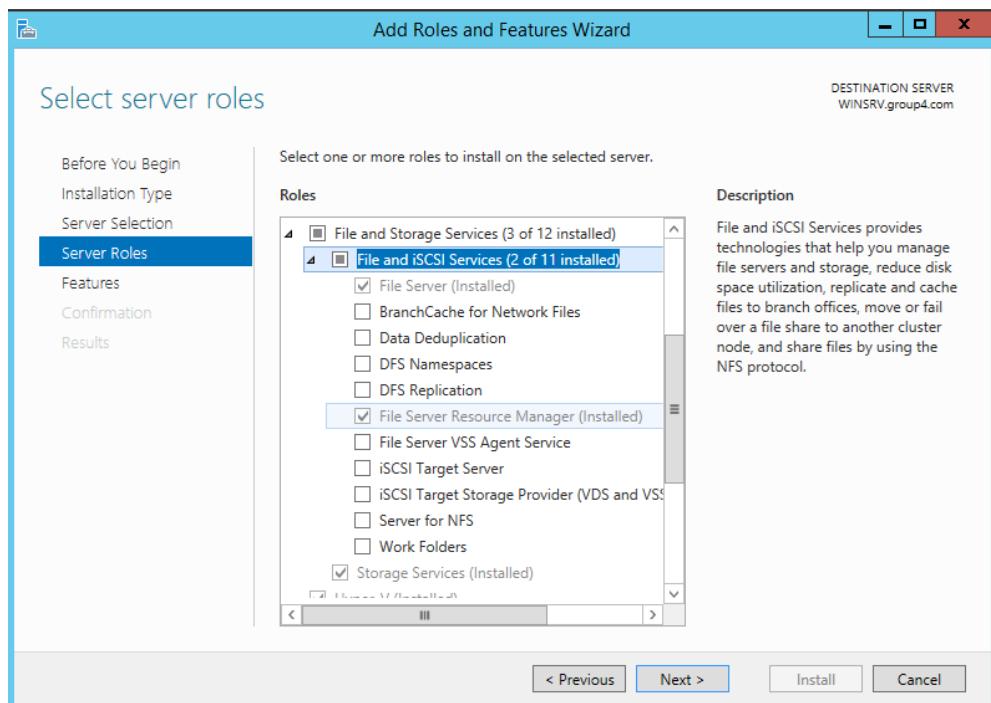


Figure 5.3.17.5: Select server roles

Step 6: Click Install after select the features

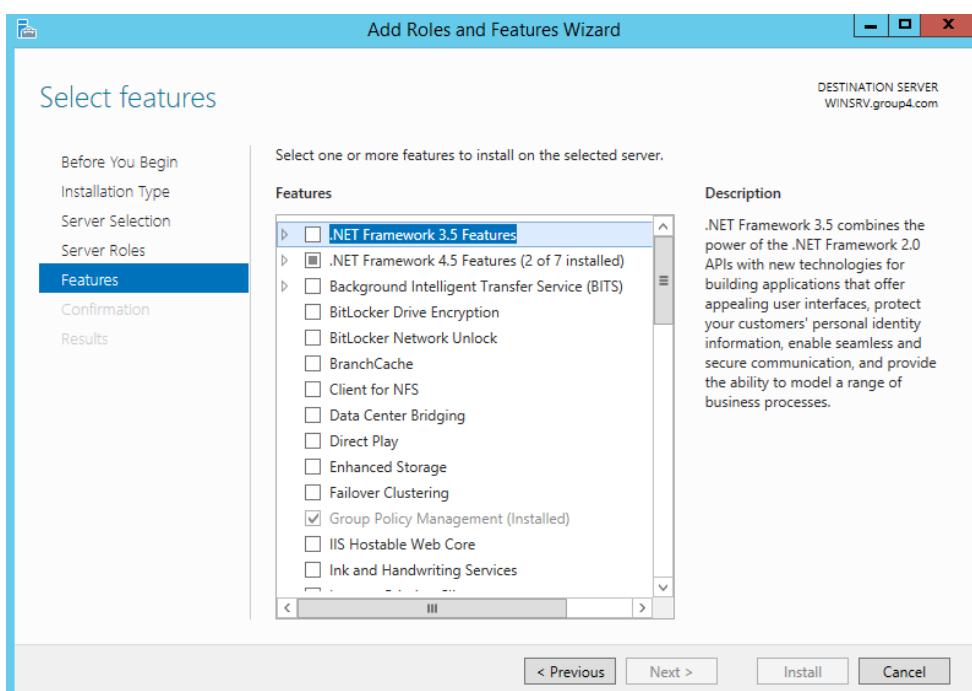


Figure 5.3.17.6: Features

Step 7: Click Install after confirm the installation selections

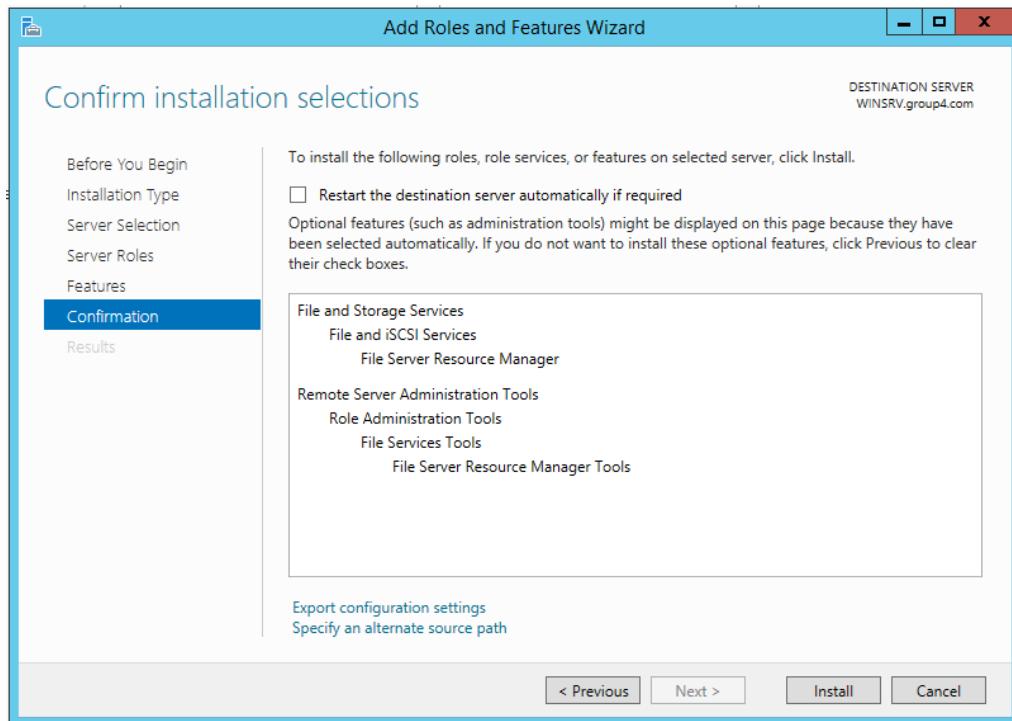


Figure 5.3.17.7: Confirmation of selections

Step 8: Close after Installation progress end

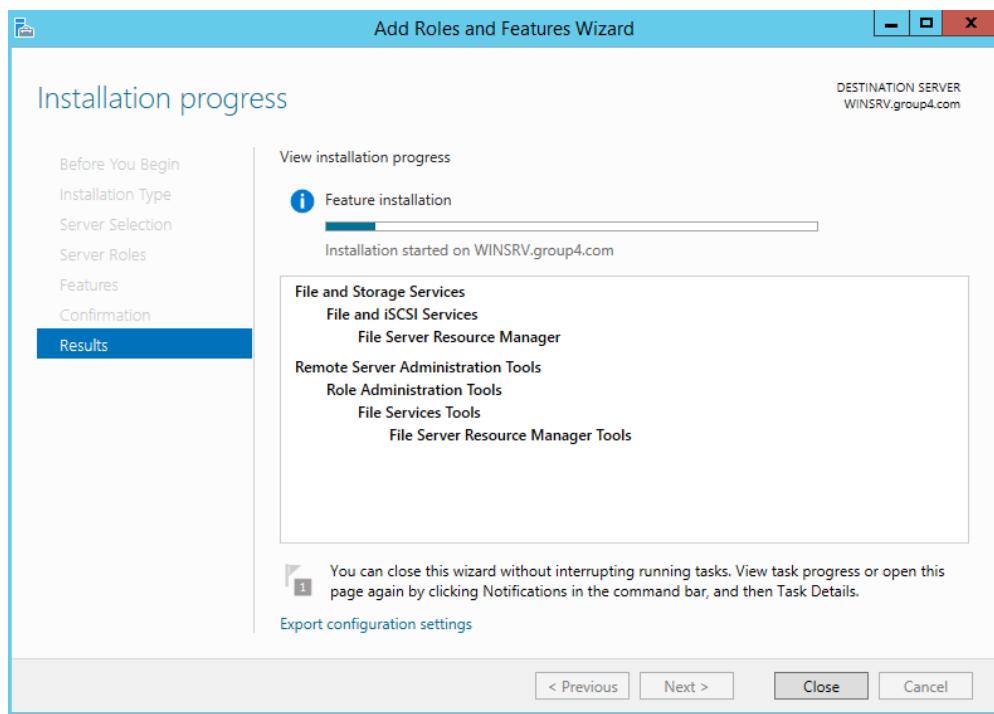


Figure 5.3.17.8: Installation progress

Step 9: On the File Server Resource Manager console, click Quota Management

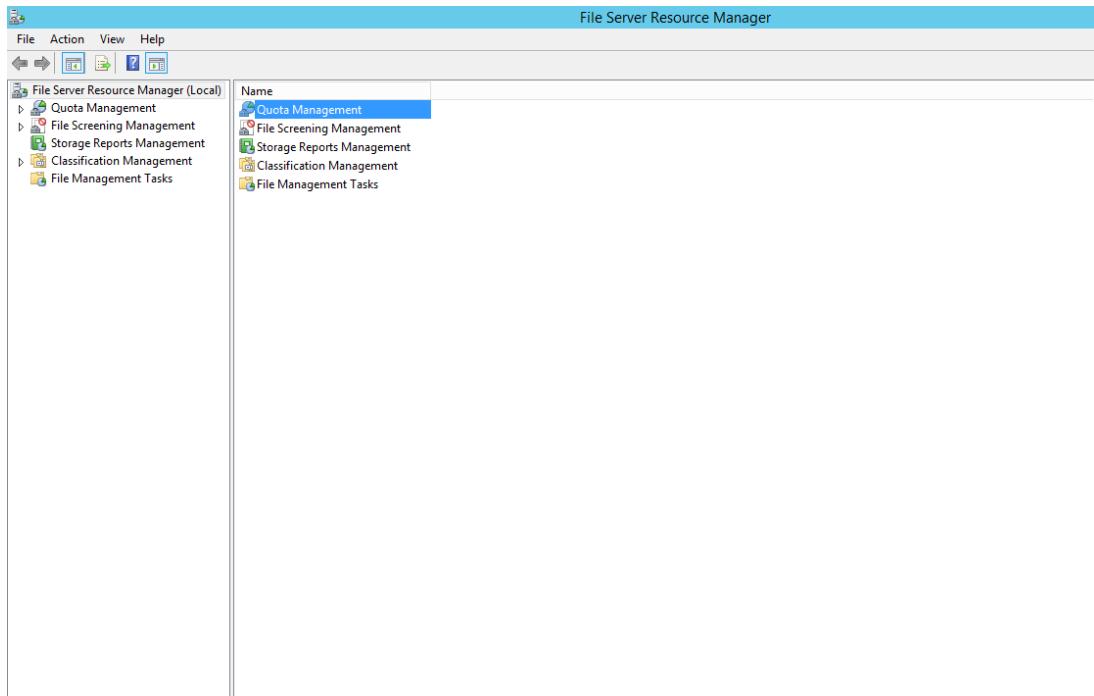


Figure 5.3.17.9: Quota Management

Step 10: Click the Quota Templates

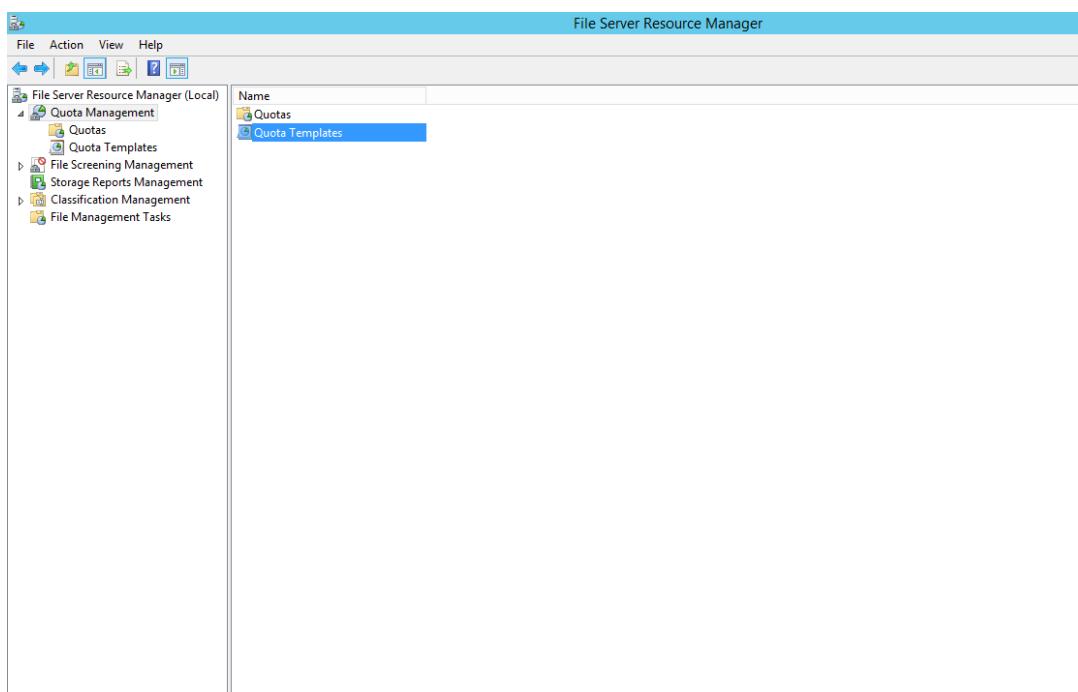


Figure 5.3.17.10: Quota Template

Step 11: Create new Quota Template. Name it ‘Home Quota’ with 5GB space limit

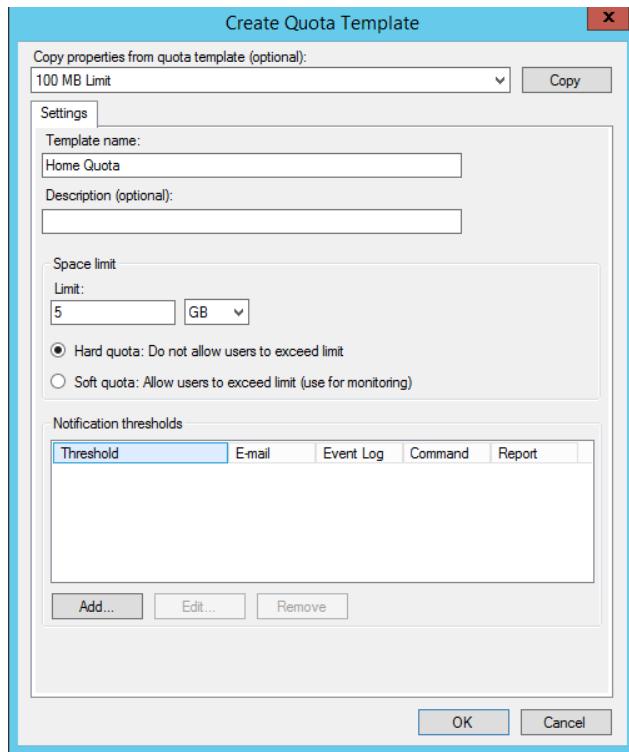


Figure 5.3.17.11: New Quota Template

Step 12: Browse for Quota Path and click Create

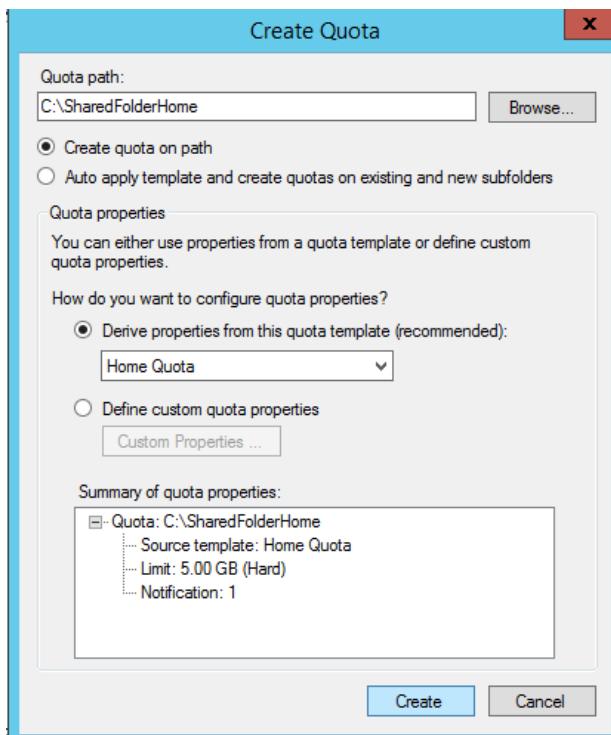
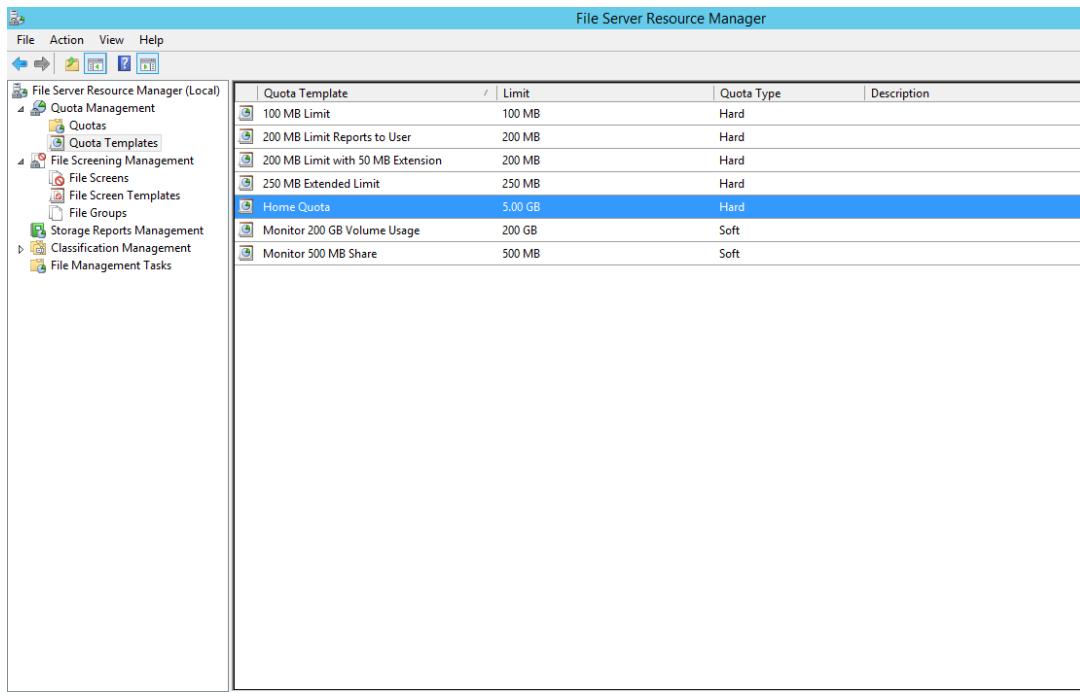


Figure 5.3.17.12: Quota Path

Step 13: New quota template now appears on the list

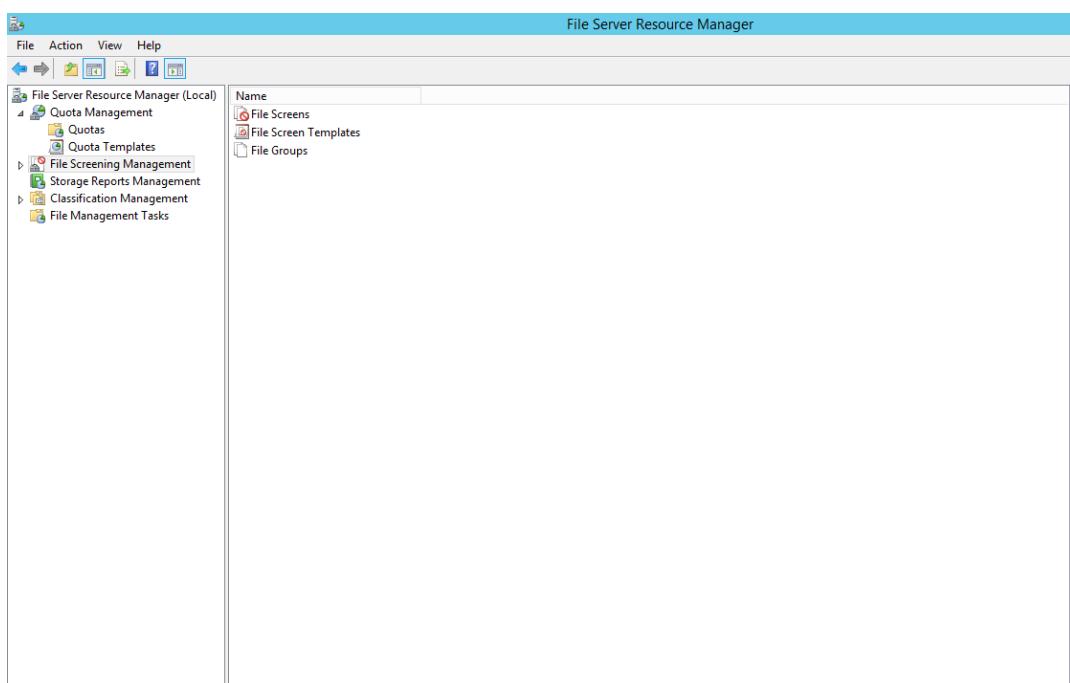


The screenshot shows the 'File Server Resource Manager' interface. The left pane displays a navigation tree with 'File Server Resource Manager (Local)' expanded, showing 'Quota Management', 'Quotas', 'Quota Templates', 'File Screening Management' (which is selected and expanded), 'File Screens', 'File Screen Templates', 'File Groups', 'Storage Reports Management', 'Classification Management', and 'File Management Tasks'. The right pane shows a table titled 'Quota Template' with the following data:

Quota Template	Limit	Quota Type	Description
100 MB Limit	100 MB	Hard	
200 MB Limit Reports to User	200 MB	Hard	
200 MB Limit with 50 MB Extension	200 MB	Hard	
250 MB Extended Limit	250 MB	Hard	
Home Quota	5.00 GB	Hard	
Monitor 200 GB Volume Usage	200 GB	Soft	
Monitor 500 MB Share	500 MB	Soft	

Figure 5.3.17.13: New Quota List

Step 14: On the File Server Resource Manager console, click File Screening Management



The screenshot shows the 'File Server Resource Manager' interface. The left pane displays a navigation tree with 'File Server Resource Manager (Local)' expanded, showing 'Quota Management', 'Quotas', 'Quota Templates', 'File Screening Management' (which is selected and expanded), 'File Screens' (selected), 'File Screen Templates', 'File Groups', 'Storage Reports Management', 'Classification Management', and 'File Management Tasks'. The right pane shows a table titled 'Name' with the following data:

Name
File Screens
File Screen Templates
File Groups

Figure 5.3.17.14: File Screening Management

Step 15: Create new File Screen Template

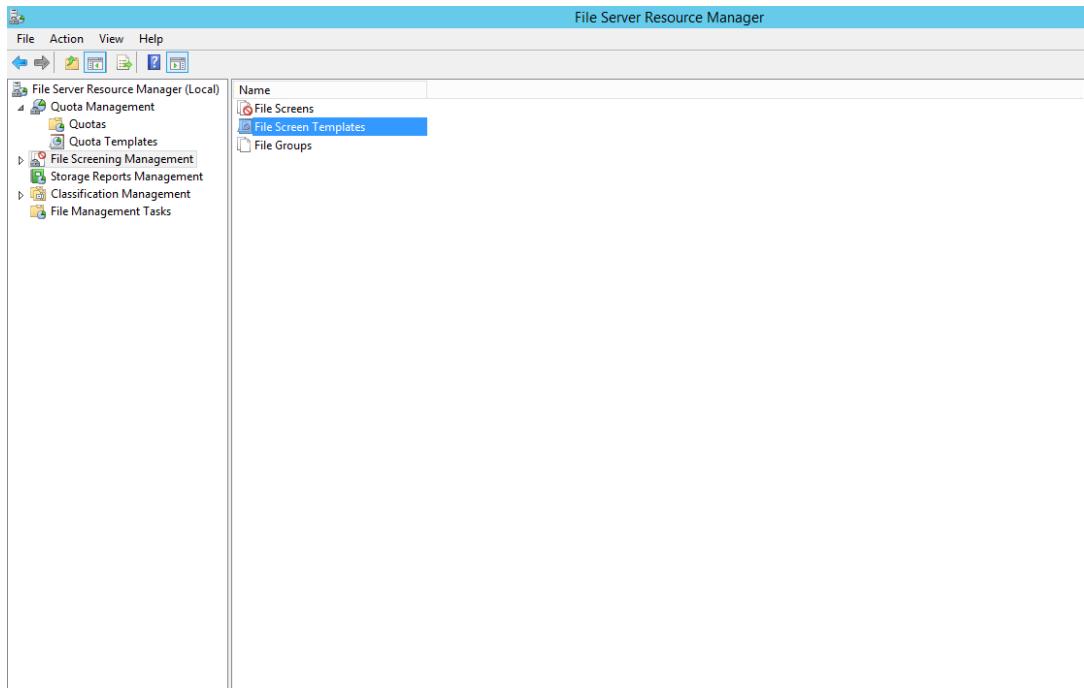


Figure 5.3.17.15: New File Screen Template

Step 16: Right-click and select Create File Screen Template

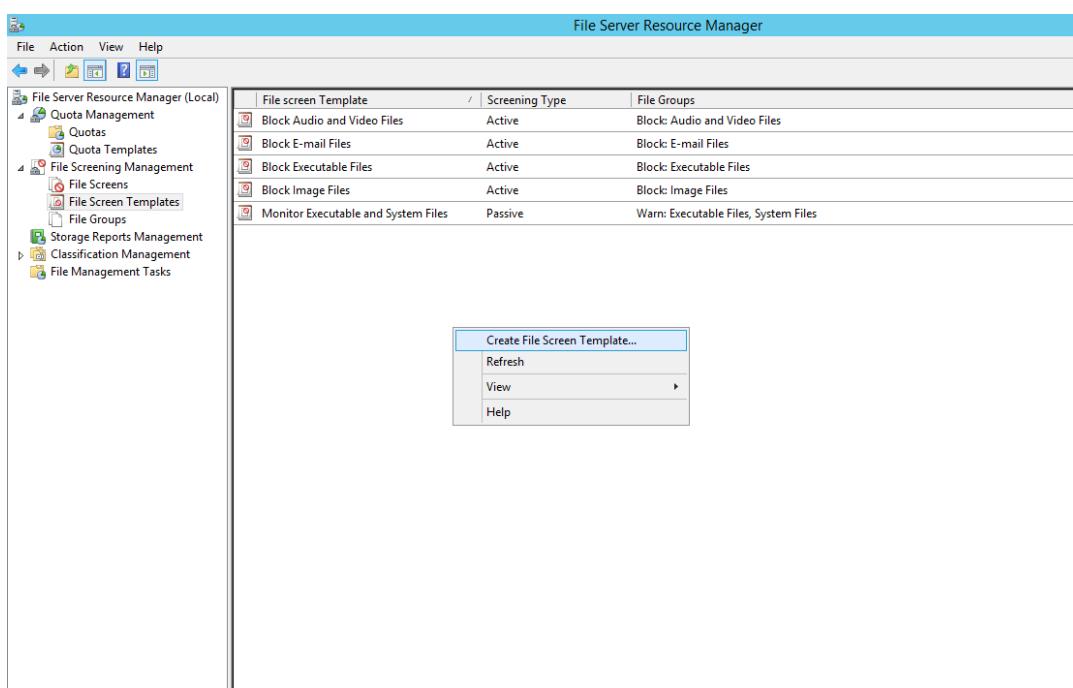


Figure 5.3.17.16: Create File Screen Template

Step 17: Create the File Group Properties

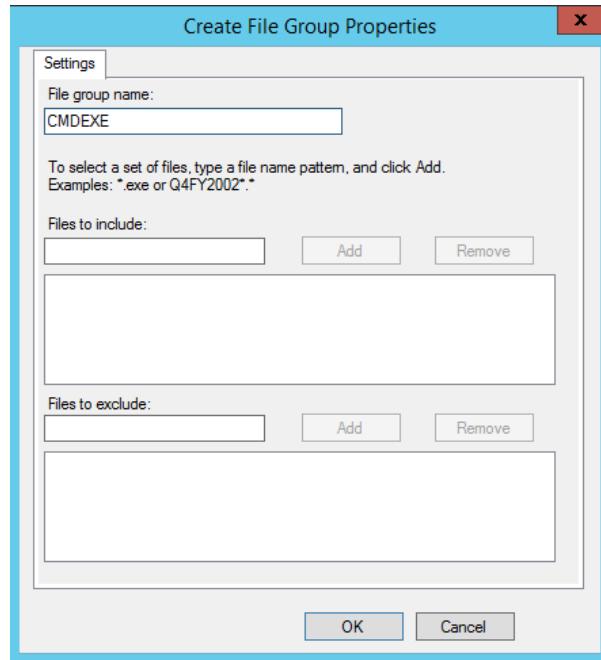


Figure 5.3.17.18: File Group Properties

Step 18: Select the CMDEXE that has been created at File Group Properties

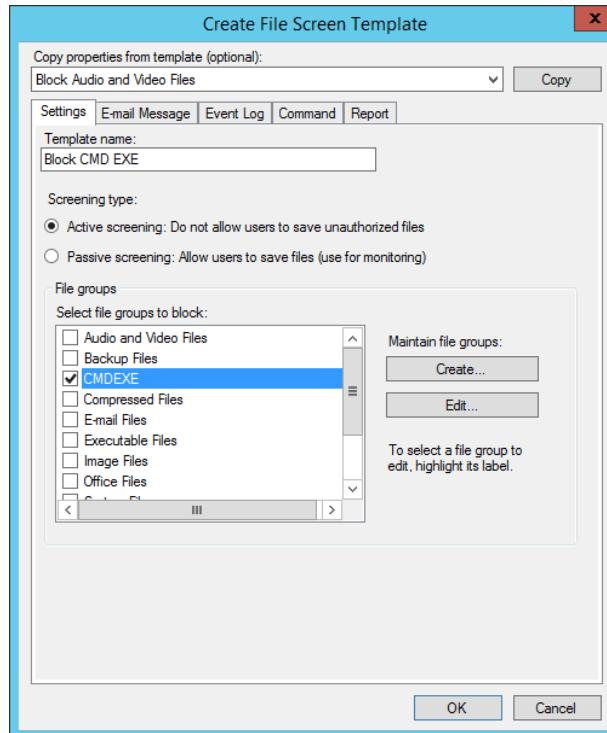


Figure 5.3.17.18: Named template

Step 19: Browse the File screen path and click Create

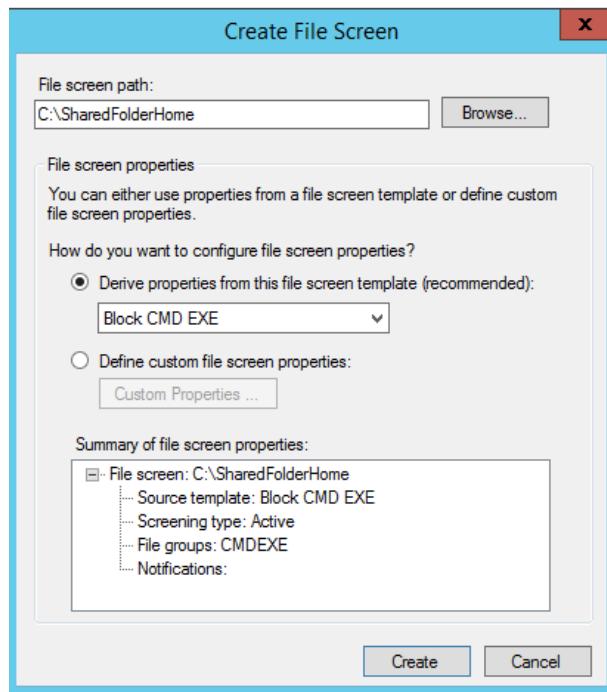


Figure 5.3.17.19: File Screen Path

Step 20: New File Screen Template now appears on the list

File Server Resource Manager

File Action View Help

File Server Resource Manager (Local)

- Quota Management
- Quotas
- Quota Templates

File Screening Management

- File Screens
- File Screen Templates
- File Groups

Storage Reports Management

Classification Management

File Management Tasks

File screen Template	Screening Type	File Groups
Block Audio and Video Files	Active	Block: Audio and Video Files
Block CMD EXE	Active	Block: CMDEXE
Block E-mail Files	Active	Block: E-mail Files
Block Executable Files	Active	Block: Executable Files
Block Image Files	Active	Block: Image Files
Monitor Executable and System Files	Passive	Warn: Executable Files, System Files

Figure 5.3.17.20: New File Screen Template List

5.3.18 IPv6 Web with IPv6 Tunneling

Step 1: Create tunnel 0 interface on router and neighbour router.

```
interface Tunnel0
 ip address 2.2.2.1 255.255.255.252
 ip ospf 4 area 0
 ipv6 address 1230:1111:AAAA:3::1/64
 ipv6 ospf 4 area 0
 tunnel source Serial0/2/1
 tunnel destination 113.114.115.2
,
```

Figure 5.3.18.1: Tunnel 0 configuration on router.

Step 2: Enable OSPFv3 for IPv6 routing.

```
ipv6 router ospf 4
 router-id 4.4.4.4
 log-adjacency-changes
!
```

Figure 5.3.18.2: OSPFv3 configuration.

Step 3: Advertise OSPFv3 to all subinterfaces that have IPv6 address

```
!
interface FastEthernet0/1.10
encapsulation dot1Q 10
ip address 10.1.1.126 255.255.255.128
ip access-group 101 in
ip helper-address 10.1.1.129
ip helper-address 10.1.1.132
ip nat inside
ip virtual-reassembly
ipv6 address 1230:1111:AAAA:1::FFFE/64
ipv6 ospf 4 area 0
!
interface FastEthernet0/1.20
encapsulation dot1Q 20
ip address 10.1.1.142 255.255.255.240
ip access-group 102 out
ip nat inside
ip virtual-reassembly
ipv6 address 1230:1111:AAAA:2::FFFE/64
ipv6 ospf 4 area 0
!
!
interface Tunnel0
ip address 2.2.2.1 255.255.255.252
ip ospf 4 area 0
ipv6 address 1230:1111:AAAA:3::1/64
ipv6 ospf 4 area 0
tunnel source Serial0/2/1
tunnel destination 113.114.115.2
!
interface FastEthernet0/0
ip address 200.200.200.1 255.255.255.240
ip nat outside
ip virtual-reassembly
duplex auto
speed auto
!
interface FastEthernet0/0.10
```

Figure 5.3.18.3: Advertise OSPFv3

5.3.19 IPSec Site-to-Site Tunelling

IPSec site-to-site is used to create tunelling between two different networks.

Step1: Configure ISAKMP and set pre shared key “WORKSHOP2”.

```
R4(config)#crypto isakmp policy 1
R4(config-isakmp)#authentication pre-share
R4(config-isakmp)#crypto isakmp key WORKSHOP2 address 113.114.115.2
```

```
R4(config)#crypto ipsec transform-set IPSEC-TS esp-aes esp-sha-hmac
R4(cfg-crypto-trans)#crypto map CMAP 1 ipsec-isakmp
R4(config-crypto-map)#set peer 113.114.115.2
R4(config-crypto-map)#set transform-set IPSEC-TS
R4(config-crypto-map)#match address IPSEC-ACL
```

Figure 5.3.19.1: Configure ISAKMP.

Step 2: Set the acl to allow specific network.

```
R4(config-if)#ip access-list extended IPSEC-ACL
R4(config-ext-nacl)#permit gre host 113.114.115.1 host 113.114.115.2
```

Figure 5.3.19.2: set the acl to allow the specific network.

Step 3: Apply the ipsec to the interface.

```
R4(config)#interface Serial0/2/1
R4(config-if)#ip address 113.114.115.1 255.255.255.248
R4(config-if)#crypto map CMAP
```

Figure 5.3.19.3: apply the ipsec.

5.3.20 Cloud Server

NextCloud on Ubuntu Server

Step 1: Login root: group@group4: \$ sudo su

```
Password group@group4: ~$ *****
```

Step 2: Update the system group@group4:~\$ apt-get update

Step 3: Install LAMP Server + PHP Extension + MariaDB + Apache

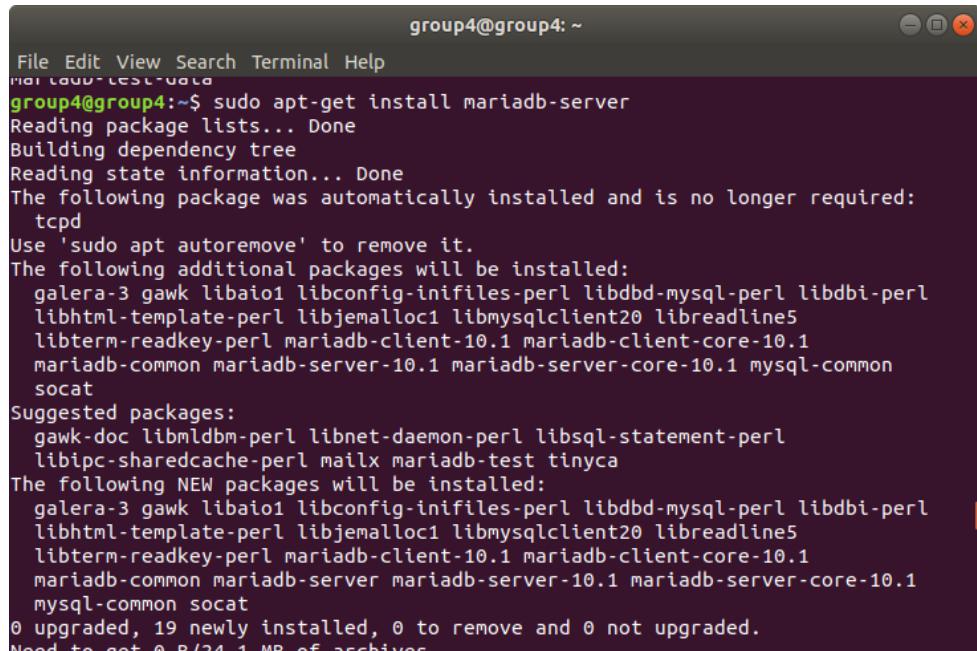
```
group4@group4: ~
File Edit View Search Terminal Help
group4@group4:~$ sudo apt-get install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  tcpd
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap libblua5.2-0
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 libblua5.2-0
0 upgraded, 9 newly installed, 0 to remove and 0 not upgraded.
1 not fully installed or removed.
Need to get 195 kB/1,713 kB of archives.
After this operation, 6,917 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://my.archive.ubuntu.com/ubuntu bionic/main amd64 libapr1 amd64 1.6.3-2 [90.9 kB]
Get:2 http://my.archive.ubuntu.com/ubuntu bionic/main amd64 libaprutil1 amd64 1.6.1-2 [84.4 kB]
```

Figure 5.3.20.1: Install Apache server

```
group4@group4: ~
File Edit View Search Terminal Help
group4@group4:~$ clear

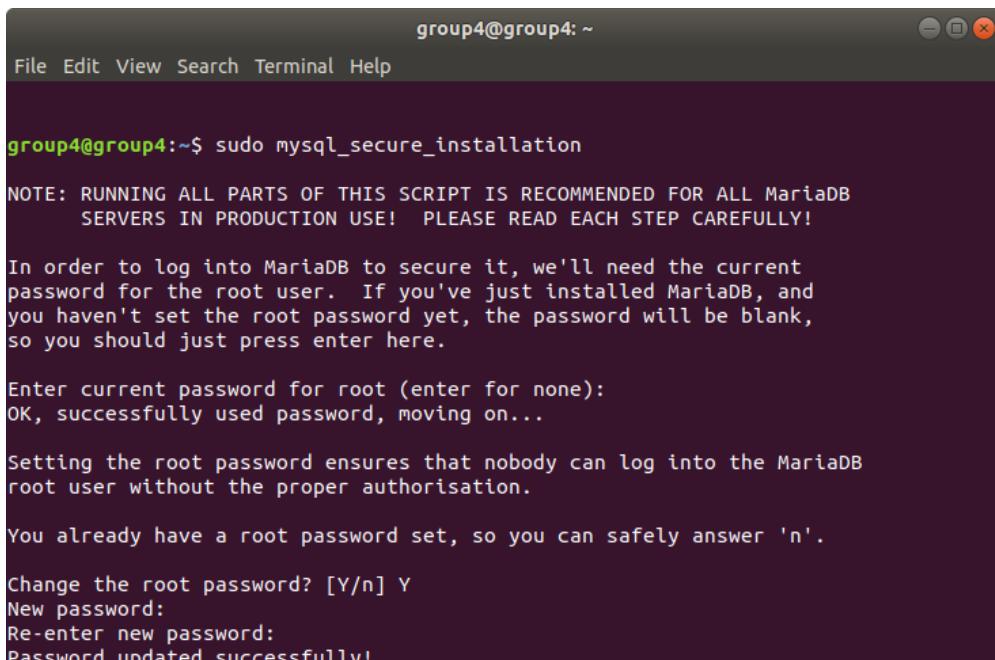
group4@group4:~$ sudo apt-get install libapache2-mod-php php7.2 php7.2-xm...
  2-curl php7.2-gd php7.2 php7.2-cgi php7.2-cli php7.2-zip php7.2-mysql php7.2-mbs
  tring wget unzip -y
  Reading package lists... Done
  Building dependency tree
  Reading state information... Done
  unzip is already the newest version (6.0-21ubuntu1).
  unzip set to manually installed.
  wget is already the newest version (1.19.4-1ubuntu2.2).
  wget set to manually installed.
  The following package was automatically installed and is no longer required:
    tcpd
  Use 'sudo apt autoremove' to remove it.
  The following additional packages will be installed:
    libapache2-mod-php7.2 libcurl4 libzip4 php-common php7.2-common php7.2-json
    php7.2-opcache php7.2-readline
  Suggested packages:
    php-pear
  The following NEW packages will be installed:
    libapache2-mod-php libapache2-mod-php7.2 libcurl4 libzip4 php-common php7.2
    php7.2-cgi php7.2-cli php7.2-common php7.2-curl php7.2-gd php7.2-json
    php7.2-mbstring php7.2-mysql php7.2-opcache php7.2-readline php7.2-xm...
```

Figure 5.3.20.2: Install php extension server



```
group4@group4: ~
File Edit View Search Terminal Help
group4@group4:~$ sudo apt-get install mariadb-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  tcpd
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  galera-3 gawk libaio1 libconfig-inifiles-perl libdbd-mysql-perl libdbi-perl
  libhtml-template-perl libjemalloc1 libmysqlclient20 libreadline5
  libterm-readkey-perl mariadb-client-10.1 mariadb-client-core-10.1
  mariadb-common mariadb-server-10.1 mariadb-server-core-10.1 mysql-common
  socat
Suggested packages:
  gawk-doc libmldb-perl libnet-daemon-perl libsql-statement-perl
  libipc-sharedcache-perl mailx mariadb-test tinyca
The following NEW packages will be installed:
  galera-3 gawk libaio1 libconfig-inifiles-perl libdbd-mysql-perl libdbi-perl
  libhtml-template-perl libjemalloc1 libmysqlclient20 libreadline5
  libterm-readkey-perl mariadb-client-10.1 mariadb-client-core-10.1
  mariadb-common mariadb-server mariadb-server-10.1 mariadb-server-core-10.1
  mysql-common socat
0 upgraded, 19 newly installed, 0 to remove and 0 not upgraded.
Need to get 0 B/24.1 MB of archives.
```

Figure 5.3.20.3: Install MariaDB server



```
group4@group4: ~
File Edit View Search Terminal Help
group4@group4:~$ sudo mysql_secure_installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

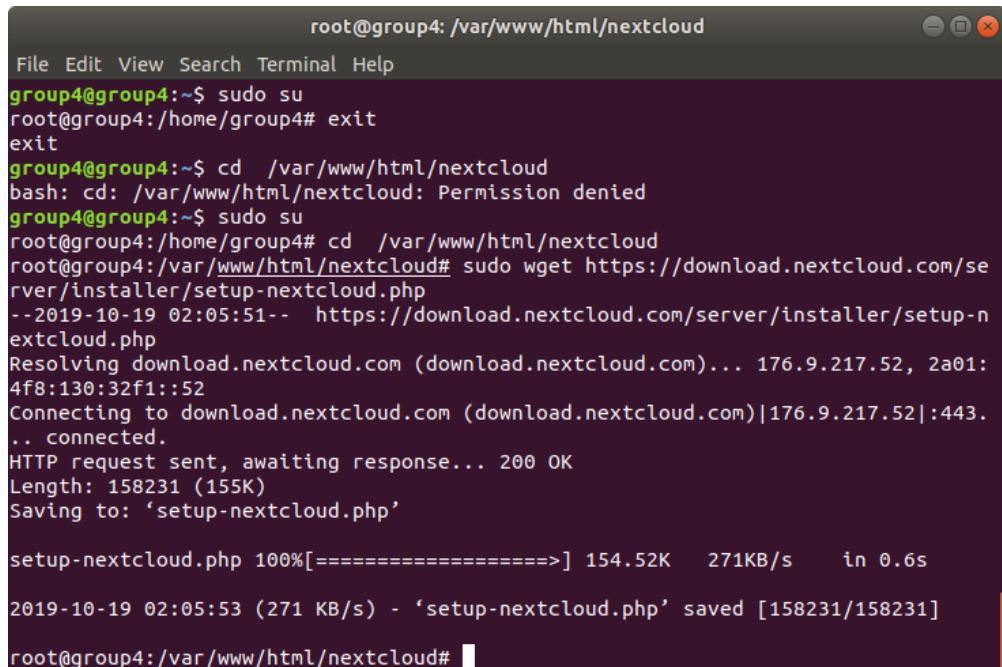
Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

You already have a root password set, so you can safely answer 'n'.

Change the root password? [Y/n] Y
New password:
Re-enter new password:
Password updated successfully!
```

Figure 5.3.20.4: Install MariaDB database server

Step 4: Download Nextcloud



```

root@group4: /var/www/html/nextcloud
File Edit View Search Terminal Help
group4@group4:~$ sudo su
root@group4:/home/group4# exit
exit
group4@group4:~$ cd /var/www/html/nextcloud
bash: cd: /var/www/html/nextcloud: Permission denied
group4@group4:~$ sudo su
root@group4:/home/group4# cd /var/www/html/nextcloud
root@group4:/var/www/html/nextcloud# sudo wget https://download.nextcloud.com/se
rver/installer/setup-nextcloud.php
--2019-10-19 02:05:51-- https://download.nextcloud.com/server/installer/setup-n
extcloud.php
Resolving download.nextcloud.com (download.nextcloud.com)... 176.9.217.52, 2a01:
4f8:130:32f1::52
Connecting to download.nextcloud.com (download.nextcloud.com)|176.9.217.52|:443.
... connected.
HTTP request sent, awaiting response... 200 OK
Length: 158231 (155K)
Saving to: 'setup-nextcloud.php'

setup-nextcloud.php 100%[=====] 154.52K 271KB/s in 0.6s
2019-10-19 02:05:53 (271 KB/s) - 'setup-nextcloud.php' saved [158231/158231]
root@group4:/var/www/html/nextcloud# 

```

Figure 5.3.20.5: Unpacking nextcloud server

Step 5:Edit file nextcloud.conf “sudo nano /etc/apache2/sites-available/nextcloud.conf”



```

GNU nano 2.5.3  File: /etc/apache2/sites-available/nextcloud.conf
<VirtualHost *:80>
ServerAdmin admin@ubuntu
DocumentRoot "/var/www/html/nextcloud/"
ServerName cloud.group3.com
ServerAlias ubuntu
<Directory "/var/www/html/nextcloud/">
Options FollowSymLinks
AllowOverride All
Order allow,deny
allow from all
</Directory>
ErrorLog /var/log/apache2/your-domain.com-error_log
CustomLog /var/log/apache2/your-domain.com-access_log common
</VirtualHost>

[ Read 14 lines (Warning: No write permission) ]
^D Get Help ^O Write Out ^W Where Is ^X Cut Text ^J Justify ^C Cur Pos
^Y Exit ^R Read File ^L Replace ^U Uncut Text ^T To Spell ^A Go To Line

```

Step 6: Restart the Apache web server: group@group4: ~\$ systemctl restart apache2.service.

Step 7: Configure the Nextcloud domain name at DNS : cloud.group4.com

Step 8: Once Nextcloud domain name entered at DNS, open the web browser and browse the cloud.group4.com. The Nextcloud interface for setup will appeared.

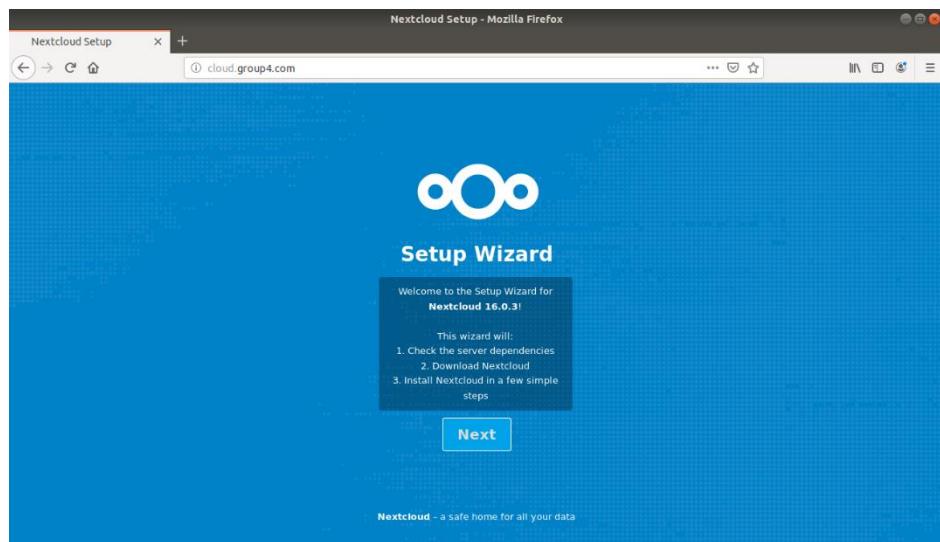


Figure 5.3.20.6: NextCloud setup wizard interface.

5.3.21 Web Hardening

INSTALLATION AND CONFIGURATION OF FIREWALL

Step 1: Check for updates (if any)

Step 1.1: Check for updates by using Debian's Advanced Package Tool with command *apt update*.

```
group4@debian:~$ su
Password:
root@debian:/home/group4# apt update
Hit:1 http://repo.zabbix.com/zabbix/4.0/debian stretch InRelease
Ign:3 http://ftp.us.debian.org/debian stretch InRelease
Get:4 http://ftp.us.debian.org/debian stretch-updates InRelease [91.0 kB]
Hit:5 http://ftp.us.debian.org/debian stretch Release
Get:2 http://security-cdn.debian.org/debian-security stretch/updates InRelease [94.3 kB]
Get:7 http://security-cdn.debian.org/debian-security stretch/updates/main Sources [190 kB]
Get:8 http://security-cdn.debian.org/debian-security stretch/updates/main amd64 Packages [500 kB]
Fetched 876 kB in 43s (20.3 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
3 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@debian:/home/group4#
```

Figure 5.3.21.4 : Check for updates

Step 1.2 : Install updates (if any) by using command *apt upgrade*.

```
root@debian:/home/group4# apt upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following package was automatically installed and is no longer required:
  libopts25
Use 'apt autoremove' to remove it.
The following NEW packages will be installed:
  firmware-linux-free irqbalance linux-image-4.9.0-11-amd64
The following packages will be upgraded:
  linux-image-amd64 openjdk-8-jre openjdk-8-jre-headless
3 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 27.4 MB/66.7 MB of archives.
After this operation, 193 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://security.debian.org/debian-security stretch/updates/main amd64 openjdk-8-jre amd64 8u232-b09-1~deb9u1 [69.5 kB]
Get:2 http://security.debian.org/debian-security stretch/updates/main amd64 openjdk-8-jre-headless amd64 8u232-b09-1~deb9u1 [27.3 MB]
Fetched 27.4 MB in 1min 36s (283 kB/s)
Reading changelogs... Done
Preconfiguring packages ...
```

Figure 5.3.21.5 : Install updates

```

group4@debian: ~
File Edit View Search Terminal Help
Selecting previously unselected package firmware-linux-free.
(Reading database ... 135932 files and directories currently installed.)
Preparing to unpack .../0-firmware-linux-free_3.4_all.deb ...
Unpacking firmware-linux-free (3.4) ...
Selecting previously unselected package linux-image-4.9.0-11-amd64.
Preparing to unpack .../1-linux-image-4.9.0-11-amd64_4.9.189-3+deb9u1_amd64.deb
...
Unpacking linux-image-4.9.0-11-amd64 (4.9.189-3+deb9u1) ...
Preparing to unpack .../2-linux-image-amd64_4.9+80+deb9u9_amd64.deb ...
Unpacking linux-image-amd64 (4.9+80+deb9u9) over (4.9+80+deb9u2) ...
Preparing to unpack .../3-openjdk-8-jre_8u232-b09-1-deb9u1_amd64.deb ...
Unpacking openjdk-8-jre-amd64 (8u232-b09-1-deb9u1) over (8u222-b10-1-deb9u1) ...
Preparing to unpack .../4-openjdk-8-jre-headless_8u232-b09-1-deb9u1_amd64.deb ...
.
Unpacking openjdk-8-jre-headless:amd64 (8u232-b09-1-deb9u1) over (8u222-b10-1-deb9u1) ...
Selecting previously unselected package irqbalance.
Preparing to unpack .../5-irqbalance_1.1.0-2.3_amd64.deb ...
Unpacking irqbalance (1.1.0-2.3) ...
Processing triggers for mime-support (3.60) ...
Processing triggers for desktop-file-utils (0.23-1) ...
Processing triggers for libc-bin (2.24-11+deb9u4) ...
Setting up linux-image-4.9.0-11-amd64 (4.9.189-3+deb9u1) ...
I: /vmlinuz is now a symlink to boot/vmlinuz-4.9.0-11-amd64

```

Figure 5.3.21.6 : Install updates

```

group4@debian: ~
File Edit View Search Terminal Help
I: /initrd.img is now a symlink to boot/initrd.img-4.9.0-11-amd64
/etc/kernel/postinst.d/initramfs-tools:
update-initramfs: Generating /boot/initrd.img-4.9.0-11-amd64
/etc/kernel/postinst.d/dz-update-grub:
Generating grub configuration file ...
Found background image: /usr/share/images/desktop-base/desktop-grub.png
Found linux image: /boot/vmlinuz-4.9.0-11-amd64
Found initrd image: /boot/initrd.img-4.9.0-11-amd64
Found linux image: /boot/vmlinuz-4.9.0-4-amd64
Found initrd image: /boot/initrd.img-4.9.0-4-amd64
Adding boot menu entry for EFI firmware configuration
done
Processing triggers for systemd (232-25+deb9u12) ...
Setting up firmware-linux-free (3.4) ...
update-initramfs: deferring update (trigger activated)
Processing triggers for man-db (2.7.6.1-2) ...
Processing triggers for gnome-menus (3.13.3-9) ...
Processing triggers for hicolor-icon-theme (0.15-1) ...
Setting up irqbalance (1.1.0-2.3) ...
Setting up openjdk-8-jre-headless:amd64 (8u232-b09-1-deb9u1) ...
Installing new version of config file /etc/java-8-openjdk/security/java.policy .
...
Installing new version of config file /etc/java-8-openjdk/security/java.security
...

```

Figure 5.3.21.7 : Install updates

```

group4@debian: ~
File Edit View Search Terminal Help
Found initrd image: /boot/initrd.img-4.9.0-4-amd64
Adding boot menu entry for EFI firmware configuration
done
Processing triggers for systemd (232-25+deb9u12) ...
Setting up firmware-linux-free (3.4) ...
update-initramfs: deferring update (trigger activated)
Processing triggers for man-db (2.7.6.1-2) ...
Processing triggers for gnome-menus (3.13.3-9) ...
Processing triggers for hicolor-icon-theme (0.15-1) ...
Setting up irqbalance (1.1.0-2.3) ...
Setting up openjdk-8-jre-headless:amd64 (8u232-b09-1-deb9u1) ...
Installing new version of config file /etc/java-8-openjdk/security/java.policy .
...
Installing new version of config file /etc/java-8-openjdk/security/java.security
...
Setting up linux-image-amd64 (4.9+80+deb9u9) ...
Setting up openjdk-8-jre:amd64 (8u232-b09-1-deb9u1) ...
Processing triggers for initramfs-tools (0.130) ...
update-initramfs: Generating /boot/initrd.img-4.9.0-11-amd64
Processing triggers for systemd (232-25+deb9u12) ...
Processing triggers for libc-bin (2.24-11+deb9u4) ...

```

Figure 5.3.21.8 : Install updates

Step 1.3 : Reboot your server by using command *apt upgrade and sudo reboot*.

```
root@debian:/home/group4# reboot
```

Figure 5.3.21.9: Reboot server

Step 2: Install and configure Uncomplicated Firewall (ufw).

Step 2.1: Install Uncomplicated Firewall by using command *apt install ufw*.

```

root@debian:/home/group4# apt install ufw
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  ufw
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 164 kB of archives.
After this operation, 848 kB of additional disk space will be used.
Get:1 http://ftp.us.debian.org/debian stretch/main amd64 ufw all 0.35-4 [164 kB]
Fetched 164 kB in 4s (38.0 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 140191 files and directories currently installed.)
Preparing to unpack .../archives/ufw_0.35-4_all.deb ...
Unpacking ufw (0.35-4) ...
Setting up ufw (0.35-4) ...

Creating config file /etc/ufw/before.rules with new version
Creating config file /etc/ufw/before6.rules with new version
Creating config file /etc/ufw/after.rules with new version
Creating config file /etc/ufw/after6.rules with new version
Created symlink /etc/systemd/system/multi-user.target.wants/ufw.service → /lib/systemd/system/ufw.service.
Processing triggers for systemd (232-25+deb9u12) ...
Processing triggers for man-db (2.7.6.1-2) ...
Processing triggers for rsyslog (8.24.0-1) ...

```

Figure 5.3.21.10 : Install ufw

Step 2.2: Check the status of ufw by using command *ufw status*.

```
root@debian:/home/group4# ufw status
Status: inactive
```

Figure 5.3.21.11 : Check ufw status

Step 2.3: Modify the default rules by using command *ufw default deny incoming* and *ufw default allow outgoing*.

```
root@debian:/home/group4# ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
root@debian:/home/group4# ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
```

Figure 5.3.21.12 : Modify default rules

Step 2.4: Enable access to the port used by SSH which is port 22 by using command *ufw allow ssh*.

```
root@debian:/home/group4# ufw allow ssh
Rules updated
Rules updated (v6)
```

Figure 5.3.21.13 : Enable port

Step 2.5: Set the actual port number by using command *ufw allow 10.1.1.6 from to any port 22*

```
root@debian:/home/group4# ufw allow from 10.1.1.6 to any port 22
Rules updated
```

Figure 5.3.21.14 : Set port nummber

Step 2.6: Start and enable ufw by using command *ufw enable*.

```
root@debian:/home/group4# ufw enable
Firewall is active and enabled on system startup
```

Figure 5.3.21.15: Enable ufw

CREATE A NON-ROOT ACCOUNT

Step 1: Create a non-root account

Step 1.1: Create a non-root account by using command *adduser potheng* on Debian. A non-root account is used to make sure that an hacker doesn't get all access if he exploits a program which runs in a non-root context.

```
root@debian:/home/group4# adduser potheng
Adding user `potheng' ...
Adding new group `potheng' (1001) ...
Adding new user `potheng' (1001) with group `potheng' ...
Creating home directory `/home/potheng' ...
Copying files from `/etc/skel' ...
Current Kerberos password:
Current Kerberos password:
passwd: Authentication token manipulation error
passwd: password unchanged
Try again? [y/N] n
Changing the user information for potheng
Enter the new value, or press ENTER for the default
      Full Name []: CHONG POH THENG
      Room Number []: C-01-07
      Work Phone []: 018-2554662
      Home Phone []:
      Other []:
Is the information correct? [Y/n] Y
```

Figure 5.3.21.16 : Create a non-root account

Step 1.2: The new user doesn't have the access to obtain administrative rights by default. We can change the default mode by adding new user to the group by using command *usermod -aG sudo potheng*. View all groups of a user by using command *groups potheng*.

```
root@debian:/home/group4# usermod -aG sudo potheng
root@debian:/home/group4# groups potheng
potheng : potheng sudo
```

Figure 5.3.21.17 : Change user default mode

Step 1.3: Test to switch to new account by entering command *su potheng*.

```
root@debian:/home/group4# su potheng
potheng@debian:/home/group4$ █
```

Figure 5.3.21.18 : Test new user

INSTALLATION OF APACHE2

Step 1: Update and install apache2.

Step 1.1: Check for updates by using Debian's Advanced Package Tool with command *apt update*.

```
root@debian:/home/group4# apt update
Hit:1 http://repo.zabbix.com/zabbix/4.0/debian stretch InRelease
Ign:2 http://ftp.us.debian.org/debian stretch InRelease
Hit:3 http://security.debian.org/debian-security stretch/updates InRelease
Hit:4 http://ftp.us.debian.org/debian stretch-updates InRelease
Hit:5 http://ftp.us.debian.org/debian stretch Release
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
```

Figure 5.3.21.19 : Check updates

Step 1.2: Install apache2 by entering command *apt install apache2*

```
root@debian:/home/group4# apt install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
apache2 is already the newest version (2.4.25-3+deb9u9).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Figure 5.3.21.20 : Install apache2

Step 2: Install Certbot which is needed to easily obtain a TLS certificate.

Step 2.1: Install Certbot with command `apt install python-certbot-apache`

```
root@debian:/home/group4# apt install python-certbot-apache
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  augeas-lenses certbot libaugeas0 python3-acme python3-augeas python3-certbot
  python3-certbot-apache python3-cffi-backend python3-configargparse
  python3-configobj python3-cryptography python3-idna python3-josepy
  python3-mock python3-openssl python3-parsedatetime python3-pbr
  python3-pyasn1 python3-requests-toolbelt python3-rfc3339 python3-setuptools
  python3-tz python3-zope.component python3-zope.event python3-zope.hookable
  python3-zope.interface
Suggested packages:
  augeas-doc python3-certbot-nginx python-certbot-doc augeas-tools
  python-acme-doc python-certbot-apache-doc python-configobj-doc
  python-cryptography-doc python3-cryptography-vectors python-mock-doc
  python-openssl-doc python3-openssl-dbg doc-base python-setuptools-doc
Recommended packages:
  python3-pycu
```

Figure 5.3.21.21 : Install Certbot

```
The following NEW packages will be installed:
augeas-lenses certbot libaugeas0 python-certbot-apache python3-acme
python3-augeas python3-certbot python3-cffi-backend python3-cryptography
python3-configargparse python3-configobj python3-idna python3-josepy
python3-mock python3-openssl python3-parsedatetime python3-pbr
python3-pyasn1 python3-requests-toolbelt python3-rfc3339 python3-setuptools
python3-tz python3-zope.component python3-zope.event python3-zope.hookable
python3-zope.interface
0 upgraded, 27 newly installed, 0 to remove and 0 not upgraded.
Need to get 2,164 kB of archives.
After this operation, 10.4 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ftp.us.debian.org/debian stretch/main amd64 augeas-lenses all 1.8.0-1+deb9u1 [420 kB]
Get:2 http://ftp.us.debian.org/debian stretch/main amd64 libaugeas0 amd64 1.8.0-1+deb9u1 [288 kB]
Get:3 http://ftp.us.debian.org/debian stretch/main amd64 python3-cffi-backend amd64 1.9.1-2 [70.1 kB]
Get:4 http://ftp.us.debian.org/debian stretch/main amd64 python3-idna all 2.2-1 [32.7 kB]
Get:5 http://ftp.us.debian.org/debian stretch/main amd64 python3-pyasn1 all 0.1.9-2 [34.5 kB]
Get:6 http://ftp.us.debian.org/debian stretch/main amd64 python3-setuptools all 33.1.1-1 [215 kB]
Get:7 http://ftp.us.debian.org/debian stretch/main amd64 python3-cryptography amd64 1.7.1-3+deb9u1 [210 kB]
Get:8 http://ftp.us.debian.org/debian stretch/main amd64 python3-openssl all 16.2.0-1 [43.8 kB]
Get:9 http://ftp.us.debian.org/debian stretch/main amd64 python3-josepy all 1.1.0-2+deb9u1 [27.8 kB]
Get:10 http://ftp.us.debian.org/debian stretch/main amd64 python3-pbr all 1.10.0-1 [52.5 kB]
Get:11 http://ftp.us.debian.org/debian stretch/main amd64 python3-mock all 2.0.0-3 [59.9 kB]
Get:12 http://ftp.us.debian.org/debian stretch/main amd64 python3-requests-toolbelt all 0.7.0-1 [36.7 kB]
Get:13 http://ftp.us.debian.org/debian stretch/main amd64 python3-tz all 2016.7-0.3 [27.1 kB]
Get:14 http://ftp.us.debian.org/debian stretch/main amd64 python3-rfc3339 all 1.0-4 [6,282 B]
Get:15 http://ftp.us.debian.org/debian stretch-updates/main amd64 python3-acme all 0.28.0-1+deb9u2 [49.9 kB]
Get:16 http://ftp.us.debian.org/debian stretch/main amd64 python3-augeas all 0.5.0-1 [9,046 B]
Get:17 http://ftp.us.debian.org/debian stretch/main amd64 python3-configargparse all 0.11.0-1 [22.3 kB]
Get:18 http://ftp.us.debian.org/debian stretch/main amd64 python3-configobj all 5.0.6-2 [35.2 kB]
Get:19 http://ftp.us.debian.org/debian stretch/main amd64 python3-parsedatetime all 2.1.3+deb9u1 [37.7 kB]
Get:20 http://ftp.us.debian.org/debian stretch/main amd64 python3-zope.hookable amd64 4.0.4-4+b2 [10.3 kB]
Get:21 http://ftp.us.debian.org/debian stretch/main amd64 python3-zope.interface amd64 4.3.2-1 [89.8 kB]
Get:22 http://ftp.us.debian.org/debian stretch/main amd64 python3-zope.event all 4.2.0-1 [8,412 B]
Get:23 http://ftp.us.debian.org/debian stretch/main amd64 python3-zope.component all 4.3.0-1 [43.0 kB]
```

Figure 5.3.21.22 : Install Certbot

Step 2.2 Run Certbot to obtain an [RSA certificate](#) using command certbot --apache -d www.[your-domain-name],[your-domain-name]--rsa-key-size 4096

```
root@debian:/home/group4# certbot --apache -d www.group4.com --rsa-key-size 4096
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator apache, Installer apache
Enter email address (used for urgent renewal and security notices) (Enter 'c' to cancel): hafiz@group4.com

-----
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. You must
agree in order to register with the ACME server at
https://acme-v02.api.letsencrypt.org/directory
-----
(A)gree/(C)ancel: A

Would you be willing to share your email address with the Electronic Frontier
Foundation, a founding partner of the Let's Encrypt project and the non-profit
organization that develops Certbot? We'd like to send you email about our work
encrypting the web, EFF news, campaigns, and ways to support digital freedom.
-----
(Y)es/(N)o: Y
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for www.group4.com
Enabled Apache rewrite module
Cleaning up challenges
Unable to find a virtual host listening on port 80 which is currently needed for Certbot to prove to the CA that you control your domain. Please add a
virtual host for port 80.

IMPORTANT NOTES:
- Your account credentials have been saved in your Certbot
  configuration directory at /etc/letsencrypt. You should make a
  secure backup of this folder now. This configuration directory will
  also contain certificates and private keys obtained by Certbot so
  making regular backups of this folder is ideal.
```

Figure 5.3.21.23 : Run Certbot

Step 3: Configure apache2.conf

Step 3.1 : In order to enable HTTP/2 over TLS, you have to enable the HTTP/2 module of Apache first by enter command *a2enmod http2* and restart apache 2 by entering command *systemctl restart apache2*

```
root@debian:/# a2enmod headers
Enabling module headers.
To activate the new configuration, you need to run:
  systemctl restart apache2
root@debian:/# systemctl restart apache2■
```

Figure 5.3.21.24 : Enable HTTP/2 module and restart apache2

Step 3.2: Go to apache2.conf file in /etc/apache2/apache2.conf by entering command
nano /etc/apache2/conf-available/security.conf

```
root@debian:/etc# ls /etc/apache2/
apache2.conf      conf-enabled/    magic          mods-enabled/   sites-available/
conf-available/  envvars        mods-available/ ports.conf     sites-enabled/
root@debian:/etc# ls /etc/apache2/conf-available/
charset.conf      other-vhosts-access-log.conf  security.conf
localized-error-pages.conf  roundcube.conf       serve-cgi-bin.conf
root@debian:/etc# ls /etc/apache2/conf-available/security.conf
/etc/apache2/conf-available/security.conf
root@debian:/etc# nano /etc/apache2/conf-available/security.conf
```

Figure 5.3.21.25 : Enter config file

Step 3.3: Apply the settings as figure below. (or modify them based on self-requirement)

```
# Send only necessary header responses
ServerTokens Prod

# Reduces server signature which exposes your OS and web server information
# like "Apache/2.4.25(Debian) Server" to "Apache"
ServerSignature Off

# Add security-related HTTP headers
# The following settings are fine for static blogs but have to be modified
# for Wordpress etc.

# Enable Content Security Policy (Level 2)
Header always set Content-Security-Policy "default-src 'none'; img-src 'self'; style-src 'self'; font-src 'self', base-uri 'none'; frame-ancestors 'self'"

# Disable Referrer which isn't needed when you don't use authentication
Header always set Referrer-Policy "no-referrer"

# Enable HSTS
Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload" env=HTTPS

# Enforce MIME types for script and style elements
Header always set X-Content-Type-Options "nosniff"

# Enable OCSP stapling
SSLUseStapling on
SSLStaplingResponderTimeout 5
SSLStaplingReturnResponderErrors off
SSLStaplingCache shmc:/var/run/apache2/ocsp(128000)

# Legacy HTTP response headers
# ( Set these only if you want to support really old web browsers ! )
```

Figure 5.3.21.26 : Apply settings

ENABLE PASSWORD AUTHENTICATION

Step 1: Create a password file.

```
root@debian:/home/azimgroup4# htpasswd -c /etc/apache2/.htpasswd group4
New password:
Re-type new password:
Adding password for user group4
```

Figure 5.3.21.27 : Create password file

Step 2 : Save and close the file when you are finished. Restart Apache and The directory you specified should now be password protected.

```
root@debian:/# systemctl restart apache2
```

Figure 5.3.21.25: Restart Apache2

Step 2. Go to apache2.conf file in /etc/apache2/apache2.conf. For the AuthName, choose a realm name that will be displayed to the user when prompting for credentials. Use the AuthUserFile directive to point Apache to the password file we created.

```
AuthType Basic
AuthName "Basic Authentication"
AuthUserFile /etc/apache2/.htpasswd
require valid-user
```

Figure 5.3.21.28 : Configure Apache Password Authentication

ENABLE CLICKJACKING PROTECTION

Step 1: Go to apache2.conf file in /etc/apache2/apache2.conf and enter *Header always set X-Frame-Options "DENY".*

```
# Enable Clickjacking protection
# ( Uncomment, if needed. Only necessary, if you support old web browsers that
# don't support the CSP level 2 directive "frame-ancestors". )
Header always set X-Frame-Options "DENY"
```

Figure 5.3.21.29 : Enable Clickjacking Protection

Step 2: Restart apache2 by command systemctl restart apache2

```
root@debian:/# systemctl restart apache2
```

Figure 5.3.21.30 : Restart Apache2

ENABLE XSS PROTECTION

Step 1: Go to apache2.conf file in /etc/apache2/apache2.conf and enter *Header always set X-Xss-Protection "1; mode=block"*.

```
# Enable XSS protection
# ( Uncomment, if needed. Only necessary, if you support old web browsers that
# don't support the Content Security Policy header. )
Header always set X-Xss-Protection "1; mode=block" ■
```

Figure 5.3.21.31 : Enable XSS Protection

DISABLE DIRECTORY BROWSER LISTING

Step 1: Go to apache2.conf file in /etc/apache2/apache2.conf and enter settings based on figure below.

```
<Directory /opt/apache/htdocs>
    Options None
</Directory>
```

Figure 5.3.21.32 : Disable directory browser listing

Step 2: Restart apache2 by command systemctl restart apache2.

```
root@debian:/# systemctl restart apache2
```

Figure 5.3.21.33 : Restart Apache2

SYSTEM SETTINGS PROTECTION

Step 1: For default installation, users can override apache configuration using .htaccess. If you want to prevent users from modifying your apache server settings, you can add AllowOverride to None as shown below.

```
<Directory />
    Options -Indexes
    AllowOverride None
</Directory>
```

Figure 5.3.21.34 : System settings protection

INSTALLATION OF MODSECURITY

ModSecurity need to installed in Debian server to disable the server signature completely.

Step 1: Use command *apt install libapache2-modsecurity* to install ModSecurity

```
root@debian:/# apt install libapache2-modsecurity
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libapache2-mod-security2 liblua5.1-0 modsecurity-crs
Suggested packages:
  lua geoip-database-contrib ruby
The following NEW packages will be installed:
  libapache2-mod-security2 libapache2-modsecurity liblua5.1-0 modsecurity-crs
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 111 kB/620 kB of archives.
After this operation, 2,339 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ftp.us.debian.org/debian stretch/main amd64 liblua5.1-0 amd64 5.1.5-8.1+b2 [111 kB]
Fetched 111 kB in 3s (35.4 kB/s)
Selecting previously unselected package liblua5.1-0:amd64.
(Reading database ... 143402 files and directories currently installed.)
Preparing to unpack .../liblua5.1-0_5.1.5-8.1+b2_amd64.deb ...
Unpacking liblua5.1-0:amd64 (5.1.5-8.1+b2) ...
Selecting previously unselected package libapache2-mod-security2.
Preparing to unpack .../libapache2-mod-security2_2.9.1-2_amd64.deb ...
Unpacking libapache2-mod-security2 (2.9.1-2) ...
Selecting previously unselected package libapache2-modsecurity.
Preparing to unpack .../libapache2-modsecurity_2.9.1-2_all.deb ...
Unpacking libapache2-modsecurity (2.9.1-2) ...
Selecting previously unselected package modsecurity-crs.
Preparing to unpack .../modsecurity-crs_3.0.0-3_all.deb ...
Unpacking modsecurity-crs (3.0.0-3) ...
Setting up modsecurity-crs (3.0.0-3) ...
Processing triggers for libc-bin (2.24-11+deb9u4) ...
Setting up liblua5.1-0:amd64 (5.1.5-8.1+b2) ...
Setting up libapache2-mod-security2 (2.9.1-2) ...
apache2_invoke: Enable module security2
Setting up libapache2-modsecurity (2.9.1-2) ...
Processing triggers for libc-bin (2.24-11+deb9u4) ...
```

Figure 5.3.21.35 : Install ModSecurity

Step 2: Open the security2.conf file in /etc/apache2/mods-enabled/.

```
root@debian:/etc# cd /etc/apache2
root@debian:/etc/apache2# ls
apache2.conf  conf-available  conf-enabled  envvars  magic  mods-available  mods-enabled  ports.conf  sites-available  sites-enabled
root@debian:/etc/apache2# nano apache2.conf
Use "fg" to return to nano.
```

Figure 5.3.21.36 : Open config file

Step 2.1: Edit the following settings.

```
# Disable the server signature
SecServerSignature " "
/IfModule>
```

Figure 5.3.21.37 : Edit settings

Step 3: Restart apache2 by command systemctl restart apache2

```
root@debian:/# systemctl restart apache2
```

Figure 5.3.21.38 : Restart Apache2

BACKUP CONFIGURATION

Finally, back up the configuration as it is useful in case of errors or lockout since user can reinstall server and web server without configuring everything again.

Step 1: Apply a small bash script.

```
root@debian:/# mkdir apache
root@debian:/# scp -i ~/.ssh/root -root@10.1.1.130:/etc/apache2/* apache/
usage: scp [-1234567cpqrsv] [-c cipher] [-F ssh_config] [-i identity_file]
           [-l limit] [-o ssh_option] [-P port] [-S program]
           [[user@]host1:]file1 ... [[user@]host2:]file2
root@debian:/# DATE=$(date +"%F %H:%M:%S")
root@debian:/# rm -rf apache/
```

Figure 5.3.21.39 : Apply a small bash script

5.3.22 Samba and Samba Security Services

Samba

Step 1: Install the Samba package with the following command

```
group4@group4:~$ sudo apt-get install samba
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  attr ibverbs-providers libcephfs2 libibverbs1 libnl-route-3-200
  libpython-stdlib librados2 python python-crypto python-dnspython python-ldb
  python-minimal python-samba python-tdb python2.7 python2.7-minimal
  samba-common samba-common-bin samba-dsdb-modules samba-vfs-modules tdb-tools
Suggested packages:
  python-doc python-tk python-crypto-doc python-gpgme python2.7-doc
  binfmt-support bind9 bind9utils ctdb ldb-tools ntp | chrony smbldap-tools
  winbind heimdal-clients
The following NEW packages will be installed:
  attr ibverbs-providers libcephfs2 libibverbs1 libnl-route-3-200
  libpython-stdlib librados2 python python-crypto python-dnspython python-ldb
  python-minimal python-samba python-tdb python2.7 python2.7-minimal samba
  samba-common samba-common-bin samba-dsdb-modules samba-vfs-modules tdb-tools
0 upgraded, 22 newly installed, 0 to remove and 96 not upgraded.
Need to get 9,504 kB of archives.
After this operation, 52.7 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://my.archive.ubuntu.com/ubuntu bionic-updates/main amd64 python2.7-mi
nimal amd64 2.7.15-4ubuntu4~18.04.1 [1,293 kB]
```

Figure 5.3.22.1: Installation of samba

Step 2: Once the installation is completed, the Samba service will start automatically. To check whether the Samba server is running, type

```
group4@group4:~$ sudo systemctl status nmbd
● nmbd.service - Samba NMB Daemon
  Loaded: loaded (/lib/systemd/system/nmbd.service; enabled; vendor preset: ena
  Active: active (running) since Tue 2019-10-01 00:20:26 +08; 3min 37s ago
    Docs: man:nmbd(8)
          man:samba(7)
          man:smb.conf(5)
   Main PID: 5368 (nmbd)
     Status: "nmbd: ready to serve connections..."
      Tasks: 1 (limit: 4915)
     CGroup: /system.slice/nmbd.service
             └─5368 /usr/sbin/nmbd --foreground --no-process-group

Okt 01 00:20:26 group4 systemd[1]: Starting Samba NMB Daemon...
Okt 01 00:20:26 group4 systemd[1]: Started Samba NMB Daemon.
lines 1-14/14 (END)
```

Figure 5.3.22.2: status running of samba

Step 3: Configuring firewall to allow incoming UDP connections.

```
group4@group4:~$ sudo ufw allow 'Samba'
Rules updated
Rules updated (v6)
```

Figure 5.3.22.3: Allow SAMBA in Firewall

Step 4: Configuring global Samba options as figure below. To open this file, use this command “sudo nano /etc/samba/smb.conf”

```
[global]
## Browsing/Identification ##

# Change this to the workgroup/NT-domain name your Samba server will part of
workgroup = GROUP4
password server = winsrv.group4.com
realm = GROUP4.COM
security = ads
idmap uid = 16777216-33554431
idmap gid = 16777216-33554431
template homedir = /home/%u
template shell = /bin/bash
winbind use default domain = true
winbind offline logon = false

# server string is the equivalent of the NT Description field
server string = %h server (Samba, Ubuntu)
```

Figure 5.3.22.4: Integrate Active Directory with Samba

Step 5: For easier maintainability and flexibility instead of using the standard home directories (/home/user) all Samba directories and data will be located in the /samba directory.

```
root@ubuntu:~# mkdir /samba
```

Figure 5.3.22.5: Create samba directory

Step 6: create the folder that want to share with the public. The folder can be anywhere but set its permission so that everyone in active directory can access it. Then set the share permission so everyone has full access to it.

```
root@ubuntu:~# mkdir /samba/Public
root@ubuntu:~# chmod 0777 /samba/Public
root@ubuntu:~# chown -R nobody:ituser /samba/Public
root@ubuntu:~# 
```

Figure 5.3.22.6:Change file permission and owner

Step 7: Next, modify the directive settings to share a folder.

```
[Public]
    path = /samba/Public
    writeable = yes
    guest ok = yes
    guest only = yes
    read only = no
    create mask = 770
    directory mode = 770
    force user = nobody
```

Figure 5.3.22.7: Shared path

Step 8: Restart the Samba service with following command “sudo systemctl restart smbd” and check the status

```
root@ubuntu:~# systemctl status smbd
● smbd.service - Samba SMB Daemon
  Loaded: loaded (/lib/systemd/system/smbd.service; enabled; vendor preset: ena
  Active: active (running) since Sat 2019-12-14 19:18:55 +08; 46min ago
    Docs: man:smbd(8)
          man:samba(7)
          man:smb.conf(5)
   Main PID: 6833 (smbd)
     Status: "smbd: ready to serve connections..."
       Tasks: 4 (limit: 4915)
      CGroup: /system.slice/smbd.service
              ├─6833 /usr/sbin/smbd --foreground --no-process-group
              ├─6835 /usr/sbin/smbd --foreground --no-process-group
              ├─6836 /usr/sbin/smbd --foreground --no-process-group
              └─6837 /usr/sbin/smbd --foreground --no-process-group

Dec 14 19:18:55 ubuntu systemd[1]: Starting Samba SMB Daemon...
Dec 14 19:18:55 ubuntu systemd[1]: Started Samba SMB Daemon.
lines 1-17/17 (END)
```

Figure 5.3.22.8: Restart samba

Samba Security

Samba Group Based Directory

```
[Management]
comment = File sharing only for management group
path = /samba/Management
browseable = yes
read only = no
create mask = 640
directory mask = 750
valid users = +management
```

Figure 5.3.22 9: Samba group configuration

Step 1: Add a local group (non-UNIX) in samba database The group gid will be allocated out of the winbind range.

```
root@ubuntu:/home/group4# net sam createlocalgroup management
Created local group management with RID 1002
```

Figure 5.3.22 10: Create group

Step 2: Add a member to a local group. The group can be specified only by name, the member can be specified by name or SID.

```
root@ubuntu:/home/group4# net sam addmem management GROUP4\ammar
Added GROUP4\ammar to UBUNTU\management
```

Figure 5.3.22 11: Add member to group

Step 3: Change group of the shared path to local group as below.

```
root@ubuntu:/home/group4# chgrp -R "UBUNTU\management" /samba/client
root@ubuntu:/home/group4# ls -l /samba
total 8
drwxr-xr-x 2 root UBUNTU\management 4096 Nov 12 17:17 client
```

Figure 5.3.22 12: Change group owner

Step 4: Add the local group in file smb.conf as below.

```
[Management]
comment = File sharing only for management group
path = /samba/Management
browseable = yes
read only = no
create mask = 640
directory mask = 750
valid users = +management
```

Figure 5.3.22 13: Assign valid user

5.3.23 Linux Server Hardening

Linux hardening Installation

System Update

Keeping the system up to date is necessary after installing any operating system. This initial step will reduce known vulnerabilities in the system.

Step 1: Go to the terminal

Step 2: Type sudo su and apt-get update

```
group4@ubuntu:~$ sudo su
root@ubuntu:/home/group4# apt-get update
Ign:1 http://dl.google.com/linux/chrome/deb stable InRelease
Get:2 http://repo.zabbix.com/zabbix/4.0/ubuntu bionic InRelease [7,096 B]
Get:3 http://dl.google.com/linux/chrome/deb stable Release [943 B]
Hit:4 http://my.archive.ubuntu.com/ubuntu bionic InRelease
Get:5 http://dl.google.com/linux/chrome/deb stable Release.gpg [819 B]
Get:6 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Get:7 http://repo.zabbix.com/zabbix/4.0/ubuntu bionic/main Sources [1,181 B]
Get:8 http://dl.google.com/linux/chrome/deb stable/main amd64 Packages [1,086 B]
Get:9 http://repo.zabbix.com/zabbix/4.0/ubuntu bionic/main i386 Packages [2,682 B]
Get:10 http://my.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Get:11 http://repo.zabbix.com/zabbix/4.0/ubuntu bionic/main amd64 Packages [2,683 B]
Get:12 http://security.ubuntu.com/ubuntu bionic-security/main i386 Packages [413 kB]
Get:13 http://my.archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]
Get:14 http://security.ubuntu.com/ubuntu bionic-security/main amd64 Packages [593 kB]
Get:15 http://my.archive.ubuntu.com/ubuntu bionic-updates/main amd64 Packages [817 kB]
Get:16 http://security.ubuntu.com/ubuntu bionic-security/main Translation-en [194 kB]
```

Figure 5.3.23.1: Install System Update

```
n [319 kB]
Get:43 http://my.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 DEP-11
Metadata [264 kB]
Get:44 http://my.archive.ubuntu.com/ubuntu bionic-updates/universe DEP-11 48x48
Icons [196 kB]
Get:45 http://my.archive.ubuntu.com/ubuntu bionic-updates/universe DEP-11 64x64
Icons [455 kB]
Get:46 http://my.archive.ubuntu.com/ubuntu bionic-updates/multiverse amd64 Packa
ges [9,284 B]
Get:47 http://my.archive.ubuntu.com/ubuntu bionic-updates/multiverse i386 Packag
es [7,484 B]
Get:48 http://my.archive.ubuntu.com/ubuntu bionic-updates/multiverse Translation
-en [4,508 B]
Get:49 http://my.archive.ubuntu.com/ubuntu bionic-updates/multiverse amd64 DEP-1
1 Metadata [2,468 B]
Get:50 http://my.archive.ubuntu.com/ubuntu bionic-backports/universe i386 Packag
es [4,024 B]
Get:51 http://my.archive.ubuntu.com/ubuntu bionic-backports/universe amd64 Packa
ges [4,028 B]
Get:52 http://my.archive.ubuntu.com/ubuntu bionic-backports/universe amd64 DEP-1
1 Metadata [7,980 B]
Fetched 8,798 kB in 27s (325 kB/s)
Reading package lists... Done
root@ubuntu:/home/group4# 
```

Figure 5.3.23.2: Updating system done

1. Shellshock Bash Vulnerability

The shellshock vulnerability allows remote attackers to execute arbitrary code given certain conditions, by assigning Bash environment variables and gain unauthorized access to the system. This vulnerability very easy to exploit.

Step 1: Check system vulnerability based on following command

```
root@ubuntu:/home/group4# env VAR='() { :;}; echo Bash is vulnerable' bash -c "
echo Bash Test"
Bash Test
```

Figure 5.3.23.3: Check vulnerability

Step 2: If it is show Bash in Vulnerable! Or Bash Test means it is vulnerable

That command above is to check whether the system is vulnerable and the output did not show that the system is at risk which could lead the attacker exploit system. To know the system at risk, the output could come as shown.

Step 3: Type following command to update the bash

```
root@ubuntu:/home/group4# apt-get update && install --only-upgrade bash
Hit:1 http://repo.zabbix.com/zabbix/4.0/ubuntu bionic InRelease
Hit:2 http://security.ubuntu.com/ubuntu bionic-security InRelease
Hit:3 http://my.archive.ubuntu.com/ubuntu bionic InRelease
Ign:4 http://dl.google.com/linux/chrome/deb stable InRelease
Hit:5 http://dl.google.com/linux/chrome/deb stable Release
Hit:7 http://my.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:8 http://my.archive.ubuntu.com/ubuntu bionic-backports InRelease
Reading package lists... Done
install: unrecognized option '--only-upgrade'
Try 'install --help' for more information.
root@ubuntu:/home/group4# apt-get install --only-upgrade bash
Reading package lists... Done
Building dependency tree
Reading state information... Done
bash is already the newest version (4.4.18-2ubuntu1.2).
0 upgraded, 0 newly installed, 0 to remove and 105 not upgraded.
root@ubuntu:/home/group4# 
```

Figure 5.3.23.4: Done updating system and upgrade bash

2. Password Expired

Step 1: Type following command

```
group4@ubuntu:~$ sudo chage -l group4
Last password change : Okt 23, 2019
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
group4@ubuntu:~$
```

Figure 5.3.23.5: View password current status

Step 2: Edit the details as below

```
group4@ubuntu:~$ sudo chage -E 2/23/2020 -m 5 -M 6 -I 40 -W 5 group4
```

Figure 5.3.23.6: Command for change expiration date

Step 3: Verify the change

```
group4@ubuntu:~$ sudo chage -l group4
Last password change : Okt 23, 2019
Password expires      : Okt 29, 2019
Password inactive     : Dis 08, 2019
Account expires        : Feb 23, 2020
Minimum number of days between password change : 5
Maximum number of days between password change : 6
Number of days of warning before password expires : 5
group4@ubuntu:~$
```

Figure 5.3.23.7: Change expiration date of password

3. Software and Update

Step 1: Click at the Software & Updates

Step 2: Choose Updates

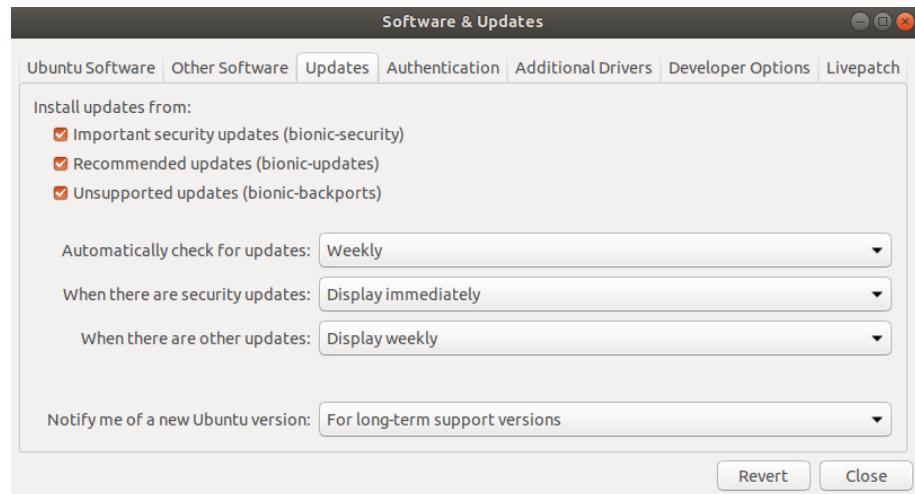


Figure 5.3.23.8: Changing system update

4. Install Firewall UFW

Installing firewall for the Ubuntu. Uncomplicated Firewall (UFW) is a basic firewall that works very well and easy to configure with firewall configuration tool.

Step 1: Open terminal and install UFW firewall

```
group4@ubuntu:~$ su
Password:
root@ubuntu:/home/group4# apt-get install ufw
Reading package lists... Done
Building dependency tree
Reading state information... Done
ufw is already the newest version (0.36-0ubuntu0.18.04.1).
ufw set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 105 not upgraded.
root@ubuntu:/home/group4#
```

Figure 5.3.23.9: Install UFW firewall

Step 2: Next, allow SSH and HTTP services

```
root@ubuntu:/home/group4# ufw allow ssh
Rules updated
Rules updated (v6)
root@ubuntu:/home/group4# ufw allow http
Rules updated
Rules updated (v6)
```

Figure 5.3.23.10: Allow SSH and HTTP services

Step 3: Enable firewall and check the status of the firewall

```
root@ubuntu:/home/group4# ufw enable
Firewall is active and enabled on system startup
root@ubuntu:/home/group4# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To           Action    From
--           --        --
137,138/udp (Samba) ALLOW IN  Anywhere
139,445/tcp (Samba) ALLOW IN  Anywhere
22/tcp        ALLOW IN  Anywhere
80/tcp        ALLOW IN  Anywhere
137,138/udp (Samba (v6)) ALLOW IN  Anywhere (v6)
139,445/tcp (Samba (v6)) ALLOW IN  Anywhere (v6)
22/tcp (v6)   ALLOW IN  Anywhere (v6)
80/tcp (v6)   ALLOW IN  Anywhere (v6)
```

Figure 5.3.23.11: Enable firewall and check status

5.3.24 User Authentication by Integrating Active Directory with Linux

Step 1: Open Terminal in Ubuntu.

Step 2: On the terminal, using command “`apt install winbind libpam-winbind libnss-winbind krb5-config`” to install Winbind Kerberos.

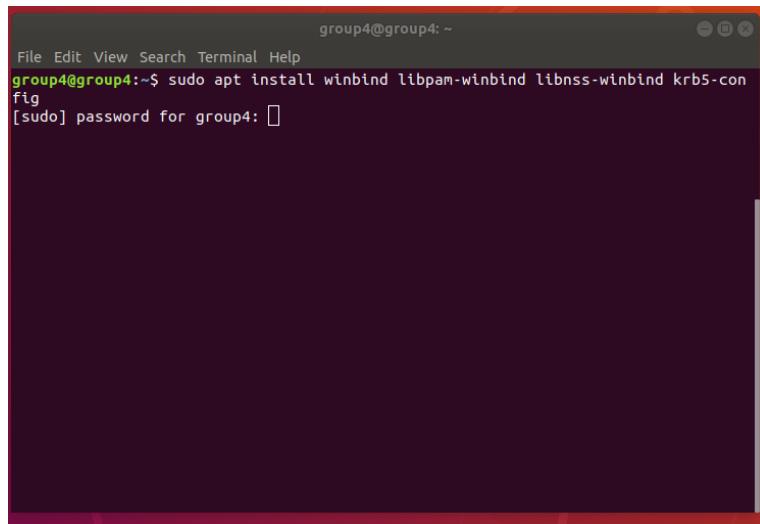


Figure 5.3.24 1: Install Winbind Kerberos

Step 3: After successfully running the command, there will be 3 input need to insert during installation. For the first input which is Kerberos Realm, insert Workgroup Name (GROUP4). Then, second input which is Admin Realm, insert Domain Name (winsrv.group4.com). Lastly, for Domain Local Realm, insert Domain Name (winsrv.group4.com).

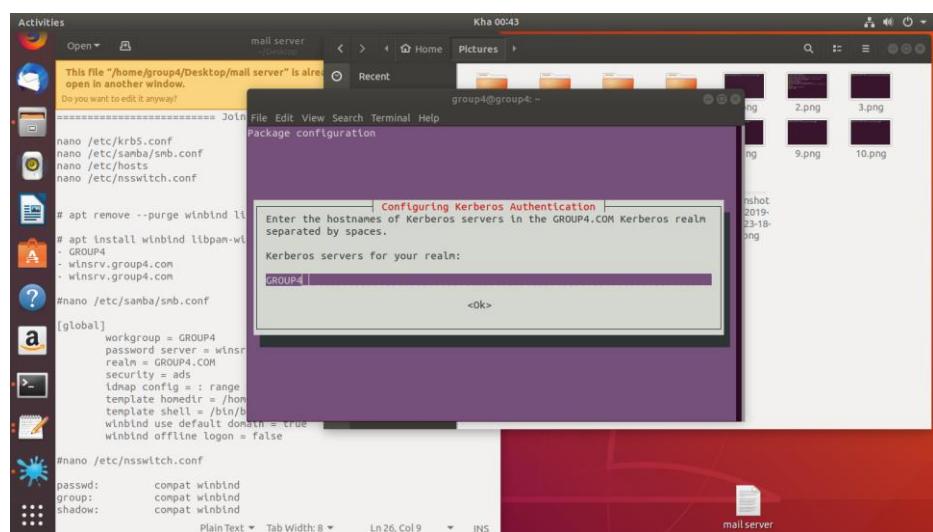
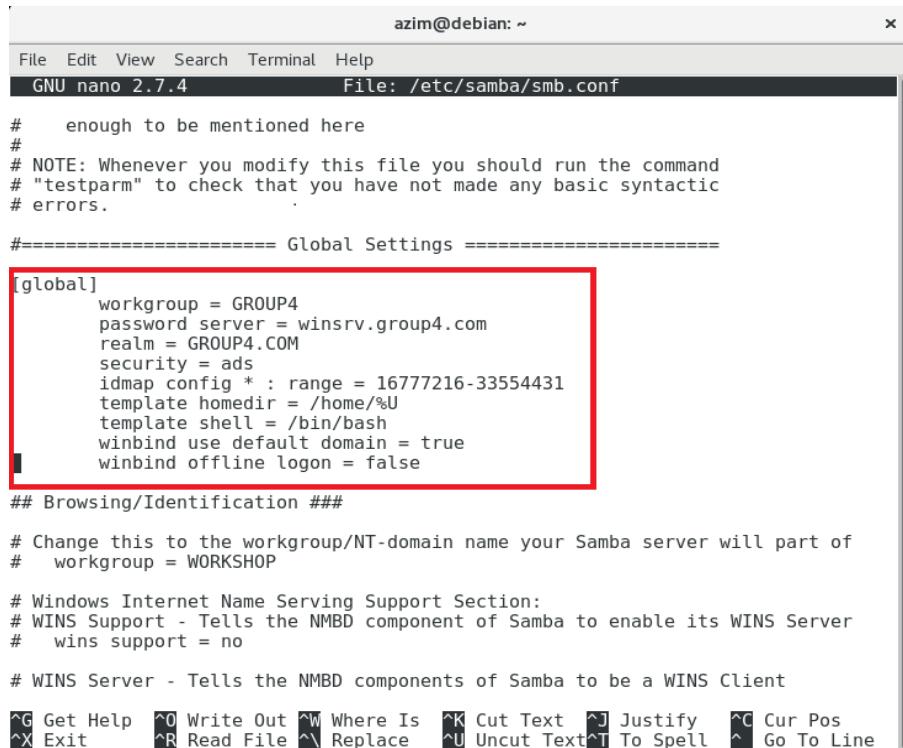


Figure 5.3.24 2: Insert requirement for installation

Step 4 : After successfully installed, on the terminal, enter command “nano /etc/samba/smb.conf” to edit Global Setting. Then, save the setting.



```

azim@debian: ~
File Edit View Search Terminal Help
GNU nano 2.7.4          File: /etc/samba/smb.conf

#     enough to be mentioned here
#
# NOTE: Whenever you modify this file you should run the command
# "testparm" to check that you have not made any basic syntactic
# errors.

#===== Global Settings =====

[global]
workgroup = GROUP4
password server = winsrv.group4.com
realm = GROUP4.COM
security = ads
idmap config * : range = 16777216-33554431
template homedir = /home/%U
template shell = /bin/bash
winbind use default domain = true
winbind offline logon = false

## Browsing/Identification ##

# Change this to the workgroup/NT-domain name your Samba server will part of
# workgroup = WORKSHOP

# Windows Internet Name Serving Support Section:
# WINS Support - Tells the NMBD component of Samba to enable its WINS Server
#   wins support = no

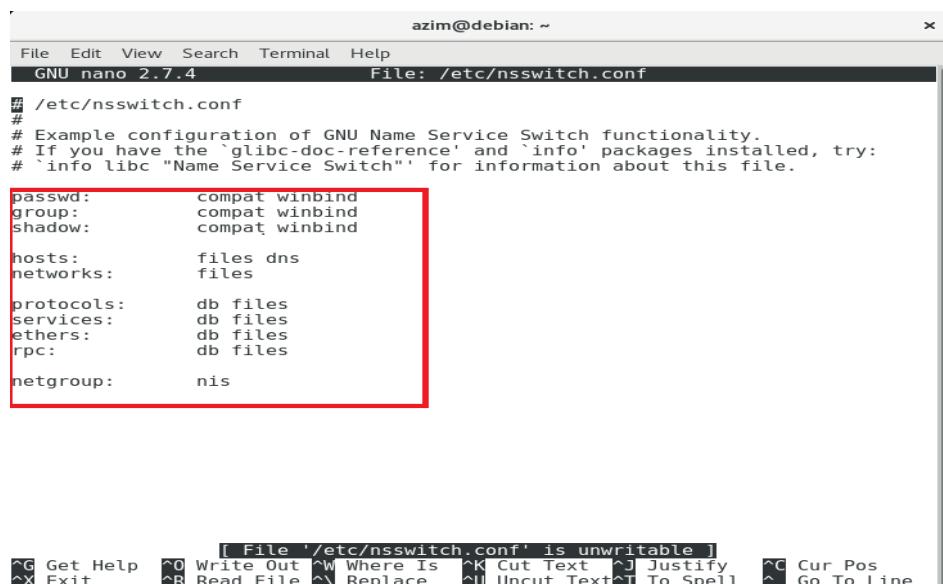
# WINS Server - Tells the NMBD components of Samba to be a WINS Client

^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 5.3.24 3: Setting on Global Setting

Step 5: Next, on the new terminal, insert command “nano /etc/nsswitch.conf”. Change the setting by following figure below. Then, save the file.



```

azim@debian: ~
File Edit View Search Terminal Help
GNU nano 2.7.4          File: /etc/nsswitch.conf

# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference` and `info` packages installed, try:
# `info libc "Name Service Switch"` for information about this file.

passwd:      compat winbind
group:       compat winbind
shadow:      compat winbind

hosts:        files dns
networks:    files

protocols:   db files
services:    db files
ethers:      db files
rpc:         db files

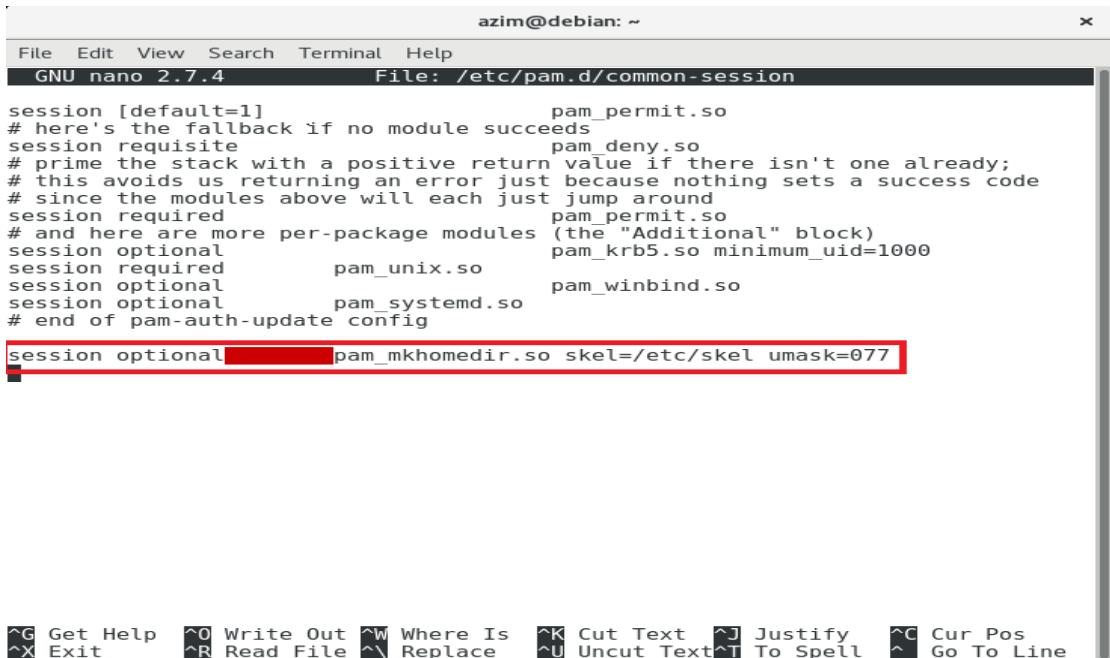
netgroup:    nis

[ File '/etc/nsswitch.conf' is unwritable ]
^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 5.3.24 4: Setting the nsswitch.conf file

Step 6: Next, on the new terminal, insert command “nano /etc/pam.d/common-session”. Add “session optional pam_mkhomedir.so skel=/etc/skel umask=077” on the config file. Then, save the file.



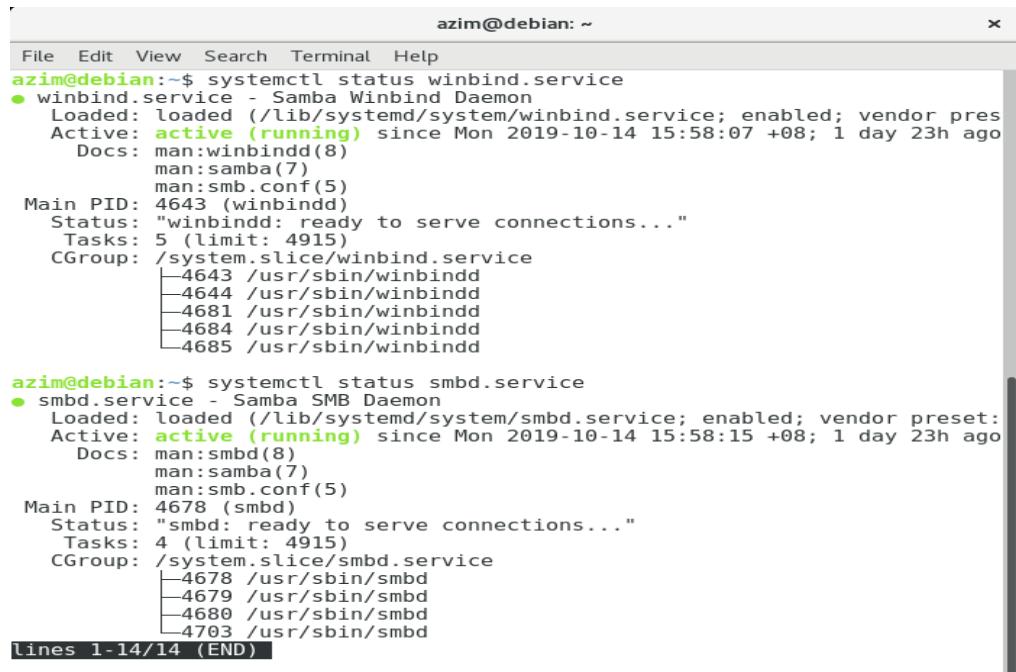
```
azim@debian: ~
File Edit View Search Terminal Help
GNU nano 2.7.4 File: /etc/pam.d/common-session

session [default=1] pam_permit.so
# here's the fallback if no module succeeds
session requisite pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
session required pam_permit.so
# and here are more per-package modules (the "Additional" block)
session optional pam_krb5.so minimum_uid=1000
session required pam_unix.so
session optional pam_winbind.so
session optional pam_systemd.so
# end of pam-auth-update config

session optional pam_mkhomedir.so skel=/etc/skel umask=077
```

Figure 5.3.24 5: Adding session option in common-session file

Step 7: Restart winbind service and smbd service. Verify the service status is active.



```
azim@debian: ~
File Edit View Search Terminal Help
azim@debian:~$ systemctl status winbind.service
● winbind.service - Samba Winbind Daemon
  Loaded: loaded (/lib/systemd/system/winbind.service; enabled; vendor pres
  Active: active (running) since Mon 2019-10-14 15:58:07 +08; 1 day 23h ago
    Docs: man:winbindd(8)
          man:samba(7)
          man:smb.conf(5)
 Main PID: 4643 (winbindd)
   Status: "winbindd: ready to serve connections..."
      Tasks: 5 (limit: 4915)
     CGroup: /system.slice/winbind.service
             └─4643 /usr/sbin/winbindd
                  ├─4644 /usr/sbin/winbindd
                  ├─4681 /usr/sbin/winbindd
                  ├─4684 /usr/sbin/winbindd
                  ├─4685 /usr/sbin/winbindd

azim@debian:~$ systemctl status smbd.service
● smbd.service - Samba SMB Daemon
  Loaded: loaded (/lib/systemd/system/smbd.service; enabled; vendor preset:
  Active: active (running) since Mon 2019-10-14 15:58:15 +08; 1 day 23h ago
    Docs: man:smbd(8)
          man:samba(7)
          man:smb.conf(5)
 Main PID: 4678 (smbd)
   Status: "smbd: ready to serve connections..."
      Tasks: 4 (limit: 4915)
     CGroup: /system.slice/smbd.service
             ├─4678 /usr/sbin/smbd
             ├─4679 /usr/sbin/smbd
             ├─4680 /usr/sbin/smbd
             ├─4703 /usr/sbin/smbd

lines 1-14/14 (END)
```

Figure 5.3.24 6: Verifying status is active

Step 8: After successfully configuring the config file, join the domain by insert command “net ads join -U Administrator”.

```
azim@debian:~$ net ads join -U Administrator
```

Figure 5.3.24 7: Command to join domain

Step 9: Debian is added inside the computer file of Active Directory Users and Computers in Windows Server 2012

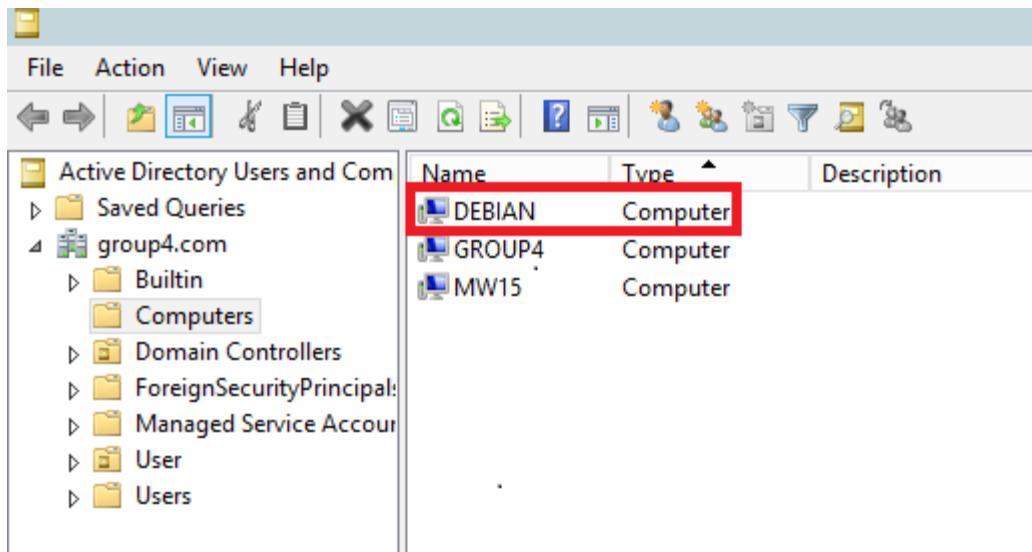


Figure 5.3.24 8: AD Users and Computer addition of Debian

5.3.25 Windows Server Hardening

Step 1: Go to Start > Administrative Tools > Security Configuration Wizard.

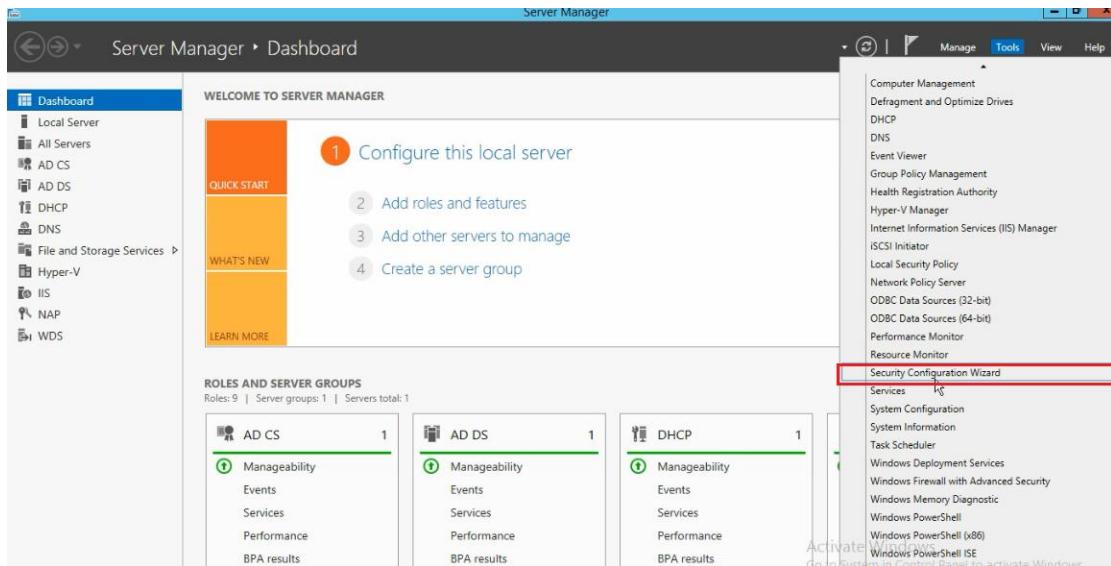


Figure 5.3.25.1: Server Manager Dashboard

Step 2: This is the open page of the Security Configuration Wizard. Click “Next” to go to the next page.



Figure 5.3.25 2: Security configuration wizard

Step 3: Select create a new security policy and click “Next”.



Figure 5.3.25 3: Create new security policy

Step 4: Insert the Server Name and click “Next”.

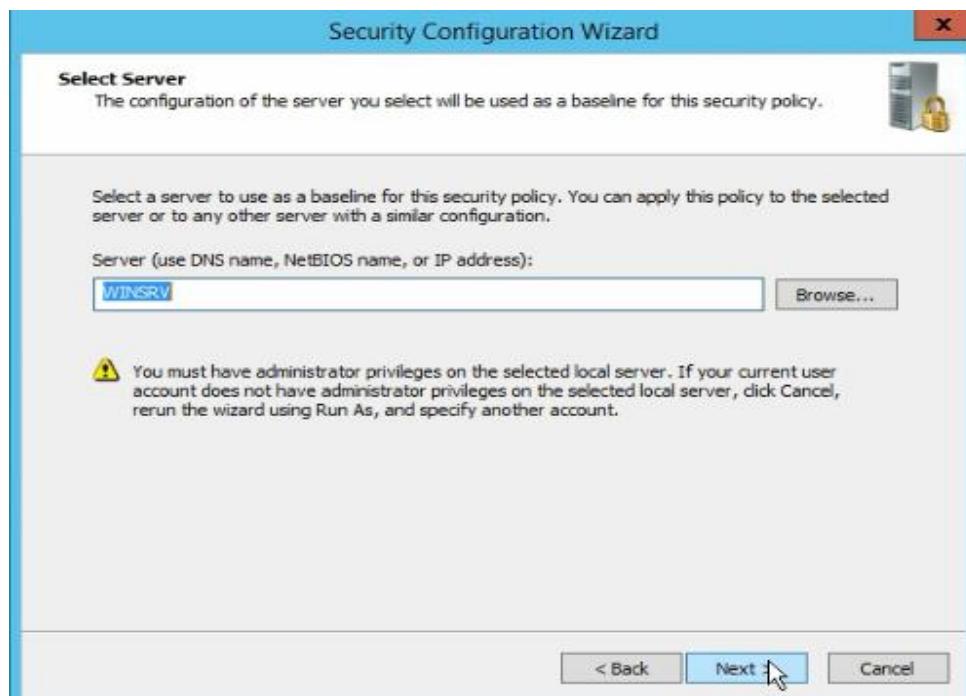


Figure 5.3.25 4: Insert Server name

Step 5: Wait until the processing complete and after its completed, click “Next”.



Figure 5.3.25 5: Complete the processing

Step 6: Role-Based Service Configuration will be shown up and click “Next”.

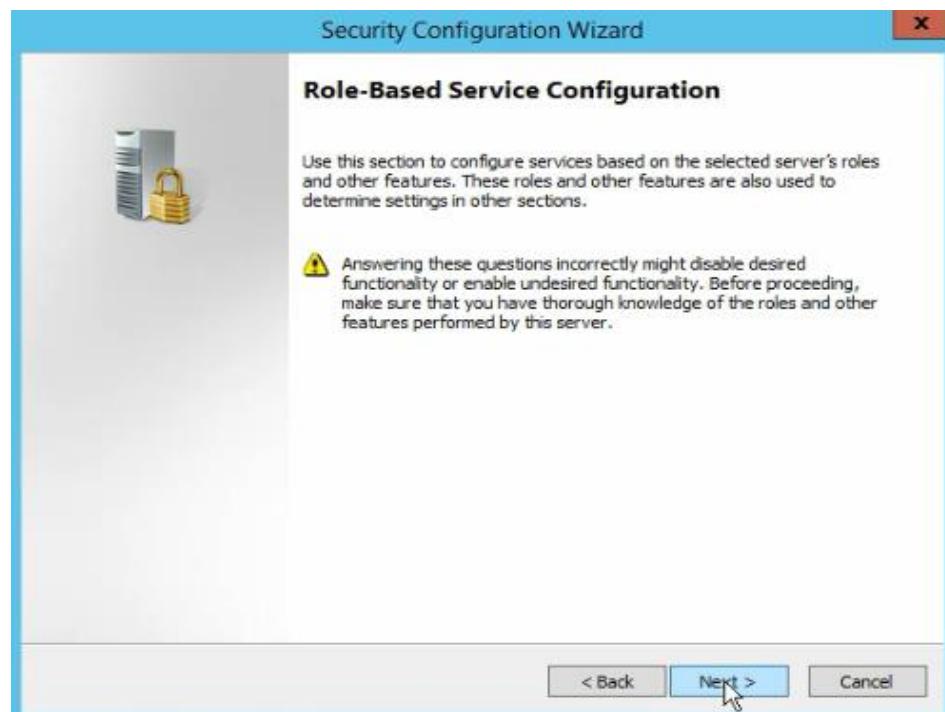


Figure 5.3.25 6: Role-based service configuration

Step 7: Select the server roles that the selected server performs and click “Next”.

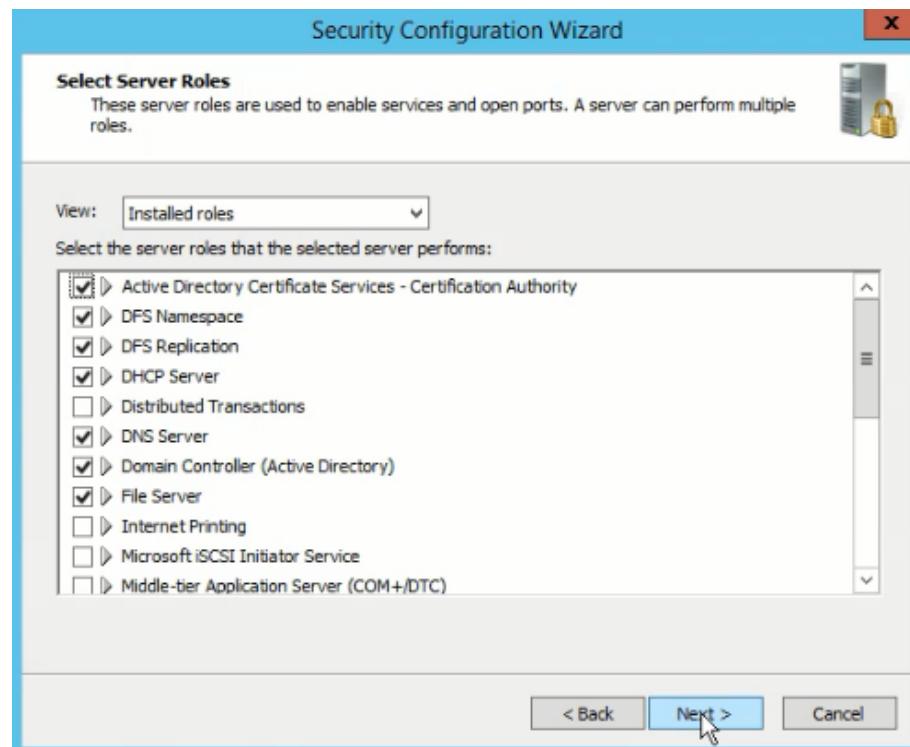


Figure 5.3.25 7: Select server roles



Figure 5.3.25 8: Select server roles

Step 8: Select the client features that the selected server performs. Then, click “Next”.



Figure 5.3.25 9: Select client features

Step 9: Select the options used to administrate the selected server and click “Next” > “Next” > “Next”.

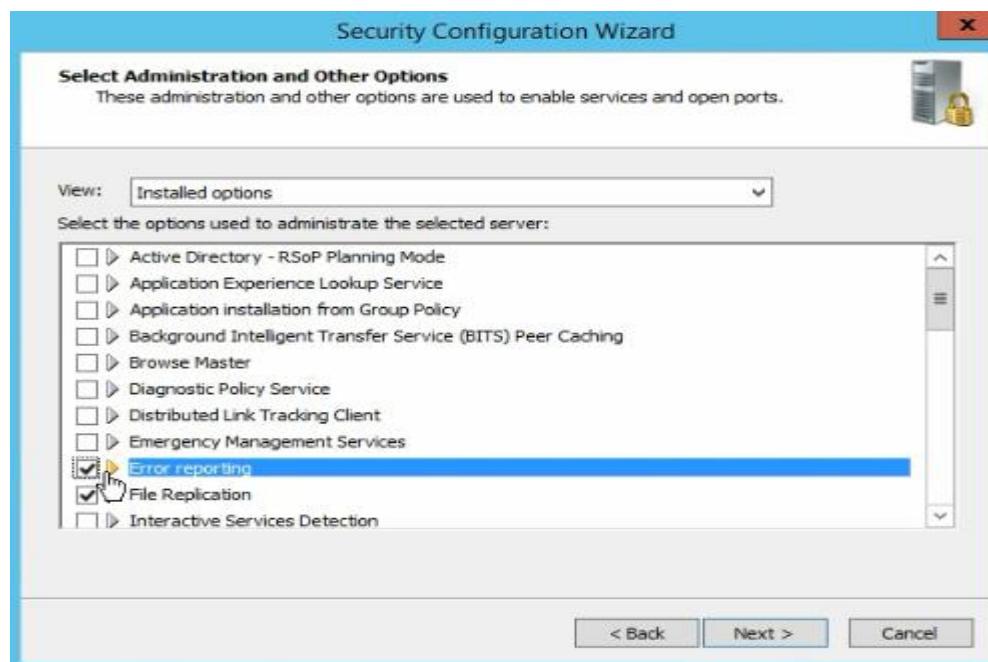


Figure 5.3.25 10: Select options used to administrate the selected server

Step 10: Select the additional services that the selected server requires and click “Next”.

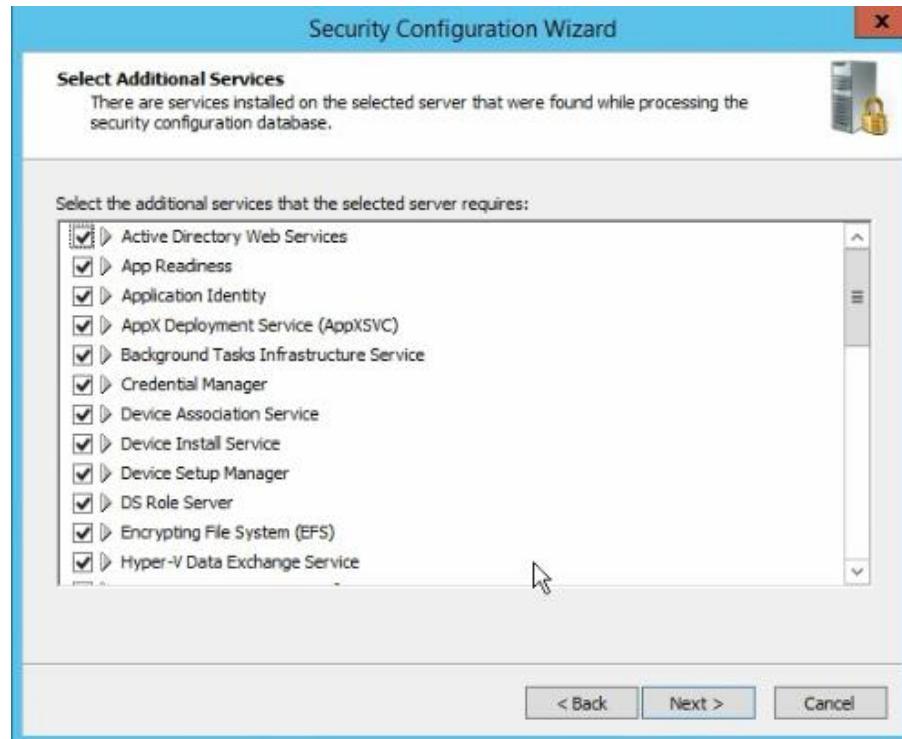


Figure 5.3.25.11: Select Additional services

Step 11: Select the “Do not change the start-up mode of the service” and click “Next”.

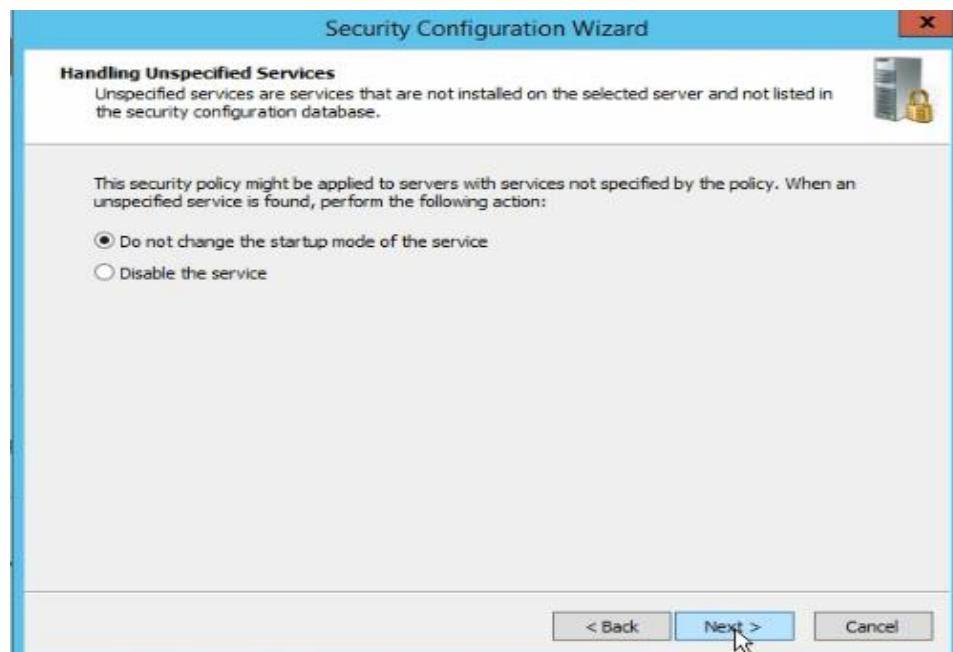


Figure 5.3.25.12: Select Handling Unspecified Services

Step 12: Confirm the service changes then click “Next”.

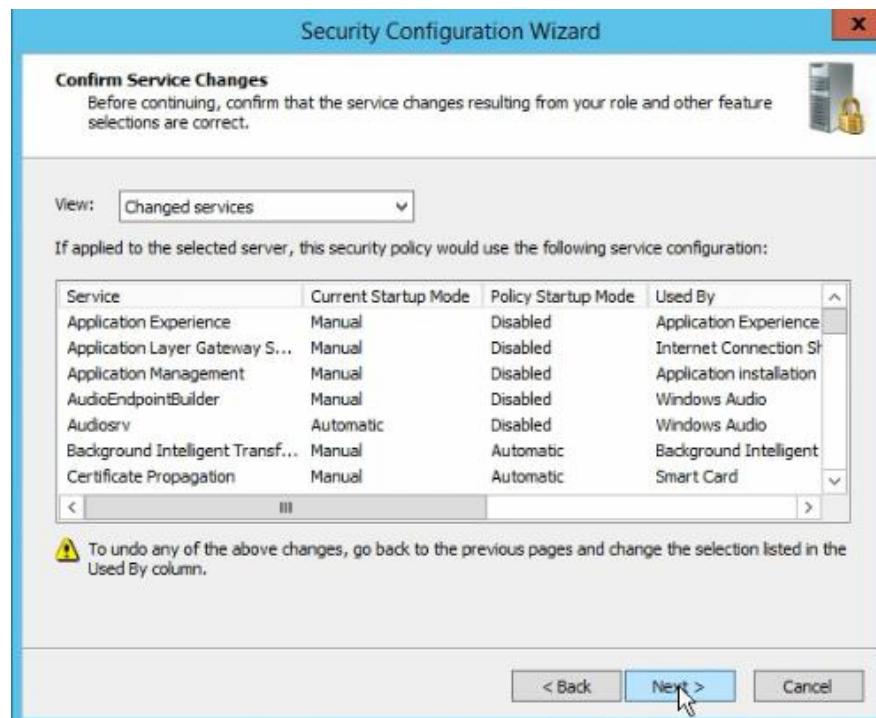


Figure 5.3.25.13: Confirm service changes

Step 13: The first page of Network Security will show and click “Next”.



Figure 5.3.25.14: Network security first page

Step 14: Select the network security rules and click “Next”.

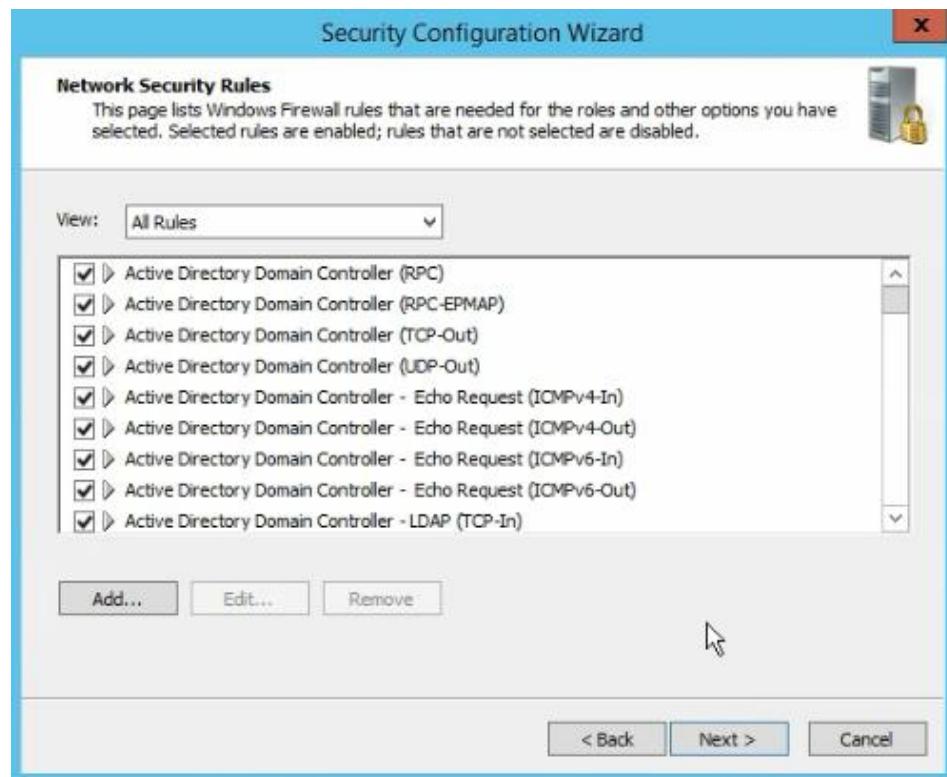


Figure 5.3.25.15: Select network security rules

Step 15: The first page of the registry setting will be shown up. Then, click “Next”.



Figure 5.3.25.16: Registry setting first page

Step 16: Select the attributes that is needed for the Server Maessage Block (SMB) Security Signatures and click “Next”.



Figure 5.3.25.17: Select attributes needed for SMB Security Signature

Step 17: Determines whether LDAP Signing is required by the security policy and click “Next”.

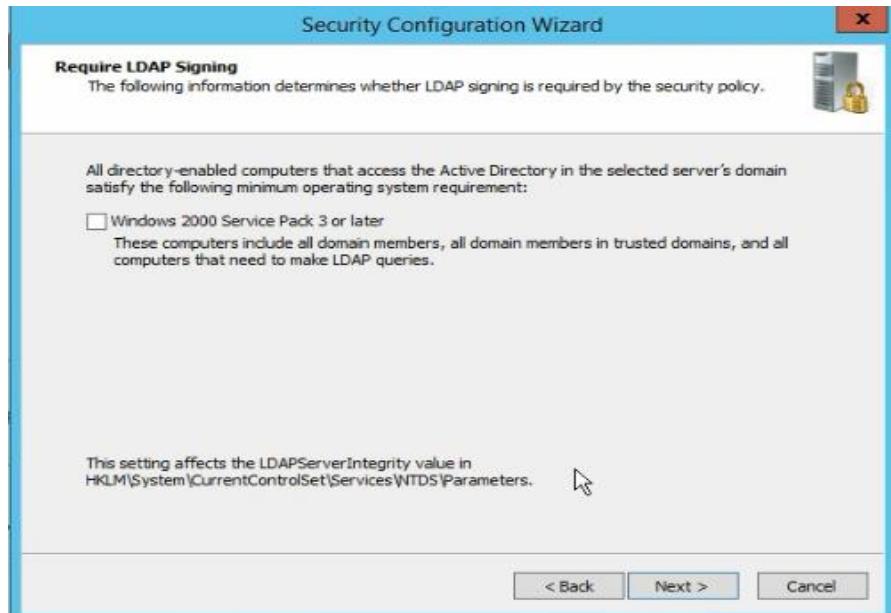


Figure 5.3.25.18: Determine: LDAP Signing

Step 18: Select the Domain Accounts as the methods uses to authenticate with remote computers and click “Next”.

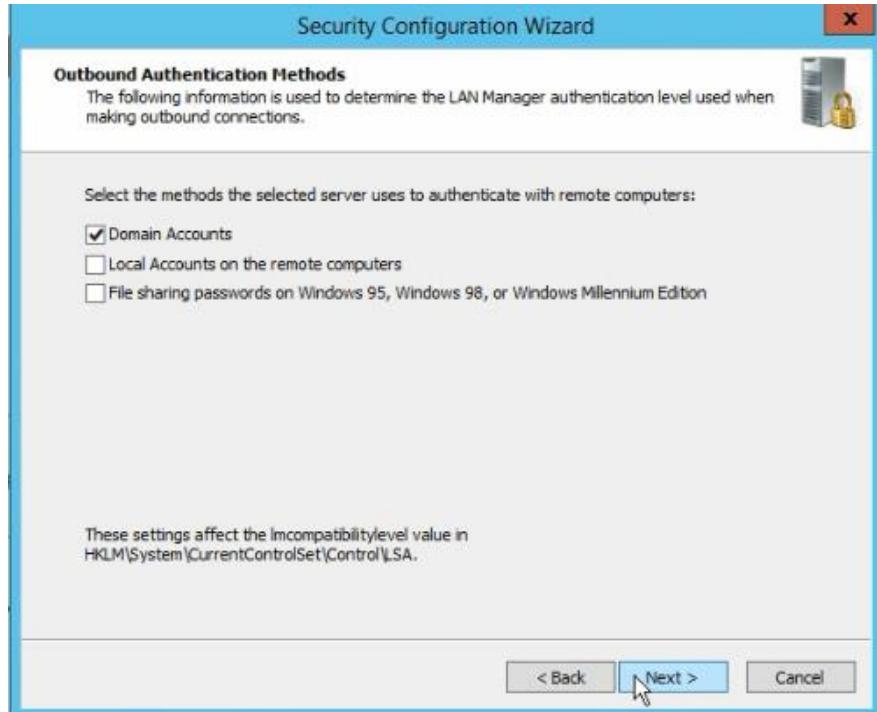


Figure 5.3.25.19: Select outbound authentication method

Step 19: Select Windows NT 4.0 Service Pack 6a or later operating systems and then click “Next”.

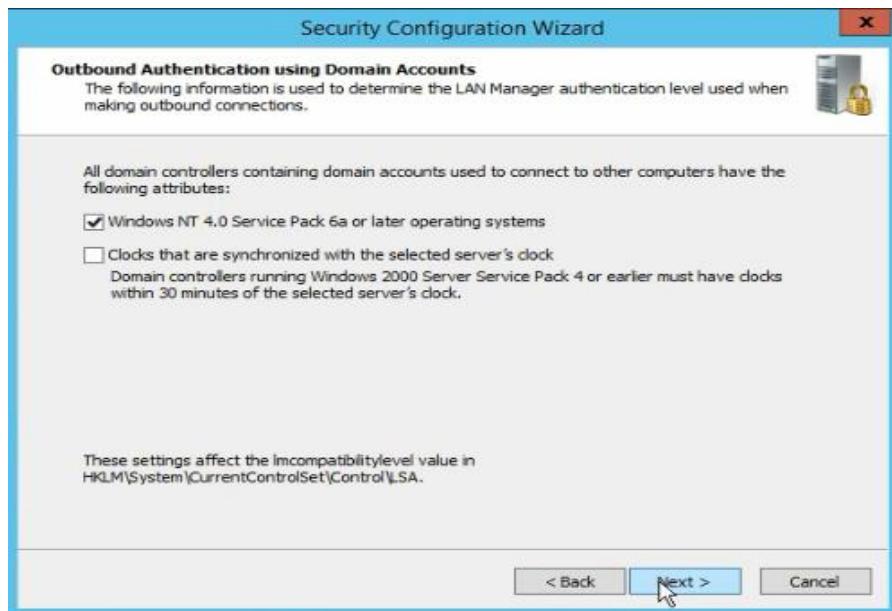


Figure 5.3.25.20: Select outbound authentication using Domain Accounts

Step 20: Then, it will show the registry settings summary and click “Next”.

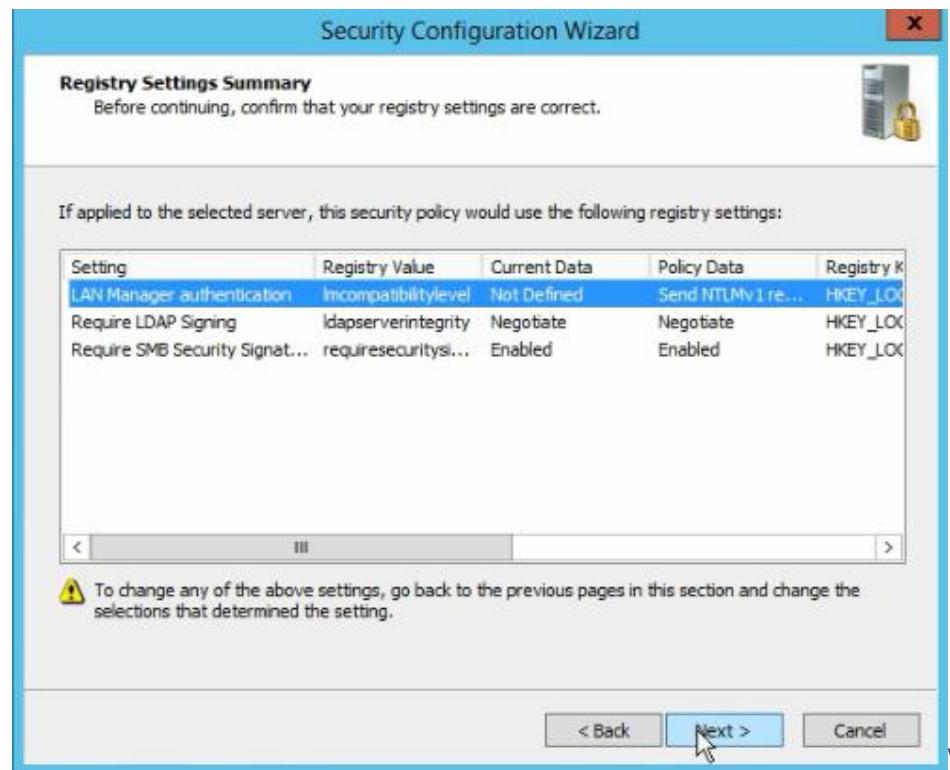


Figure 5.3.25.21: Registry setting summary

Step 21: The first page of the Audit Policy will be shown. Then, click “Next”.



Figure 5.3.25.22: First page of Audit Policy

Step 22: Then, select the “Audit successful and unsuccessful activities”. Then, click “Next”.



Figure 5.3.25.23: Select system audit policy

Step 23: This page shows the summary of the audit policy. Then, click “Next”.

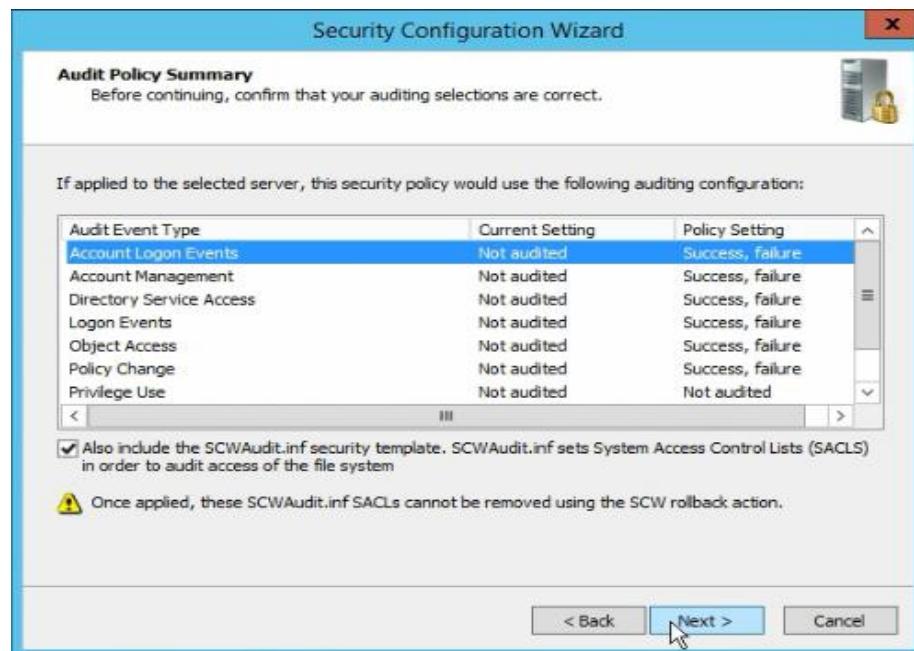


Figure 5.3.25.24: Summary of audit policy

Step 24: This page show that the security policy has been save. Then, click “Next”.



Figure 5.3.25.25: Saving Security policy

Step 25: Save the name and location for the security policy file. Then, click “Next”.



Figure 5.3.25.26: Saving the policy name and file location

Step 26: Then, select Apply Now to apply the security policy and click “Next”.



Figure 5.3.25.27: Select to apply security policy

Step 27: This page show that Security Configuration Wizard has been completed successful. Then, click “Next”.

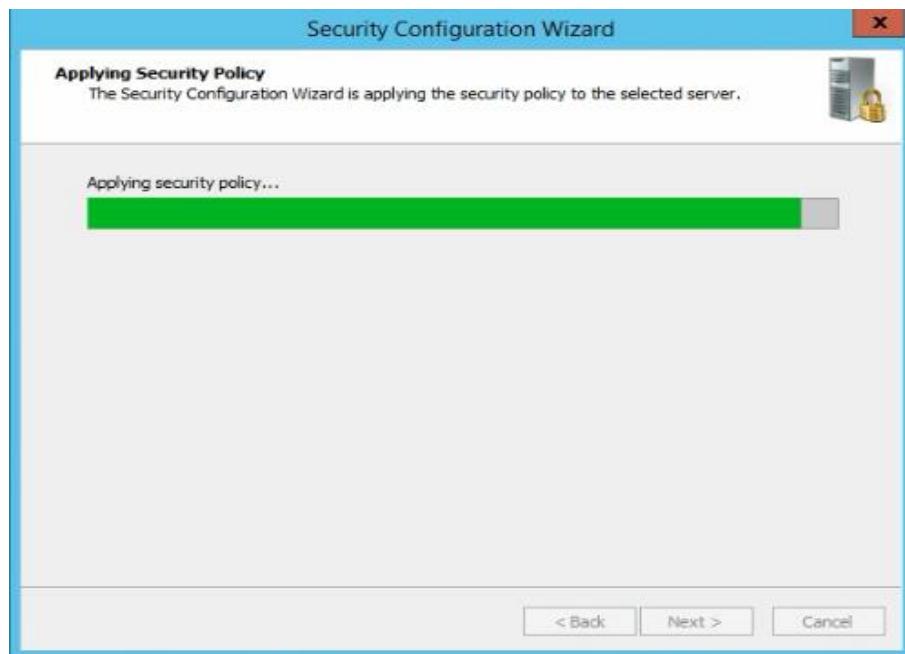


Figure 5.3.25.28: Security Configuration Wizard has completed

Disable or Delete Unnecessary Accounts

Step 1: Go to Server Manager > Active Directory Domain Service > Active Directory Users and Computers > group4.com > Users.

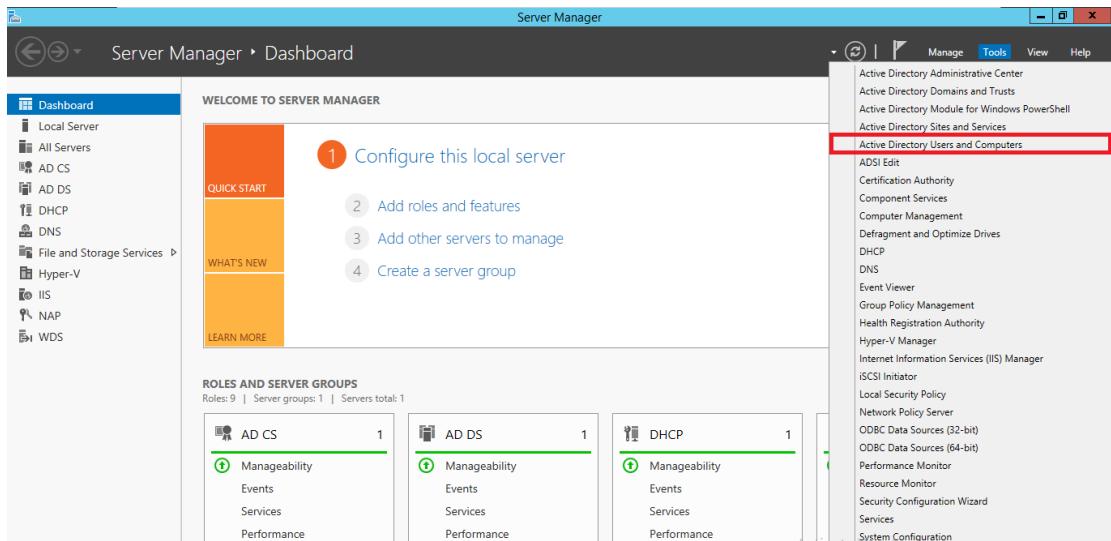


Figure 5.3.25.29: Server Manager Dashboard

Step 2: Right click “hafiz” and choose “Disable Account”.

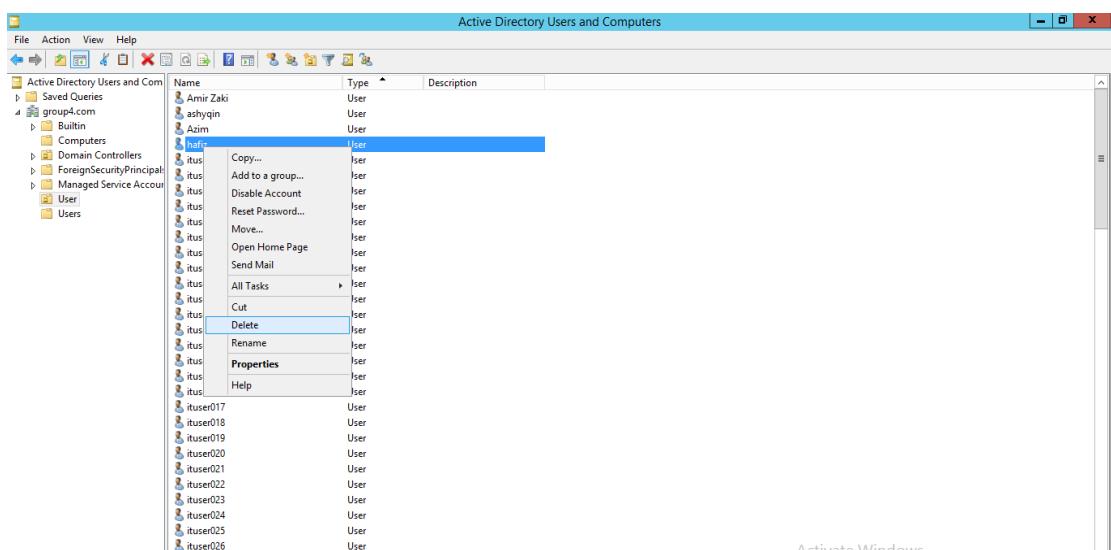


Figure 5.3.25.30: Disable account for hafiz

Configuring Auditing

Step 1: Go to Start > Administrative Tools > Local Security Policy.

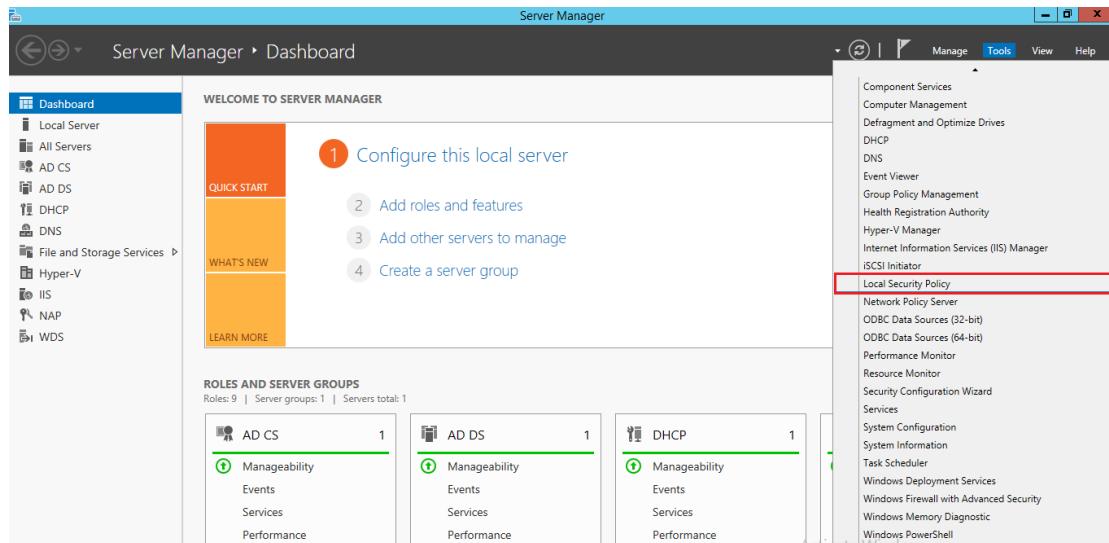


Figure 5.3.25.31: Local security policy

Step 2: Go to Security Setting > Local Policies > Audit Policies

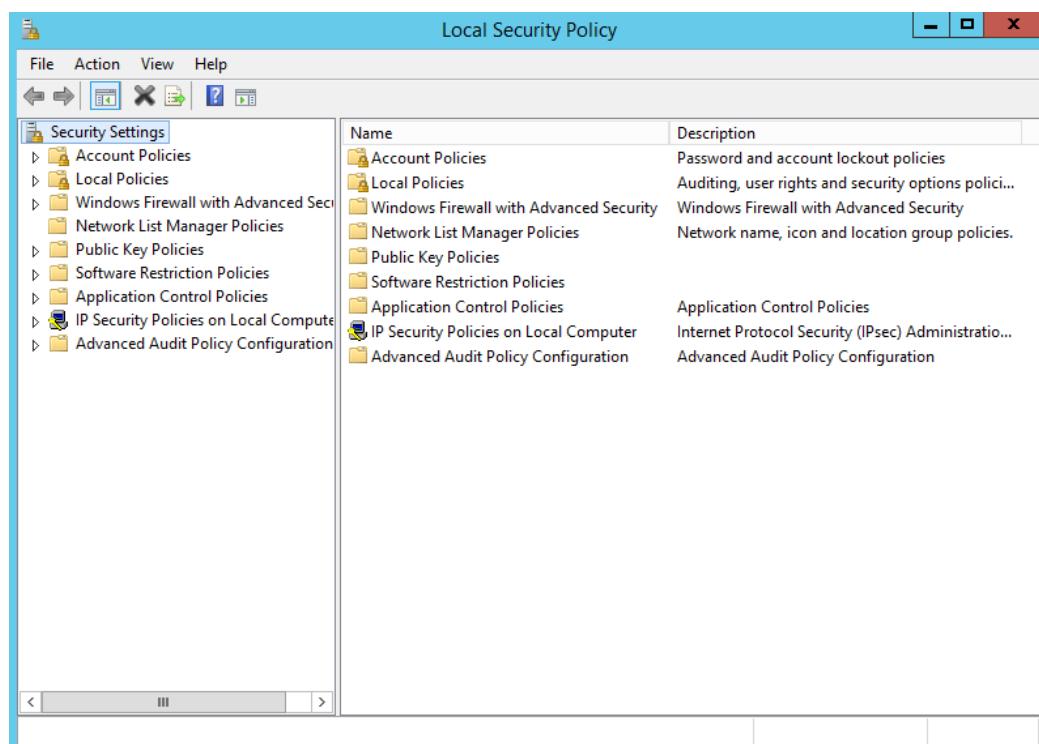


Figure 5.3.25.32: Audit Policy

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”.

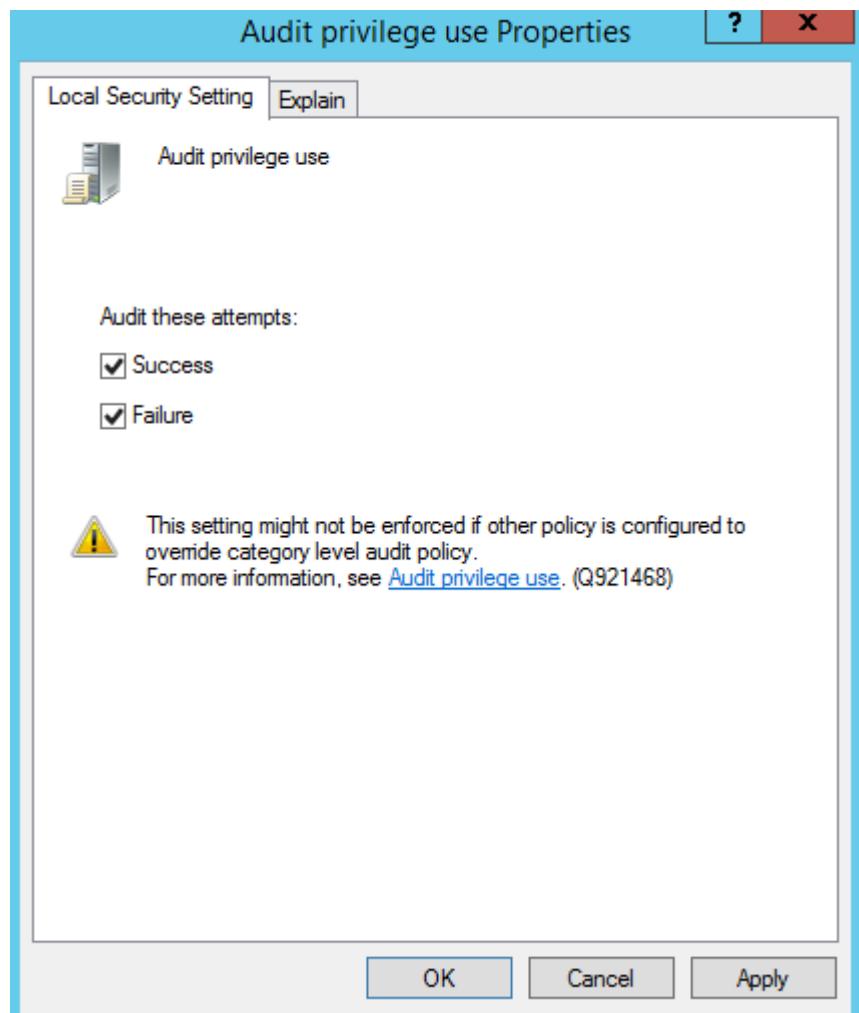


Figure 5.3.25.33: Local security setting for audit privilege use

Updates and Patches

Step 1: Go to Start > Windows Update.

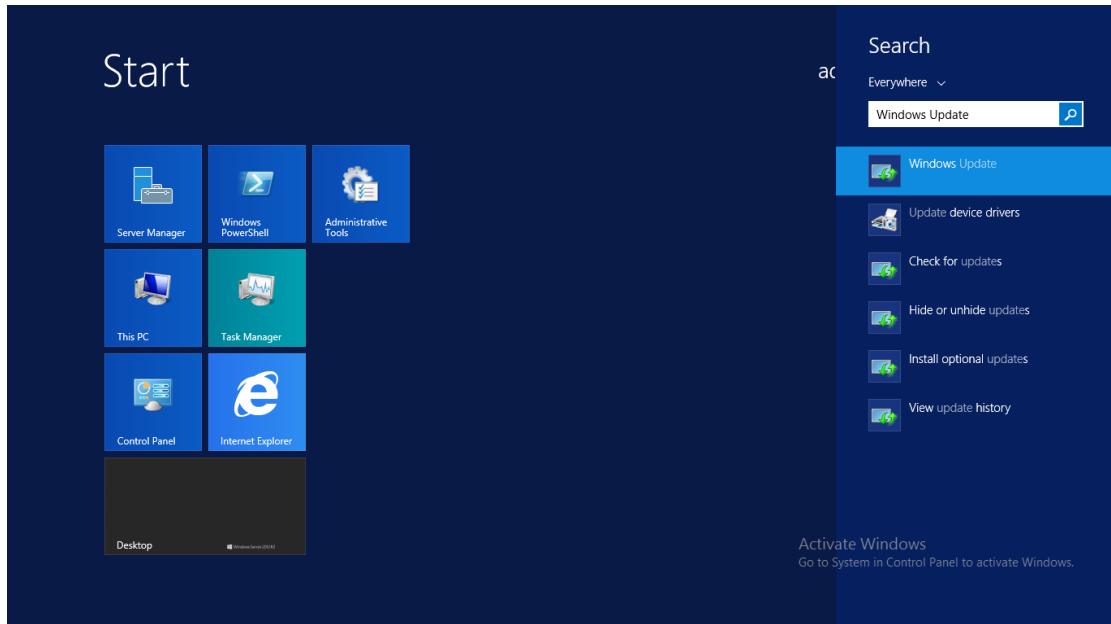


Figure 5.3.25.34: Search for Windows Update

Step 2: Change the setting become “Install Updates Automatically” and click “OK”.

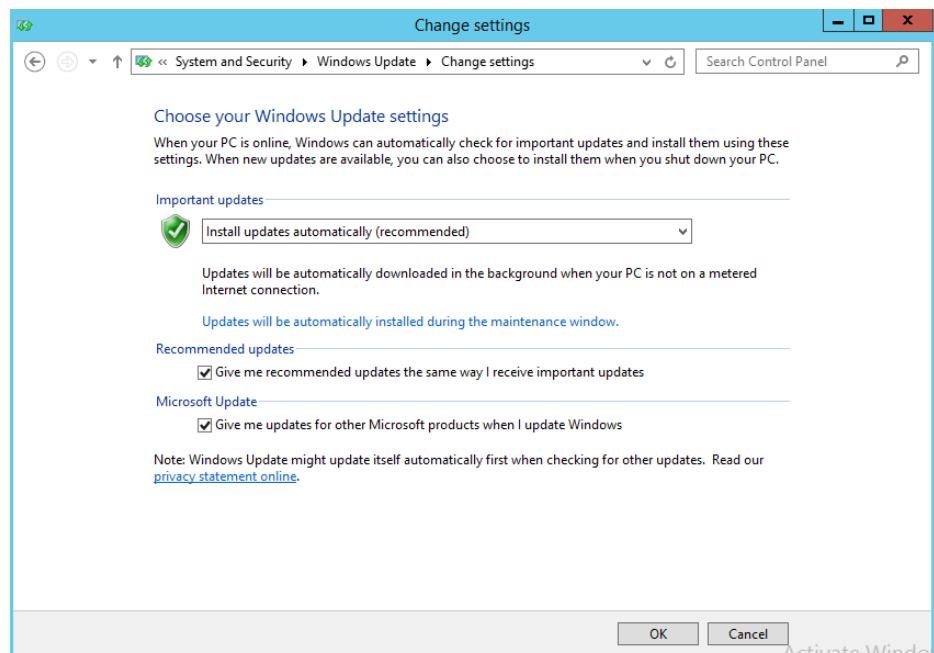


Figure 5.3.25.35: Change the setting of installation updates

Step 3: Check for view available updates to check the updates and install new updates.



Figure 5.3.25.36: Check for available updates

Enable Windows Firewall

Step 1: Open Windows Firewall with Advanced Security

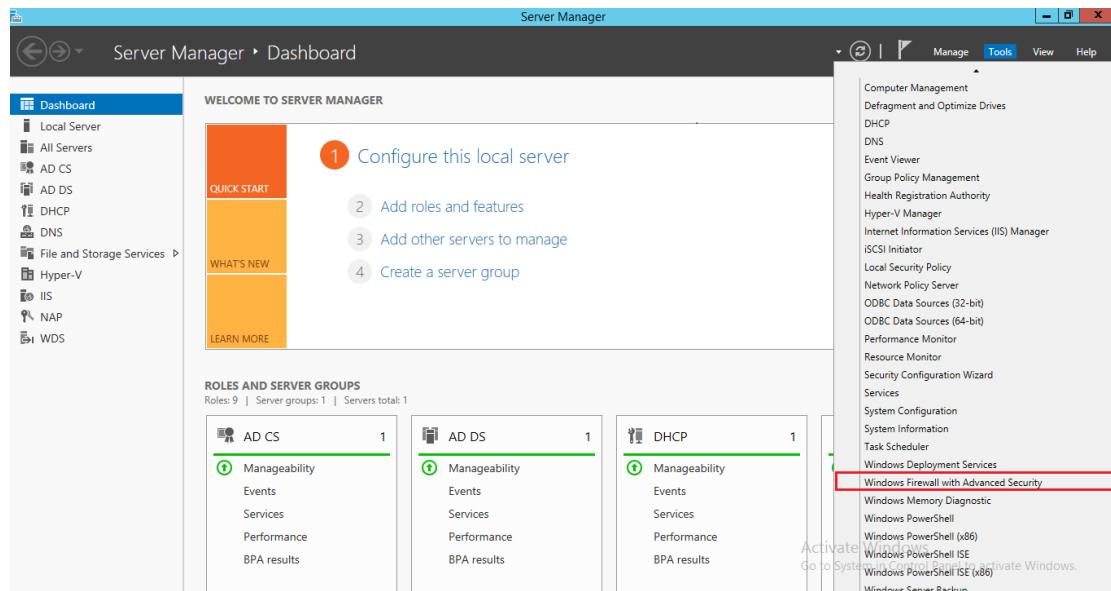


Figure 5.3.25.37: Server Manager Dashboard

Step 2: Enable the firewall.

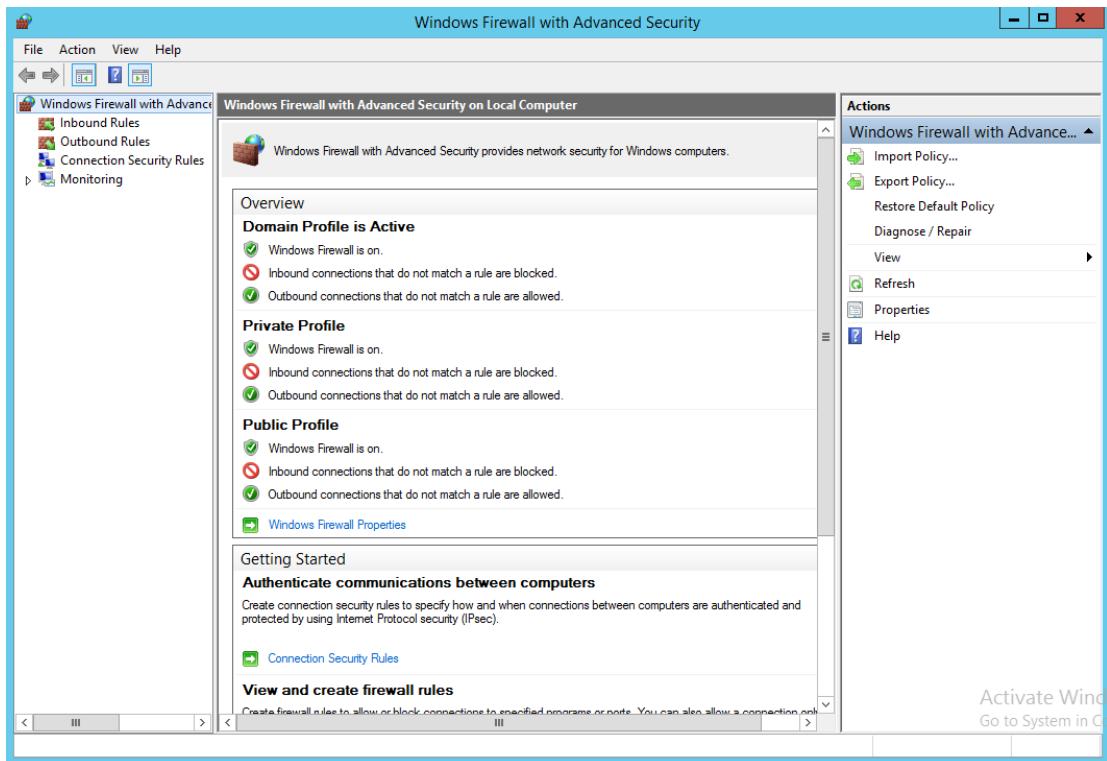


Figure 5.3.25.38: Enabling firewall

Disable Automatic Services

Step 1: Go to start and open “Run”, type in “services.msc” to open Services.

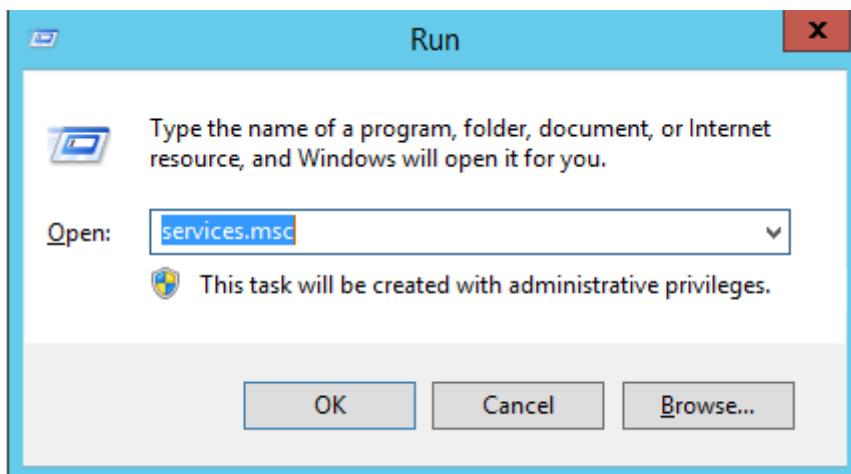


Figure 5.3.25.39: Search for services.msc

Step 2: Change the Startup Type of Distributed Transaction Coordinator Properties from Automatic to Disabled.

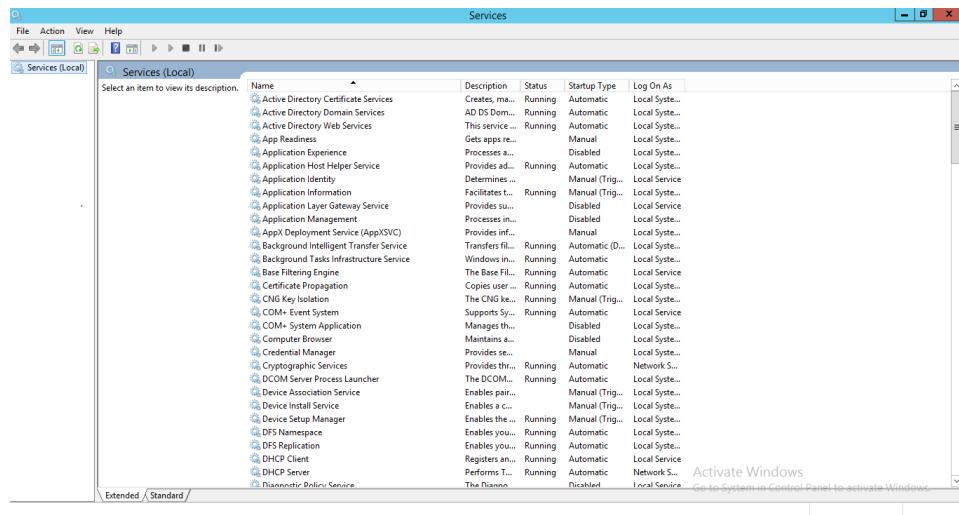


Figure 5.3.25.40: Change the Startup Type of Distributed Transaction Coordinator Properties

Step 3: Change the Startup Type of KtmRm for Distributed Transaction Coordinator Properties from Automatic to Disabled.

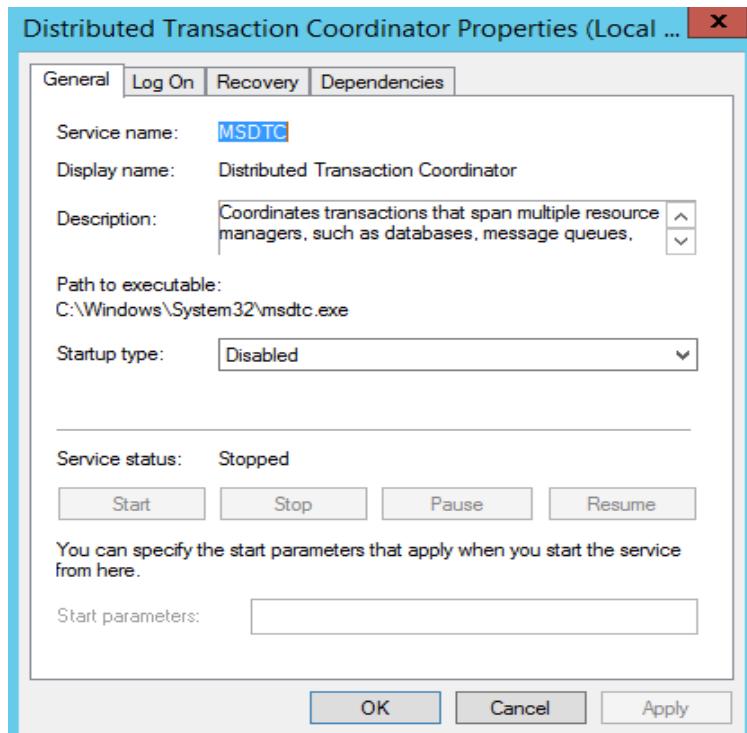


Figure 5.3.25.41: Change the Startup Type of KtmRm for Distributed Transaction Coordinator Properties

Enable Automatic Services

Step 1: Go to “Start” and open “Run”. Then, type in “services.msc” to open services.

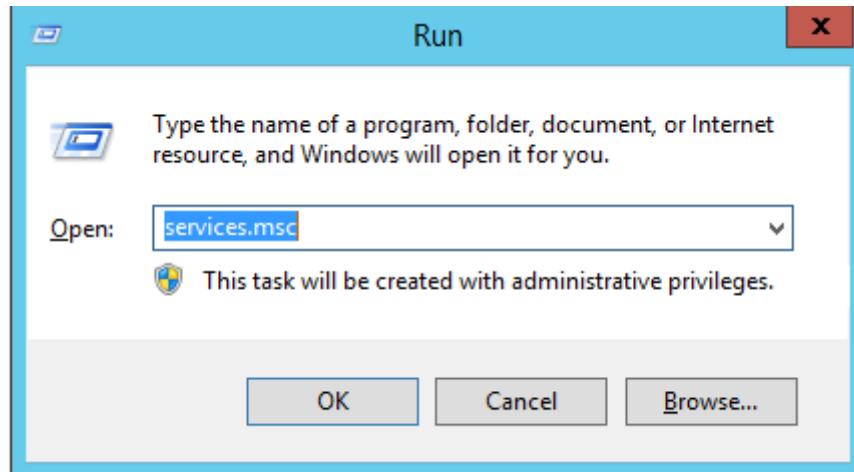


Figure 5.3.25.42: Search for Services.msc

Step 2: Change the Startup Type of Windows Error Reporting Service to “Automatic” and start the service

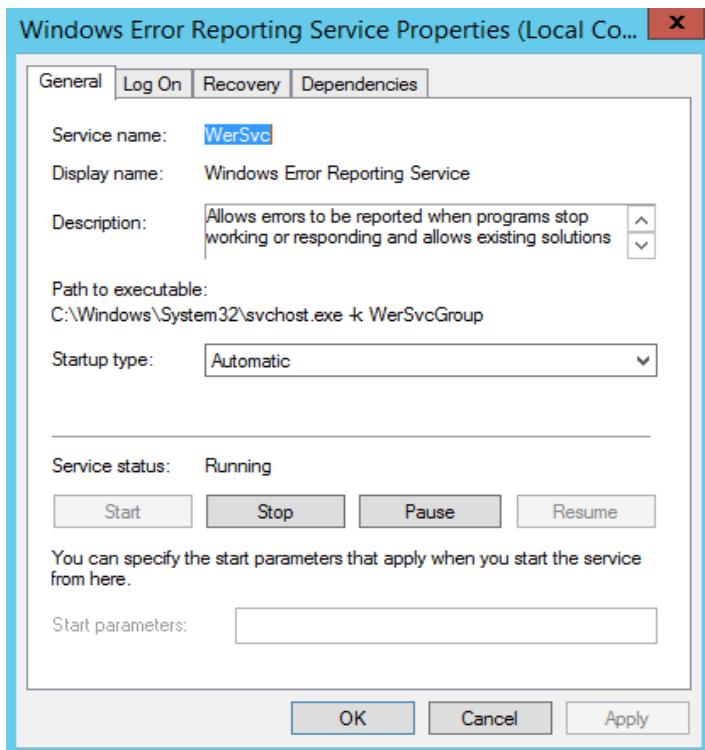


Figure 5.3.25.43: Change the Startup Type of Windows Error Reporting Service

Step 3: Change the Startup Type of Secure Socket Tunneling Protocol Service Properties to “Automatic” and start the service.

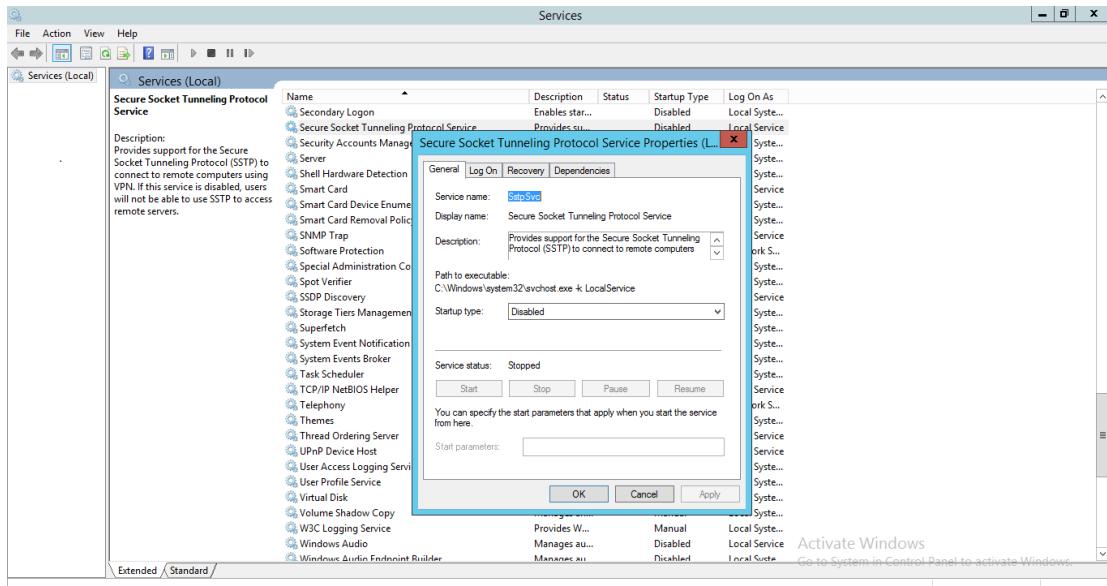


Figure 5.3.25.44: Change the Startup Type of Secure Socket Tunneling Protocol Service Properties

Step 4: Change the Startup Type of Certificate Propagation Service Properties to “Automatic” and start the service.

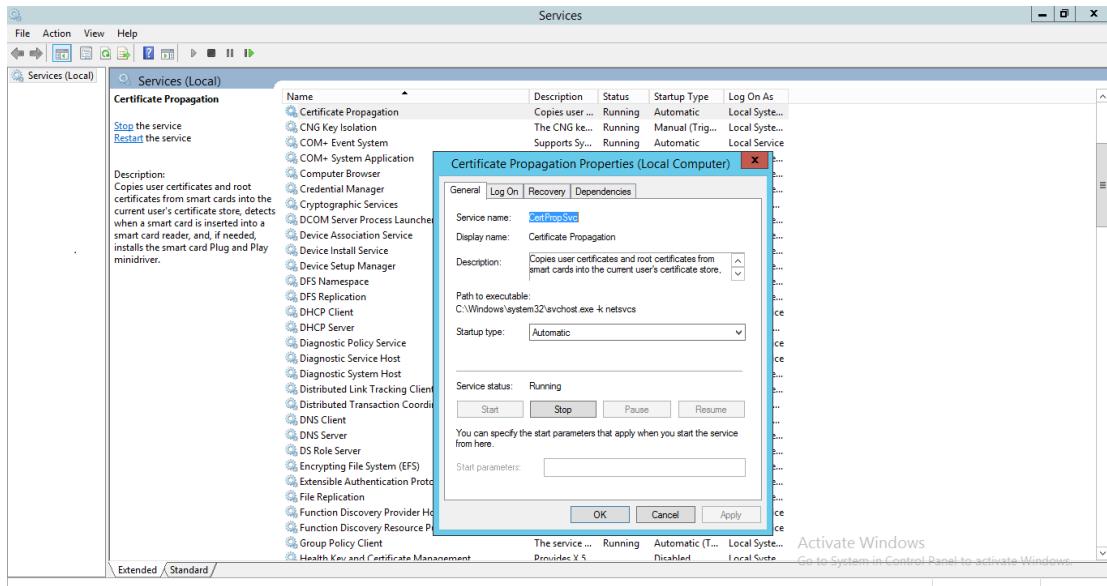


Figure 5.3.25.45: Change the Startup Type of Certificate Propagation Service Properties

Step 5: Change the Startup Type of Netlogon Service Properties to “Automatic” and start the service.

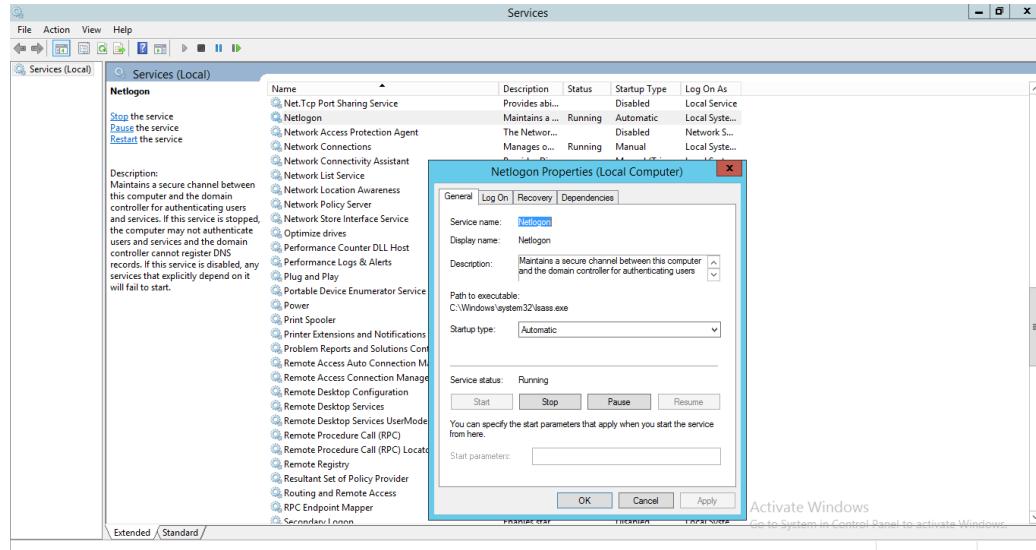


Figure 5.3.25.46: Change the Startup Type of Netlogon Service Properties

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.

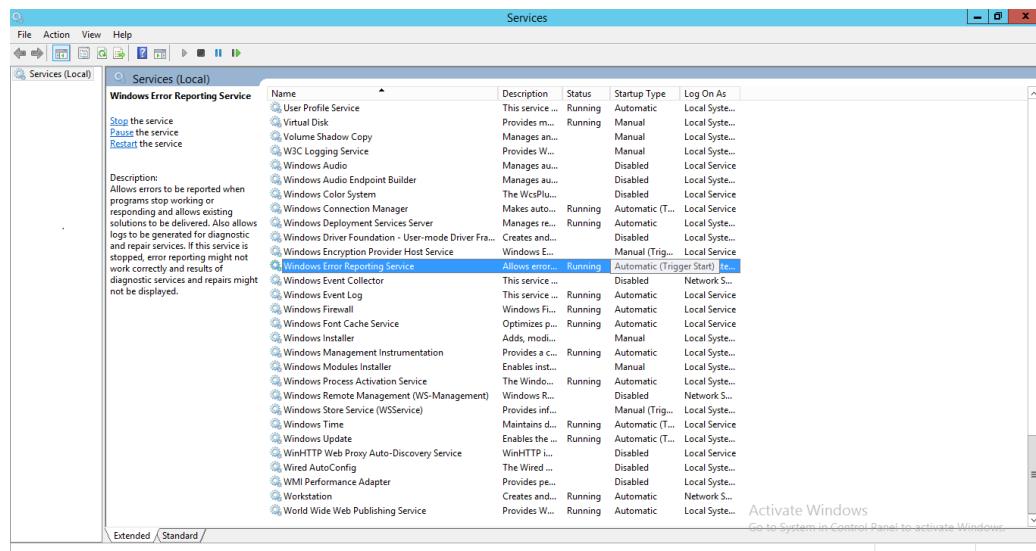


Figure 5.3.25.47: Windows Error Reporting

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.

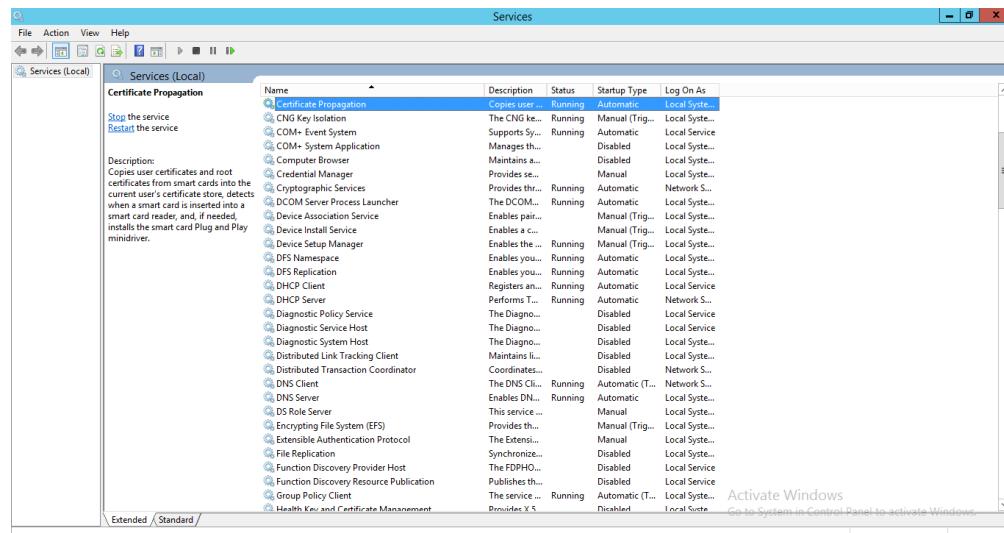


Figure 5.3.25.48: Check the status of Certificate Propagation

Step 3: Ensure NetLogon startup is Automatic and started. This maintains a channel between computer and domain controller. The NetLogon sub-key stores information for the NetLogon service. The NetLogon service verifies log-on request and it registers, authenticates and locates domain controllers.

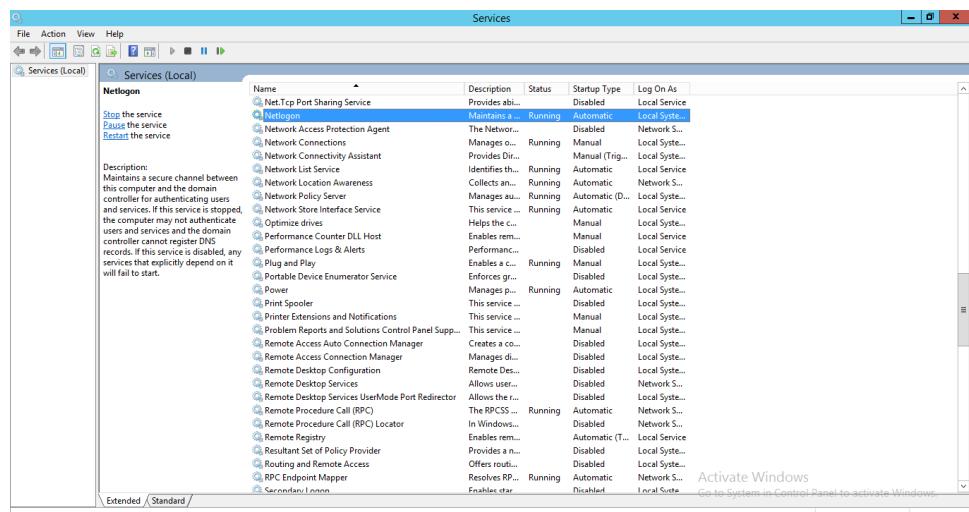


Figure 5.3.25.49: Checking on NetLogon startup type

5.3.26 IPSec VPN server for remote employees

SoftEther VPN Server Installation

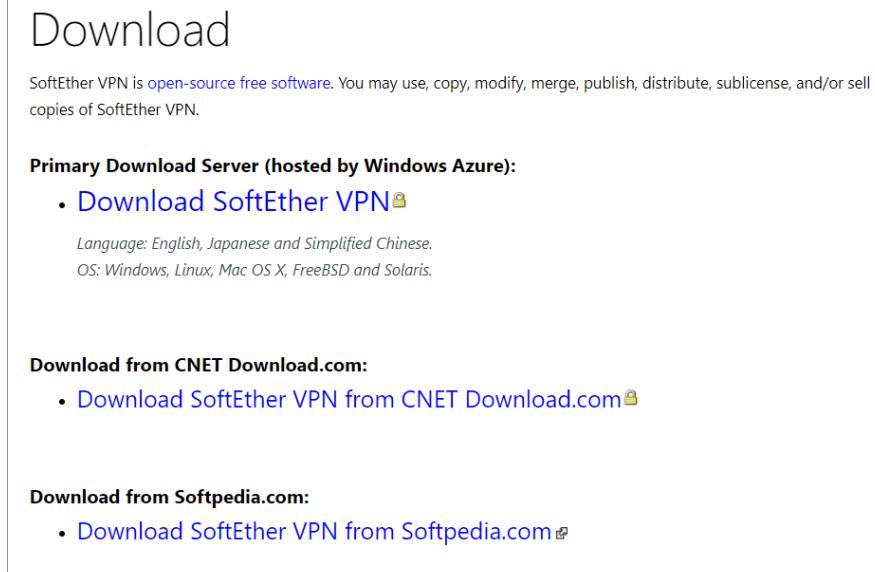
Step 1: Access to <https://www.softether.org/5-download> and select **Download** button.



The screenshot shows the official SoftEther VPN Project website. The navigation bar includes links for Top, Why SoftEther VPN, Documents, Download, Support, and About Project. The main content area is titled "SoftEther VPN Project" and discusses the project's development and distribution of the SoftEther VPN program. A sidebar on the left contains a "Table of contents" with various VPN-related topics. The "Download" link in the sidebar is circled in red.

Figure 5.3.26.40 : Go to website and click download

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



The screenshot shows the "Download" section of the SoftEther VPN website. It starts with a heading "Download" and a statement about the software being open-source free software. Below this, there is a section titled "Primary Download Server (hosted by Windows Azure):" which includes a link to "Download SoftEther VPN" and notes about the language (English, Japanese, Simplified Chinese) and operating systems (Windows, Linux, Mac OS X, FreeBSD, Solaris). There are also sections for "Download from CNET Download.com:" and "Download from Softpedia.com:", each with a corresponding download link.

Figure 5.3.26.41 : Download SoftEther VPN

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

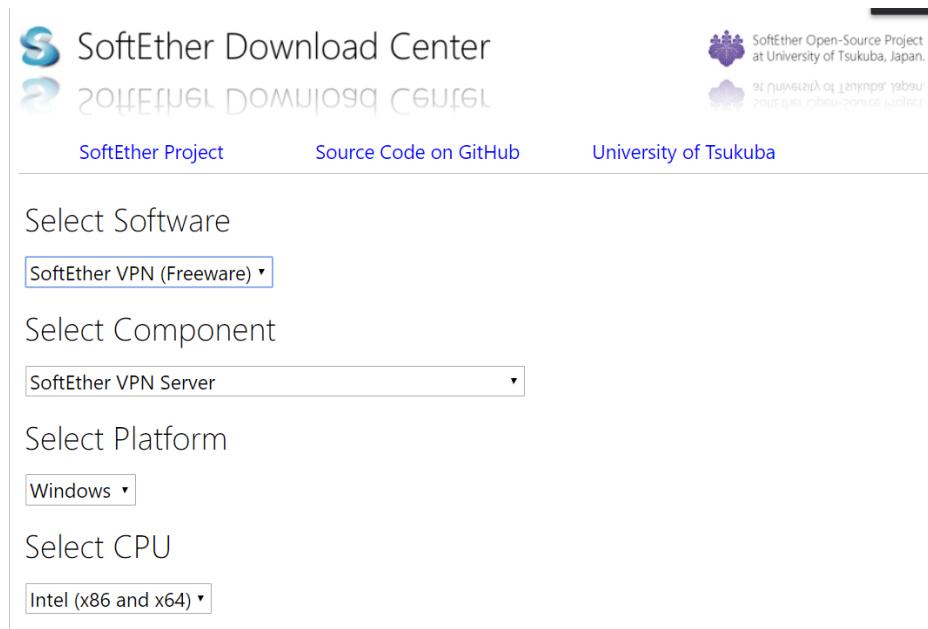


Figure 5.3.26.42 : Choose requirement

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

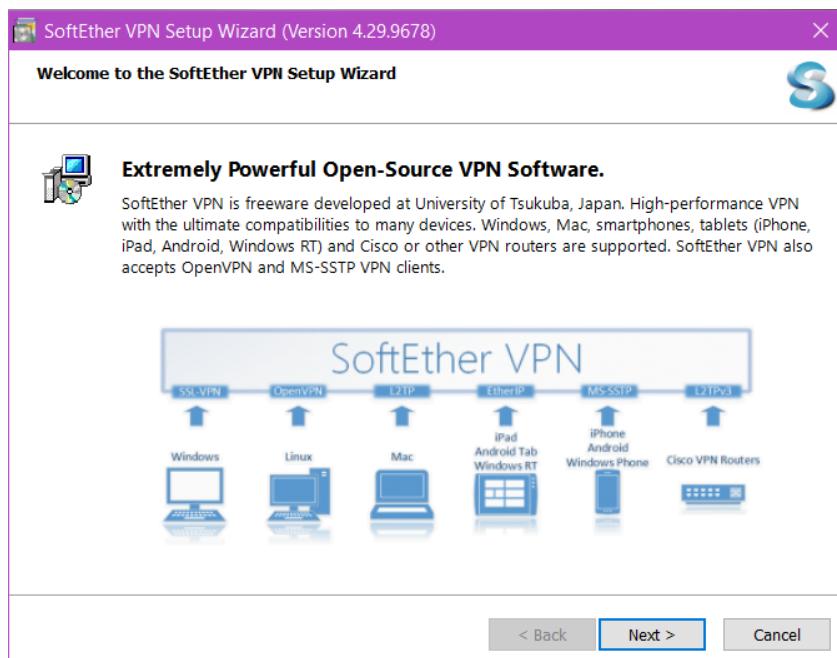


Figure 5.3.26.43 : Download section

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

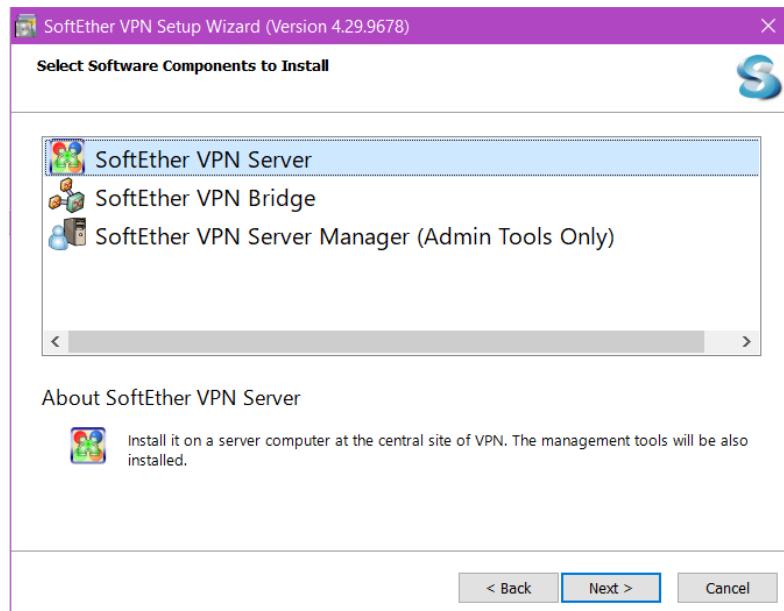


Figure 5.3.26.44: Choose software component to install

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

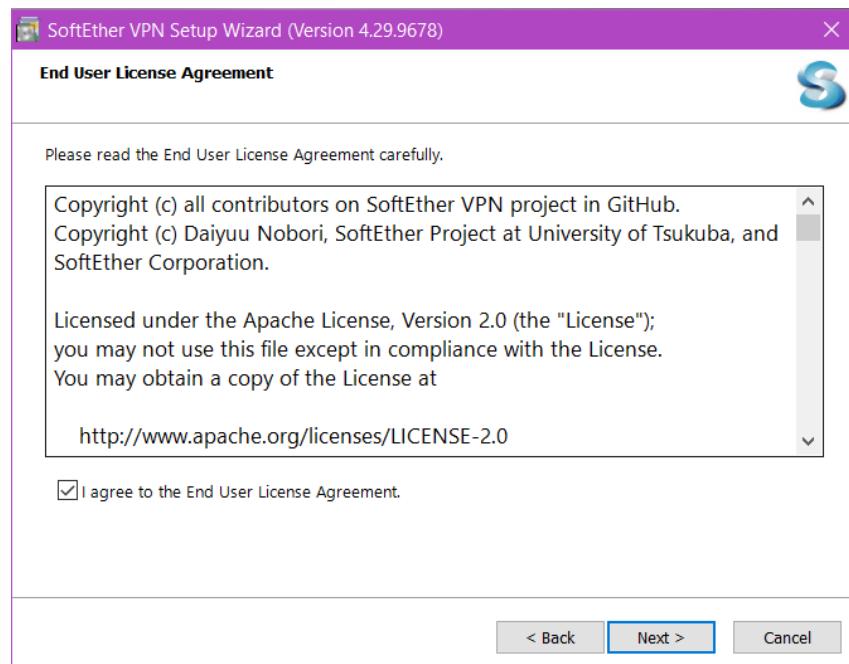


Figure 5.3.26.45 : Agree to End user Agreement

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

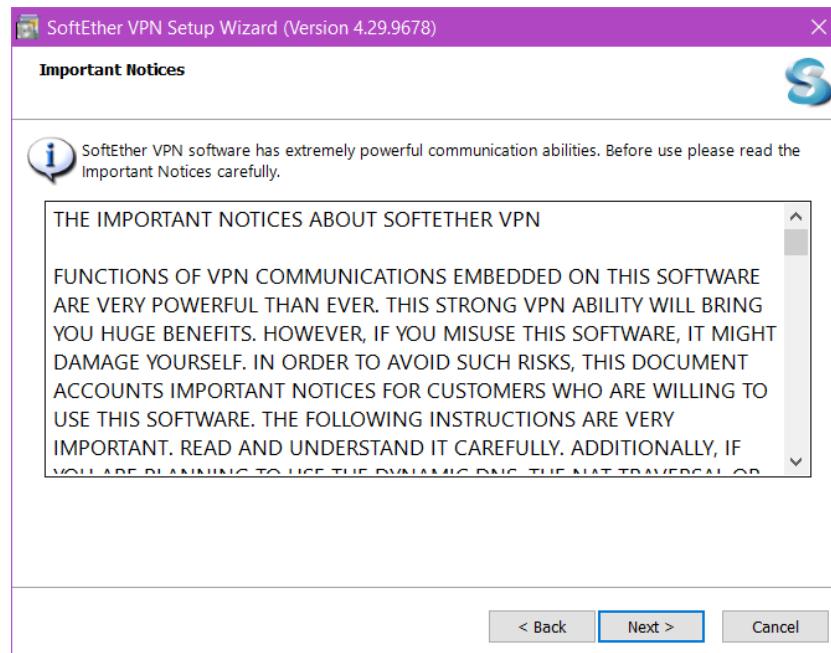


Figure 5.3.26.46 : Important Notice

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

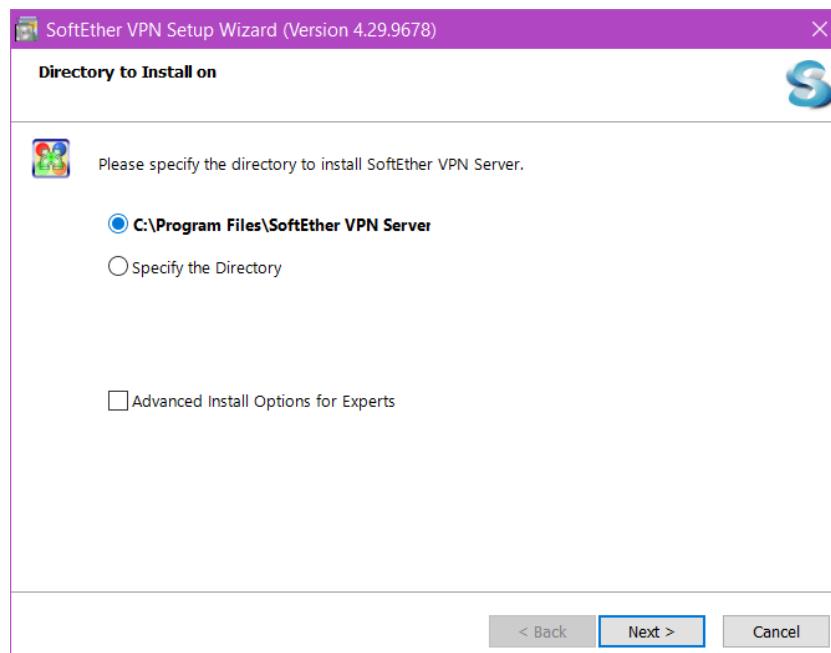


Figure 5.3.26.47 : Path Selection

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

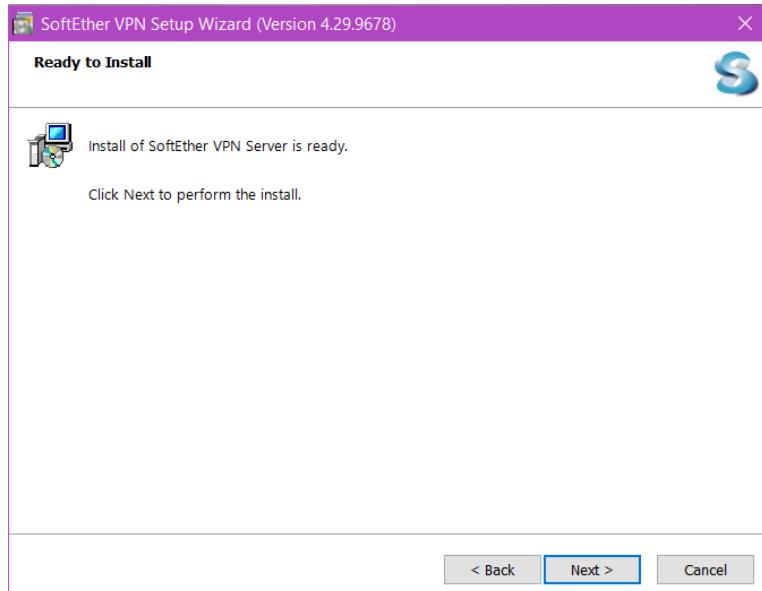


Figure 5.3.26.48 : Wait for installation

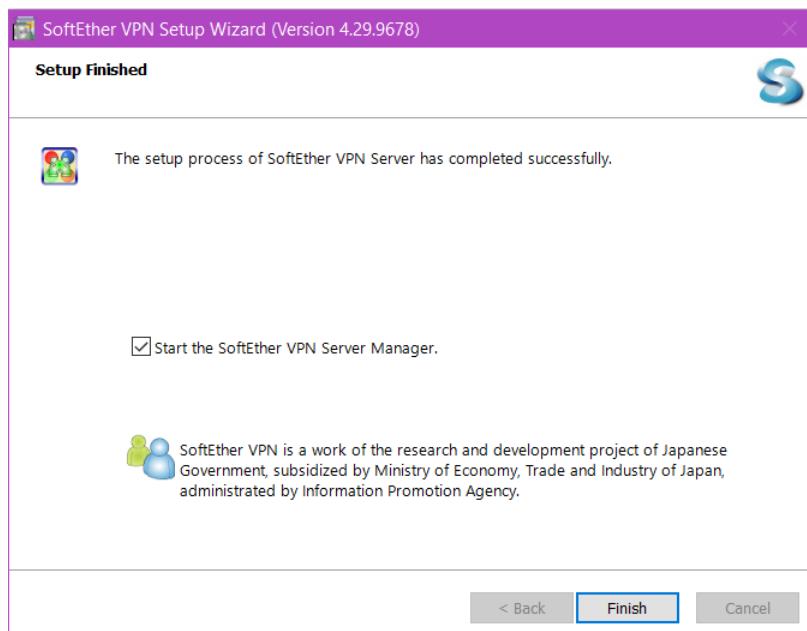


Figure 5.3.26.49 : Finish installation

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

Configuration of SoftEther VPN Server

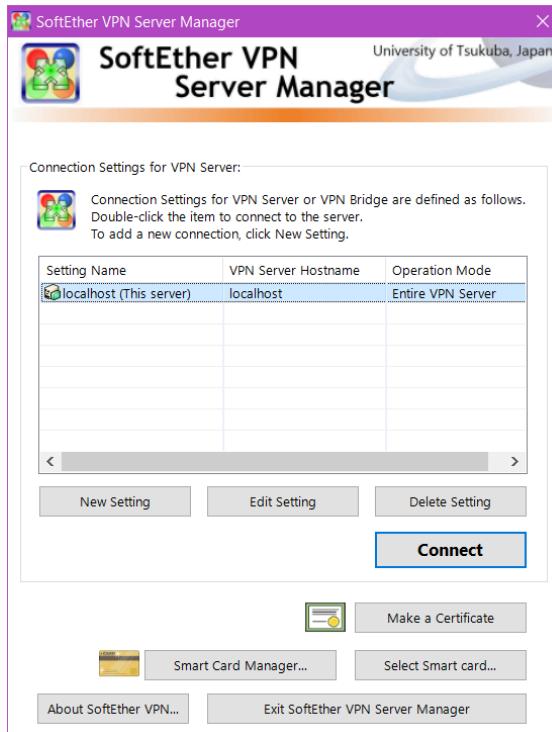


Figure 5.3.26.50 : Select local host

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

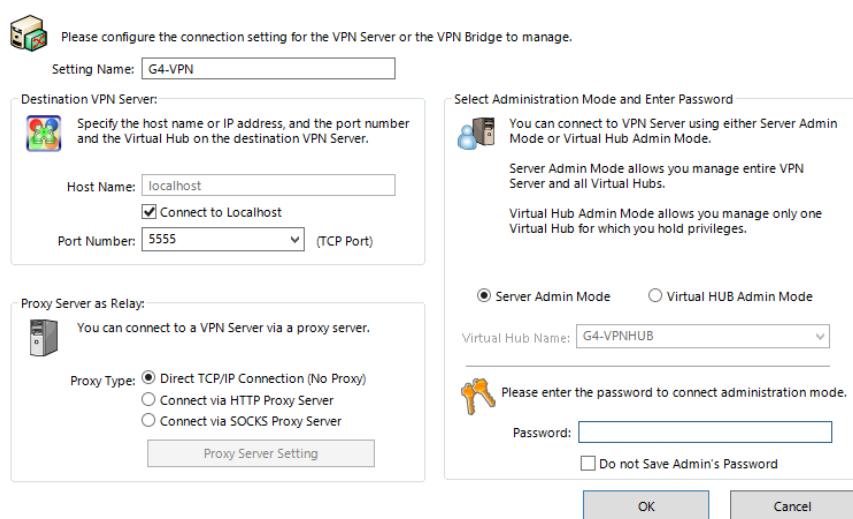


Figure 5.3.26.51 : Set up local host

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



Figure 5.3.26.52 : Set administrator password

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

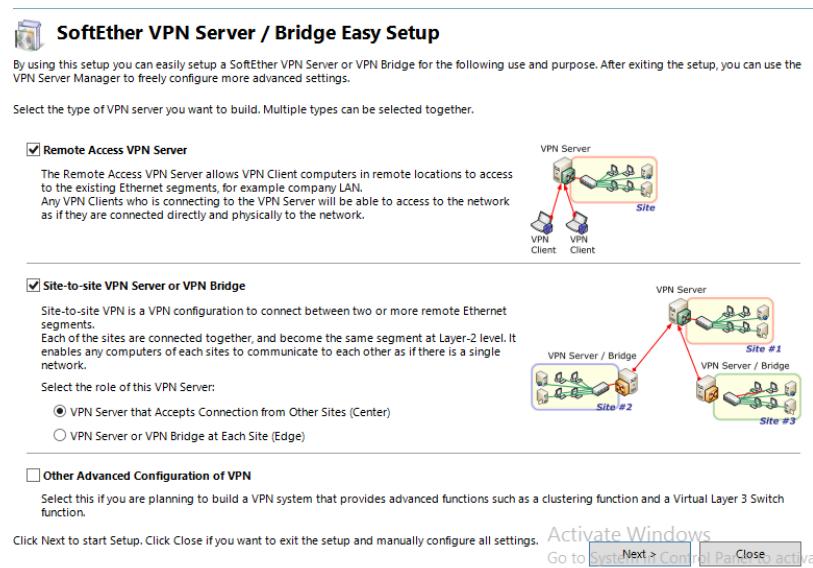


Figure 5.3.26.53 : Set up bridge



Figure 5.3.26.54 : Set up confirmation notice

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

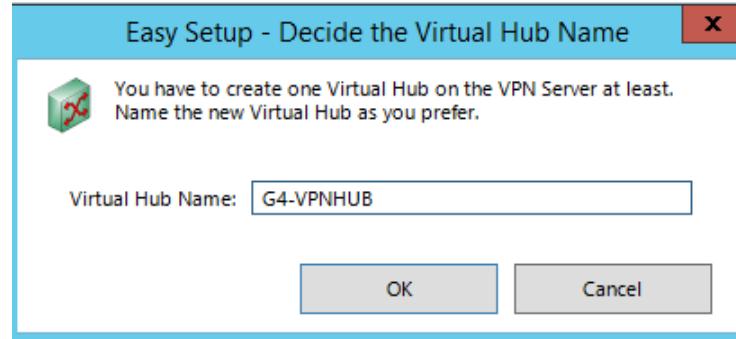


Figure 5.3.26.55 : Setup Virtual Hub Name

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

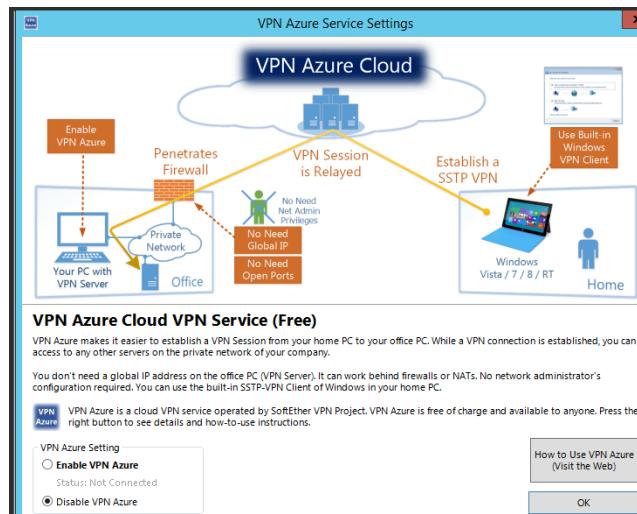


Figure 5.3.26.56 : Disable VPN Azure Services

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

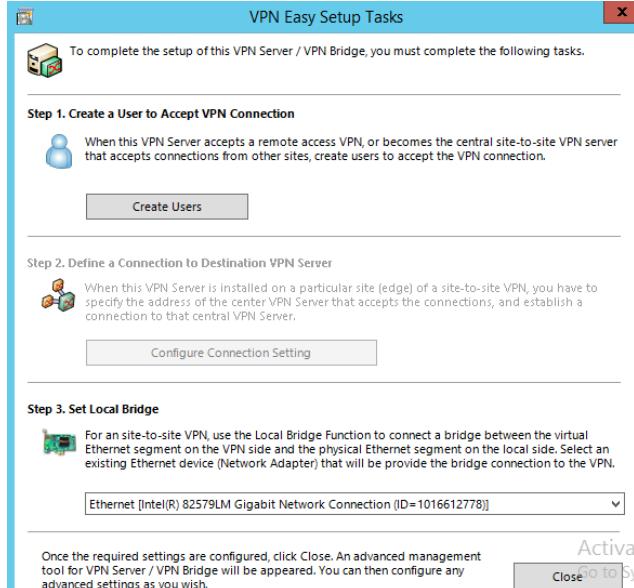


Figure 5.3.26.57 : Create a new user

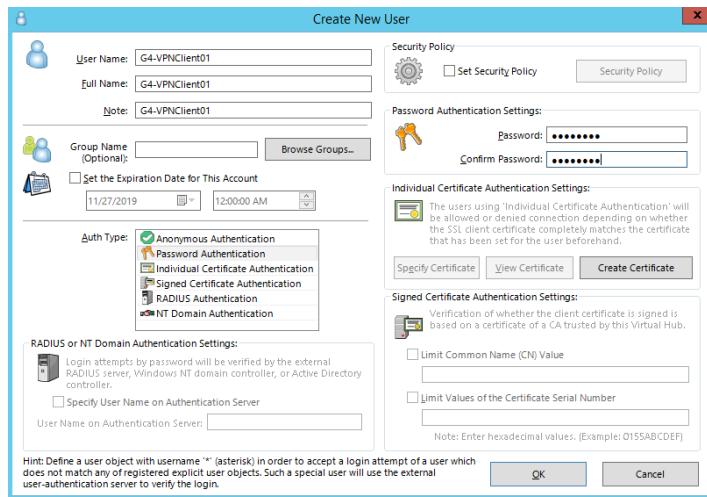


Figure 5.3.26.58 : Set up new user

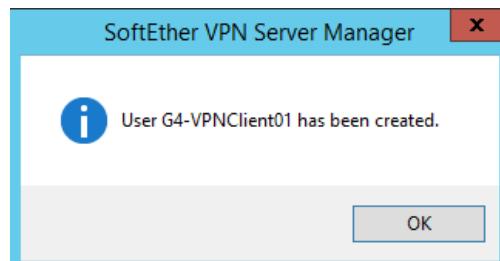


Figure 5.3.26.59 : Confirmation alert of user created

A screenshot of the "Manage Users" window. The title bar says "Manage Users". Below it, a message states "Virtual Hub "G4-VPNHUB" has the following users." A table lists one user: G4-VPNClient01. The table columns are: User Name, Full Name, Group Name, Description, Auth Method, Num Logins, and Last Login. The "Auth Method" column shows "Password Authe...". The "Num Logins" column shows "0" and "Last Login" shows "(None)". At the bottom are buttons for New, Edit, View User Info, Remove, Refresh, and Exit.

Figure 5.3.26.60 : Manage user

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

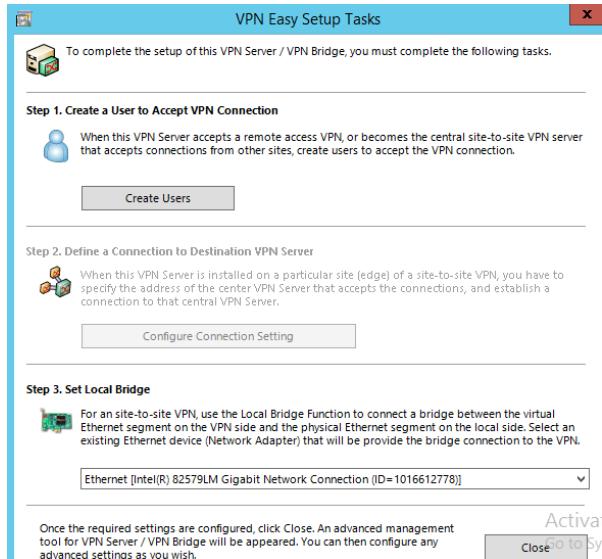


Figure 5.3.26.61 : Set up local bridge

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

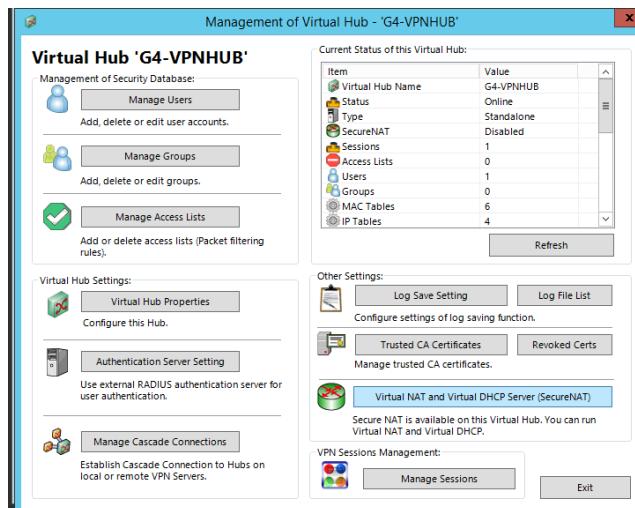


Figure 5.3.26.62: Manage Virtual Hub

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

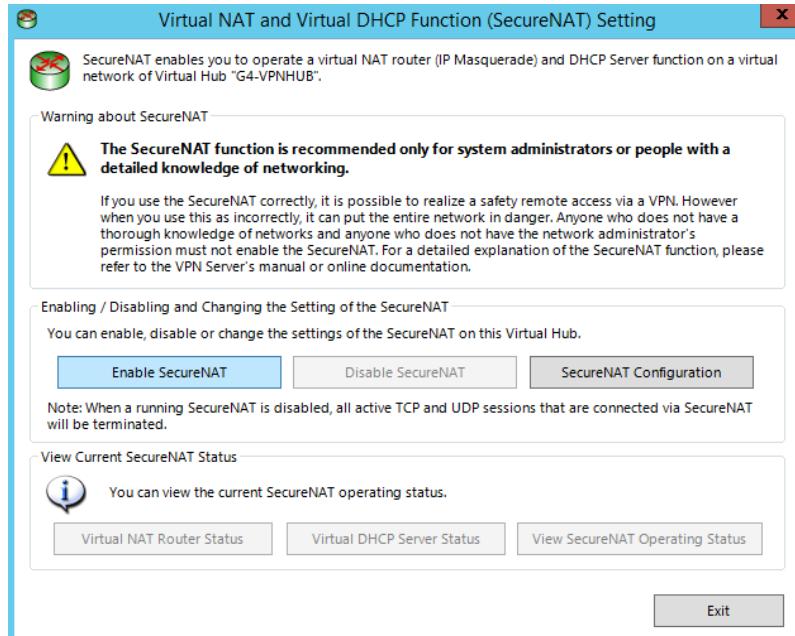


Figure 5.3.26.63 : Enable SecueNAT

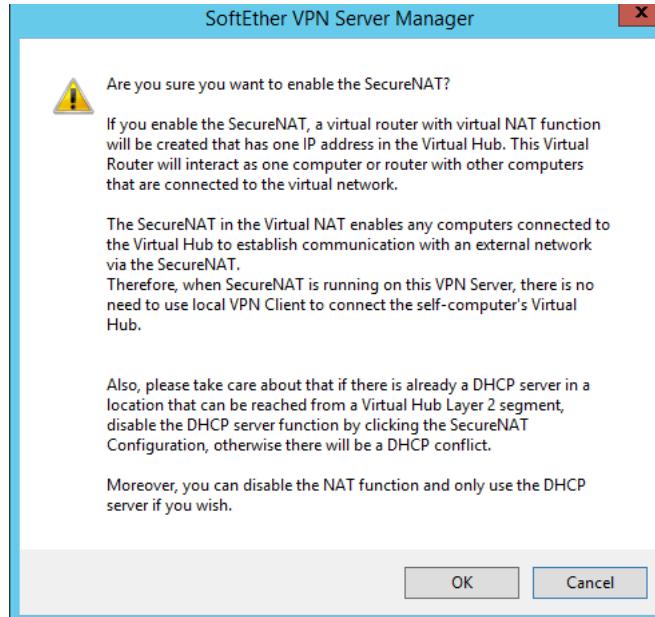


Figure 5.3.26.64 : Enable SecureNAT alert

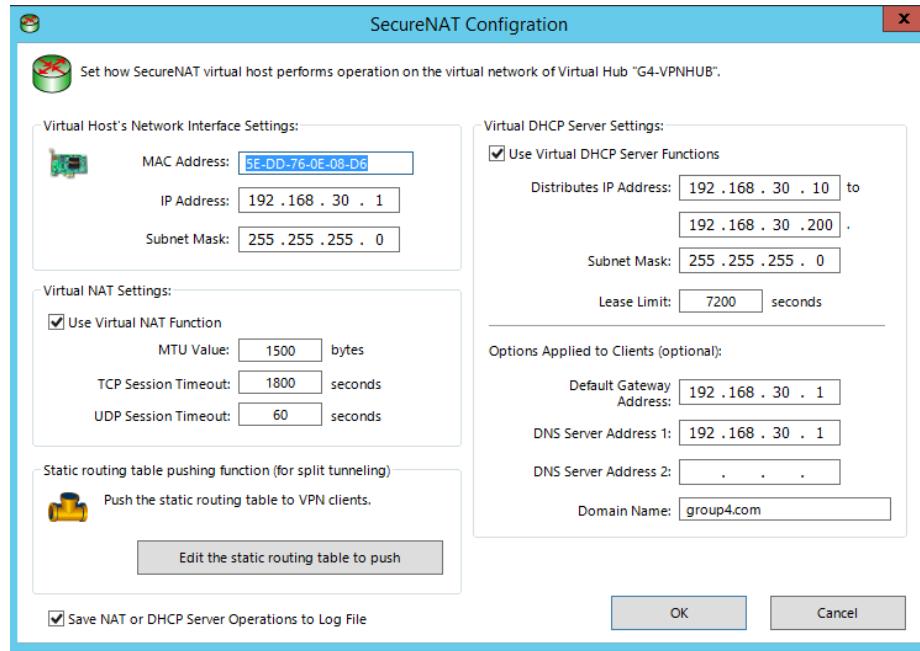


Figure 5.3.26.65 : Ip address provided by SecureNAT

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

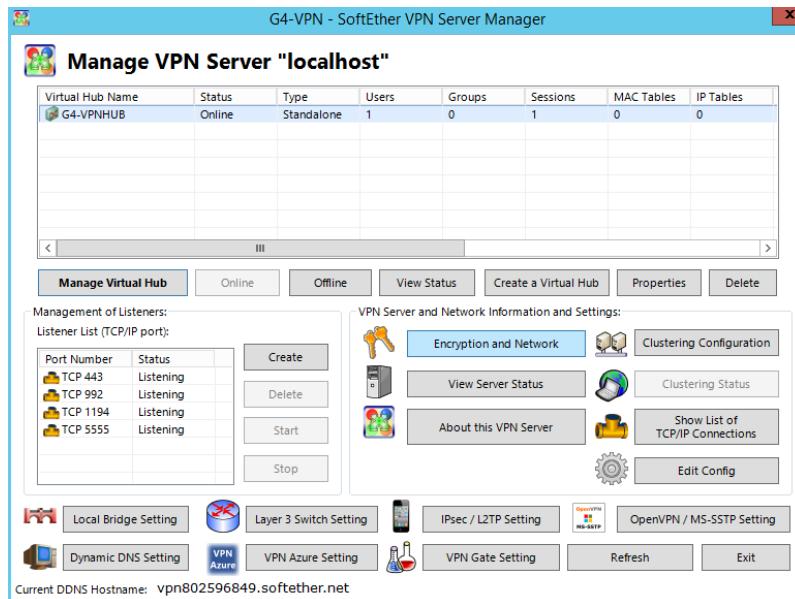


Figure 5.3.26.66 : Manage encryption and network

Step 11: Go back to Manager VPN Server Section, select Encryption and Network option.

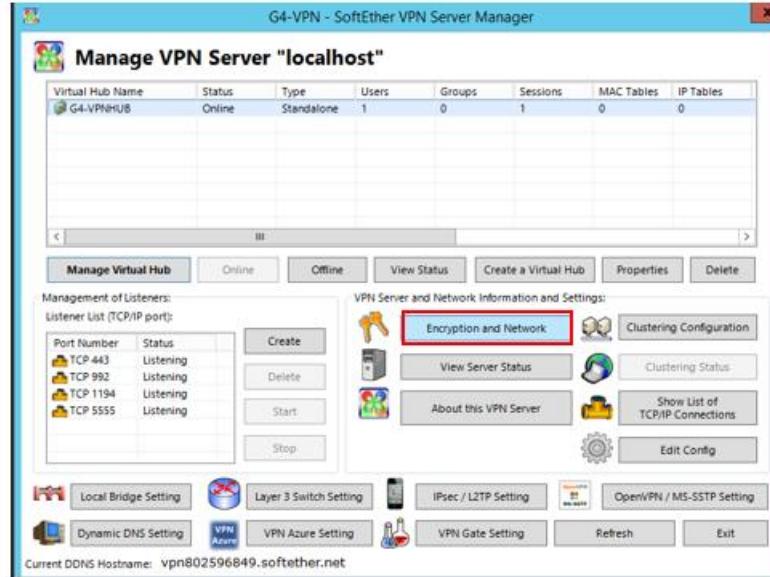


Figure 5.3.26.67 : Select Encryption and Network

Step 12: Change Encryption Algorithm Name to AES128-SHA and select OK.

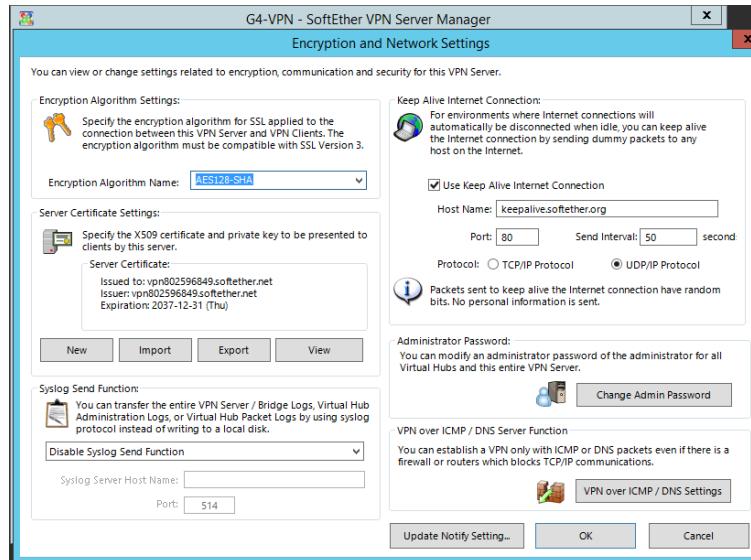


Figure 5.3.26.68 : Modify encryption algorithm name

Step 13: Go back to Manager VPN Server Section, select IPsec / L2TP Setting.

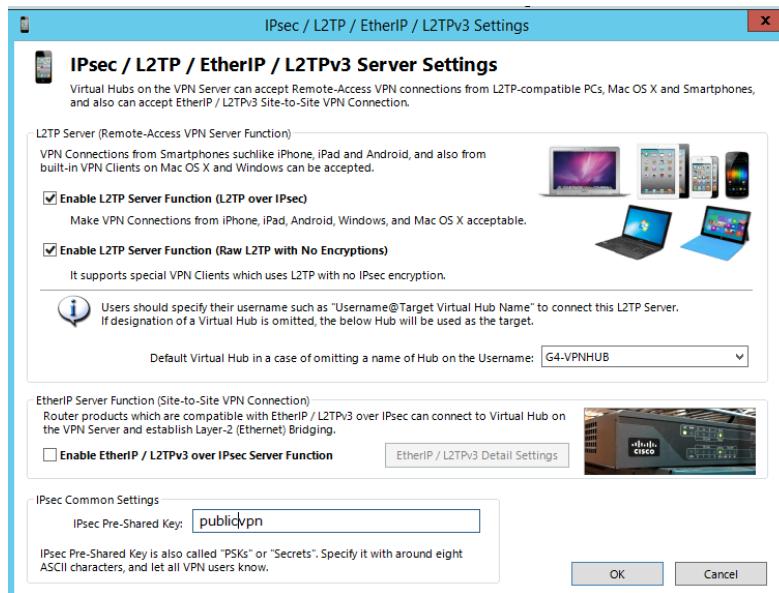


Figure 5.3.26.69 : Select IPsec / L2TP Setting

Step 14: The Virtual Hub is created and the VPN server is ready to be connected.

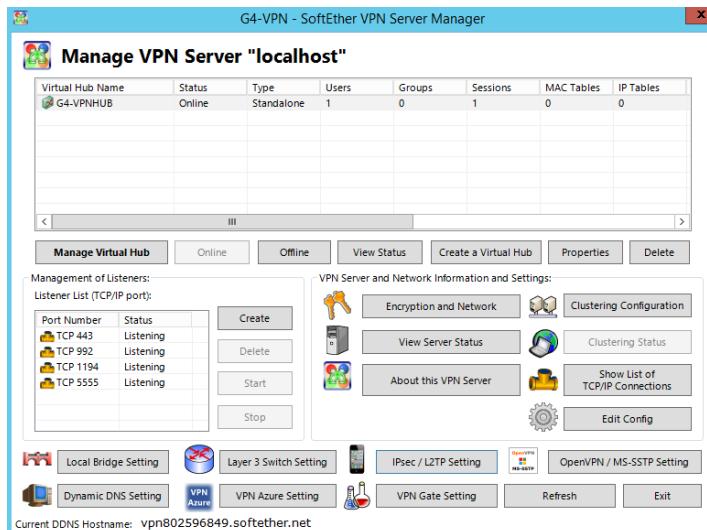


Figure 5.3.26.70 : Virtual Hub is created

SoftEther VPN Client Installation

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

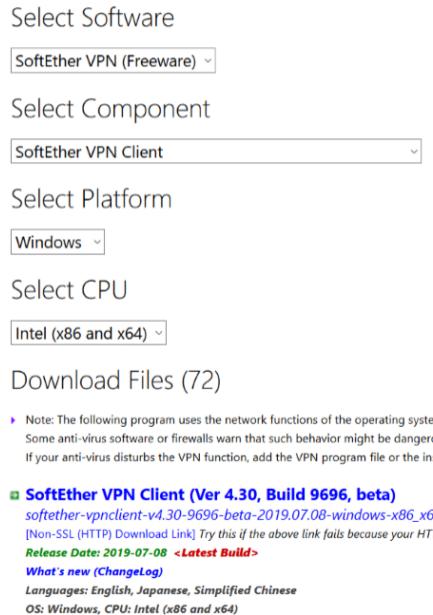


Figure 5.3.26.71 : Go to website and click download

Step 2: Select Download SoftEther VPN.

The screenshot displays a 'Download' section. It starts with a heading 'Primary Download Server (hosted by Windows Azure)': a bullet point 'Download SoftEther VPN' with a download icon. Below this, it specifies: 'Language: English, Japanese and Simplified Chinese.' and 'OS: Windows, Linux, Mac OS X, FreeBSD and Solaris.' Further down, there's a 'Download from CNET Download.com:' section with a single bullet point 'Download SoftEther VPN from CNET Download.com' with a download icon. At the bottom, there's a 'Download from Softpedia.com:' section with a single bullet point 'Download SoftEther VPN from Softpedia.com' with a download icon.

Figure 5.3.26.72 : Download SoftEther VPN

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

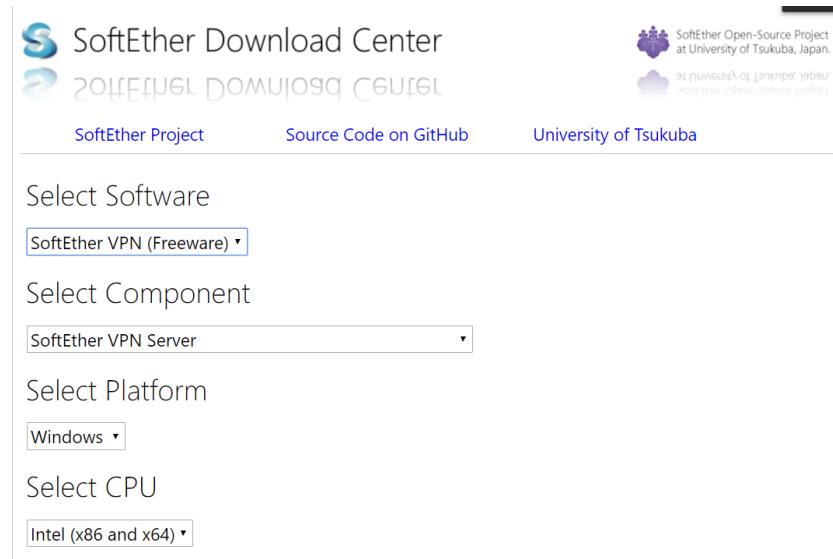


Figure 5.3.26.73 : Choose requirement

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

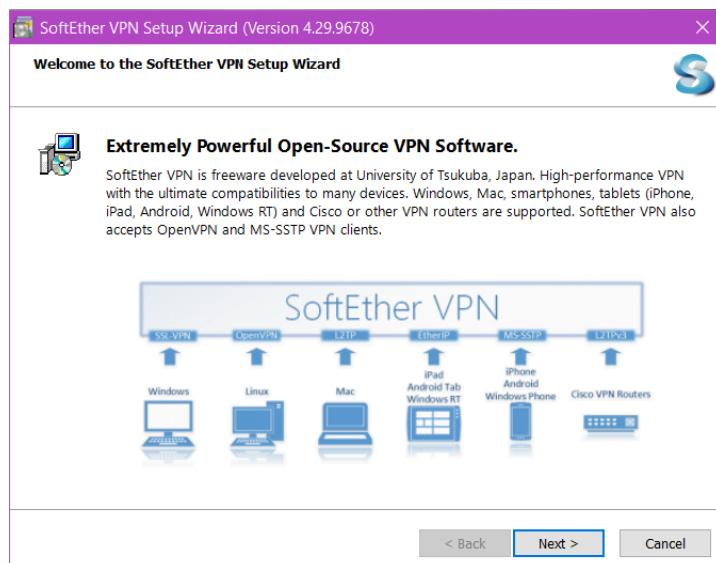


Figure 5.3.26.74 : Download section

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

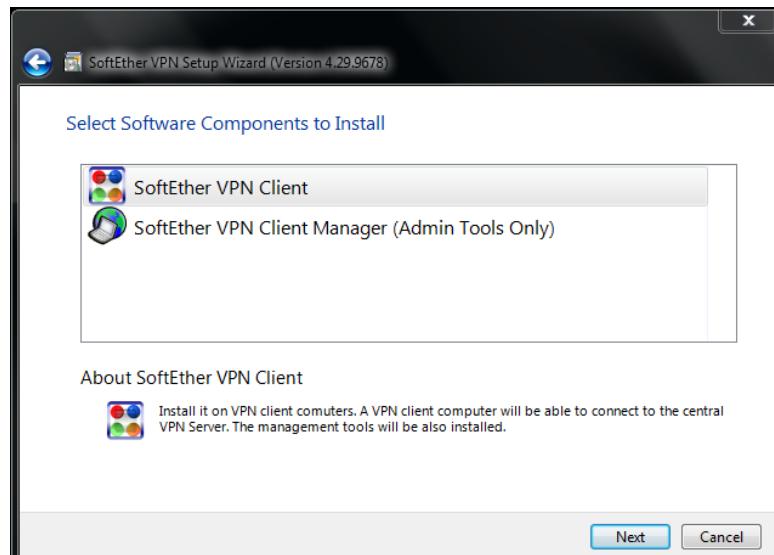


Figure 5.3.26.75 : Choose software component to install

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

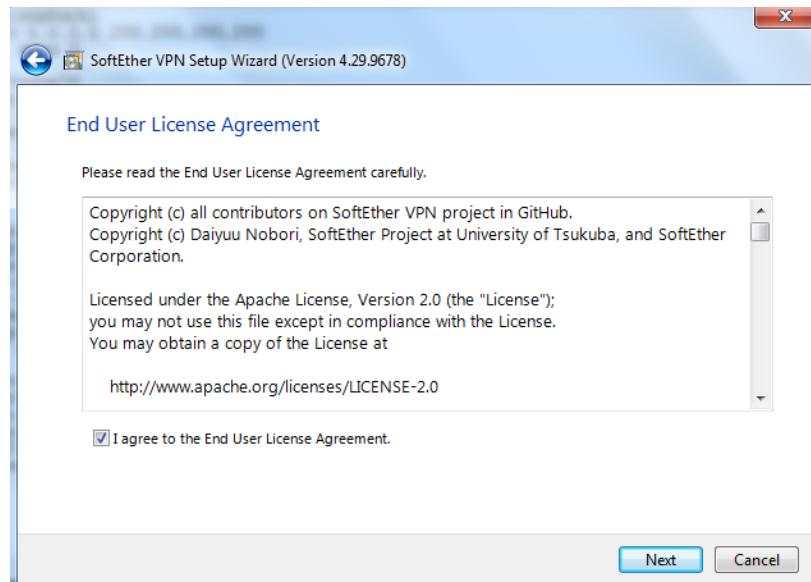


Figure 5.3.26.76 : Agree to End user Agreement

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

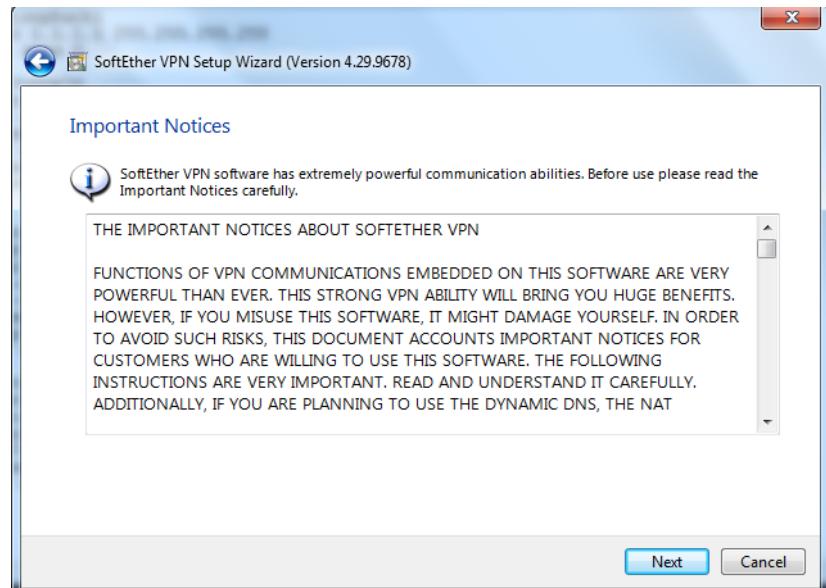


Figure 5.3.26.77 : Important Notice

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

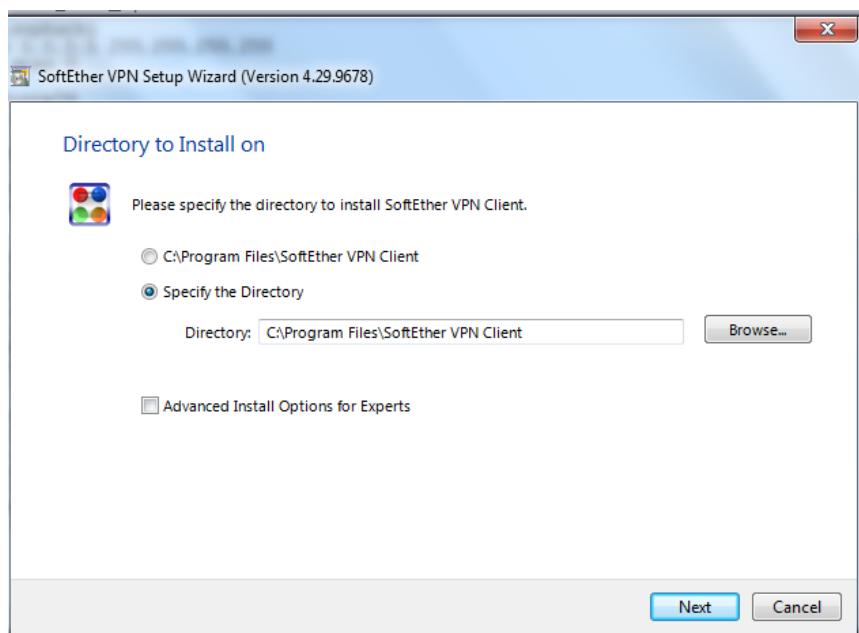


Figure 5.3.26.78 : Path Selection

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

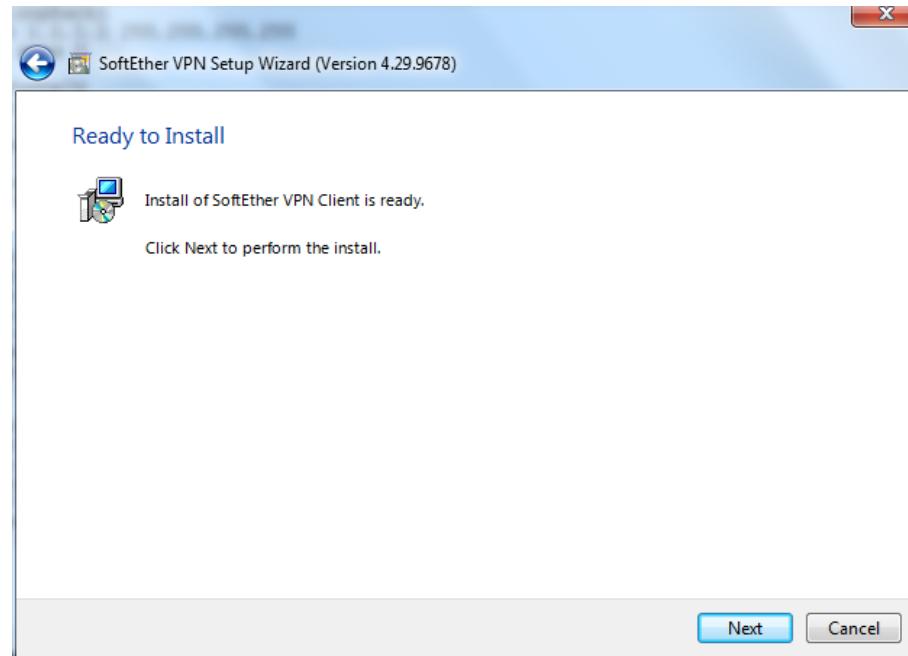


Figure 5.3.26.79 : Wait for installation

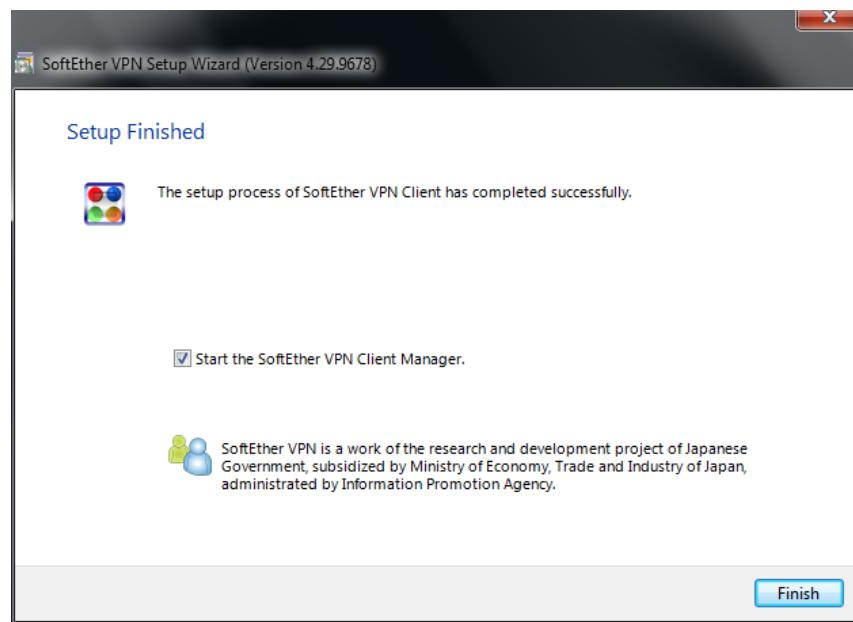


Figure 5.3.26.80 : Finish installation

Configuration of SoftEther VPN Client

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

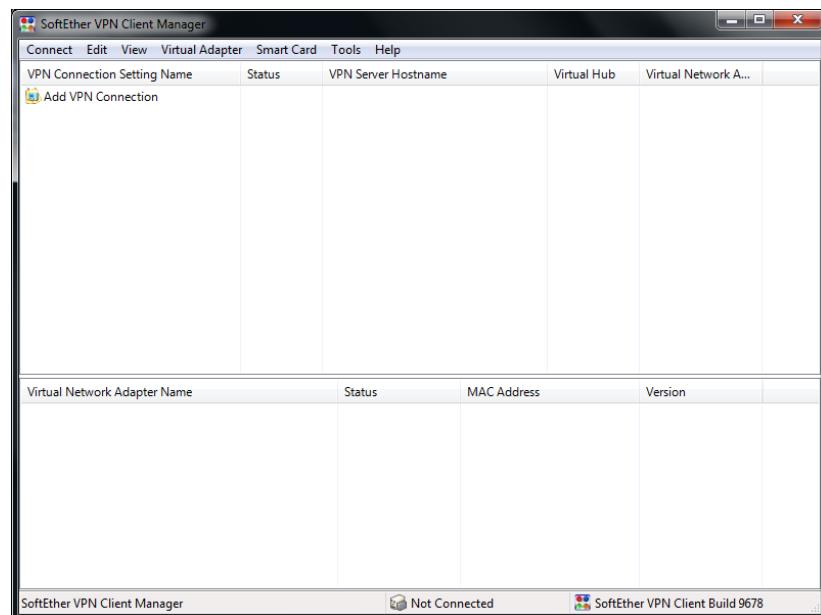


Figure 5.3.26.81 : GUI of SoftEther VPN Client Manager

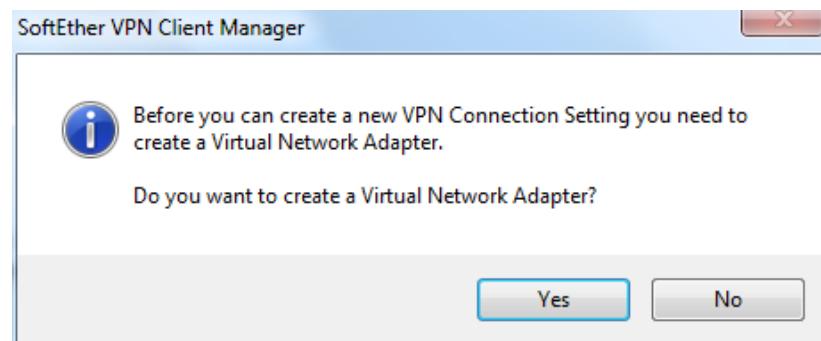


Figure 5.3.26.82 : Create new Virtual Network Adapter

Step 2: Change the name as (G4VPNAdapter). Click OK button.

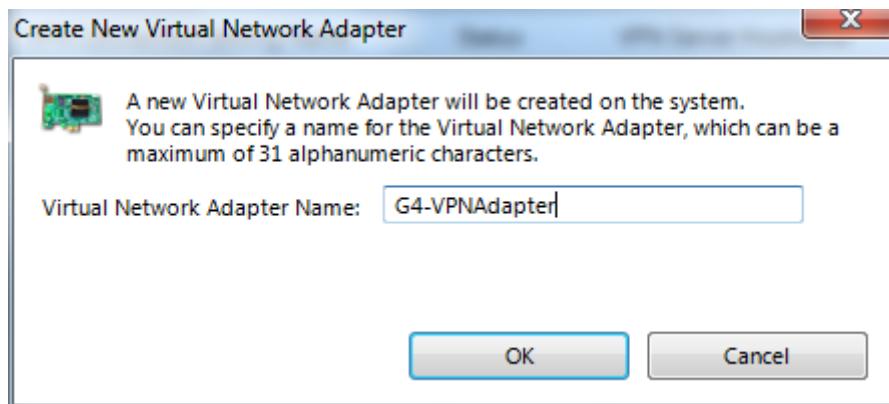


Figure 5.3.26.83 : Set up Virtual Network Adapter name

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

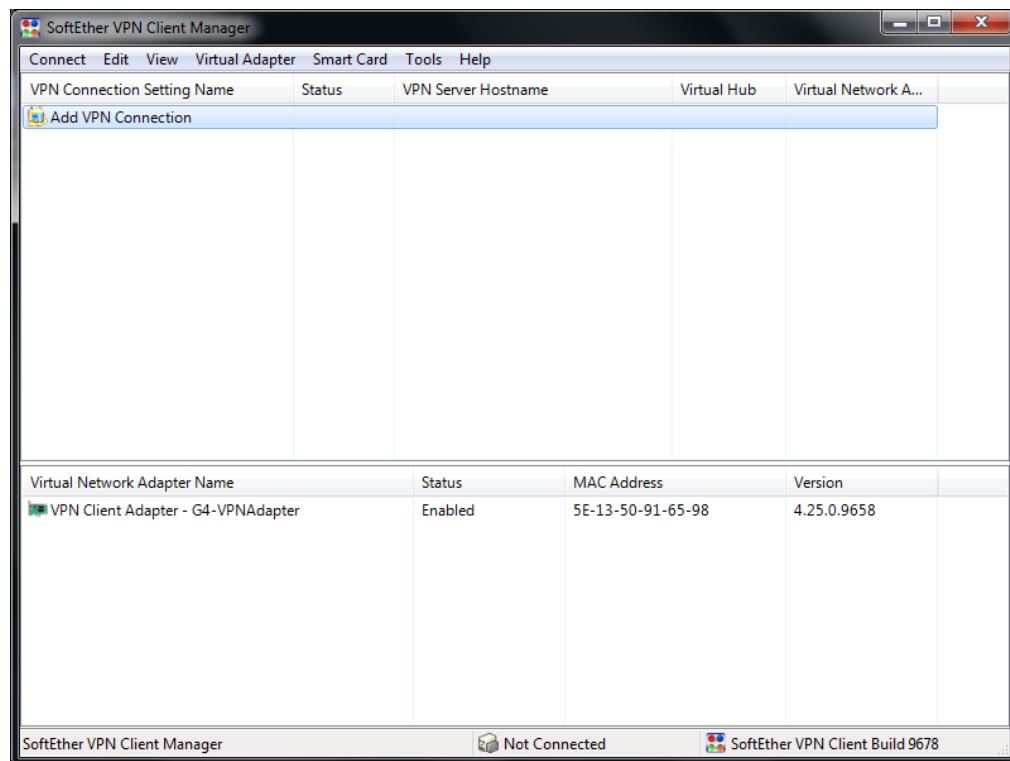


Figure 5.3.26.84 : New virtual network adapter

Step 4: Next, select Add VPN Connection again, a New VPN Connection Setting Properties window will pop out. Change the Setting Name as (G4VPNConnect), Host Name as < SoftEther VPN Server IP Address >, Port 5555 and Virtual Hub name as (G4-VPNHUB). On User Authentication Settings, change Auth Type to Standard Password Authentication and insert the username (G4-VPNClient01) and password that want to be login. Lastly, click the OK button.

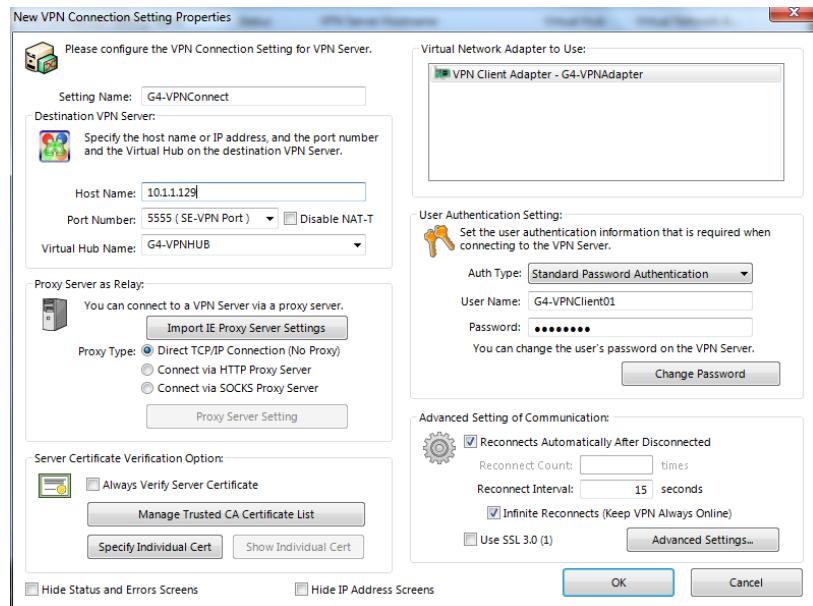


Figure 5.3.26.85 : Set up VPN Connection

Step 5: Success to create a New VPN Connection.

SoftEther VPN Client Manager				
VPN Connection Setting Name	Status	VPN Server Hostname	Virtual Hub	Virtual Network A...
Add VPN Connection				
G4-VPNConnect	Offline	10.1.1.129 (Direct TCP/IP Connection)	G4-VPNHUB	G4-VPNAdapter

Figure 5.3.26.86 : VPN Connection created

5.3.27 VLAN and Port Security

Step 1: To prevent switch spoofing, disable DTP by using command *switchport nonegotiate* on fa0/1.

```
SW4#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
SW4(config)#int fa0/1
SW4(config-if)#switchport nonegotiate
SW4(config-if)#end
```

Figure 5.3.27.87 : *switchport nonegotiate* command

Step 2: To prevent double tagging, make sure there is no host in native VLAN 5.

VLAN	Name	Status	Ports
1	default	active	Fa0/11, Fa0/12, Fa0/14, Gi0/1 Gi0/2
5	Trunk	active	
10	IT	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10
15	UsedP UnusedPort	suspended	
20	DMZ	active	Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24
99	MANAGEMENT	active	

Figure 5.3.27.88 : VLAN list

Step 3: Create a VLAN 15 to place all Unused ports and suspend it so that there is no communication between VLAN 15 and other VLANs.

```
SW4(config)#vlan 15
SW4(config-vlan)#name UnusedPort
SW4(config-vlan)#end
```

Figure 5.3.27.89 : *create VLAN 15*

```
SW4(config)#vlan 15
SW4(config-vlan)#state suspend
SW4(config-vlan)#end
```

Figure 5.3.27.90 : *Suspend VLAN 15*

Step 4: Configure all unused ports in VLAN 15.

```
SW4(config)#int range g0/1,g0/2,fa0/2
SW4(config-if-range)#switchport mode access
SW4(config-if-range)#switchport access vlan 15
SW4(config)#int range fa0/5-12
SW4(config-if-range)#switchport mode access
SW4(config-if-range)#switchport access vlan 15
SW4(config-if-range)#int range fa0/14-21
SW4(config-if-range)#switchport mode access
SW4(config-if-range)#switchport access vlan 15
SW4(config-if-range)#end
```

Figure 5.3.27.91: Configure unused ports in VLAN 15

Step 5: Assign used vlans in trunk port.

```
SW4(config)#int fa0/1
SW4(config-if)#switchport mode trunk
SW4(config-if)#switchport trunk allowed vlan 1,5,10,20,99
SW4(config-if)#end
```

Figure 5.3.27.92 : Assign VLAN into trunk port

5.4 Conclusion

Installation and configuration are importance procedure before testing the service. Installation of the program is the act of putting the program onto a computer system so that it can be executed. This is because the requisite process varies for each program and each computer, many program come with a general-purpose or dedicated installer. This stage must be done carefully to make sure the service can be run efficiently during the testing part.

CHAPTER 6: TESTING

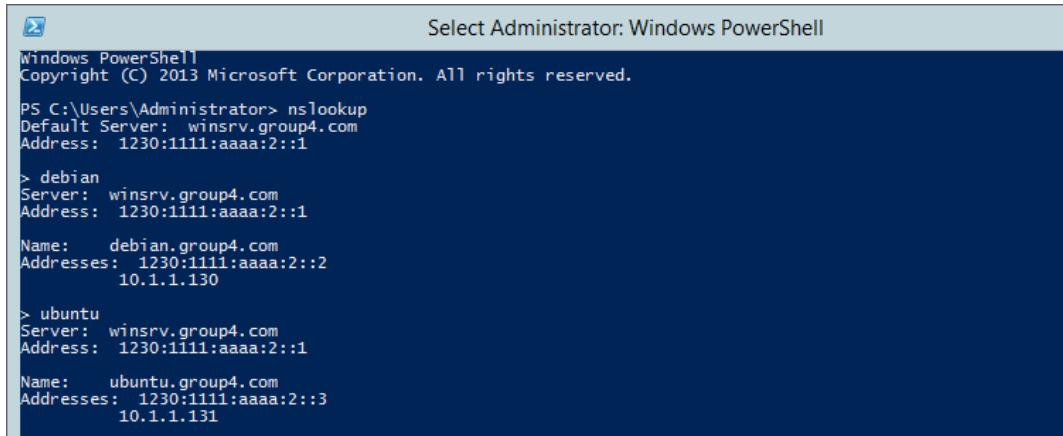
6.1 Introduction

In this chapter, all the testing approach and results for each services will be explain. There might be different approach to test the service but we only focus on one as our goal is to ensure the service is up and correctly configured.

6.2 Service Testing

6.2.1 Domain Name Server (IPV4 & IPV6)

Step 1: Open cmd and type nslookup as well as IPv4 and IPv6 address and domain name of Windows Server, Ubuntu server and Debian.



```
PS C:\Users\Administrator> nslookup
Default Server: winsrv.group4.com
Address: 1230:1111:aaaa:2::1

> debian
Server: winsrv.group4.com
Address: 1230:1111:aaaa:2::1

Name: debian.group4.com
Addresses: 1230:1111:aaaa:2::2
          10.1.1.130

> ubuntu
Server: winsrv.group4.com
Address: 1230:1111:aaaa:2::1

Name: ubuntu.group4.com
Addresses: 1230:1111:aaaa:2::3
          10.1.1.131
```

Figure 6.2.1.1: Testing DNS

6.2.2 Dynamic Host Configuration Protocol (IPv4 & IPv6)

Testing on Client Machine

Step 1: Type ipconfig/all at cmd on client machine.

```
Windows IP Configuration

Host Name . . . . . : MW15
Primary Dns Suffix . . . . . : group4.com
Node Type . . . . . : Mixed
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : group4.com

Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix . . . . . : group4.com
  Description . . . . . : Intel(R) 82579LM Gigabit Network Connecti
on
  Physical Address . . . . . : 34-17-EB-CA-92-D7
  DHCP Enabled. . . . . : Yes
  Autoconfiguration Enabled . . . . . : Yes
  IPv6 Address . . . . . : 1230:1111:aaaa:1:8d44:4b56:239d:1749<Preferred>
  Temporary IPv6 Address. . . . . : 1230:1111:aaaa:1:cobe:b30c:643e:f7ab<Preferred>
  Link-local IPv6 Address . . . . . : fe80::8d44:4b56:239d:1749%11<Preferred>
  IPv4 Address. . . . . : 10.1.1.2<Preferred>
  Subnet Mask . . . . . : 255.255.255.128
  Lease Obtained. . . . . : Tuesday, December 10, 2019 10:19:37 PM
  Lease Expires . . . . . : Thursday, December 19, 2019 1:52:50 PM
  Default Gateway . . . . . : fe80::216:c8ff:fea1:35d7%11
                                10.1.1.126
  DHCP Server . . . . . : 10.1.1.129
  DNS Servers . . . . . : 10.1.1.129
  NetBIOS over Tcpip. . . . . : Enabled
```

Figure 6.2.2.1: Show port-security address command

6.2.3 Vlan & Port Security

Step 1: By using command *show vlan* on switch, we can know that fa0/2, fa0/5, fa0/6, fa0/7, fa0/8, fa0/9, fa0/10, fa0/11, fa0/12, fa0/14, fa0/15, fa0/16, fa0/17, fa0/18, fa0/19, fa0/20, fa0/21, gi0/1 and gi0/2 are assigned in UnusedPort which is suspended in VLAN.

VLAN	Name	Status	Ports
1	default	active	
5	Trunk	active	
10	IT	active	Fa0/3, Fa0/4
15	UnusedPort	suspended	Fa0/2, Fa0/5, Fa0/6, Fa0/7 Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Gi0/1, Gi0/2
20	DMZ	active	Fa0/22, Fa0/23, Fa0/24
99	MANAGEMENT	active	

Figure 6.2.3.1: Show VLAN command

Step 2: We try to connect a PC or laptop in fa0/18, the connection failed. Use command *ipconfig* to check the status.

```
Ethernet adapter Local Area Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . group4.com
```

Figure 6.2.3.2: ipconfig command

Step 3: To check VLAN trunk, use command *show interface trunk*.

```
Port      Mode          Encapsulation  Status        Native vlan
Fa0/1    on           802.1q         trunking     99

Port      Vlans allowed on trunk
Fa0/1    1,5,10,20,99

Port      Vlans allowed and active in management domain
Fa0/1    1,5,10,20,99

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1    1,5,10,20,99
```

Figure 6.2.3.3: interface trunk command

Port Security

Step 4: To check the status of port-security, enter command *show port-security* to show port-security enabled in which interface.

```
SW4#show por
*May 10 01:31:46.537: %SYS-5-CONFIG_I: Configured from console by AzimGroup4 on consolet
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
              (Count)        (Count)        (Count)
-----  

Fa0/22       10            6             0           Shutdown  

Fa0/23       1              1             0           Shutdown  

Fa0/24       1              1             0           Shutdown  

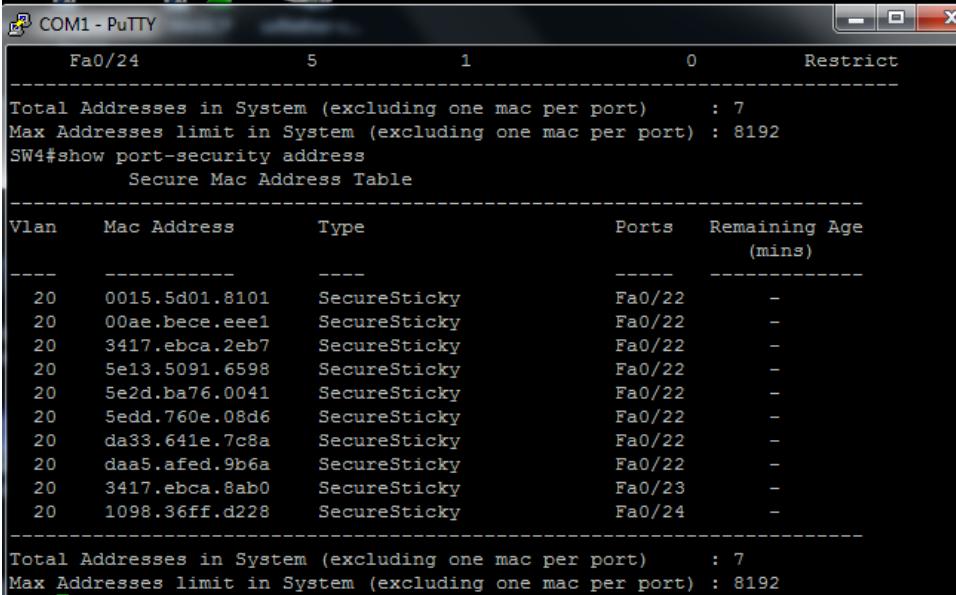
-----  

Total Addresses in System (excluding one mac per port)      : 5  

Max Addresses limit in System (excluding one mac per port) : 8192
```

Figure 6.2.3.4: Show Port-security

Step 5: To check port security address, enter command *show port-security address* to verify entries.



Vlan	Mac Address	Type	Ports	Remaining Age (mins)
20	0015.5d01.8101	SecureSticky	Fa0/22	-
20	00ae.bece.eee1	SecureSticky	Fa0/22	-
20	3417.ebca.2eb7	SecureSticky	Fa0/22	-
20	5e13.5091.6598	SecureSticky	Fa0/22	-
20	5e2d.ba76.0041	SecureSticky	Fa0/22	-
20	5edd.760e.08d6	SecureSticky	Fa0/22	-
20	da33.641e.7c8a	SecureSticky	Fa0/22	-
20	daa5.afed.9b6a	SecureSticky	Fa0/22	-
20	3417.ebca.8ab0	SecureSticky	Fa0/23	-
20	1098.36ff.d228	SecureSticky	Fa0/24	-

```
SW4#show port-security address
      Secure Mac Address Table
-----  

Total Addresses in System (excluding one mac per port)      : 7
Max Addresses limit in System (excluding one mac per port) : 8192
```

Figure 6.2.3.5: Show port-security address command

To test port security:

Step 1: Connect a PC or laptop which never connect to the switch.

Step 2: Record PC or laptop Ethernet interface physical address. To show the physical address of PC or laptop, use command ipconfig /all.

```
Ethernet adapter Ethernet:

  Connection-specific DNS Suffix . : group4.com
  Description . . . . . : Realtek PCIe FE Family Controller
  Physical Address. . . . . : 54-E1-AD-18-25-34
  DHCP Enabled. . . . . : Yes
  Autoconfiguration Enabled . . . . . : Yes
  Link-local IPv6 Address . . . . . : fe80::fd50:e242:c9e8:bf53%13(PREFERRED)
  IPv4 Address. . . . . : 10.1.1.141(Preferred)
  Subnet Mask . . . . . : 255.255.255.240
  Lease Obtained. . . . . : Wednesday, December 11, 2019 1:35:39 PM
  Lease Expires . . . . . : Wednesday, December 11, 2019 3:35:40 PM
  Default Gateway . . . . . : 10.1.1.142
  DHCP Server . . . . . : 10.1.1.139
  DHCPv6 IAID . . . . . : 72671661
  DHCPv6 Client DUID. . . . . : 00-01-00-01-24-00-84-E5-54-E1-AD-18-25-34
  DNS Servers . . . . . : 10.1.1.129
  NetBIOS over Tcpip. . . . . : Enabled
```

Figure 6.2.3.6: Show physical address

Step 3: Connect the PC or laptop into switch port.

Step 4: Check switch configuration. It shows that the MAC address is recorded in interface fa0/23.

20	3417.ebca.8ab0	SecureSticky	Fa0/23	-
----	----------------	--------------	--------	---

Figure 6.2.3.7: Shows MAC address port

Step 5: Connect the PC or laptop into other port. PC or laptop unable to connect to switch.

Step 6: Check status of switch port fa0/24 by using command show int status. It will show the port is down (err-disable).

Fa0/22	connected	20	a-full	a-100	10/100BaseTX
Fa0/23	connected	20	a-full	a-100	10/100BaseTX
Fa0/24	err-disabled	20	auto	auto	10/100BaseTX
GigE/1		15			10/100/1000BaseTX

Figure 6.2.3.8: err-dissabled status

Step 7: When there is unrecognized mac-address occur, an SNMP trap notification display on the screen.

```
*May 10 02:01:35.424: %PM-4-ERR RECOVER: Attempting to recover from psecure-violation err-disable state on Fa0/24
*May 10 02:01:37.605: %PM-4-ERR DISABLE: psecure-violation error detected on Fa0/24, putting Fa0/24 in err-disable state
*May 10 02:01:37.614: %PORT SECURITY-2-PSECURE VIOLATION: Security violation occurred, caused by MAC address 54e1.ad18.2534 on port FastEthernet0/24.
```

Figure 6.2.3.9: Security violation alert

6.2.4 Web, SSL & Virtual Hosting

Step 1: Open the Windows server to check the list of certificate.

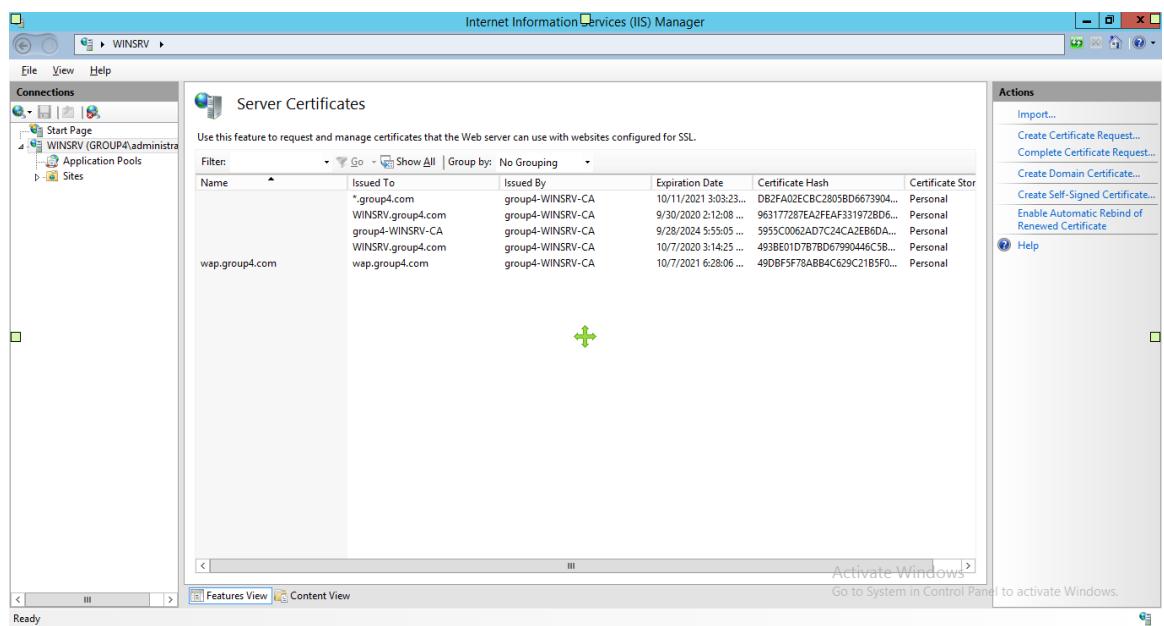


Figure 6.2.4.1: Show the list of certificate.

Step 2: To check if the SSL certificate is being request and being integrated, look at the URL. If the http is secure, then the SSL is work.



Figure 6.2.4.2: Show the https is secure.

Step 3: Then, put them in the URL ‘<https://www.group4.com>’ as the link is the web server. To test if there are change in the web page. If the page is work, it will display ‘Welcome to Group 4’ as it been setup earlier.

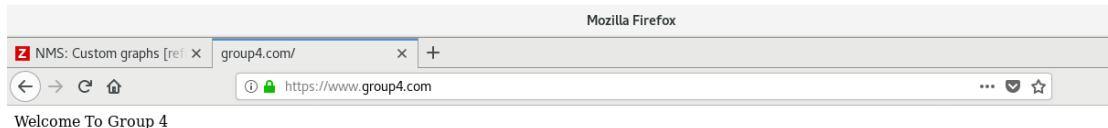
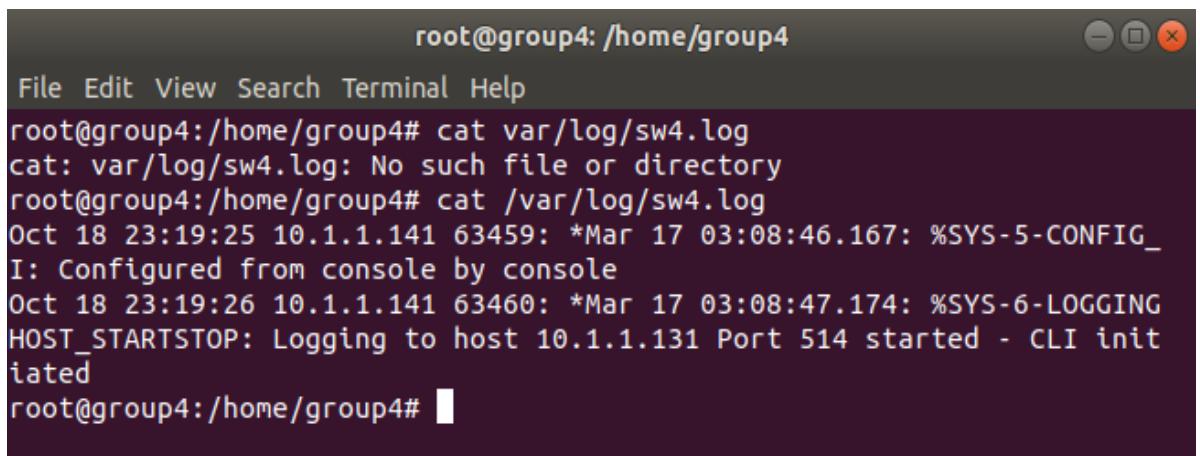


Figure 6.2.4.3: URL Testing

6.2.5 Syslog

Step 1: Open the Ubuntu server, then try open the switch log by entering the coding. It will show the log that happen in switch, such as up and downlink of the server. We can detect the problem by this log. Can be open later for research purpose.

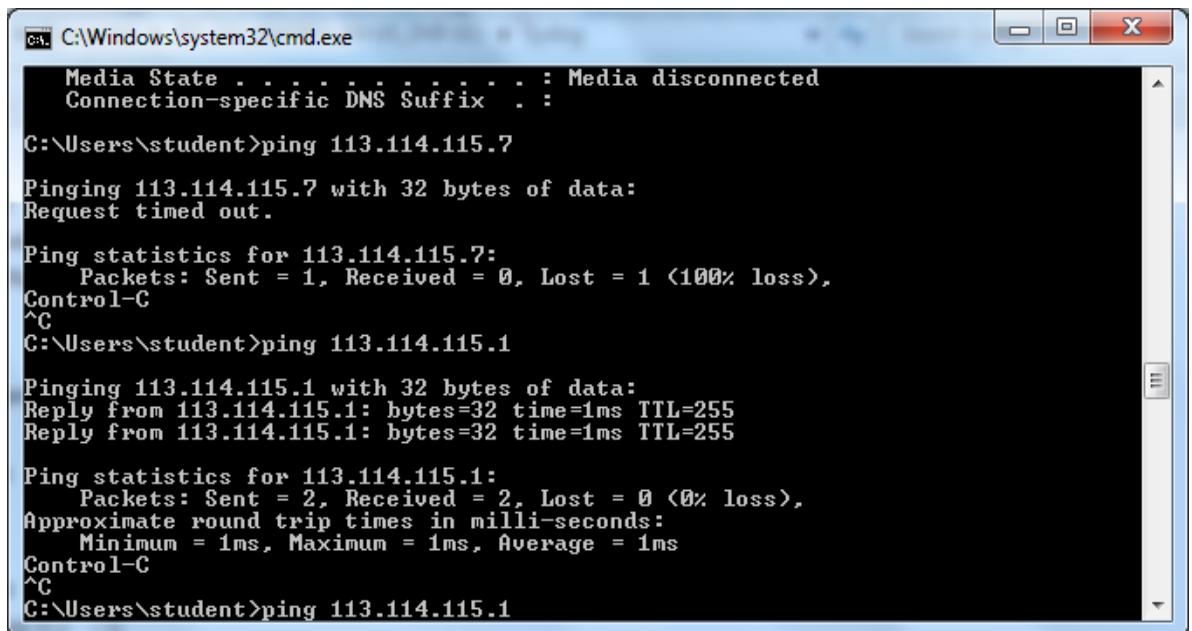


```
root@group4: /home/group4
File Edit View Search Terminal Help
root@group4:/home/group4# cat var/log/sw4.log
cat: var/log/sw4.log: No such file or directory
root@group4:/home/group4# cat /var/log/sw4.log
Oct 18 23:19:25 10.1.1.141 63459: *Mar 17 03:08:46.167: %SYS-5-CONFIG-I: Configured from console by console
Oct 18 23:19:26 10.1.1.141 63460: *Mar 17 03:08:47.174: %SYS-6-LOGGING HOST_STARTSTOP: Logging to host 10.1.1.131 Port 514 started - CLI initiated
root@group4:/home/group4#
```

Figure 6.2.5.1: Show the log for the switch

Step 2: Then, try to ping internet access at the client. To test if the log can connect to the internet access.

Step 3: Finally, the syslog is being done and ready to use.



```
C:\Windows\system32\cmd.exe
Media State . . . : Media disconnected
Connection-specific DNS Suffix . . . :
C:\Users\student>ping 113.114.115.7
Pinging 113.114.115.7 with 32 bytes of data:
Request timed out.

Ping statistics for 113.114.115.7:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
Control-C
^C
C:\Users\student>ping 113.114.115.1

Pinging 113.114.115.1 with 32 bytes of data:
Reply from 113.114.115.1: bytes=32 time=1ms TTL=255
Reply from 113.114.115.1: bytes=32 time=1ms TTL=255

Ping statistics for 113.114.115.1:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
Control-C
^C
C:\Users\student>ping 113.114.115.1
```

Figure 6.2.5.2: Show the ping to the internet access

6.2.6 Network Monitoring System

Step1: Login to the Zabbix by entering the username as ‘Admin’ and the password as ‘zabbix’ at the login page.

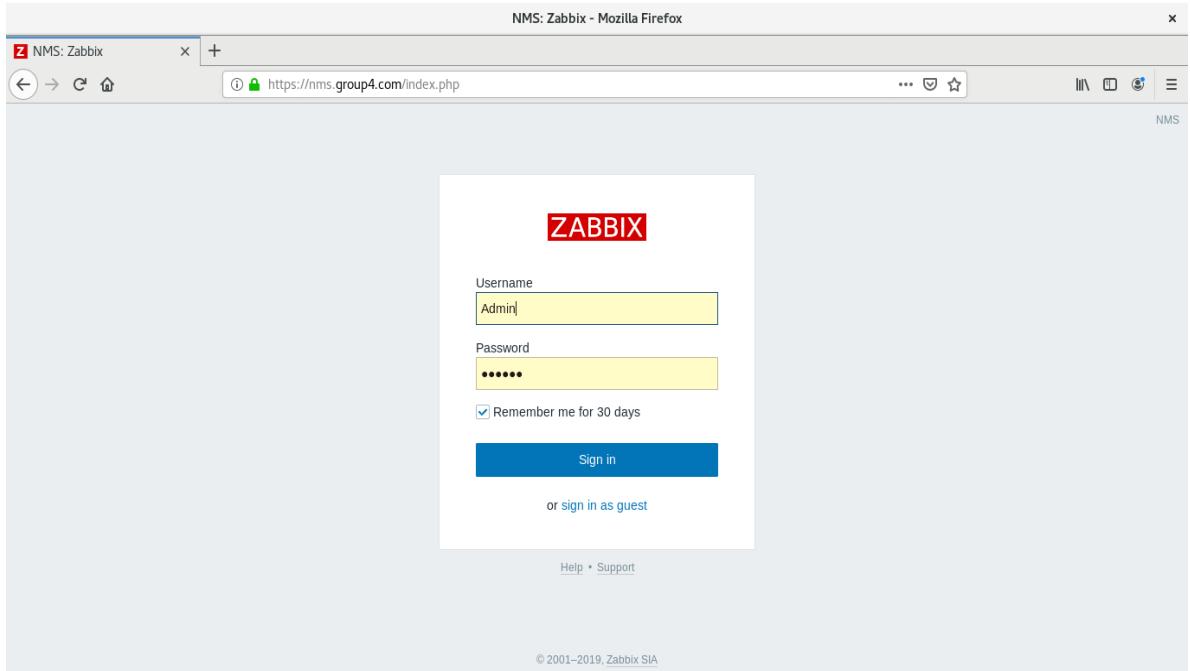


Figure 6.2.6.1: Show the login page of zabbix.

Step 2: Dashboard of the zabbix will be displayed when login is successfully.

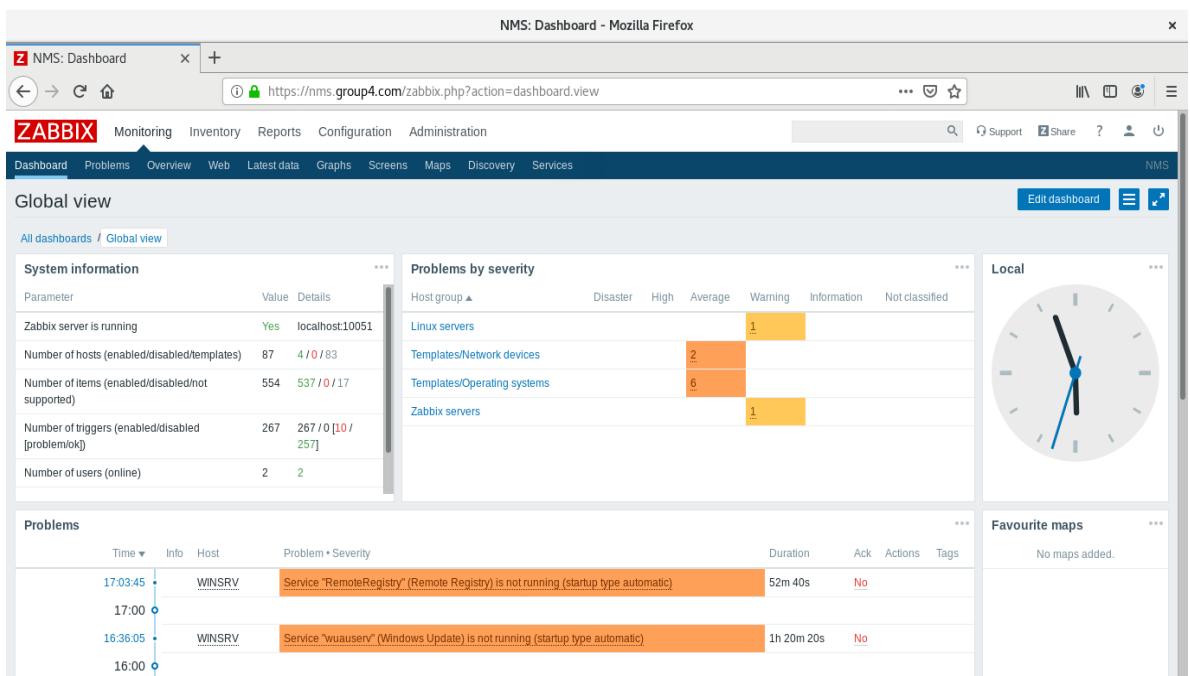


Figure 6.2.6.2: Show the dashboard of the zabbix.

Step 3: Select the ‘Configuration’ at the dashboard and then select the ‘Host’. After that, select ‘New Host’. Set the zabbix agent into zabbix server. Firstly, add Ubuntu server into the zabbix. Change the hostname into ‘ubuntu.group4.com’, the visible name into ‘UBUNTU’ as we set at the Ubuntu PC, at the group choose the Linux servers as the Ubuntu is a Linux Servers. Set IP address following the Ubuntu IP, ‘10.1.1.131’, the DNS name into ‘10.1.1.129’ and select the default port, ‘10050’.

NMS: Configuration of hosts - Mozilla Firefox

Host name: ubuntu.group4.com

Visible name: UBUNTU

Groups: Linux servers

Agent interfaces:

	IP address	DNS name	Connect to	Port	Default
10.1.1.131	10.1.1.129	IP	10050	<input checked="" type="radio"/>	Remove

Add

SNMP interfaces: Add

JMX interfaces: Add

IPMI interfaces: Add

Description: Ubuntu Server

Monitored by proxy: (no proxy)

Enabled:

Figure 6.2.6.3: Show the configuration of the Ubuntu host.

Step 4: After configure the Ubuntu host, go to its template and search for link new templates, ‘Template OS Linux’. After select the new templates, click ‘Add’. The Ubuntu host is done.

NMS: Configuration of hosts - Mozilla Firefox

ZABBIX Monitoring Inventory Reports Configuration Administration

All hosts / UBUNTU Enabled ZBX SNMP JMX IPMI Applications 10 Items 43 Triggers 17 Graphs 8 Discovery rules 2 Web scenarios

Host Templates IPMI Macros Host inventory Encryption

Linked templates Name Action
Template OS Linux Unlink Unlink and clear

Link new templates type here to search Select Add

Update Clone Full clone Delete Cancel

Zabbix 4.0.14, © 2001–2019, Zabbix SIA

Figure 6.2.6.4: Show the templates of Ubuntu server.

Step 5: Then, go to the ‘Monitoring’, then select graph. Select memory as we try to see the graph of memory usage in Ubuntu.

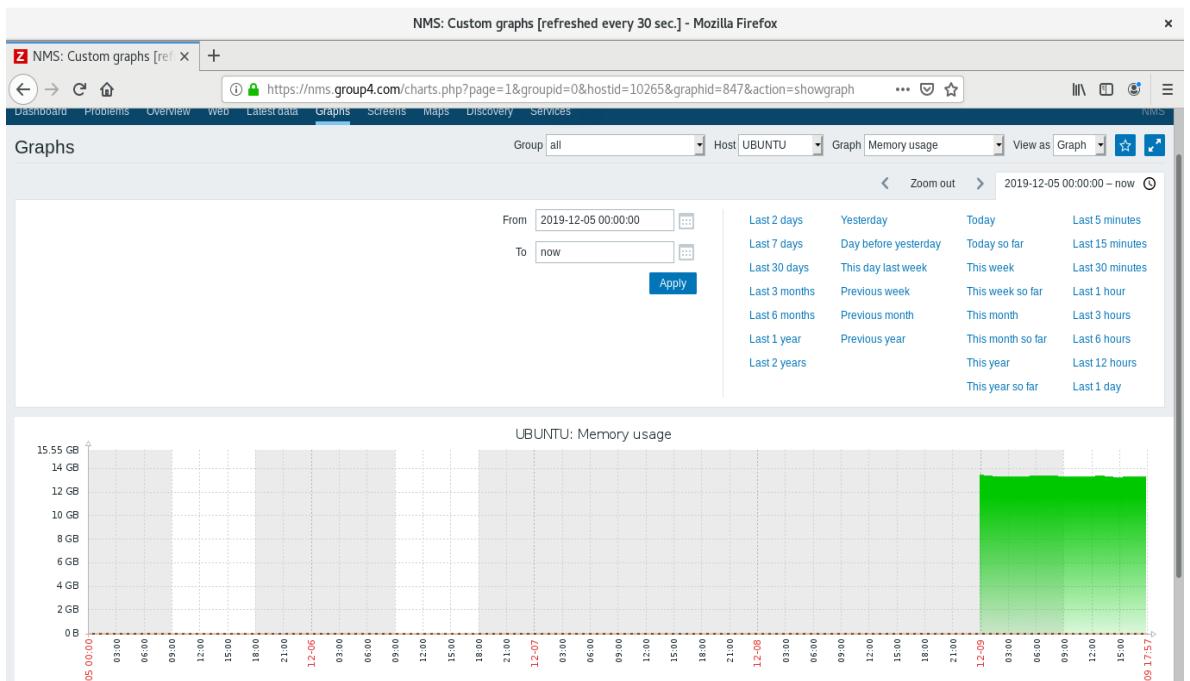


Figure 6.2.6.5: Show the graph of Ubuntu server.

Step 6: After successful add Ubuntu server into zabbix, Select the ‘Configuration’ at the dashboard and then select the ‘Host’. After that, select ‘New Host’. Set the zabbix agent into zabbix server. Add Windows server into the zabbix. Change the hostname into ‘winsrv.group4.com’, the visible name into ‘WINSRV’ as we set at the Windows Server PC, at the group choose the Templates/Operating systems as the Windows is a operating system. Set IP address following the Windows server IP, ’10.1.1.129’, the DNS name into ’10.1.1.129’ and select the default port, ‘10050’.

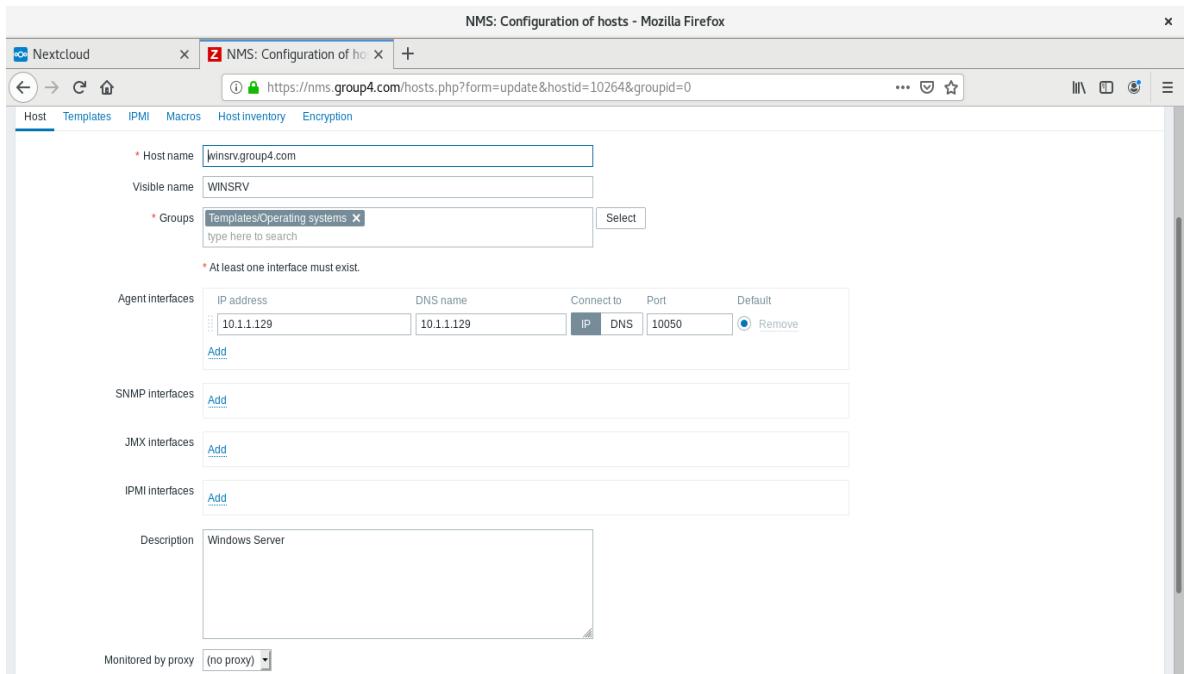


Figure 6.2.6.6: Show the configuration of the Windows server host.

Step 7: After configure the Windows server host, go to its template and search for link new templates, ‘Template OS Windows’. After select the new templates, click ‘Add’. The Windows server host is done.

The screenshot shows the Zabbix configuration interface for host WINSRV. The 'Hosts' menu is open, and the 'Templates' tab is selected. A table lists a single linked template named 'Template OS Windows' with an 'Action' column containing 'Unlink', 'Link and clear', and 'Select'. Below this is a search bar and a button labeled 'Add'.

Figure 6.2.6.7: Show the templates of Windows server.

Step 8: Then, go to the ‘Monitoring’, then select graph. Select memory as we try to see the graph of memory usage in Windows Server.

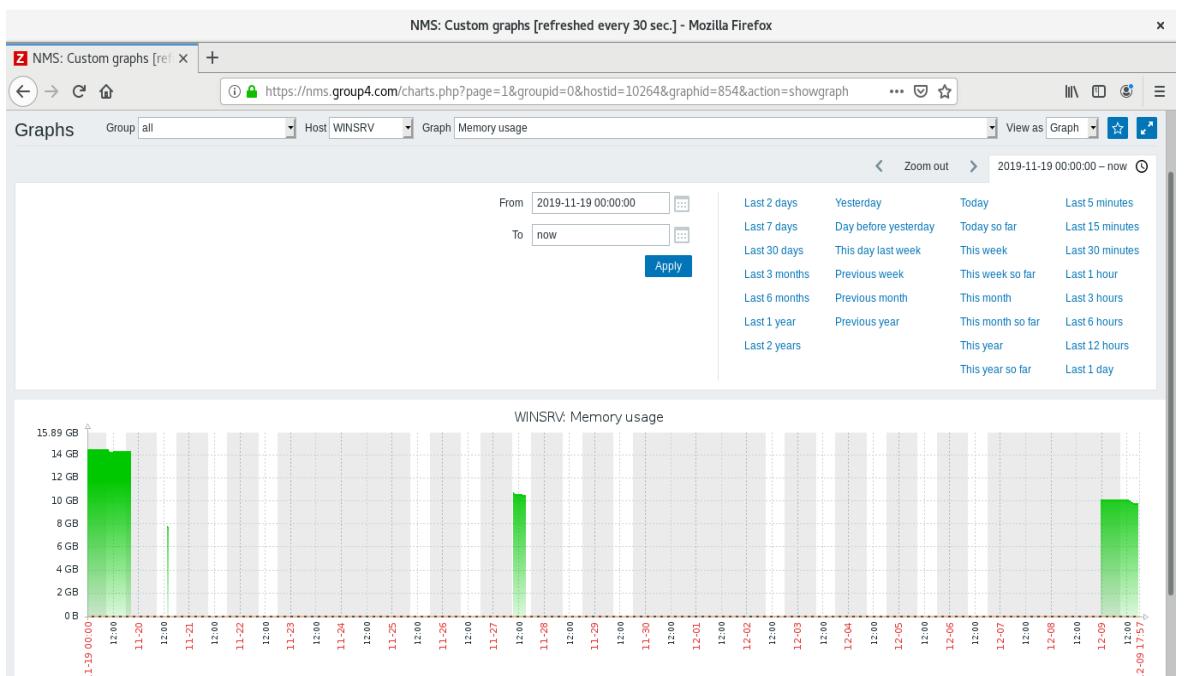


Figure 6.2.6.8: Show the graph of Windows server.

Step 9: At the monitoring graph, it also can see the switch graph.

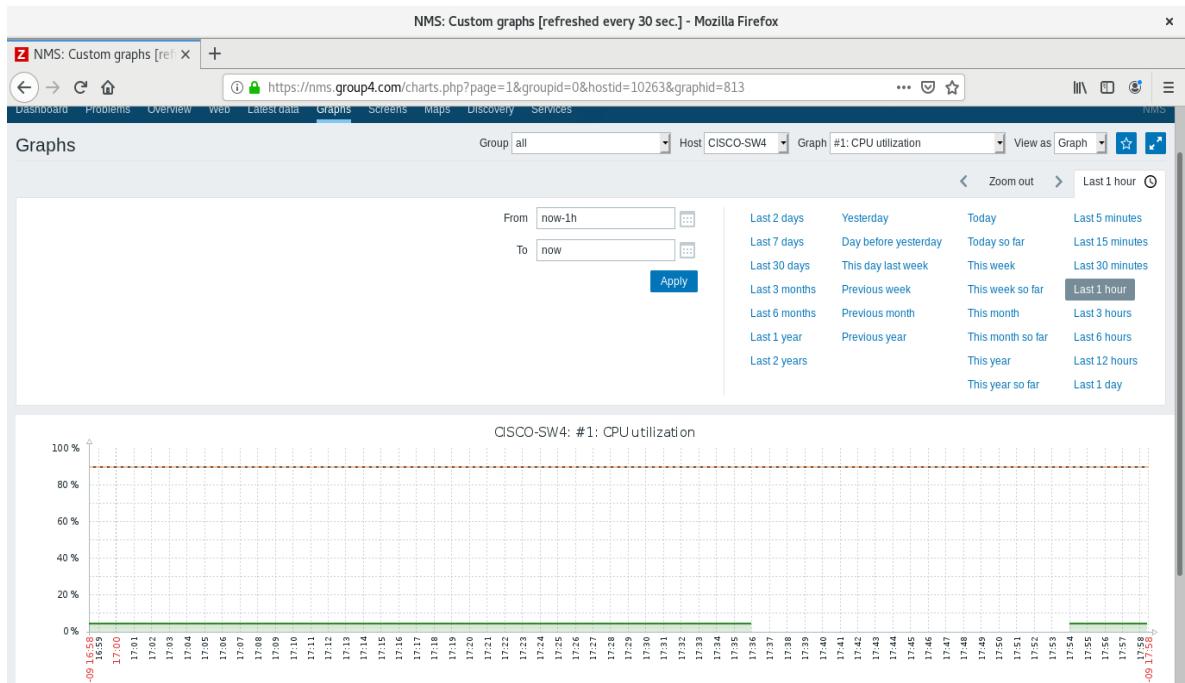


Figure 6.2.6.9: Show the switch's graph.

Step 10: At the configuration, select the host. It will list all the host in the zabbix.

The screenshot shows the 'NMS: Configuration of hosts' interface. The URL is <https://nms.group4.com/hosts.php?ddreset=1>. The top navigation bar includes 'Dashboard', 'Problems', 'Overview', 'Web', 'Latest data', 'Graphs', 'Screens', 'Maps', 'Discovery', and 'Services'. Below the navigation is a search bar with 'Name' and 'DNS', and a 'Templates' dropdown. Monitored by options include 'Any', 'Server', and 'Proxy'. A 'Proxy' dropdown is also present. Buttons for 'Apply' and 'Reset' are at the bottom. The main area is a table listing hosts:

	Name	Applications	Items	Triggers	Graphs	Discovery	Web	Port	Status	Availability	Agent encryption	Info
<input type="checkbox"/>	CISCO-SW4	Applications 9	Items 276	Triggers 129	Graphs 31	Discovery 8	Web 127.0.0.1:10050		Enabled	ZBX, SNMP, JMX, IPMI	NONE	
<input type="checkbox"/>	UBUNTU	Applications 10	Items 43	Triggers 17	Graphs 8	Discovery 2	Web 10.1.1.131:10050		Enabled	ZBX, SNMP, JMX, IPMI	NONE	
<input type="checkbox"/>	WINSRV	Applications 12	Items 152	Triggers 73	Graphs 34	Discovery 3	Web 10.1.1.129:10050		Enabled	ZBX, SNMP, JMX, IPMI	NONE	
<input type="checkbox"/>	Zabbix server	Applications 11	Items 83	Triggers 48	Graphs 13	Discovery 2	Web 127.0.0.1:10050		Enabled	ZBX, SNMP, JMX, IPMI	NONE	

At the bottom, there are buttons for '0 selected', 'Enable', 'Disable', 'Export', 'Mass update', and 'Delete'. A note says 'Displaying 4 of 4 found'.

Figure 6.2.6.10: Show the list of host in zabbix.

6.2.7 Wireless User Authentication by using RADIUS Server

Step 1: Open Wi-Fi in your mobile device or laptop. Insert your identity and password.

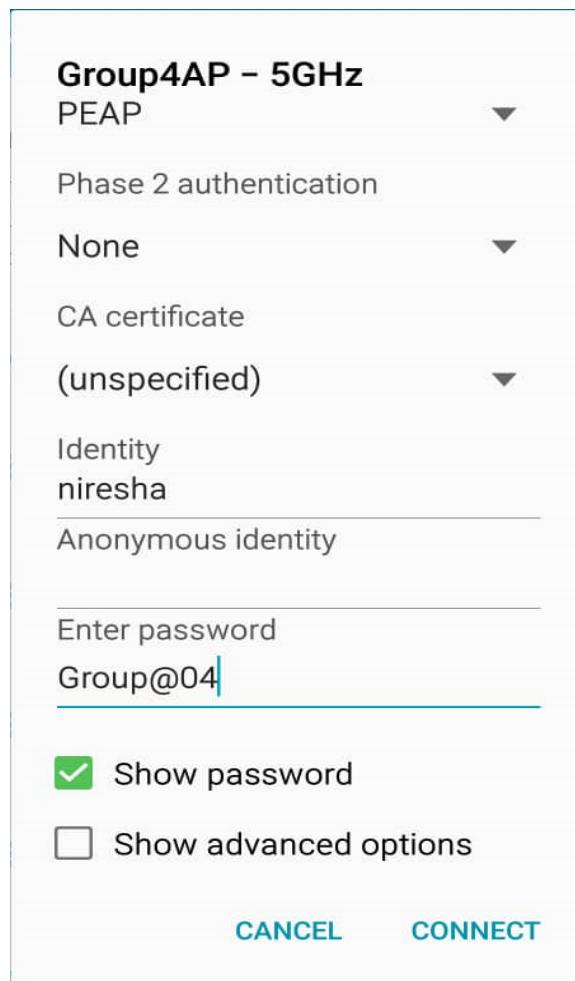


Figure 6.2.7.1: Insert identity and password

Step 2: If connected, then your wireless authentication is successful.

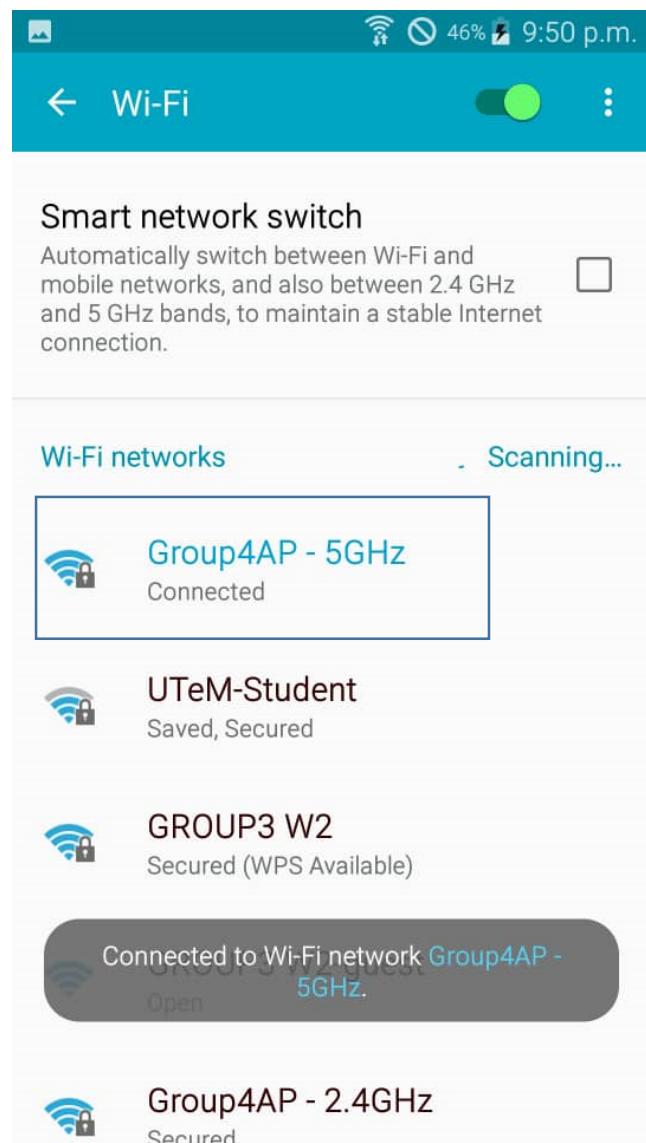


Figure 6.2.7.2: Wireless authentication successful

6.2.8 IPSec VPN Server for remote employee

Clients Server in Window Server

Testing on Internal Network

Step 1 : Open the SoftEther VPN Client Manager and test for the connection.

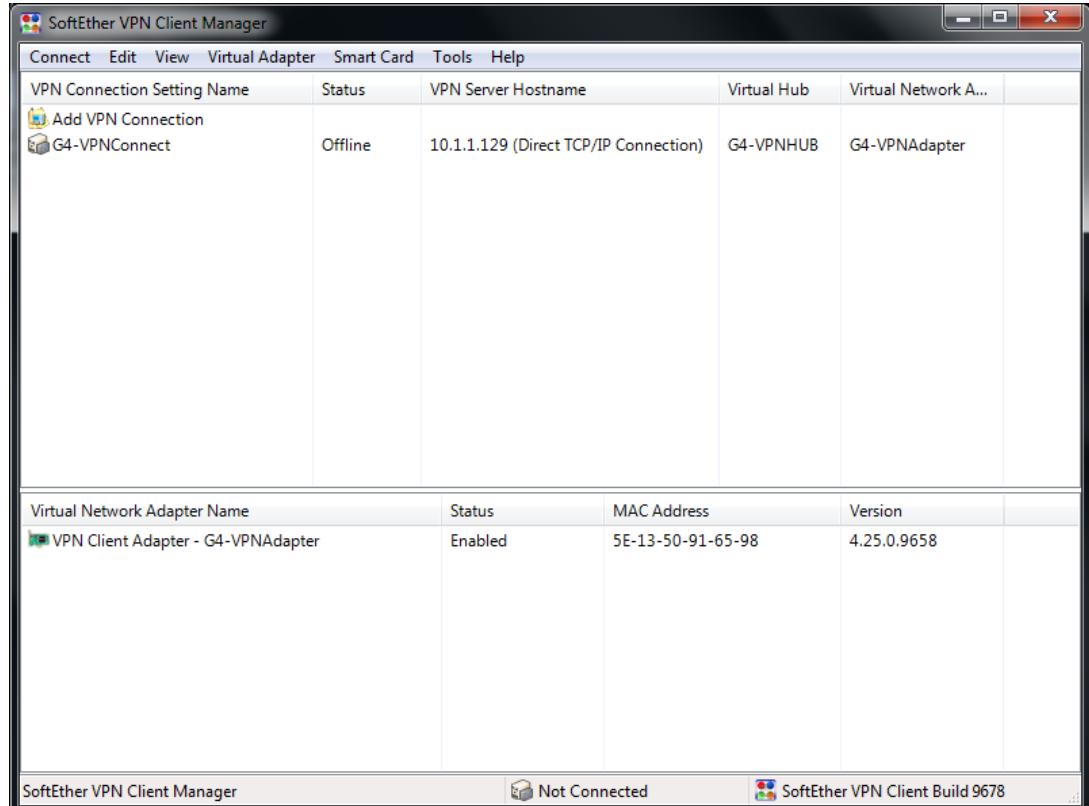


Figure 6.2.8.1: GUI of SoftEther VPN Client Manager

Step 2: Select VPN Connection (G4-VPNConnect) and select Connect.

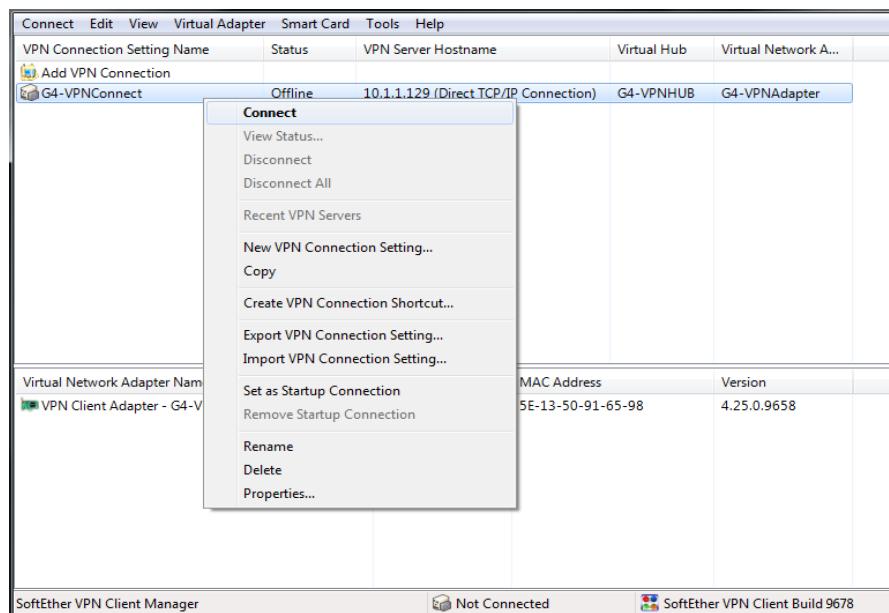


Figure 6.2.8.2: Connect to VPN

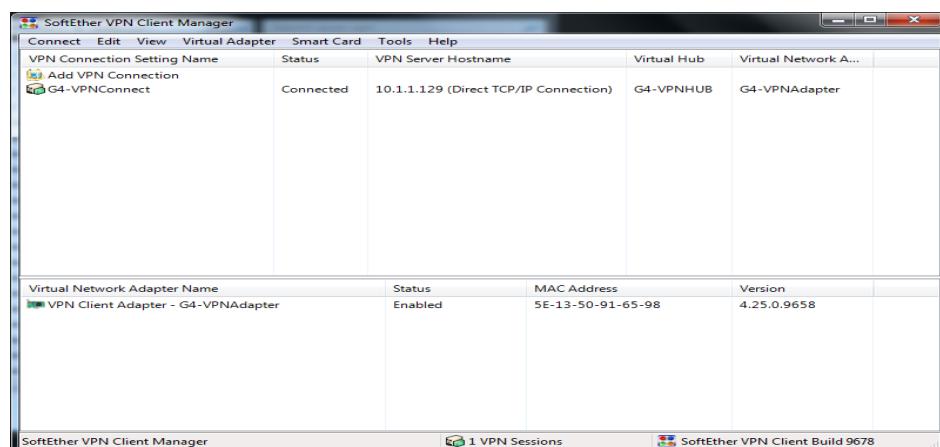


Figure 6.2.8.3: Connected to VPN

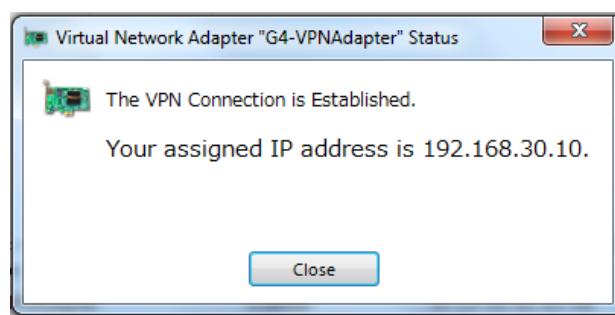


Figure 6.2.8.4: Connection sucessful

Step 3: Go to SoftEther VPN Server Manager machine and verify the VPN connection.

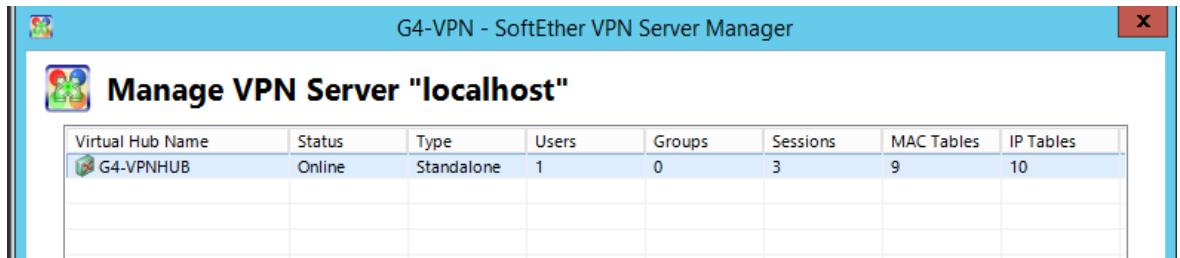


Figure 6.2.8.5: Verify VPN Connection

Step 4: Open command prompt and enter command ipconfig /all to verify the ip address assigned by SoftEther VPN.

```
Unknown adapter G4-UPNAdapter - UPN Client:
Connection-specific DNS Suffix . : group4.com
Description . . . . . : VPN Client Adapter - G4-UPNAdapter
Physical Address . . . . . : 5E-13-50-91-65-98
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IPv6 Address . . . . . : 1230:1111:aaaa:2:b14f:b1a2:ba13:5255(Pref
ered)
Temporary IPv6 Address . . . . . : 1230:1111:aaaa:2:c60:ad39:27bb:4118(Pref
ered)
Link-local IPv6 Address . . . . . : fe80::b14f:b1a2:ba13:5255%28(PREFERRED)
IPv4 Address . . . . . : 192.168.30.10<Preferred>
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, November 26, 2019 12:18:48 PM
Lease Expires . . . . . : Tuesday, November 26, 2019 2:18:48 PM
Default Gateway . . . . . : fe80::216:c8ff:fea1:35d7%28
                           192.168.30.1
DHCP Server . . . . . : 192.168.30.1
DNS Servers . . . . . : 192.168.30.1
NetBIOS over Tcpip . . . . . : Enabled
```

Figure 6.2.8.6: Verify IP address

Testing on External Network

Step 1: Connect to Group 3 client network and receive assigned IP address from Group 3 DHCP server.

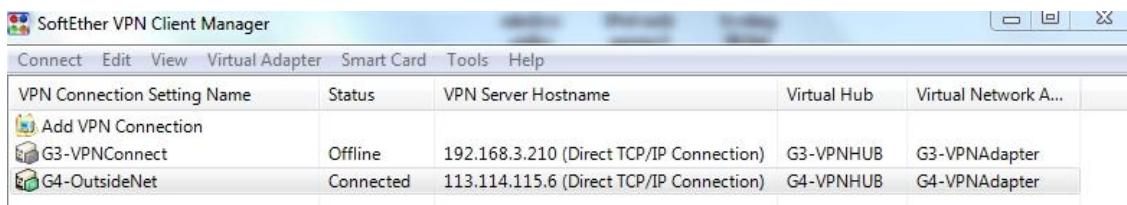


Figure 6.2.8.7: GUI of SoftEther VPN Client Manager

Step 2: Open the SoftEther VPN Client Manager and make new configuration for Group 4 VPN Connection.

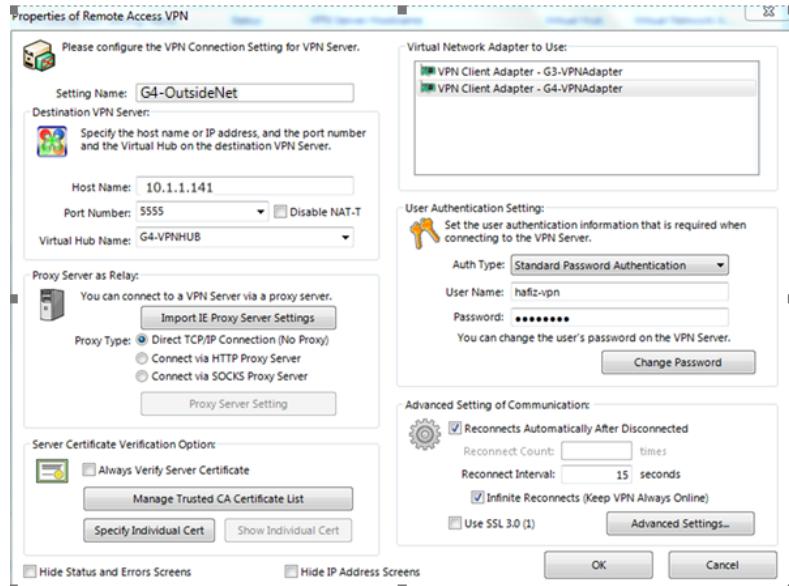


Figure 6.2.8.8: Properties of G4-OutsideNet

Step 3: Connect to Group 4 VPN Server on Group 3 client PC.

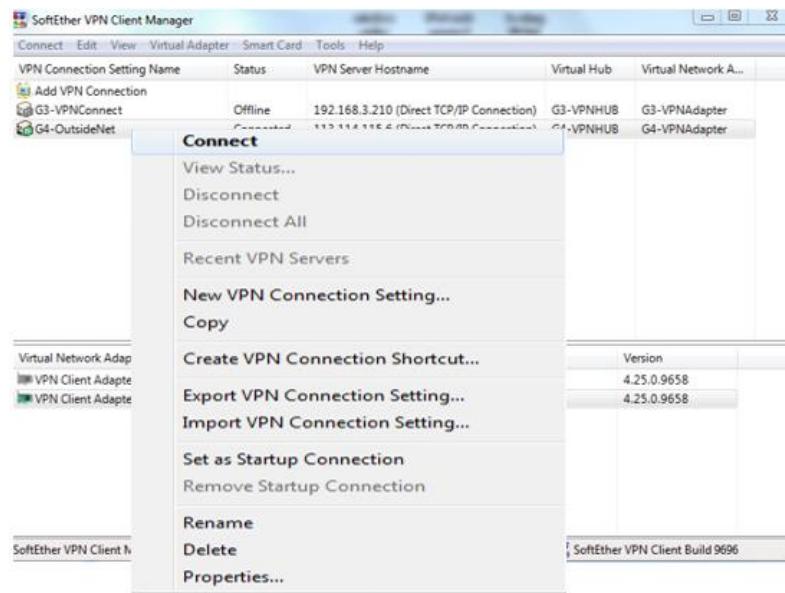


Figure 6.2.8.9: Connect to VPN Server

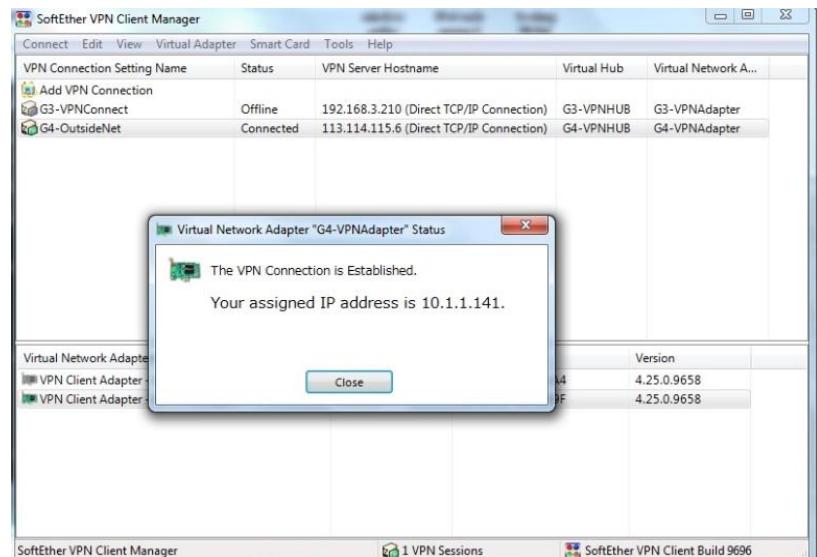


Figure 6.2.8.10: VPN Connection Established

Step 4 : Open command prompt in Group 3 client PC and enter command ipconfig /all to verify the ip address assigned by SoftEther VPN

```
C:\Windows\system32\cmd.exe
Windows IP Configuration

Unknown adapter Local Area Connection 2:

Connection-specific DNS Suffix . : group4.com
IPv6 Address . . . . . : 1230:1111:aaaa:2:89aa:412e:342f:dad
Temporary IPv6 Address . . . . . : 1230:1111:aaaa:2:8874:5806:6426:2d30
Link-local IPv6 Address . . . . . : fe80::89aa:412e:342f:dad%22
IPv4 Address . . . . . : 10.1.1.141
Subnet Mask . . . . . : 255.255.255.240
Default Gateway . . . . . : fe80::216:c8ff:fea1:35d?%22
                           10.1.1.142

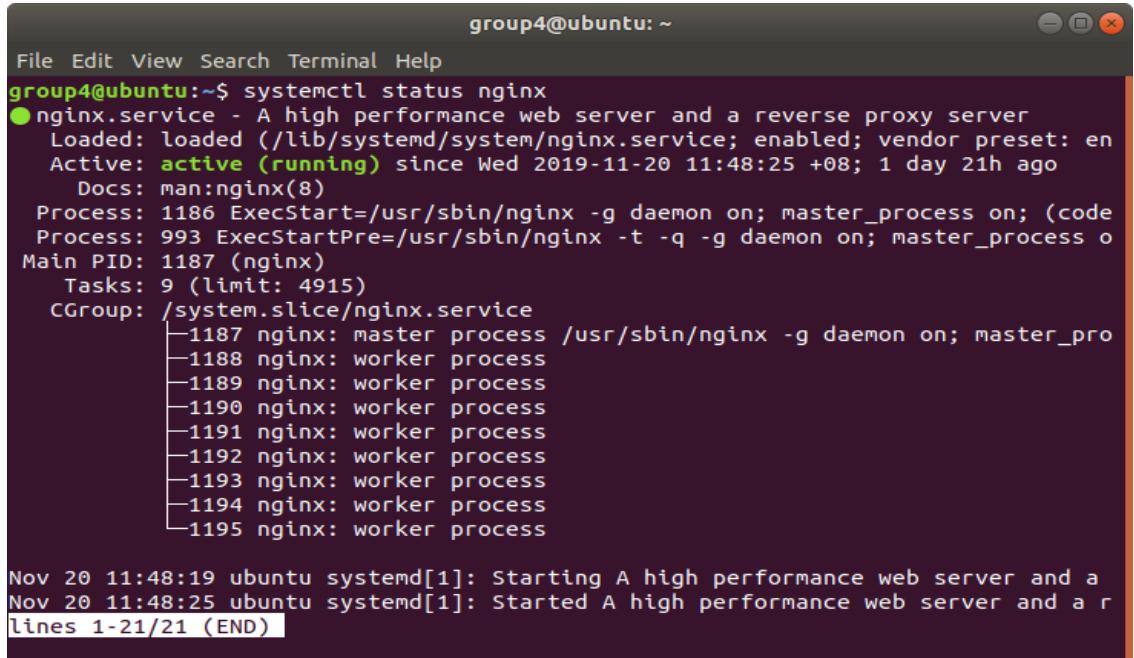
Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : group3.com
IPv6 Address . . . . . : 1011:1011:1111:100:e4d8:c9e0:2983:dfe1
Temporary IPv6 Address . . . . . : 1011:1011:1111:100:b475:5116:f7a:1e3
Link-local IPv6 Address . . . . . : fe80::e4d8:c9e0:2983:dfe1%11
IPv4 Address . . . . . : 192.168.3.11
Subnet Mask . . . . . : 255.255.255.128
Default Gateway . . . . . : fe80::226:cbff:fed:a:b169%11
                           192.168.3.1
```

Figure 6.2.8.11: Verify ip address in cmd

6.2.9 Reverse Proxy Server

Step 1: Check the status of proxy service and make sure the service is running.



```
group4@ubuntu:~$ systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: en
   Active: active (running) since Wed 2019-11-20 11:48:25 +08; 1 day 21h ago
     Docs: man:nginx(8)
 Process: 1186 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code
Process: 993 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process o
 Main PID: 1187 (nginx)
    Tasks: 9 (limit: 4915)
   CGroup: /system.slice/nginx.service
           ├─1187 nginx: master process /usr/sbin/nginx -g daemon on; master_pro
           ├─1188 nginx: worker process
           ├─1189 nginx: worker process
           ├─1190 nginx: worker process
           ├─1191 nginx: worker process
           ├─1192 nginx: worker process
           ├─1193 nginx: worker process
           ├─1194 nginx: worker process
           └─1195 nginx: worker process

Nov 20 11:48:19 ubuntu systemd[1]: Starting A high performance web server and a
Nov 20 11:48:25 ubuntu systemd[1]: Started A high performance web server and a r
lines 1-21/21 (END)
```

Figure 6.2.9.1: Reverse Proxy Status.

Step 2: <https://www.group4.com> is the website that have been requested by the client through proxy server.

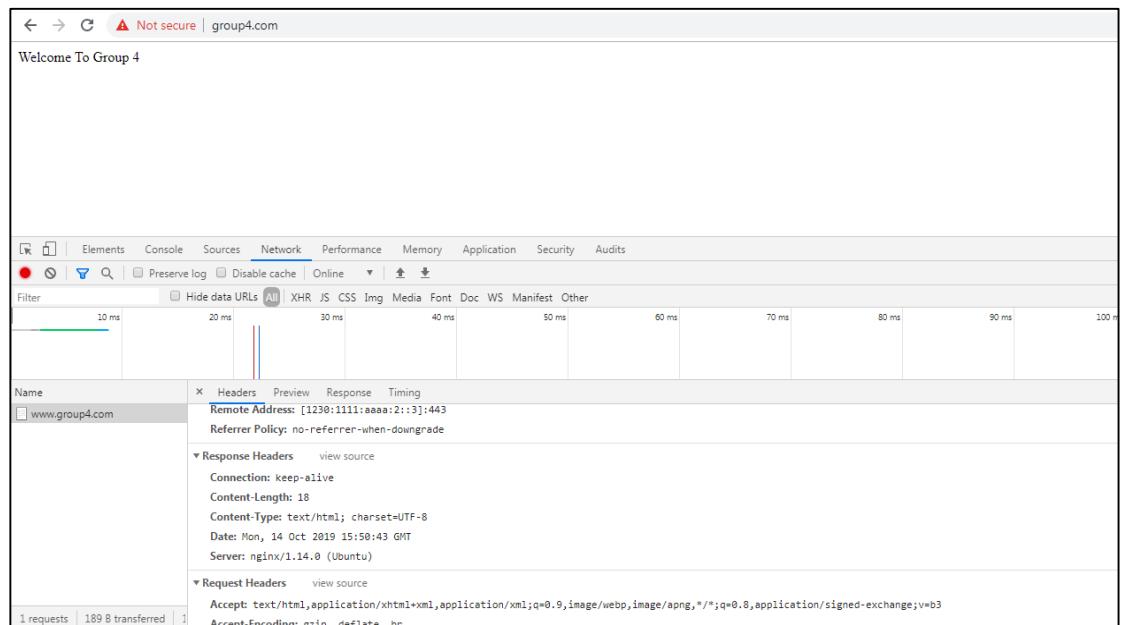


Figure 6.2.9.2: Requested Website.

6.2.10 Trivial File Transfer Protocol (TFTP)

Step 1: Check the status of tftp service and make sure the service is active.

```
root@debian:/home/group4# service tftpd-hpa status
● tftpd-hpa.service - LSB: HPA's tftp server
  Loaded: loaded (/etc/init.d/tftpd-hpa; generated; vendor preset: enabled)
  Active: active (running) since Sat 2019-11-16 18:28:38 +08; 3min 46s ago
    Docs: man:systemd-sysv-generator(8)
 Process: 9977 ExecStop=/etc/init.d/tftpd-hpa stop (code=exited, status=0/SUCCESS)
 Process: 10014 ExecStart=/etc/init.d/tftpd-hpa start (code=exited, status=0/SUCCESS)
   Tasks: 1 (limit: 4915)
  CGroup: /system.slice/tftpd-hpa.service
          └─10021 /usr/sbin/in.tftpd --listen --user tftp --address 0.0.0.0:69 --secure -c /srv/tftp

Nov 16 18:28:38 debian systemd[1]: Starting LSB: HPA's tftp server...
Nov 16 18:28:38 debian tftpd-hpa[10014]: Starting HPA's tftpd: in.tftpd.
Nov 16 18:28:38 debian systemd[1]: Started LSB: HPA's tftp server.
root@debian:/home/group4#
```

Figure 6.2.10.1: Tftp Status

Step 2: Get into PuTTY of the Switch and terminal and type “copy running-config tftp” to save the switch configuration via Tftp.

```
SW4>
SW4>en
SW4#copy running-config tftp
Address or name of remote host []? 10.1.1.130
Destination filename [sw4-config]?
! !
7933 bytes copied in 1.283 secs (6183 bytes/sec)
SW4#
```

Figure 6.2.10.2: command to save the switch configuration.

6.2.11 IPsec site-to-site

Step 1: Show the settings used by IPsec security associations (SAs) by enter the command ‘*show crypto ipsec sa*’.

```

COM1 - PuTTY

interface: Serial0/2/1
Crypto map tag: CMAP, local addr 113.114.115.1

protected vrf: (none)
local ident (addr/mask/prot/port): (113.114.115.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (113.114.115.2/255.255.255.255/47/0)
current_peer 113.114.115.2 port 500
    PERMIT, flags={origin_is_acl,}
#pkts encaps: 467652, #pkts encrypt: 467652, #pkts digest: 467652
#pkts decaps: 299765, #pkts decrypt: 299765, #pkts verify: 299765
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 11, #recv errors 5

local crypto endpt.: 113.114.115.1, remote crypto endpt.: 113.114.115.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/2/1
current outbound spi: 0xF417EA85(4095208069)

inbound esp sas:
    spi: 0xD5DD37DC(3588044764)
        transform: esp-aes esp-sha-hmac ,
--More-- □

```

Figure 62.2.11.1: *show crypto ipsec sa*.

Step 2: Show detailed information about the session which is the session status is up and active.

```

R4#show crypto session
Crypto session current status

Interface: Serial0/2/1
Session status: UP-ACTIVE
Peer: 113.114.115.2 port 500
IKE SA: local 113.114.115.1/500 remote 113.114.115.2/500 Active
IPSEC FLOW: permit 47 host 113.114.115.1 host 113.114.115.2
    Active SAs: 2, origin: crypto map

R4#

```

Figure 6.2.11.2: *Show crypto session*

Step 3: Ping to the router of the other group.

```

R4#ping 192.168.3.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/31/32 ms
R4#

```

Figure 6.2.11.3: *ping 192.168.3.2*

6.2.12 Windows Server Hardening

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.

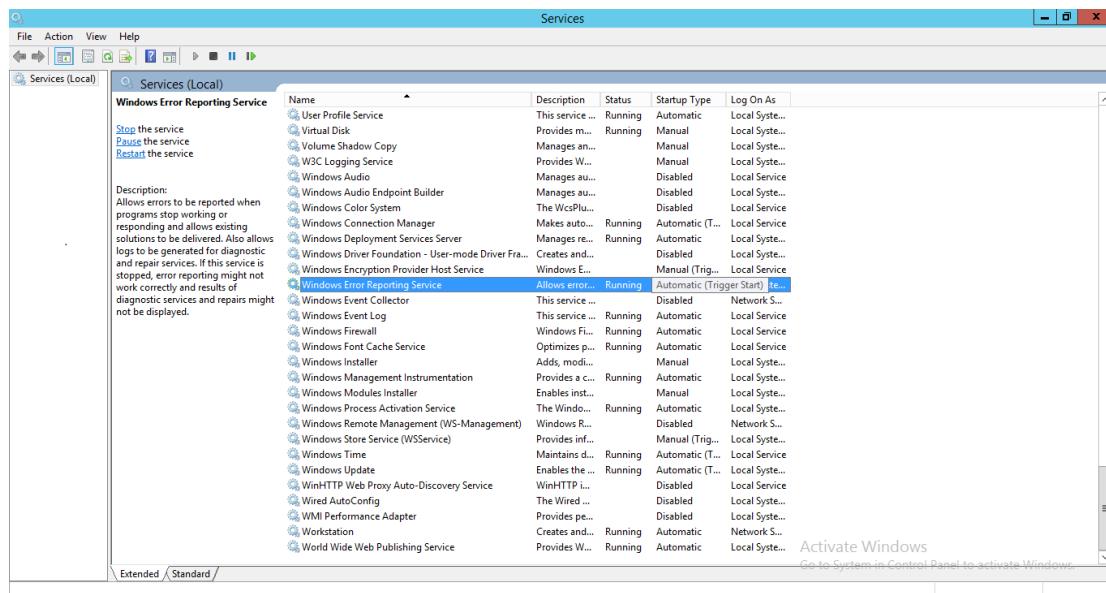


Figure 6.2.12.1: Windows Error Reporting

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.

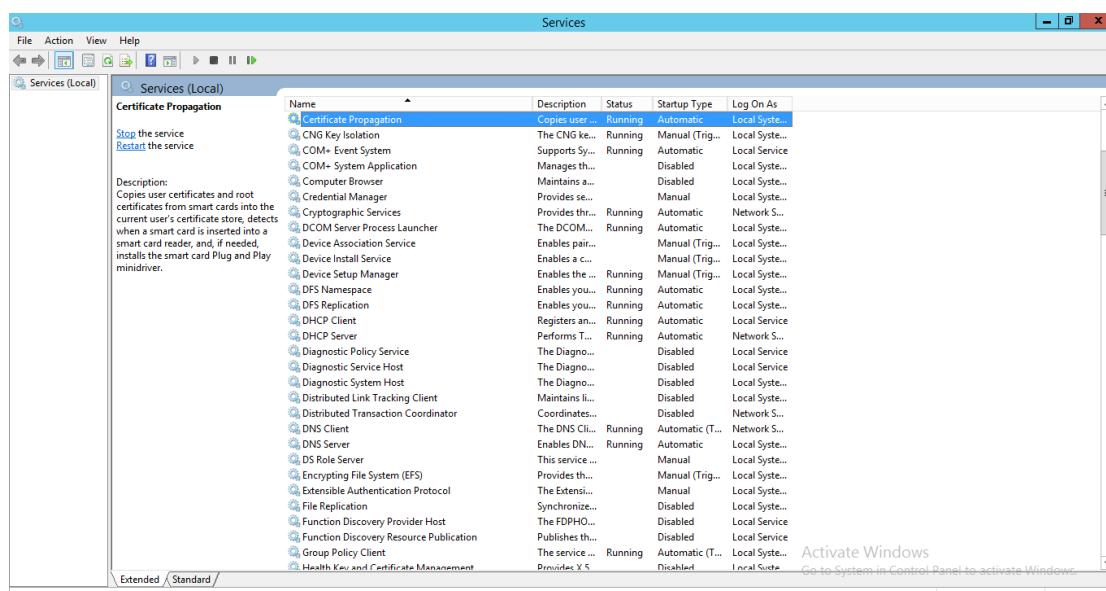


Figure 6.2.12.2: Check the status of Certificate Propagation

Step 3: Ensure NetLogon startup is Automatic and started. This maintains a channel between computer and domain controller. The NetLogon sub-key stores information for the NetLogon service. The NetLogon service verifies log-on request and it registers, authenticates and locates domain controllers.

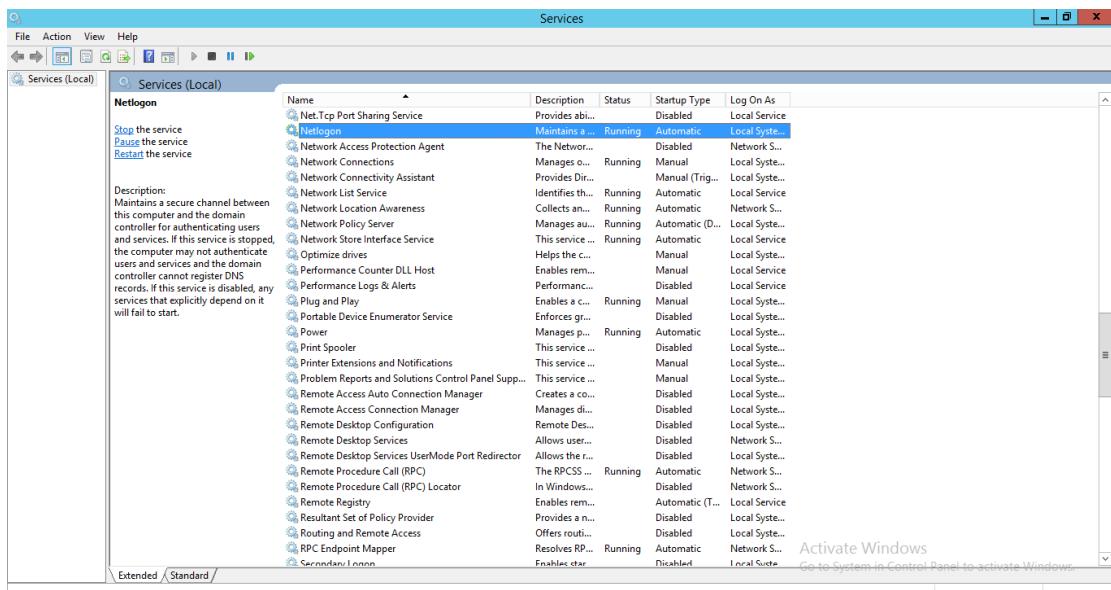


Figure 6.2.12.3: Checking on NetLogon startup type

Step 4: Show that packets has been encrypt.

The screenshot shows a PuTTY terminal window titled 'COM1 - PuTTY'. The terminal displays a log of IPsec traffic. A red box highlights a section of the log where the number of encrypted and decrypted packets is being tracked. The log includes details about the crypto map, local and remote identifiers, current peer, and various statistics for compressed and decompressed packets. It also shows the local and remote crypto endpoints, path MTU, and current outbound SPI.

```

interface: Serial0/2/1
Crypto map tag: CMAP, local addr 113.114.115.1

protected vrf: (none)
local ident (addr/mask/prot/port): (113.114.115.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (113.114.115.2/255.255.255.255/47/0)
current_peer 113.114.115.2 port 500
    PERMIT, flags={origin_is acl,}
#pkts encaps: 467652, #pkts encrypt: 467652, #pkts digest: 467652
#pkts decaps: 299765, #pkts decrypt: 299765, #pkts verify: 299765
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 11, #recv errors 5

local crypto endpt.: 113.114.115.1, remote crypto endpt.: 113.114.115.2
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/2/1
current outbound spi: 0xF417EA85(4095208069)

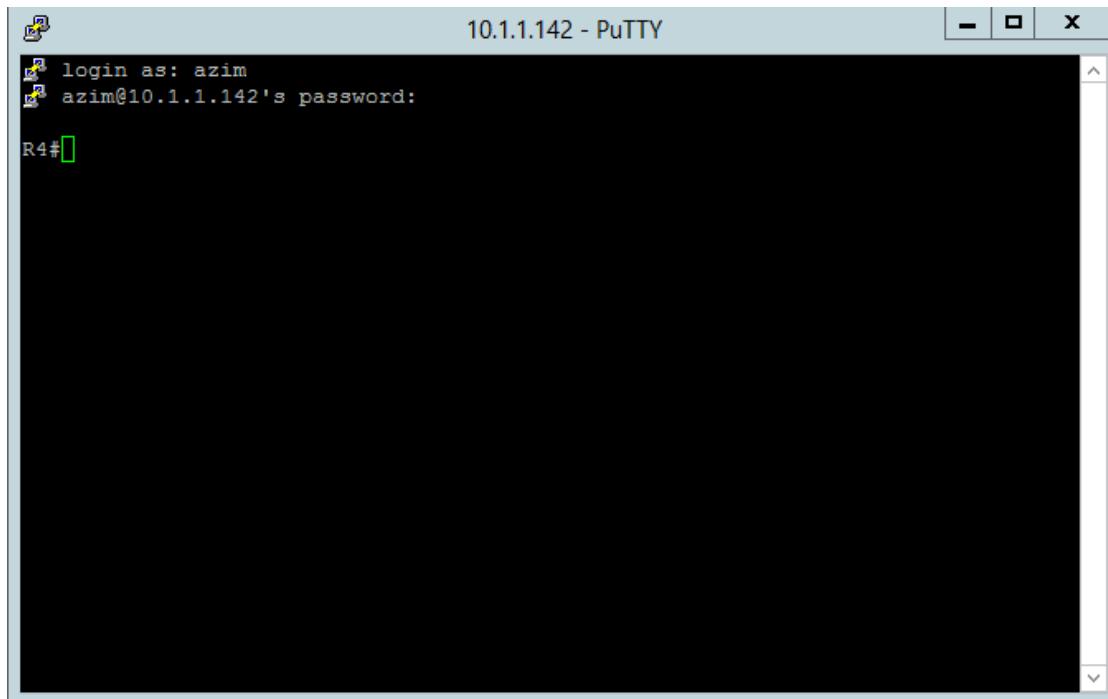
inbound esp sas:
    spi: 0xD5DD37DC(3588044764)
        transform: esp-aes esp-sha-hmac ,
--More-- 

```

Figure 6.2.12.4: Show crypto ipsec sa

6.2.13 Authentication, Authorization and Accounting (AAA) Using Radius

Step 1: User need to login the username and password that already set in Active Directory. Insert username “azim” and password “Skills39”.



A screenshot of a PuTTY terminal window titled "10.1.1.142 - PuTTY". The window shows a login session. The text in the terminal is:
login as: azim
azim@10.1.1.142's password:
R4#

Figure 6.2.13.1: Show crypto ipsec sa

6.2.14 Authentication User by Integrating Active Directory with Linux

Step 1: Log in as “Azim”

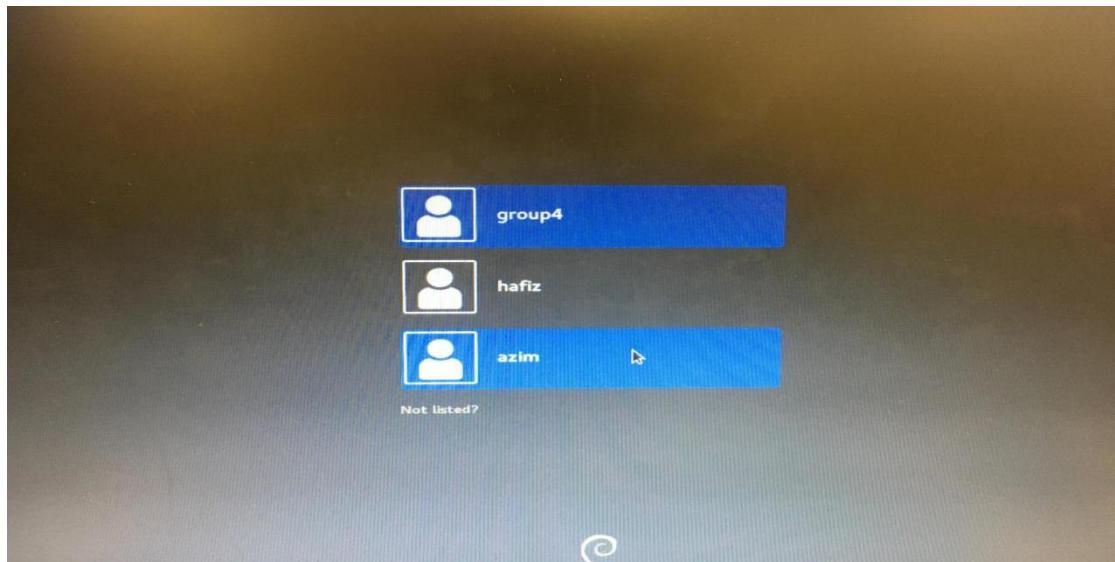


Figure 6.2.14.1: User Login

Step 2: Enter the user password for “Azim” and will successfully login.

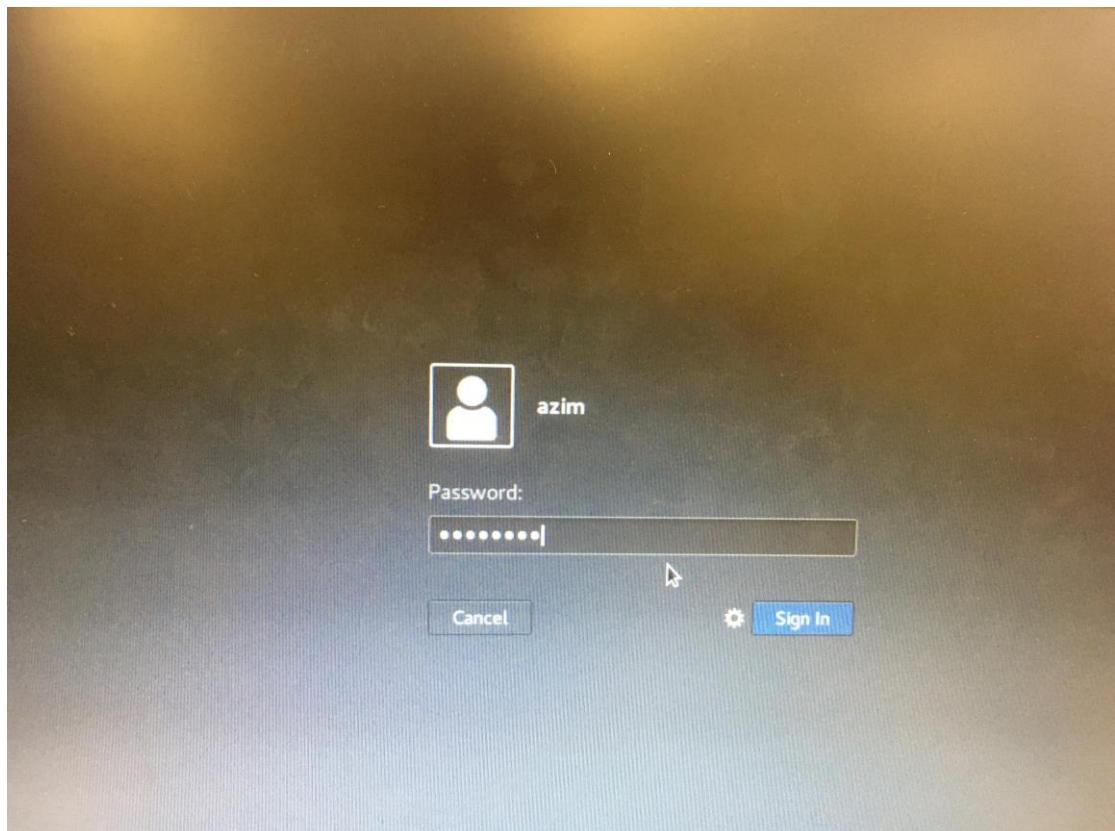


Figure 6.2.14.2: Enter User Password

6.2.15 Quota Screening

Step 1: This step for testing quota. Sign in into user account, which is ‘ituser001’. Open files and select Computer and on the Network Selection that have ituser001 folder. Can see that total size of the folder is 5GB

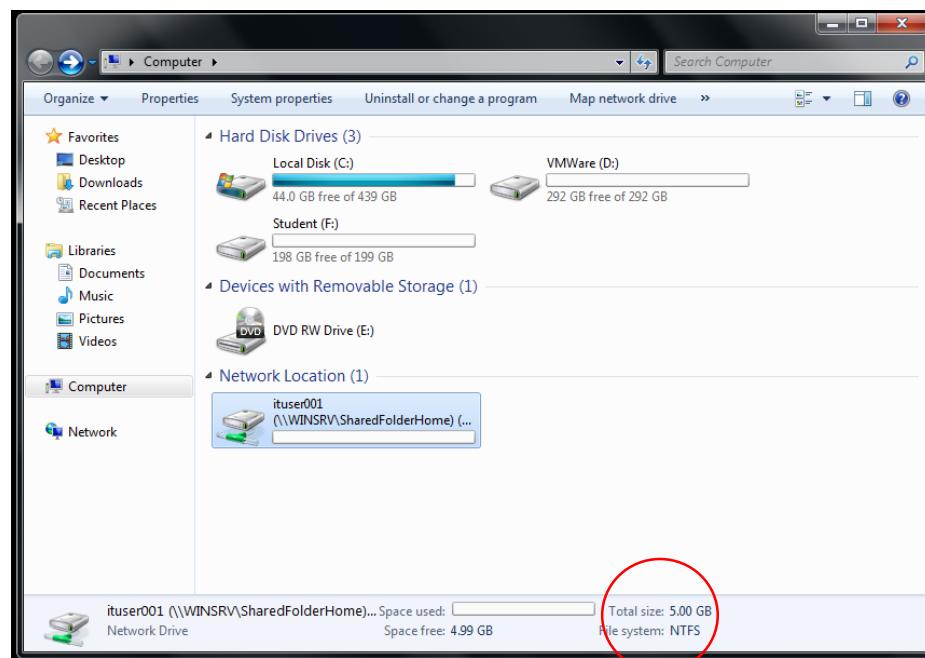


Figure 6.2.15.1: Test Quota

Step 2: For testing file screening, click the ituser001 folder. Right-click and select New and Text Document

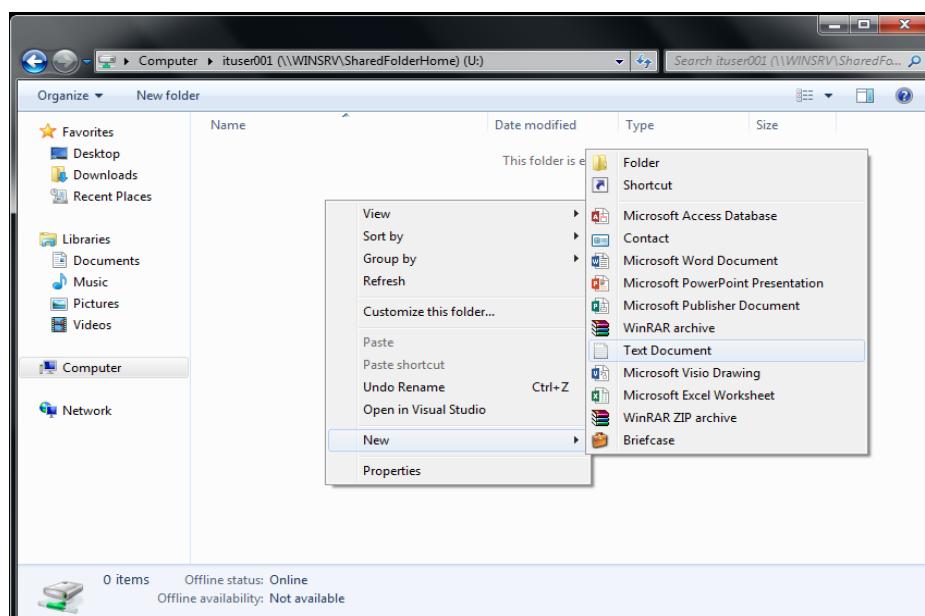


Figure 6.2.15.2: Test Quota

Step 3: For Text Document will using extension .txt

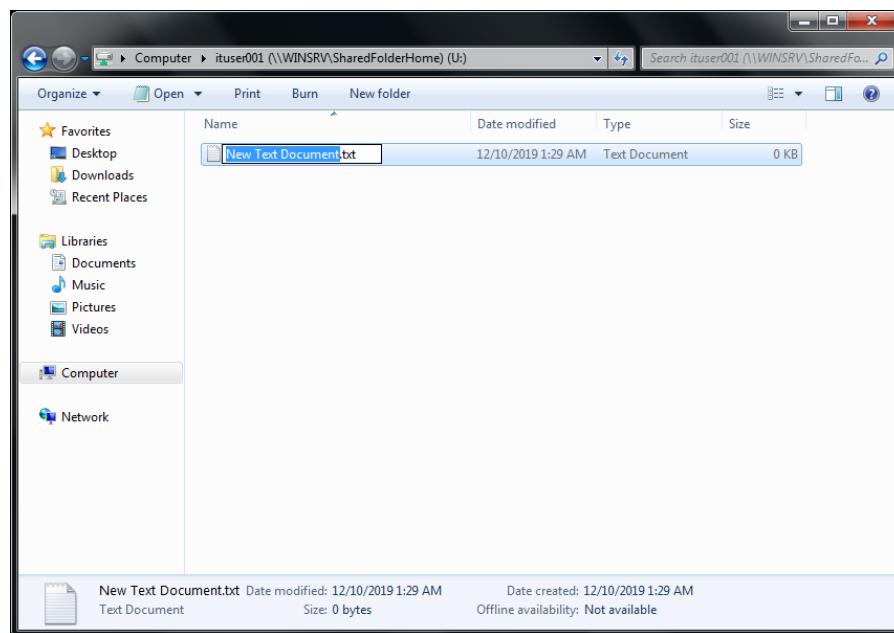


Figure 6.2.15.3: Create new Text Document

Step 4: Try to change the extension to .exe but it fails because changing extension has been blocked

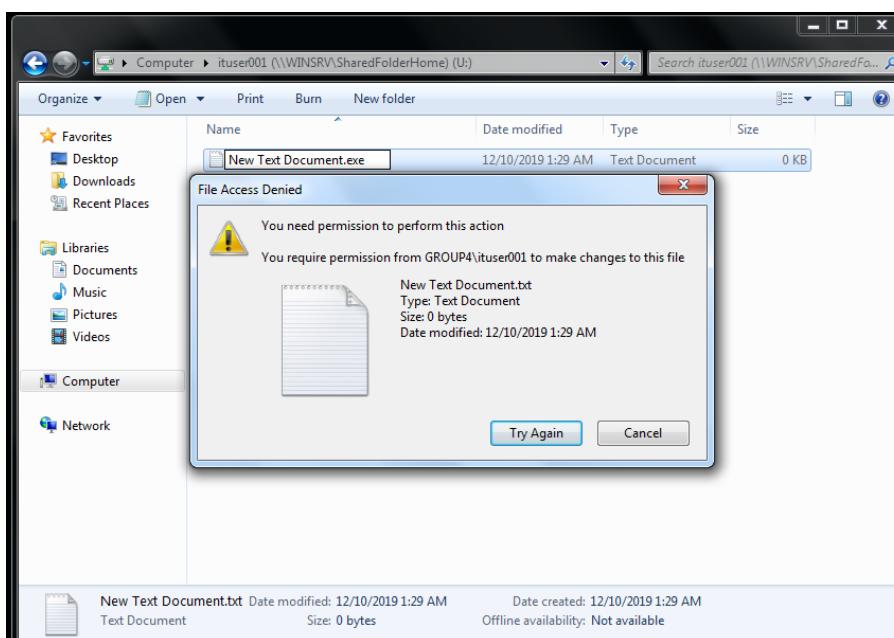


Figure 6.2.15.4: Change extension fail

6.2.16 TESTING SERVER VIRTUALIZATION

Step 1: View all the Client IP address. 10.1.1.2 is the hostname

Client IP Address	Name	Lease Expiration	Type	Unique ID	Description	Network Access Protection	Pro
10.1.1.1	WAP	Reservation (inactive)	None	58ef680d9...	Full Access	N/A	
10.1.1.2	MW15.group4.com	12/7/2019 5:15:18 PM	DHCP	3417ebca9...	Full Access	N/A	
10.1.1.3		12/15/2019 4:10:48 PM	DHCP	d89a34245...	Full Access	N/A	
10.1.1.4	HUAWEI_nova_2_lit...	12/13/2019 12:45:55 PM	DHCP	bc3d85890...	Full Access	N/A	

Figure 6.2.16.1: Hostname IP address on primary server

Step 2: show ipconfig/all

```
C:\>ipconfig /all
Windows IP Configuration

Host Name . . . . . : MW15
Primary Dns Suffix . . . . . : group4.com
Node Type . . . . . : Mixed
IP Routing Enabled . . . . . : No
WINS Proxy Enabled . . . . . : No
DNS Suffix Search List . . . . . : group4.com

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . . . . : group4.com
Description . . . . . : Intel(R) 82579LM Gigabit Network Connection
Physical Address . . . . . : 34-17-EB-CA-92-D7
DHCP Enabled . . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IPv6 Address . . . . . : 1230:1111:aaaa:1:8d44:4b56:239d:1749 <Preferred>
Temporary IPv6 Address . . . . . : 1230:1111:aaaa:1:865:552a:fefd:eb0a<Preferred>
Link-local IPv6 Address . . . . . : fe80::8d44:4b56:239d:1749%11<Preferred>
IPv4 Address . . . . . : 10.1.1.2<Preferred>
Subnet Mask . . . . . : 255.255.255.128
Lease Obtained . . . . . : Saturday, December 07, 2019 4:15:18 PM
Lease Expires . . . . . : Saturday, December 07, 2019 5:15:18 PM
Default Gateway . . . . . : fe80::216:c8ff:fe1:35d7%11
                                     10 . 1 . 1 . 126
DHCP Server . . . . . : 10.1.1.129
DNS Servers . . . . . : 10.1.1.2
NetBIOS over Tcpip . . . . . : Enabled

Tunnel adapter isatap.group4.com:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . : group4.com
Description . . . . . : Microsoft ISATAP Adapter
Physical Address . . . . . : 00-00-00-00-00-00-E0
DHCP Enabled . . . . . : No
Autoconfiguration Enabled . . . . . : Yes

Tunnel adapter Teredo Tunneling Pseudo-Interface:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . : Teredo Tunneling Pseudo-Interface
Description . . . . . : Teredo Tunneling Pseudo-Interface
Physical Address . . . . . : 00-00-00-00-00-00-E0
DHCP Enabled . . . . . : No
Autoconfiguration Enabled . . . . . : Yes
```

Figure 6.2.16.2: IP address for primary server

Step 3: Select tools > DHCP > right-click and choose All Tasks > click Stop

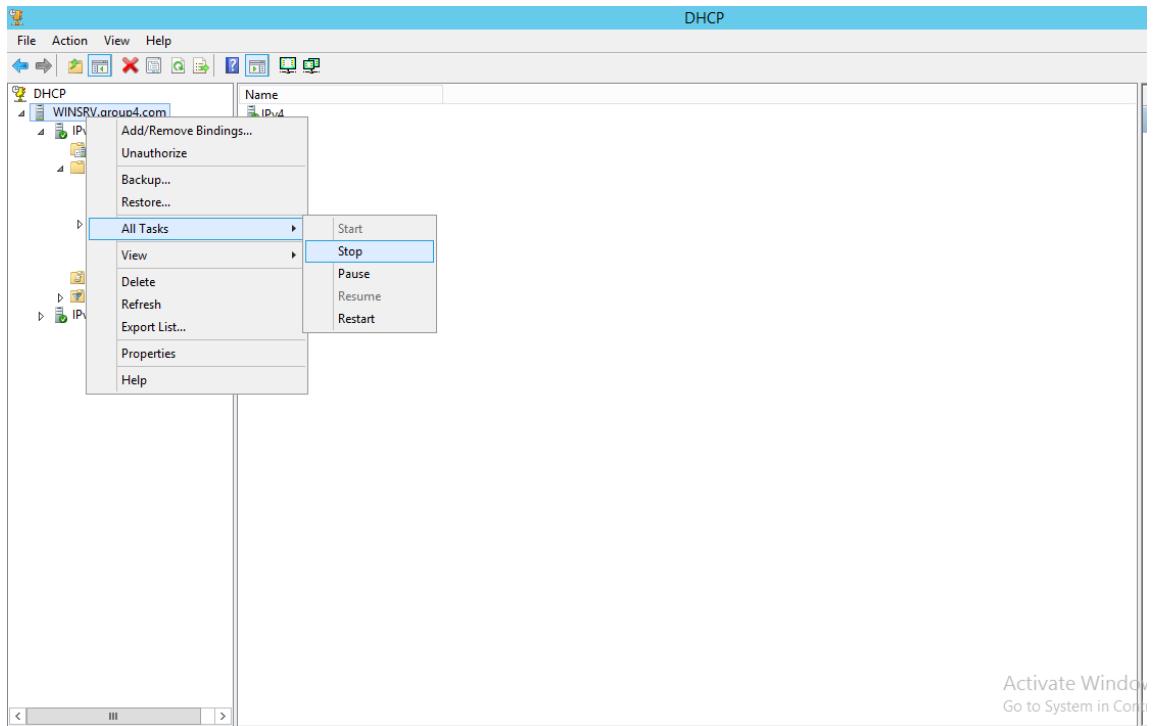


Figure 6.2.16.3: Stop DHCP from primary server

Step 4: Wait for stopping the DHCP from the server



Figure 6.2.16.4: Wait to stop

Step 5: The server are now stopped and the service is not running

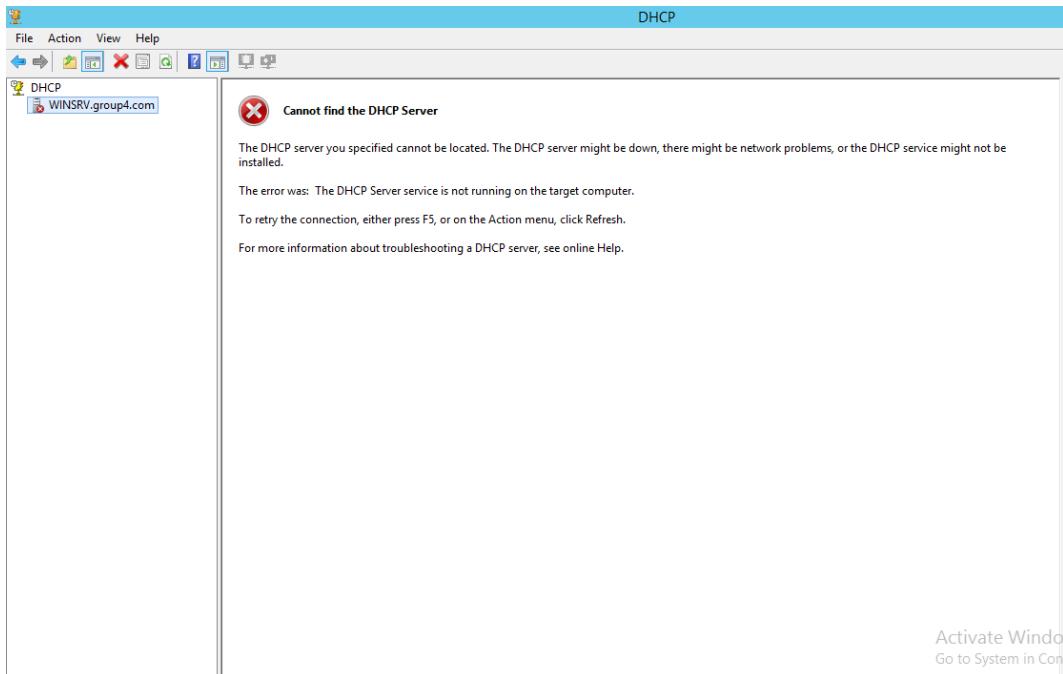


Figure 6.2.16.5: DHCP failure on primary server

Step 6: Using command prompt, type *ipconfig /release* for release old IPv4

```
C:\>ipconfig /release

Windows IP Configuration

An error occurred while releasing interface Loopback Pseudo-Interface 1 : The system cannot find the file specified.

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
IPv6 Address . . . . . : 1230:1111:aaaa:1:8d44:4b56:239d:1749
Temporary IPv6 Address . . . . . : 1230:1111:aaaa:1:865:552a:fefd:eb0a
Link-local IPv6 Address . . . . . : fe80::8d44:4b56:239d:1749%11
Default Gateway . . . . . : fe80::216:c8ff:fea1:35d7%11

Tunnel adapter isatap.group4.com:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
```

Figure 6.2.16.6: ipconfig /release

Step 7: Using command prompt, type `ipconfig /renew` for renew new IPv4

```
C:\Users\student>ipconfig /renew

Windows IP Configuration

An error occurred while releasing interface Loopback Pseudo-Interface 1 : The system cannot find the file specified.

Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix . . . . . group4.com
  IPv6 Address . . . . . 1230:1111:aaaa:1:8d44:4b56:239d:1749
  Temporary IPv6 Address . . . . . 1230:1111:aaaa:1:865:552a:fefd:eb0a
  Link-local IPv6 Address . . . . . fe80::8d44:4b56:239d:1749%11
  IPv4 Address . . . . . 10.1.1.2
  Subnet Mask . . . . . 255.255.255.128
  Default Gateway . . . . . fe80::216:c8ff:fea1:35d7%11
                                10.1.1.126

Tunnel adapter isatap.{849D60E6-6E9E-4930-B6DA-54C74FAACE38}:

  Media State . . . . . Media disconnected
  Connection-specific DNS Suffix . . .

Tunnel adapter Teredo Tunneling Pseudo-Interface:

  Media State . . . . . Media disconnected
  Connection-specific DNS Suffix . . .
```

Figure 6.2.16.7: `ipconfig /renew`

Step 8: Switch on Hyper-V > Tools > DHCP > refresh the virtual machine. IP address before is 10.1.1.2 has been changed to 10.1.1.66

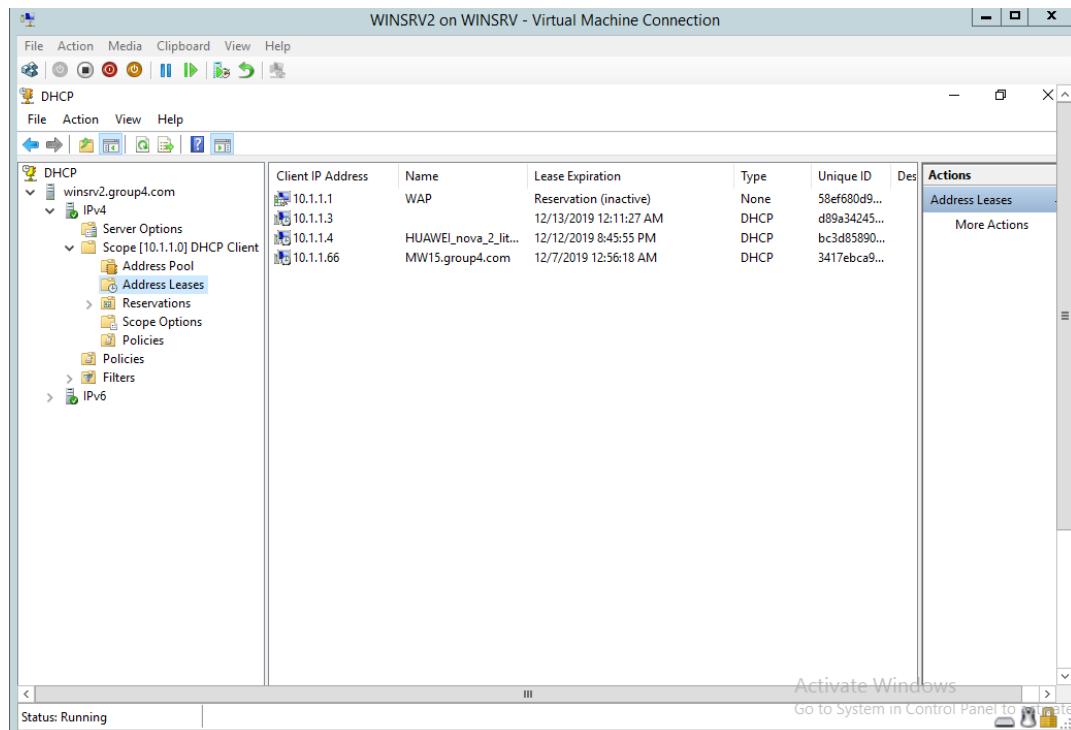


Figure 6.2.16.8: Hostname IP address has changed

Step 9: IP address change from 10.1.1.129 to 10.1.1.132 after the primary server down. 10.1.1.132 is IP address for virtual machine that running for backup primary server. It turn to Hyper-V address because of the real DHCP (in primary server) fail to connect server.

```
C:\>ipconfig /all
Windows IP Configuration

Host Name . . . . . : MW15
Primary Dns Suffix . . . . . : group4.com
Node Type . . . . . : Mixed
IP Routing Enabled . . . . . : No
WINS Proxy Enabled . . . . . : No
DNS Suffix Search List . . . . . : group4.com

Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix . . . . . : group4.com
  Description . . . . . : Intel(R) 82579LM Gigabit Network Connecti
on
  Physical Address. . . . . : 34-17-EB-CA-92-D7
  DHCP Enabled. . . . . : Yes
  Autoconfiguration Enabled . . . . . : Yes
  IPv6 Address. . . . . : 1230:1111:aaaa:1:8d44:4b56:239d:1749(Pref
ered)
  Temporary IPv6 Address. . . . . : 1230:1111:aaaa:1:865:552a:fefd:eb0a(Prefe
red)
  Link-local IPv6 Address . . . . . : fe80::8d44:4b56:239d:1749%11(PREFERRED)
  IPv4 Address. . . . . : 10.1.1.66(Preferred)
  Subnet Mask . . . . . : 255.255.255.128
  Lease Obtained. . . . . : Saturday, December 07, 2019 3:56:18 PM
  Lease Expires . . . . . : Saturday, December 07, 2019 4:56:17 PM
  Default Gateway . . . . . : fe80::216:c8ff:fea1:35d7%11
                                10.1.1.126
  DHCP Server . . . . . : 10.1.1.132
  DNS Servers . . . . . : 10.1.1.129
  NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatap.group4.com:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . : group4.com
  Description . . . . . : Microsoft ISATAP Adapter
  Physical Address. . . . . : 00-00-00-00-00-00-E0
  DHCP Enabled. . . . . : No
  Autoconfiguration Enabled . . . . . : Yes

Tunnel adapter Teredo Tunneling Pseudo-Interface:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :
  Description . . . . . : Teredo Tunneling Pseudo-Interface
  Physical Address. . . . . : 00-00-00-00-00-00-E0
  DHCP Enabled. . . . . : No
  Autoconfiguration Enabled . . . . . : Yes
```

Figure 6.2.16.9: Virtual Machine IP Address

6.2.17 Inter VLAN and VLSM Addressing

Step 1: Insert command “Show vlan” then Enter.

VLAN	Name	Status	Ports							
1	default	active								
5	Trunk	active								
10	IT	active	Fa0/3, Fa0/4							
15	UnusedPort	suspended	Fa0/2, Fa0/5, Fa0/6, Fa0/7 Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Gi0/1, Gi0/2							
20	DMZ	active	Fa0/22, Fa0/23, Fa0/24							
99	MANAGEMENT	active								
1002	fdci-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	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	0	0	
5	enet	100005	1500	-	-	-	-	0	0	
10	enet	100010	1500	-	-	-	-	0	0	
15	enet	100015	1500	-	-	-	-	0	0	
20	enet	100020	1500	-	-	-	-	0	0	
99	enet	100099	1500	-	-	-	-	0	0	
1002	fdci	101002	1500	-	-	-	-	0	0	
1003	tr	101003	1500	-	-	-	-	0	0	
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

Figure 6.2.17.1: Assign VLAN

6.2.18 Web Hardening

Step 1: To view status of apache2, enter command `systemctl status apache2`

```
root@debian:/# sysctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded   lib/systemd/system/apache2.service; enabled; vendor preset: enabled
   Active: active (running) since Fri 2019-11-15 15:34:45 +08; 7s ago
     Process: 8325 ExecStop=/usr/sbin/apachectl stop (code=exited, status=0/SUCCESS)
    Process: 8332 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 8336 (apache2)
      Tasks: 9 (limit: 4915)
        CGroup: /system.slice/apache2.service
                └─8336 /usr/sbin/apache2 -k start
                  ├─8337 /usr/sbin/apache2 -k start
                  ├─8338 /usr/sbin/apache2 -k start
                  ├─8339 /usr/sbin/apache2 -k start
                  ├─8340 /usr/sbin/apache2 -k start
                  ├─8341 /usr/sbin/apache2 -k start
                  ├─8343 /usr/sbin/apache2 -k start
                  ├─8344 /usr/sbin/apache2 -k start
                  └─8345 /usr/sbin/apache2 -k start

Nov 15 15:34:45 debian systemd[1]: Starting The Apache HTTP Server...
Nov 15 15:34:45 debian apachectl[8332]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Se...
Nov 15 15:34:45 debian systemd[1]: Started The Apache HTTP Server.
```

Figure 6.2.18.1: Status of Apache2

Step 2: To confirm that your content is protected, try to access your restricted content in a web browser. You should be presented with a username and password prompt that looks like figure below.

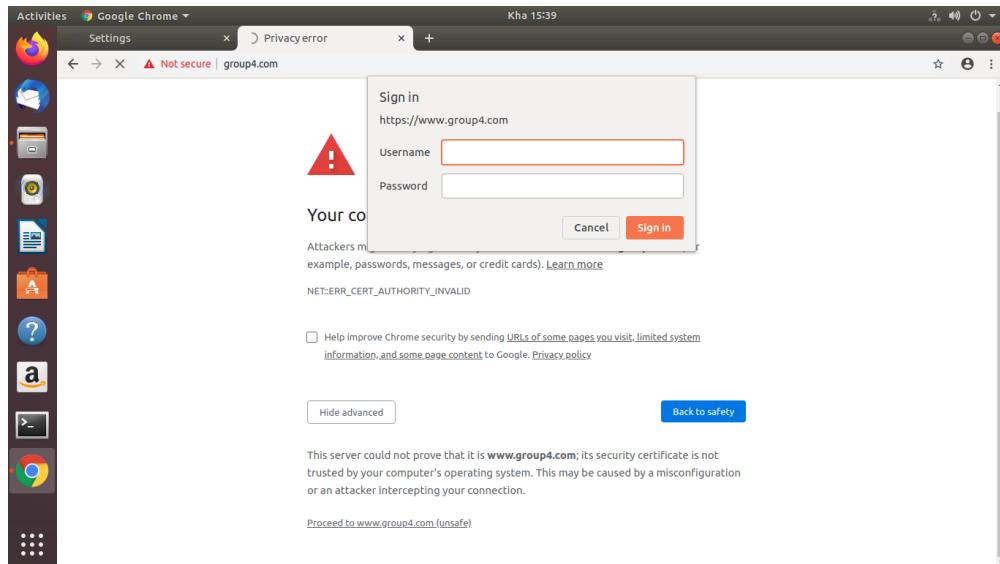


Figure 6.2.18.2: Display username and password prompt

Step 3: To display interface of error, enter <https://www.group4.com/test>.

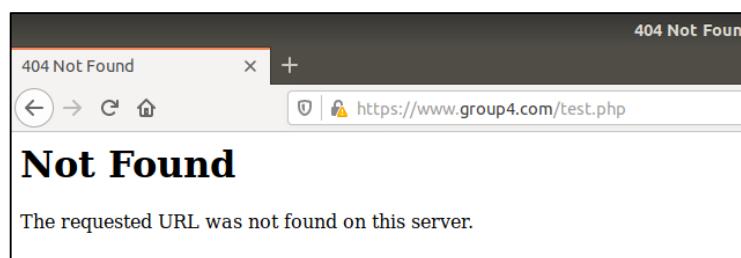


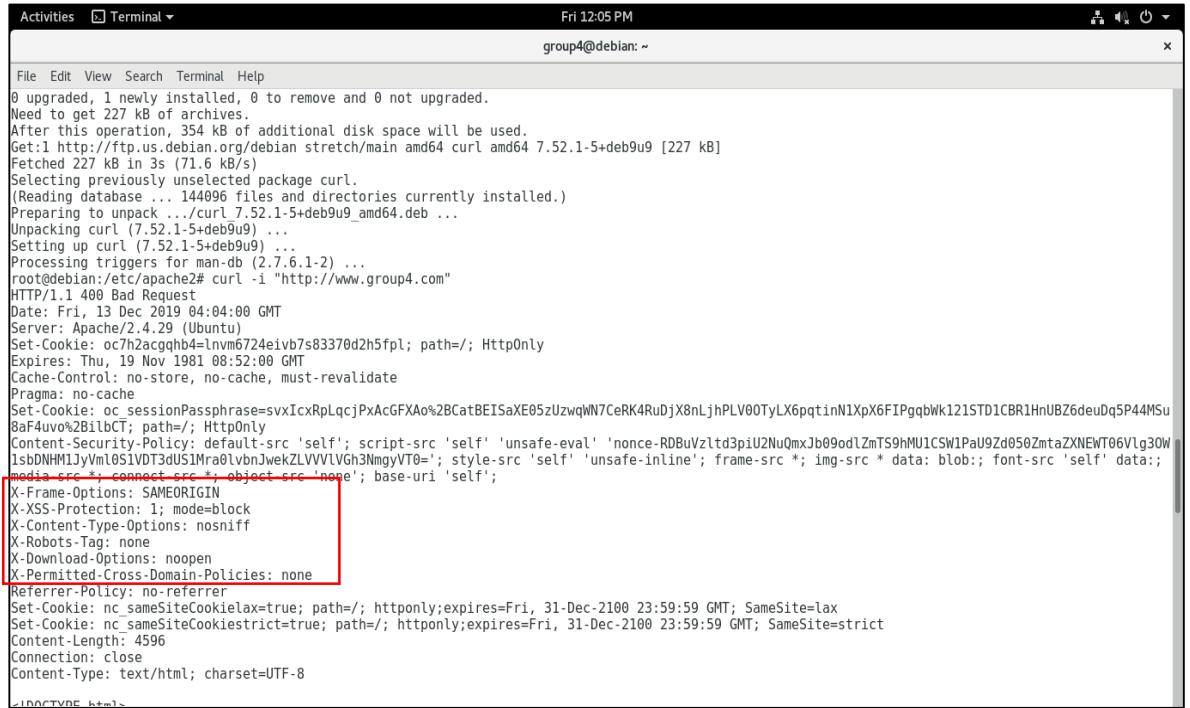
Figure 6.2.18.3: Not found error displayed

Step 4: To display HTTP respond, enter command `curl -I https://group4.com`.

```
root@debian:/etc/apache2# curl -I "http://www.group4.com"
```

Figure 6.2.18.4: Enter command

Step 5:



```
Activities Terminal Fri 12:05 PM
group4@debian: ~
File Edit View Search Terminal Help
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 227 kB of additional disk space will be used.
Get:1 http://ftp.us.debian.org/debian stretch/main amd64 curl amd64 7.52.1-5+deb9u9 [227 kB]
Fetched 227 kB in 3s (71.6 kB/s)
Selecting previously unselected package curl.
(Reading database ... 144096 files and directories currently installed.)
Preparing to unpack .../curl_7.52.1-5+deb9u9_amd64.deb ...
Unpacking curl (7.52.1-5+deb9u9) ...
Setting up curl (7.52.1-5+deb9u9) ...
Processing triggers for man-db (2.7.6.1-2) ...
root@debian:/etc/apache2# curl -I "http://www.group4.com"
HTTP/1.1 400 Bad Request
Date: Fri, 13 Dec 2019 04:04:00 GMT
Server: Apache/2.4.29 (Ubuntu)
Set-Cookie: oc7h2acgqhb4=lnvm6724eivb7s83370d2h5fpl; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: oc_sessionPassphrase=vxIxRplLqcjPxAcGFXAo%2BCatBEISaXE05zUzwqWN7CeRK4RuDjX0nLjhPLV00TyLX6pqtinN1XpX6FIPgqbWk121STD1CBR1HnUBZ6deuDq5P44MSu8aF4uvot2B1bCT; path=/; HttpOnly
Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-eval' 'nonce-RDBuVzltd3piU2NuQmxJb09odlZmTS9hMU1CSW1PaU9Zd050ZmtaZXNEWT06VLg30W1sbDNHML1yM051VDT3dUS1Mra0vbnnJwekZLVVLVGh3NmgvT0=; style-src 'self' 'unsafe-inline'; frame-src *; img-src * data: blob;; font-src 'self' data:;
media src *; connect src *; object src 'none'; base-uri 'self';
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Robots-Tag: none
X-Download-Options: noopen
X-Permitted-Cross-Domain-Policies: none
Referer-Policy: no-referrer
Set-Cookie: n_sameSiteCookie=lax=true; path=/; httponly; expires=Fri, 31-Dec-2100 23:59:59 GMT; SameSite=lax
Set-Cookie: n_sameSiteCookiestrict=true; path=/; httponly; expires=Fri, 31-Dec-2100 23:59:59 GMT; SameSite=strict
Content-Length: 4596
Connection: close
Content-Type: text/html; charset=UTF-8
<input type="hidden" value=""/>
```

Figure 6.2.18.5: HTTP respond

6.2.19 IDS Port Mirror

Step 1: Run Snort on console and on interface eno1 and ping to Ubuntu's IP from Debian which is 10.1.1.131 and monitor the result.

```
root@debian:/home/group4# ping 10.1.1.131
PING 10.1.1.131 (10.1.1.131) 56(84) bytes of data.
64 bytes from 10.1.1.131: icmp_seq=1 ttl=64 time=0.704 ms
64 bytes from 10.1.1.131: icmp_seq=2 ttl=64 time=0.672 ms
64 bytes from 10.1.1.131: icmp_seq=3 ttl=64 time=0.647 ms
64 bytes from 10.1.1.131: icmp_seq=4 ttl=64 time=0.686 ms
64 bytes from 10.1.1.131: icmp_seq=5 ttl=64 time=0.666 ms
```

Figure 6.2.19.1: Ping Ubuntu

```
--== Initialization Complete ==--  
o"--> Snort! <*-  
    Version 2.9.15 GRE (Build 7)  
    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team  
    Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.  
    Copyright (C) 1998-2013 Sourcefire, Inc., et al.  
    Using libpcap version 1.8.1  
    Using PCRE version: 8.39 2016-06-14  
    Using ZLIB version: 1.2.11  
  
    Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.1 <Build 1>  
    Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>  
    Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>  
    Preprocessor Object: SF_IMAP Version 1.0 <Build 1>  
    Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>  
    Preprocessor Object: SF_POP Version 1.0 <Build 1>  
    Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>  
    Preprocessor Object: SF_SMTP Version 1.1 <Build 9>  
    Preprocessor Object: SF_DNS Version 1.1 <Build 4>  
    Preprocessor Object: SF_SSH Version 1.1 <Build 3>  
    Preprocessor Object: SF_GTP Version 1.1 <Build 1>  
    Preprocessor Object: SF_SIP Version 1.1 <Build 1>  
    Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>  
    Preprocessor Object: appid Version 1.1 <Build 5>  
    Preprocessor Object: SF_SDF Version 1.1 <Build 1>  
    Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>  
  
Commencing packet processing (pid=5871)  
12/11-16:39:08.941593 [**] [1:10000001:1] ICMP detected to ubuntu server [**] [Priority: 0] {ICMP} 10.1.1.130 -> 10.1.1.131  
12/11-16:39:09.956778 [**] [1:10000001:1] ICMP detected to ubuntu server [**] [Priority: 0] {ICMP} 10.1.1.130 -> 10.1.1.131  
12/11-16:39:10.956357 [**] [1:10000001:1] ICMP detected to ubuntu server [**] [Priority: 0] {ICMP} 10.1.1.130 -> 10.1.1.131  
12/11-16:39:11.972724 [**] [1:10000001:1] ICMP detected to ubuntu server [**] [Priority: 0] {ICMP} 10.1.1.130 -> 10.1.1.131  
12/11-16:39:12.996686 [**] [1:10000001:1] ICMP detected to ubuntu server [**] [Priority: 0] {ICMP} 10.1.1.130 -> 10.1.1.131
```

Figure 6.2.19.2: Snort detection

Step 2: Run sudo snort -r in Snort's log file and we can see the output is same as the console

Figure 6.2.19.3: Snort's log file

6.2.20 Samba

Connecting Samba From Windows

Step 1: Check status Samba service in Linux whether it's running or not

```
root@ubuntu:~# systemctl status smbd
● smbd.service - Samba SMB Daemon
   Loaded: loaded (/lib/systemd/system/smbd.service; enabled; vendor preset: ena
   Active: active (running) since Sat 2019-12-14 19:18:55 +08; 46min ago
     Docs: man:smbd(8)
           man:samba(7)
           man:smb.conf(5)
 Main PID: 6833 (smbd)
   Status: "smbd: ready to serve connections..."
    Tasks: 4 (limit: 4915)
   CGroup: /system.slice/smbd.service
           ├─6833 /usr/sbin/smbd --foreground --no-process-group
           ├─6835 /usr/sbin/smbd --foreground --no-process-group
           ├─6836 /usr/sbin/smbd --foreground --no-process-group
           └─6837 /usr/sbin/smbd --foreground --no-process-group

Dis 14 19:18:55 ubuntu systemd[1]: Starting Samba SMB Daemon...
Dis 14 19:18:55 ubuntu systemd[1]: Started Samba SMB Daemon.
lines 1-17/17 (END)
```

Figure 6.2.20.1: Status of Samba

Step 2: Open up File Explorer and in the left pane right-click on “Network”. Click on “Map network drive...”

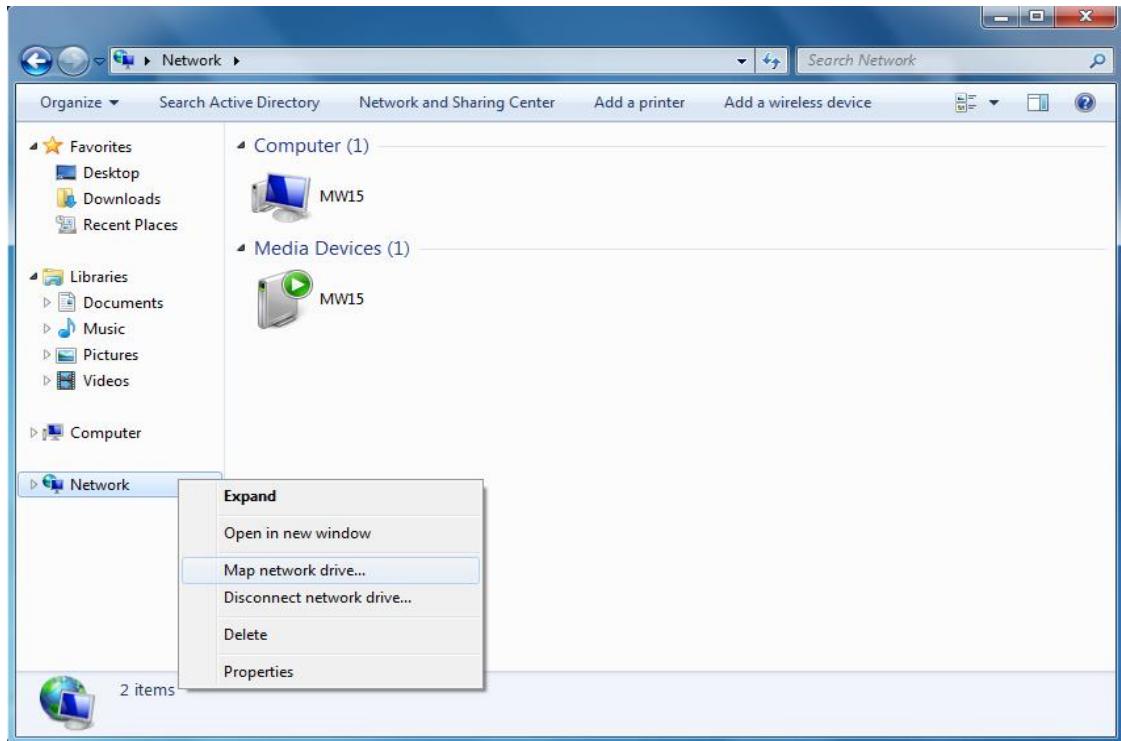


Figure 6.2.20.2: Map Network drive

Step 3: In “Folder:”, enter the address of the Samba share in the following format \\samba_hostname_or_server_ip\sharename. Then click “Finish”

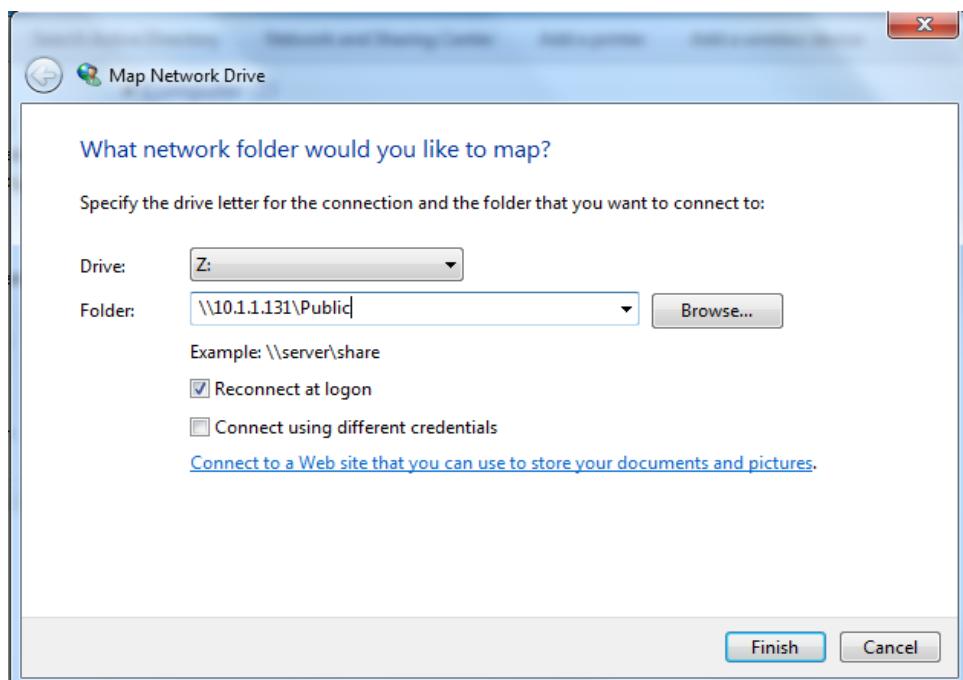


Figure 6.2.20.3: Choose network foleder

Step 4: Now we already in the File Samba Share

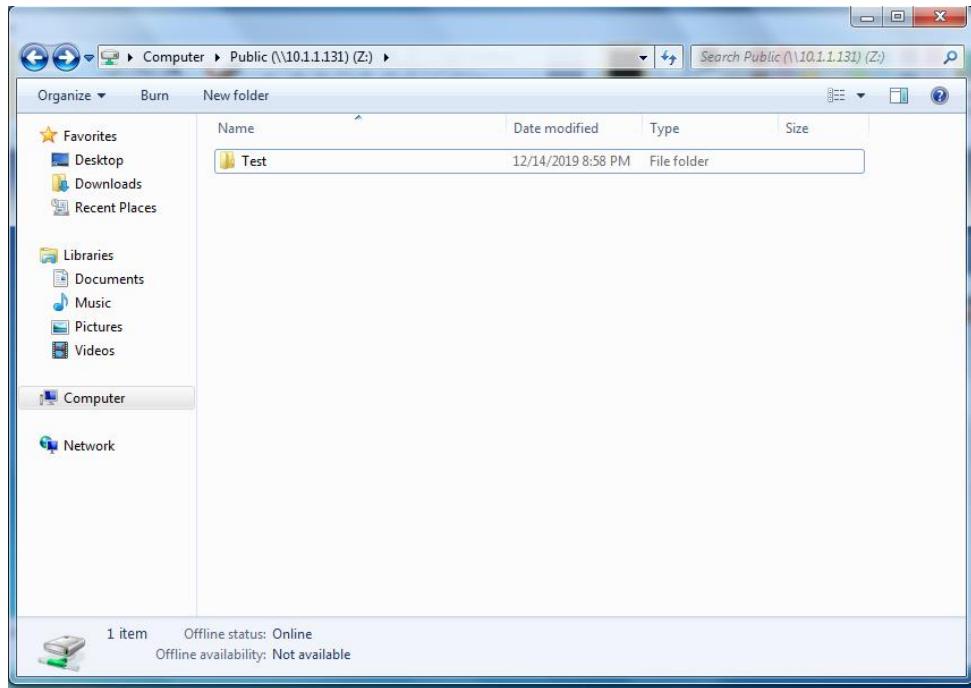


Figure 6.2.20.4: File samba share

Connecting Samba From Linux

Step 1: Smbclient is a tool that allows you to access Samba from the command line. To install smbclient on Linux run this command “`sudo apt install smbclient`”

Step 2: The syntax to access a Samba share is as follows. For example to connect to a share named public on a Samba server with IP address 192.168.121.118 as user AzimGroup4 from Active Directory you would run:

```
root4@debian:~$ smbclient //10.1.1.131/Public -U GROUP4\AzimGroup4
```

Figure 6.2.20.5: connecting samba from linux

Step 3: Once you enter the password you will be logged into the Samba command line interface

```
WARNING: The "syslog" option is deprecated
Enter GROUP4\AzimGroup4's password:
Domain=[GROUP4] OS=[Windows 6.1] Server=[Samba 4.7.6-Ubuntu]
smb: \> [ ]
```

Figure 6.2.20.6: log in samba interface

Samba Security

Step 1: Open Run dialog by pressing Win + R and key in Ubuntu's IP

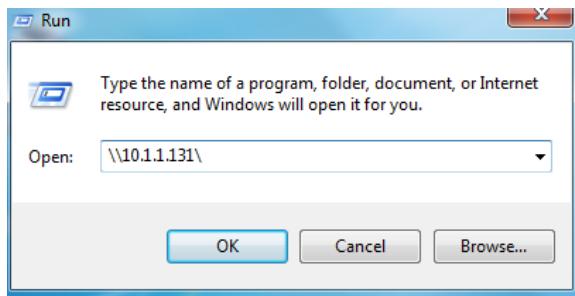


Figure 6.2.20.7: Run dialog box

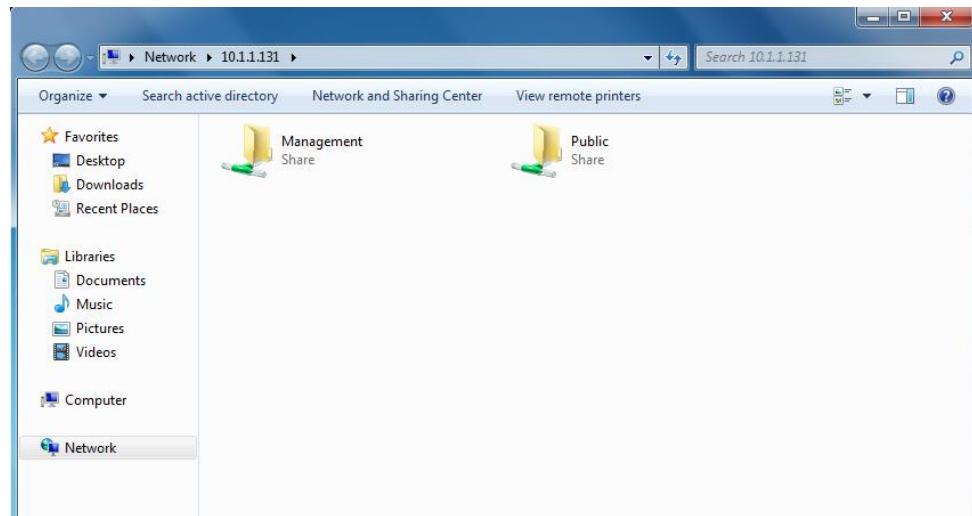


Figure 6.2.20.8: Run dialog box

Step 2: Try to access Management's File with user “AzimGroup4” from Active Directory. It cannot be accessed because Azim is not member of group “Management”

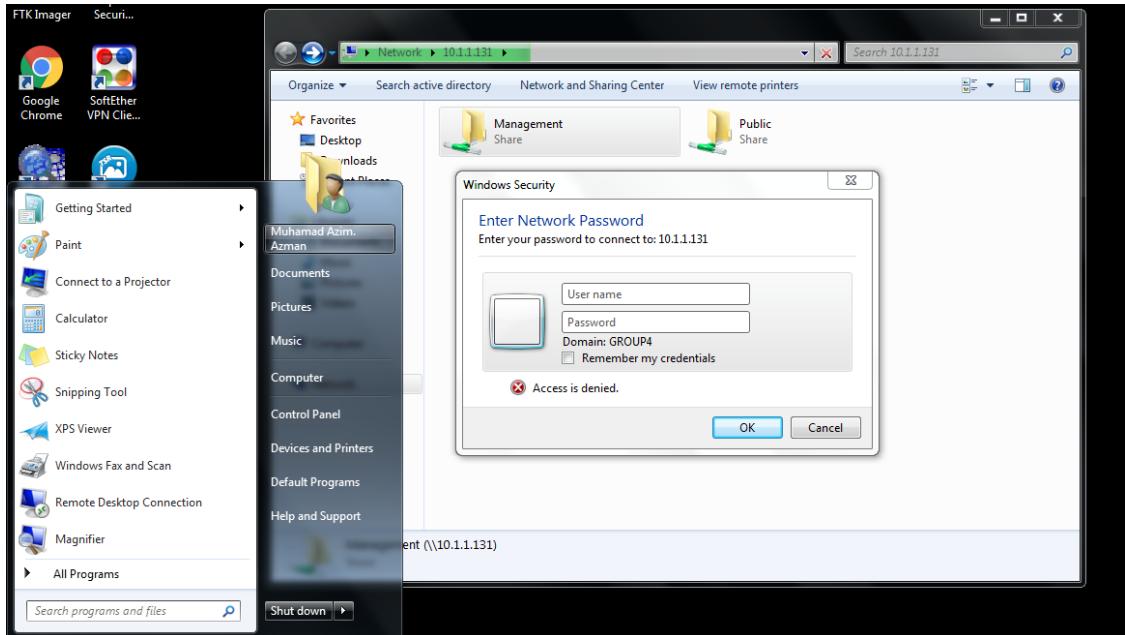


Figure 6.2.20.9: Run dialog box

Step 3: Login in user “Ammar” from Active Directory and do the same thing as step 1 and step 2. It can be accessed because Ammar is member of “Management” group.

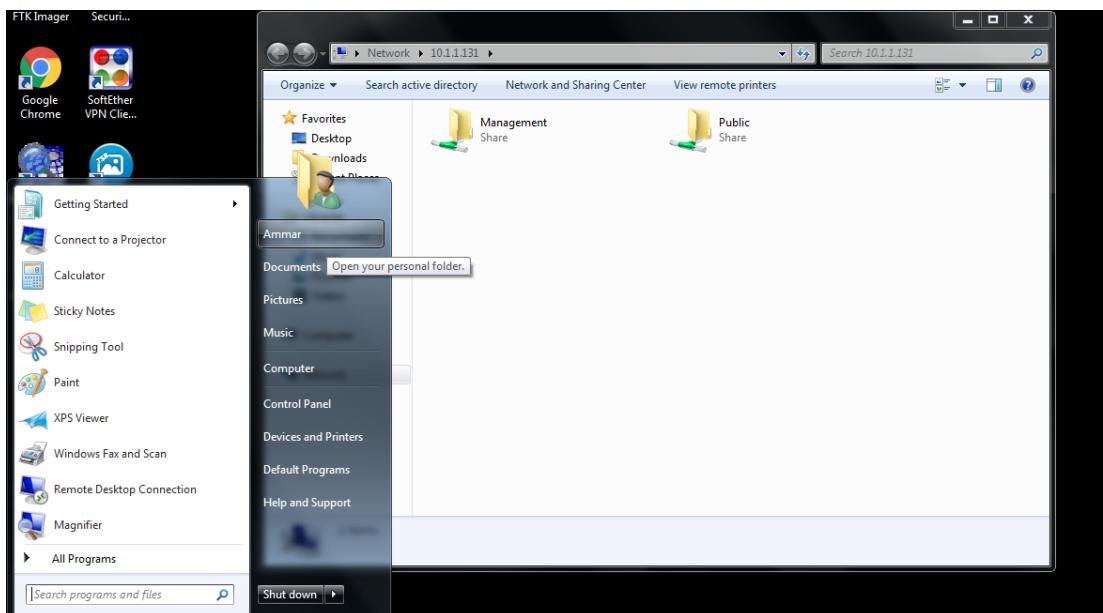


Figure 6.2.20.10: Log in user

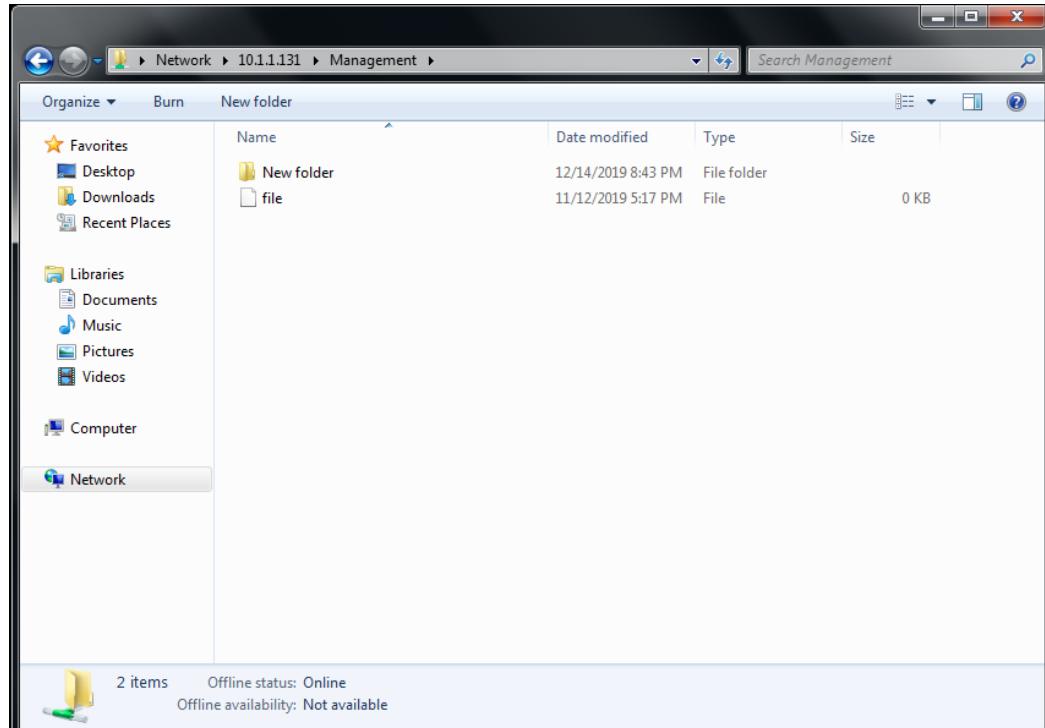


Figure 6.2.20.11: Network drive where the file saved

6.2.21 Linux Server Hardening

Step 1: Check the current status of password expiration

```
group4@ubuntu:~$ sudo chage -l group4
Last password change : Okt 23, 2019
Password expires      : Okt 29, 2019
Password inactive     : Dis 08, 2019
Account expires       : Feb 23, 2020
Minimum number of days between password change : 5
Maximum number of days between password change : 6
Number of days of warning before password expires : 5
group4@ubuntu:~$
```

Figure 6.2.21.1: Check status of password expire

Step 2: Check status of firewall

```
root@ubuntu:/home/group4# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To           Action    From
--           ----     ---
137,138/udp (Samba) ALLOW IN  Anywhere
139,445/tcp (Samba)  ALLOW IN  Anywhere
22/tcp        ALLOW IN  Anywhere
80/tcp        ALLOW IN  Anywhere
137,138/udp (Samba (v6)) ALLOW IN  Anywhere (v6)
139,445/tcp (Samba (v6)) ALLOW IN  Anywhere (v6)
22/tcp (v6)   ALLOW IN  Anywhere (v6)
80/tcp (v6)   ALLOW IN  Anywhere (v6)
```

Figure 6.2.21.2: Check status of firewall

6.2.22 Dynamic Routing & NAT

ROUTING

Step 1: Verify the OSPF process created previously and the advertised network.

```
R4#show ip protocols
Routing Protocol is "ospf 4"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 4.4.4.4
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    2.2.2.0 0.0.0.3 area 0
    10.1.1.0 0.0.0.127 area 0
    10.1.1.128 0.0.0.15 area 0
  Routing on Interfaces Configured Explicitly (Area 0):
    Tunnel0
    Loopback1
  Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway          Distance      Last Update
    3.3.3.3          110          22:08:09
  Distance: (default is 110)

R4#
```

Figure 6.2.22.94: OSPF process created.

```
R4#show ip protocols
Routing Protocol is "ospf 4"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 4.4.4.4
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    2.2.2.0 0.0.0.3 area 0
    10.1.1.0 0.0.0.127 area 0
    10.1.1.128 0.0.0.15 area 0
  Routing on Interfaces Configured Explicitly (Area 0):
    Tunnel0
    Loopback1
  Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway          Distance      Last Update
    3.3.3.3           110          22:08:09
  Distance: (default is 110)

R4#
```

Figure 6.2.22.2: Advertised IPv4 network.

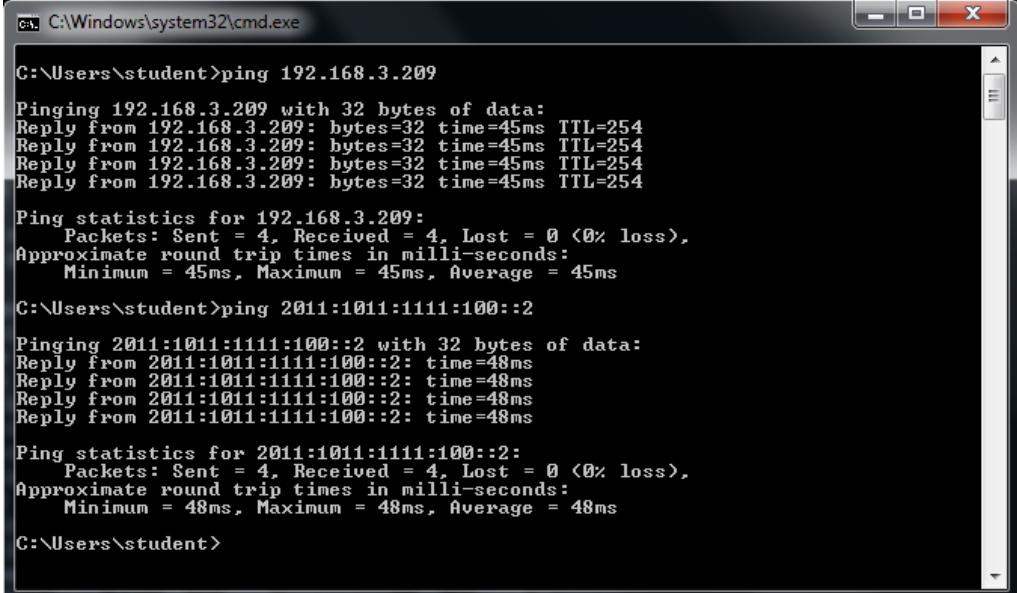
Step 2: Verify that neighbour relationship has been establish between routers.

```
R4#show ip route ospf
  3.0.0.0/32 is subnetted, 1 subnets
O     3.3.3.3 [110/11112] via 2.2.2.2, 1d03h, Tunnel0
  192.168.3.0/24 is variably subnetted, 5 subnets, 3 masks
O     192.168.3.0/25 [110/11112] via 2.2.2.2, 1d03h, Tunnel0
O     192.168.3.200/29 [110/11112] via 2.2.2.2, 1d03h, Tunnel0
O     192.168.3.192/29 [110/11112] via 2.2.2.2, 1d03h, Tunnel0
O     192.168.3.208/29 [110/11112] via 2.2.2.2, 1d03h, Tunnel0
O     192.168.3.128/26 [110/11112] via 2.2.2.2, 1d03h, Tunnel0
R4#show ipv6 route ospf
IPv6 Routing Table - 13 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
        U - Per-user Static route
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
        O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O   1011:1011:1111:100::/64 [110/11112]
    via FE80::226:CBFF:FEDA:B168, Tunnel0
O   2011:1011:1111:100::/64 [110/11112]
    via FE80::226:CBFF:FEDA:B168, Tunnel0
O   3011:1011:1111:100::/64 [110/11112]
    via FE80::226:CBFF:FEDA:B168, Tunnel0
O   4011:1011:1111:100::/64 [110/11112]
    via FE80::226:CBFF:FEDA:B168, Tunnel0
O   5011:1011:1111:100::/64 [110/11112]
    via FE80::226:CBFF:FEDA:B168, Tunnel0

R4#
```

Figure 6.2.22.3: Neighbor for IPv4 and IPv6 fully exchange routing information.

Step 3: Send ping packet from local network to remote network.



The screenshot shows a Windows Command Prompt window titled 'C:\Windows\system32\cmd.exe'. It displays two separate ping commands. The first command is 'ping 192.168.3.209' which successfully reaches a host with an IP of 192.168.3.209. The second command is 'ping 2011:1011:1111:100::2' which successfully reaches a host with an IP of 2011:1011:1111:100::2. Both pings show 0% loss and low round-trip times (45ms to 48ms).

```
C:\Users\student>ping 192.168.3.209
Pinging 192.168.3.209 with 32 bytes of data:
Reply from 192.168.3.209: bytes=32 time=45ms TTL=254

Ping statistics for 192.168.3.209:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 45ms, Maximum = 45ms, Average = 45ms

C:\Users\student>ping 2011:1011:1111:100::2
Pinging 2011:1011:1111:100::2 with 32 bytes of data:
Reply from 2011:1011:1111:100::2: time=48ms
Reply from 2011:1011:1111:100::2: time=48ms
Reply from 2011:1011:1111:100::2: time=48ms
Reply from 2011:1011:1111:100::2: time=48ms

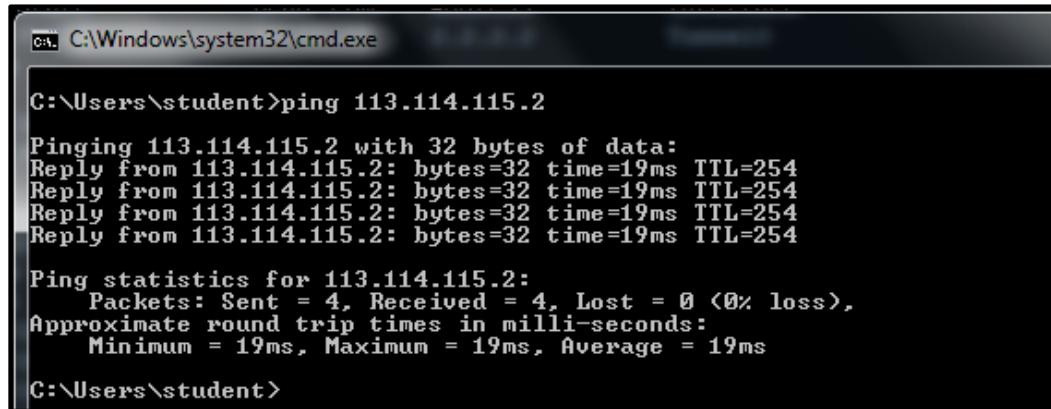
Ping statistics for 2011:1011:1111:100::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 48ms, Maximum = 48ms, Average = 48ms

C:\Users\student>
```

Figure 6.2.22.4: Internal client able to reach remote network

NAT

Step 1: Ping from internal client to neighbor router public IP address



```
C:\Windows\system32\cmd.exe
C:\>ping 113.114.115.2

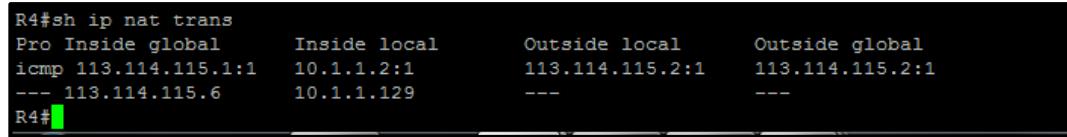
Pinging 113.114.115.2 with 32 bytes of data:
Reply from 113.114.115.2: bytes=32 time=19ms TTL=254

Ping statistics for 113.114.115.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 19ms, Maximum = 21ms, Average = 19ms

C:\>
```

Figure 6.2.22.5: Internal client able to reach public network.

Step 2: Verify PAT translation on router.



Protocol	Inside global	Inside local	Outside local	Outside global
icmp	113.114.115.1:1	10.1.1.2:1	113.114.115.2:1	113.114.115.2:1
	---	10.1.1.129	---	---
	113.114.115.6			

Figure .2.22.6: Output above shows translated IP address from internal "10.1.1.2" to "113.114.115.1" using different port number.

6.2.23 Linux Email Server

We have tested the email services using the webmail and successfully sent and received the email. Another step taken to ensure that this service running correctly by check the log files.

Step 1: Access the webmail using web browser.

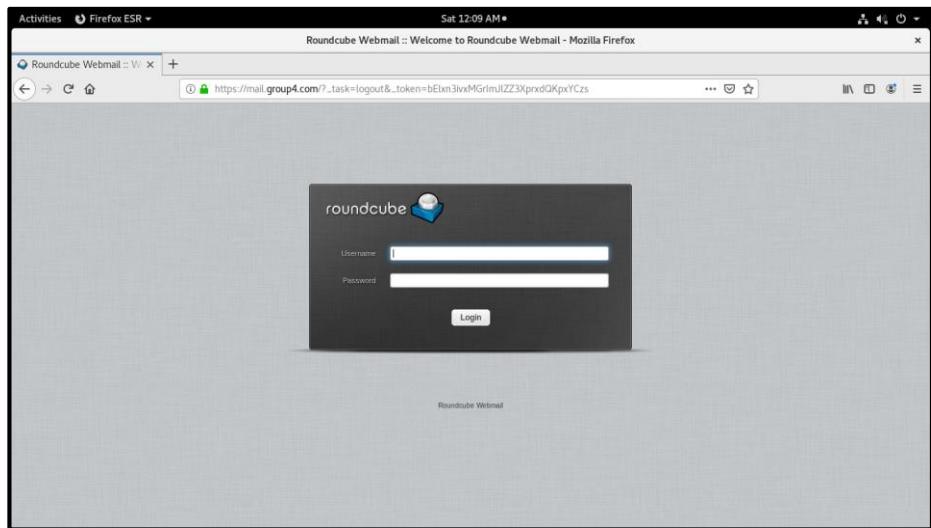
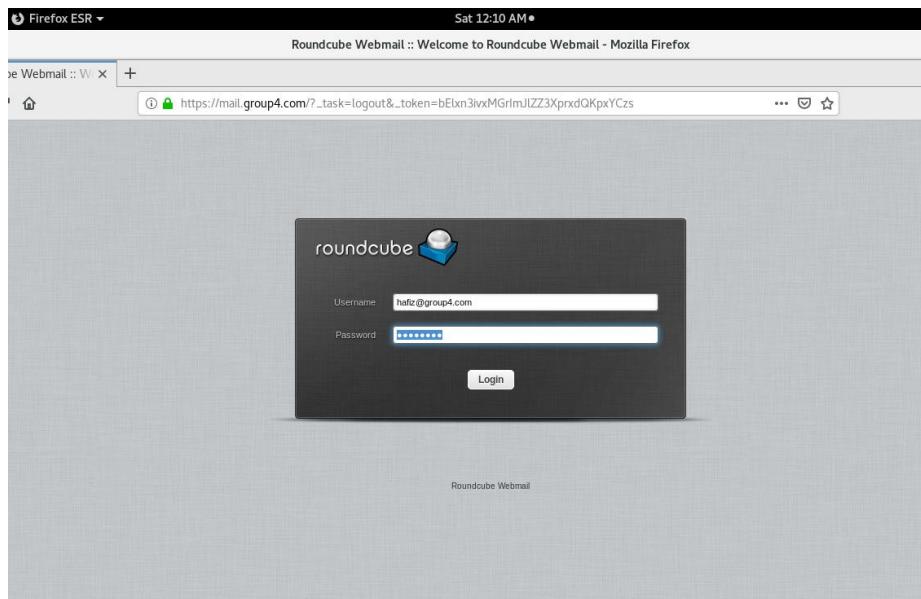


Figure 6.2.23.1: Webmail for email services.

Step 2: Login using Active Directory user account.



Step 3: Send email to another Active Directory user account.

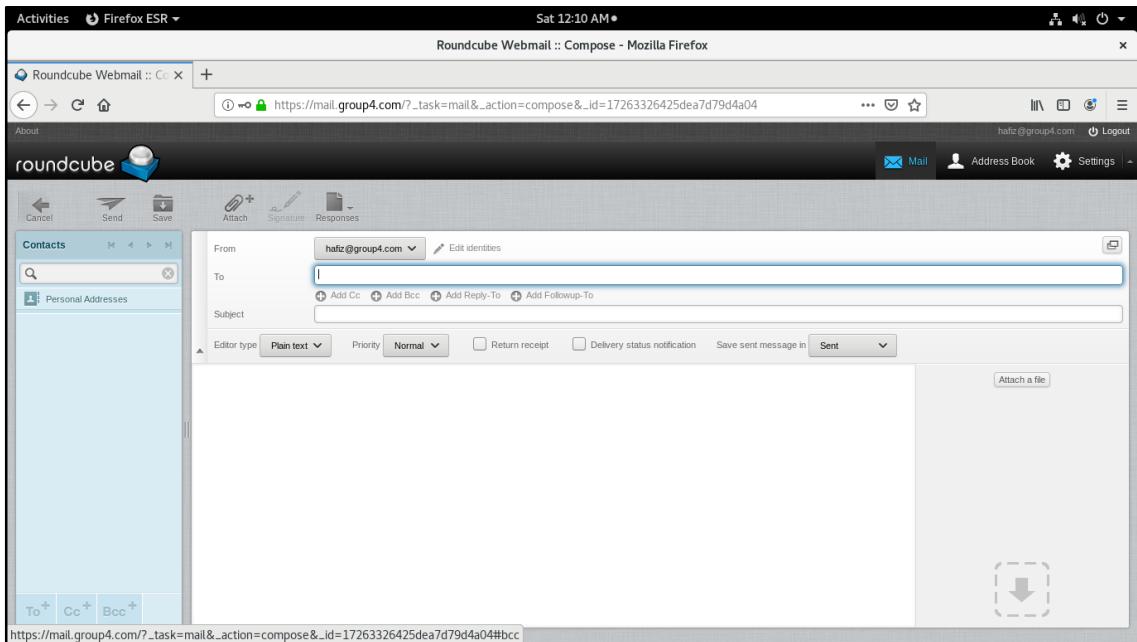


Figure 6.2.23.3: Sending email from hafiz to ammar.

Step 4: Login to the recipient account and verify that the email was successfully delivered.

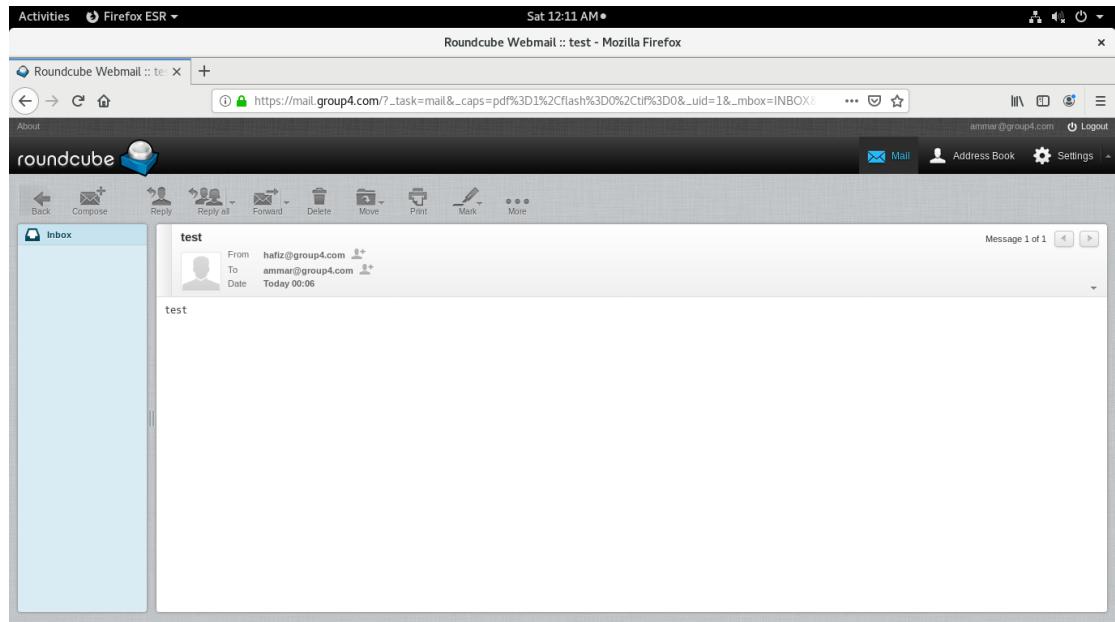


Figure 6.2.23.4: Email from hafiz received on ammar account.

Step 5: Verify your email located on the correct directory.

```
root@debian:/home/group4# telnet localhost 143
Trying ::1...
Connected to localhost.
Escape character is '^'.
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE
  STARTTLS AUTH=PLAIN] Dovecot ready.
a login ashqin Group@04
a OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE
  SORT SORT=DISPLAY THREAD=REFERENCES THREAD=REFS THREAD=ORDEREDSUBJECT MUL
  TIAPPEND URL-PARTIAL CATENATE UNSELECT CHILDREN NAMESPACE UIDPLUS LIST-EXT
  ENDED I18NLEVEL=1 CONDSTORE QRESYNC ESEARCH ESORT SEARCHRES WITHIN CONTEXT
  =SEARCH LIST-STATUS BINARY MOVE SPECIAL-USE] Logged in
a select INBOX
* FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
* OK [PERMANENTFLAGS (\Answered \Flagged \Deleted \Seen \Draft \*)] Flags
  permitted.
* 1 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 1575999727] UIDs valid
* OK [UIDNEXT 2] Predicted next UID
a OK [READ-WRITE] Select completed (0.000 + 0.000 secs).
a FETCH 1 (FLAGS BODY(HEADER.FIELDS (DATE FROM SUBJECT)))
a BAD Error in IMAP command FETCH: Invalid characters in atom (0.000 + 0.0
00 secs).
a FETCH 1 (FLAGS BODY(HEADER.FIELDS (DATE FROM SUBJECT)))
a BAD Error in IMAP command FETCH: Invalid characters in atom (0.000 + 0.0
00 secs).
a FETCH 1 (FLAGS BODY[HEADER.FIELDS (DATE FROM SUBJECT)])
* 1 FETCH (FLAGS (\Seen) BODY[HEADER.FIELDS (DATE FROM SUBJECT)] {91}
Date: Wed, 11 Dec 2019 01:54:31 +0800
From: azimgroup4@group4.com
Subject: test email

)
a OK Fetch completed (0.054 + 0.000 + 0.053 secs).
s
```

Figure 6.2.23.5: Using telnet to list the email sent from hafiz.

Step 6: verify that the email sent to the correct user.

```
Dec 7 00:06:52 debian postfix/smtpd[3399]: connect from debian.group4.com[1230:1111:aaaa:2::2]
Dec 7 00:06:52 debian postfix/smtpd[3399]: CF0A8F20270: client=debian.group4.com[1230:1111:aaaa:2::2]
Dec 7 00:06:52 debian postfix/cleanup[3404]: CF0A8F20270: message-id=<28774fb9fba27d7d232c6552a73caa4b@group4.com>
Dec 7 00:06:52 debian postfix/qmgr[2443]: CF0A8F20270: from=<hafiz@group4.com>, size=536, nrcpt=1 (queue active)
Dec 7 00:06:52 debian postfix/local[3405]: CF0A8F20270: to=<ammar@group4.com>, relay=local, delay=0.29, delays=0.25/0.01/0/0.03, dsn=2.0.0, status=se
nt (delivered to mailbox)
```

Figure 6.2.23.6: SMTP forwarded the email from hafiz to correct destination domain.

6.2.24 Cloud Server

Testing Nextcloud on Admin

Create User on Admin Account

Step 1: Open the web browser. Write on t hurl nextcloud.group4.com. Then login as Admin.

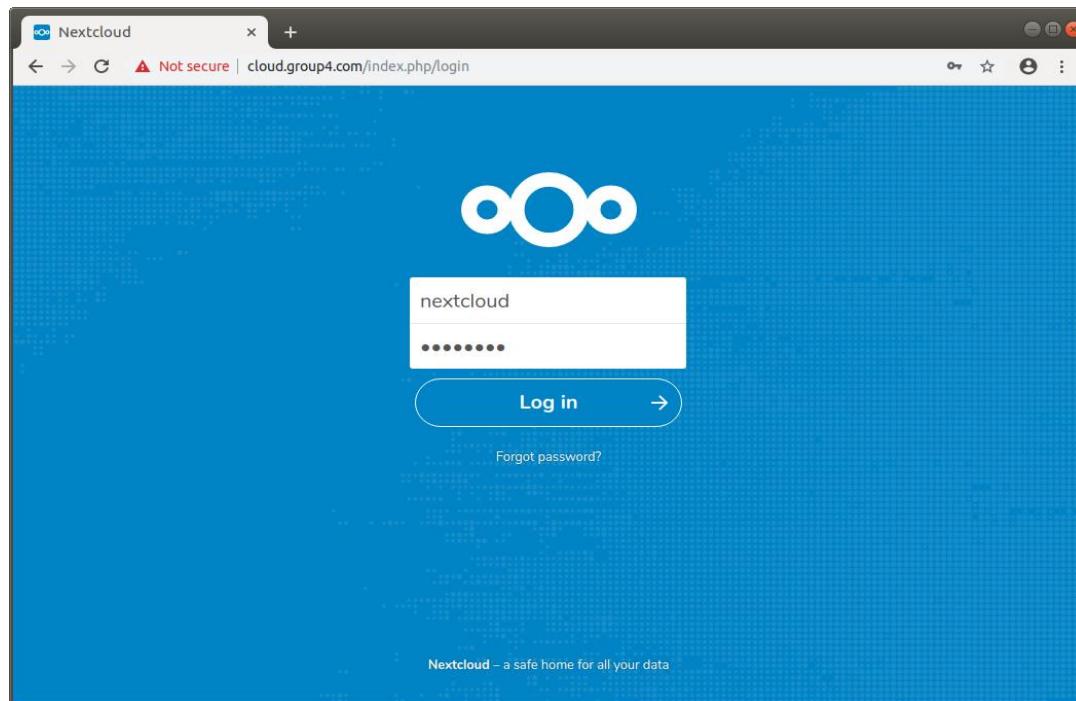


Figure 6.2.24.1: Create new user

Step 2: Once login into the Admin, it will be direct to the Admin dashboard.

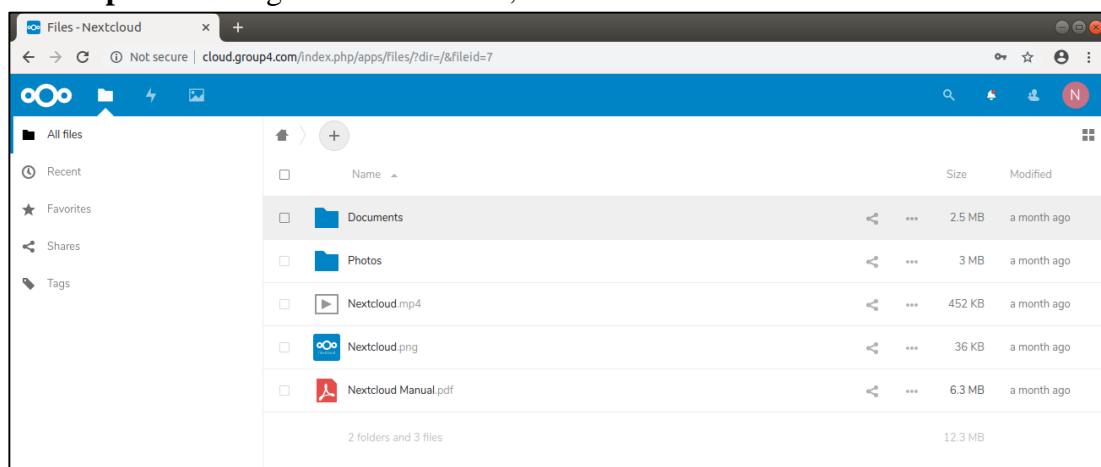


Figure 6.2.24.2: Files in nextcloud

Step 3: Go the top of the admin picture, and go the setting options and click new user.

The screenshot shows the 'Users' page in a Nextcloud web interface. On the left, there's a sidebar with buttons for '+ New user', '+ Add group', 'Everyone', 'Admins', 'Groups', and 'Group4'. The main area has a table with columns: Username, Display name, Password, Email, Groups, Group admin for, and Quota. There are four rows of data:

	Username	Display name	Password	Email	Groups	Group admin for	Quota
4	A Amir Cloud	Amir	New password		Group4	Group4	1 GB
1	Cloud	Cloud User	New password		Group4	Set user as admin for	1 GB
3	H hafiz	hafiz	New password		Group4	Group4	1 GB
	N nextcloud	nextcloud	New password	admin@group4....	admin	Set user as admin for	Unlimited

At the bottom left is a 'Settings' gear icon.

Figure 6.2.24.3: Files in nextcloud

Step 4: Add user details on the user details space bar that contain of username, password, display name, email, group, group admin for, and the quota. Once done, the user details will be fill in the list of user.

This screenshot is similar to Figure 6.2.24.3, showing the 'Users' page. The 'New user' form is open at the top left. In the main list, a new row has been added for a user named 'C Cloud User'. The table now looks like this:

	Username	Display name	Password	Email	Groups	Group admin for	Quota
4	A Amir Cloud	Amir	New password		Group4	Group4	1 GB
1	Cloud	Cloud User	New password		Group4	Set user as admin for	1 GB
3	H hafiz	hafiz	New password		Group4	Group4	1 GB
	C Cloud User	Cloud User	New password	admin@group4....	Group4	Group4	Unlimited

Figure 6.2.24.4: Files in nextcloud

Testing NextCloud on Client

Step 1: Type the url of the NextCloud on the web browser on the client site, and log in as the new user that have been created on the admin.

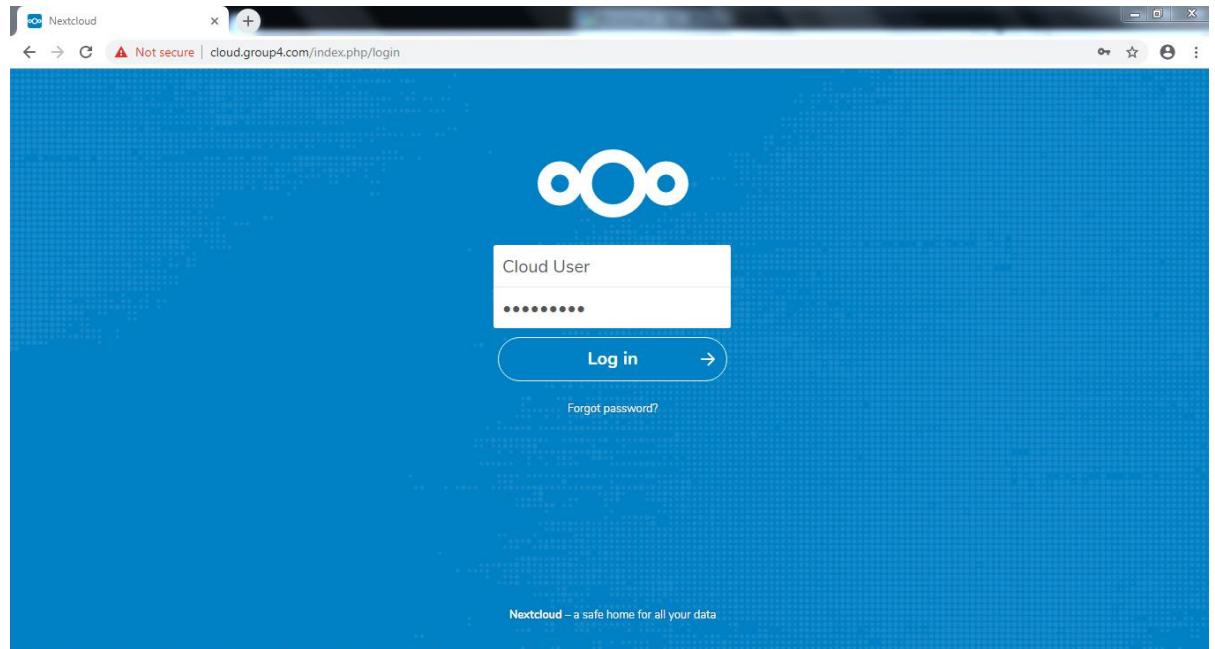


Figure 6.2.24.5: Login Page

Step 2: Once the client are successfully login then it will be direct to the client dashboard home.

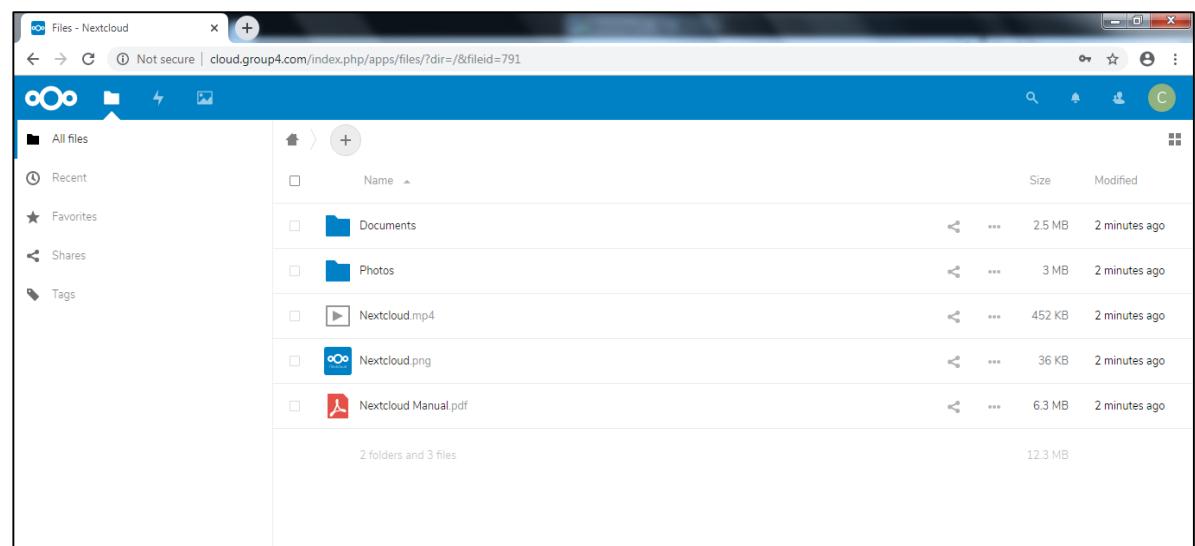


Figure 6.2.24.6: Client dashboard

Step 3: For this client, it have been given privilege for manage the group4. So this client can add any user for the group4 also instead of admin.

The screenshot shows the 'Users' settings page in a Nextcloud web interface. The URL is `cloud.group4.com/index.php/settings/users`. On the left, there's a sidebar with buttons for '+ New user', '+ Add group', and 'Everyone'. Below that is a 'Groups' section with 'Group4' listed. The main area displays a table of users:

	Username	Display name	Password	Email	Groups	Quota	...
A	Amir Cloud	Amir	New password		Group4	1 GB	...
C	Cloud	Cloud User	New password		Group4	1 GB	...
H	hafiz	hafiz	New password		Group4	1 GB	...

Figure 6.2.24.7: Files in nextcloud

6.2.25 Active Directory & GPO

Testing the Active Directory & GPO on the admin.

Step 1: Open the user section on the Active Directory for computer and user, add a new user to test the connectivity on the client.

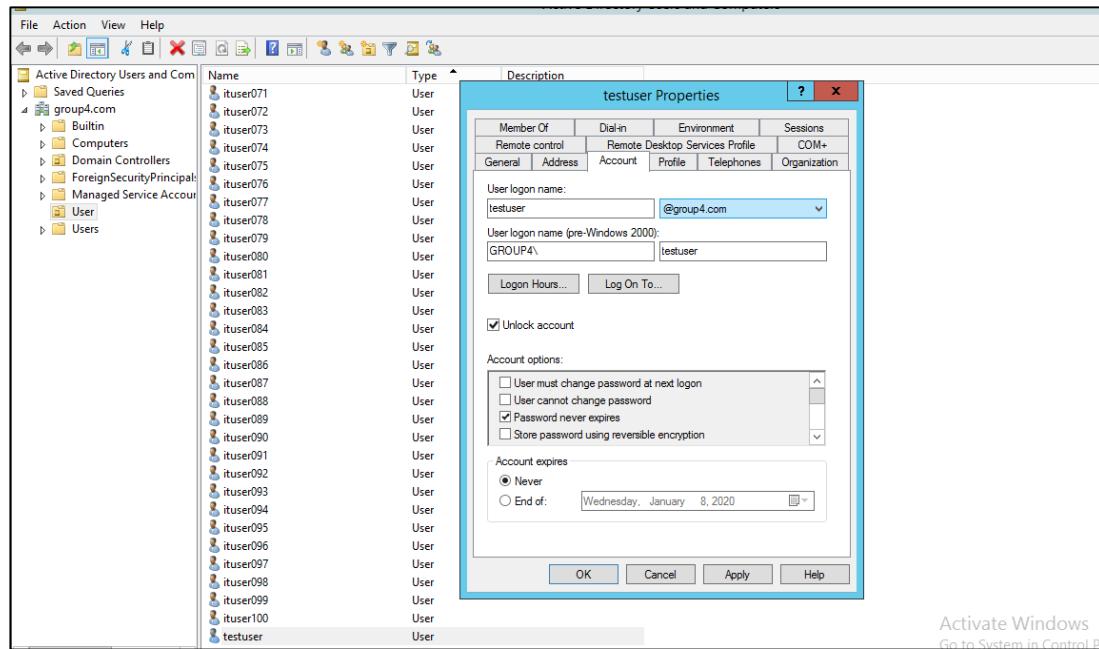


Figure 6.2.25.1: Details of the user on the Active Directory to test

Step 2: Open the GPO, then enable the policy on the computer for the client. This policy might took client for unable to access some of the features.

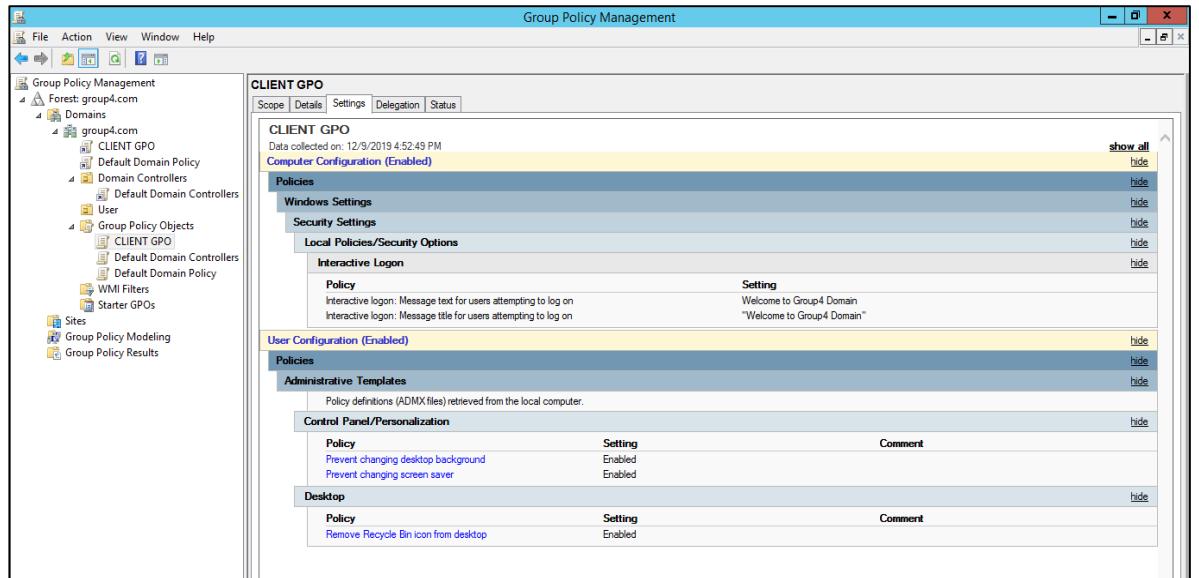


Figure 6.2.25.2: List of the policy that have been enable at the setting.

Step 3: Create some test folder on the folder path on the user profile that have been linked, to test on the client whether the client can access the shared folder that have been created by the admin or not.

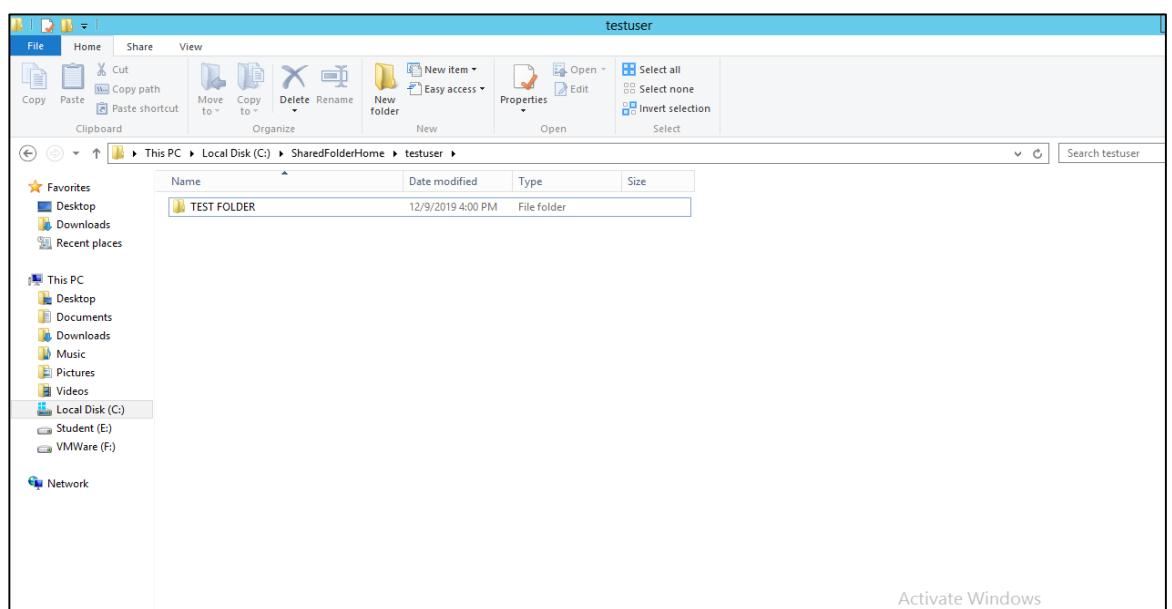


Figure 6.2.25.3: List of the policy that have been enable at the setting

Testing the Active Directory & GPO on the client.

Step 1: Before user open to log in into the client, the user will be welcomed by a text that have been set in the GPO.

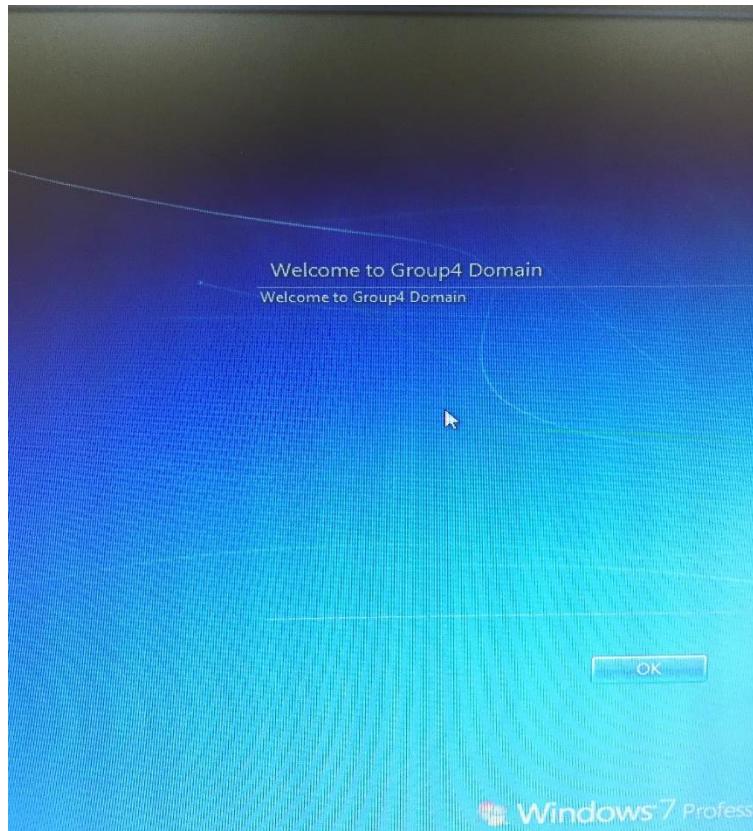


Figure 6.2.25.4: The text that have been set on the GPO once user login

Step 2: Open the client computer, and log in as the new user that have been created at the admin. Fill the password and log in.



Figure 6.2.25.5: The new user login dashboard.

Step 3: Once the user is successfully log in, open the Computer section, the new user will have a shared folder home on the list on the network location.

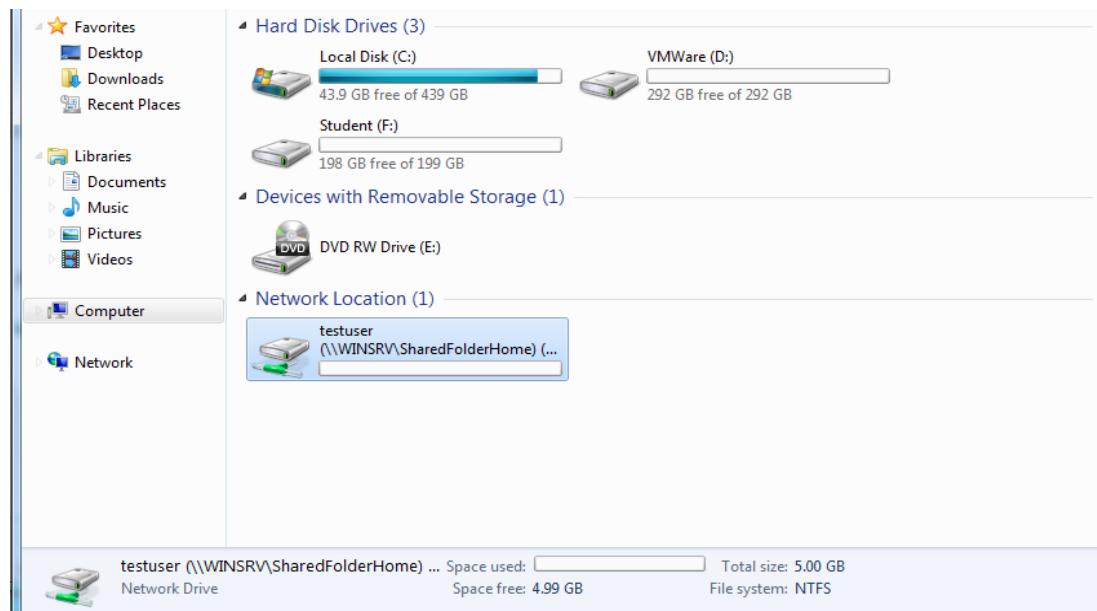


Figure 6.2.25.6: Shared folder home that have been shared on the new user by the admin.

Step 4: Click on the shared folder home, the new user will get the new folder that have been shared by the admin.

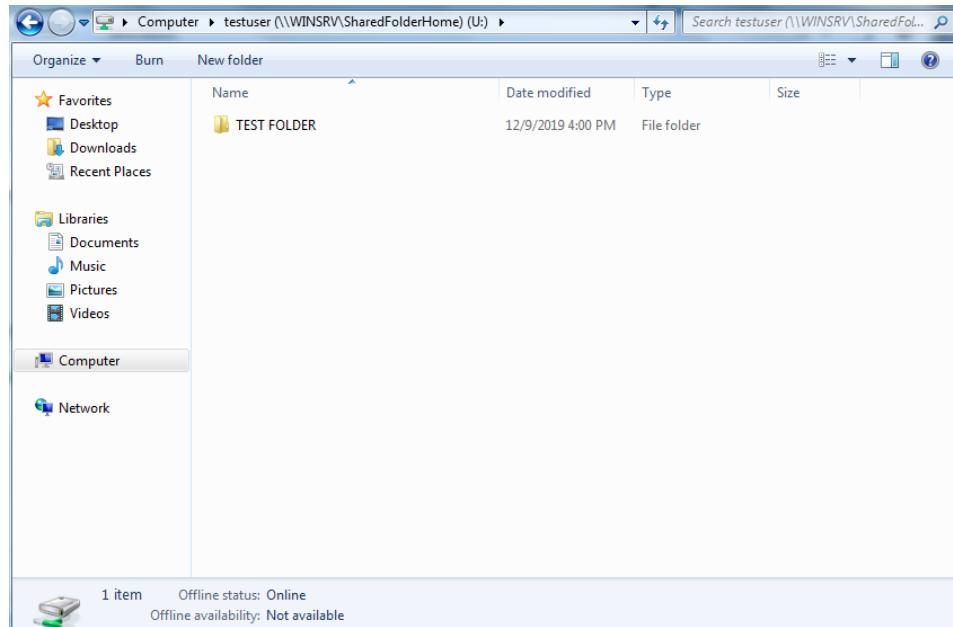


Figure 6.2.25.7: Dashboard of the new user shared folder home

Step 5: Open the personalize by right click on the desktop, and user will notified that they have not been able to change the screen background because the admin have been enable some of the policy at the GPO settings.

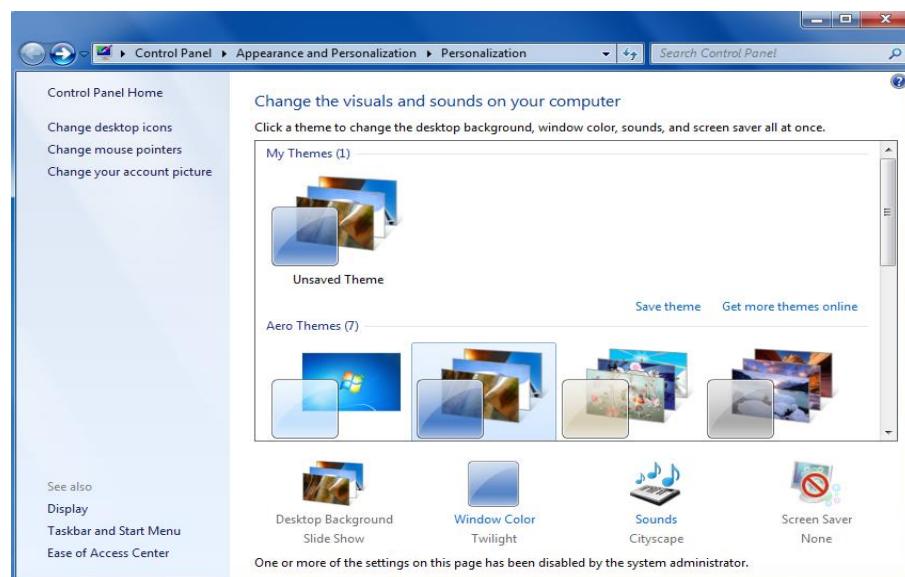


Figure 6.2.25.8: The desktop background options are not enable for user to change

Step 6: Open the desktop, the new user will not see the recycle bin icon that have been set by the admin for the new user.

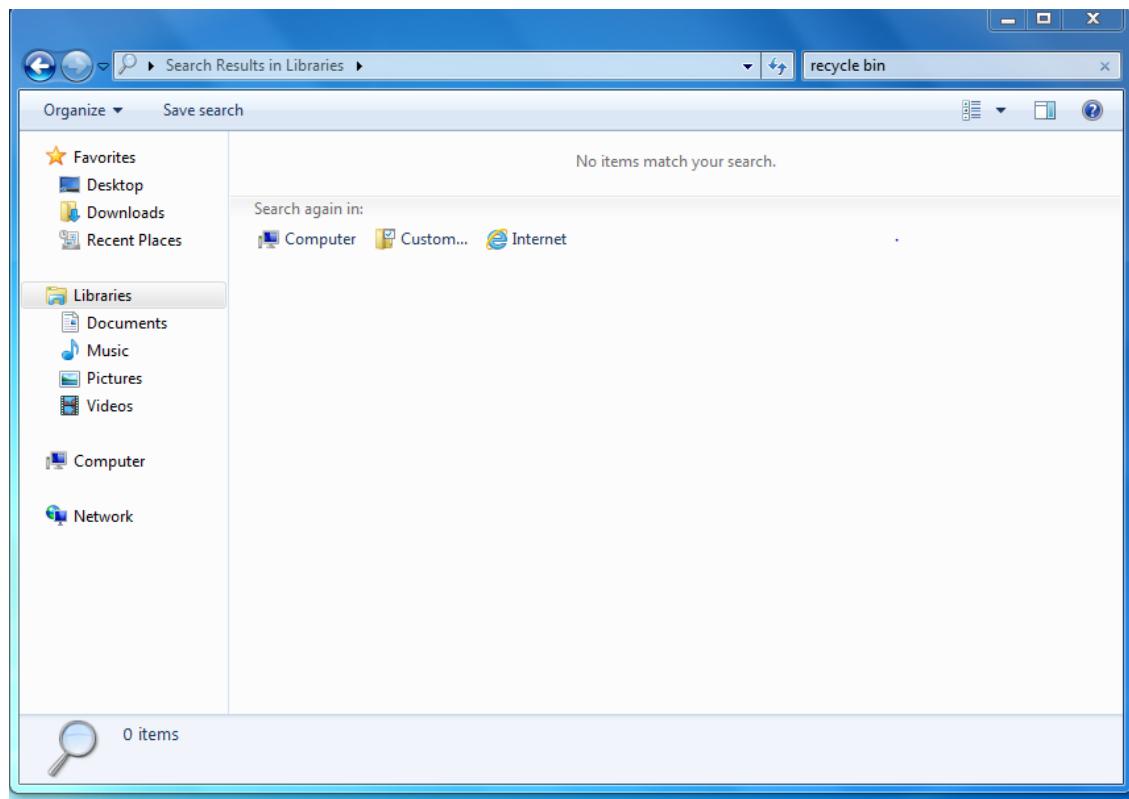
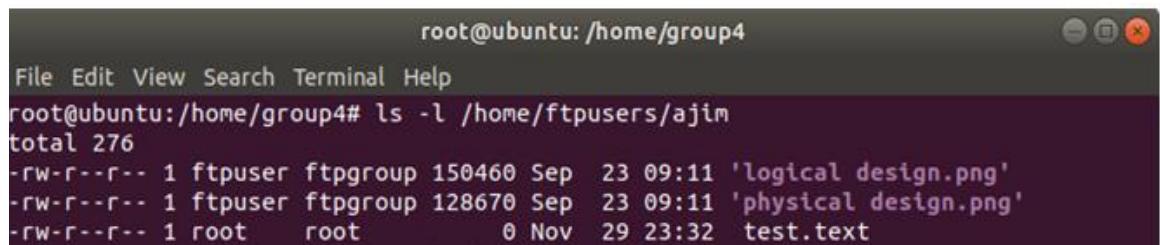


Figure 6.2.25.9: The desktop dashboard of the new user

6.2.26 Secured FTP Server

Testing on the Remote

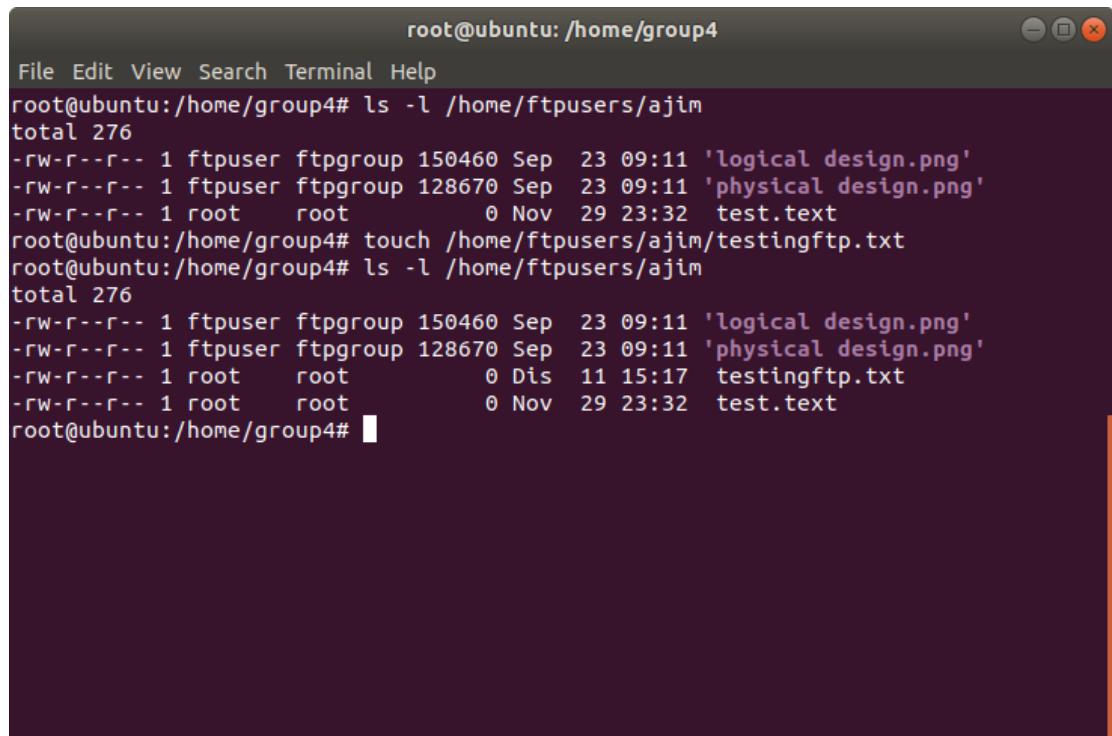
Step 1: View the user that have been created on the terminal and enter the ftp user folder to vie files



```
root@ubuntu: /home/group4
File Edit View Search Terminal Help
root@ubuntu:/home/group4# ls -l /home/ftpusers/ajim
total 276
-rw-r--r-- 1 ftpuser ftpgroup 150460 Sep 23 09:11 'logical design.png'
-rw-r--r-- 1 ftpuser ftpgroup 128670 Sep 23 09:11 'physical design.png'
-rw-r--r-- 1 root    root      0 Nov 29 23:32 test.text
```

Figure 6.2.26.1: Show the list offile created on FTP user.

Step 2: Created on the new file on the ftp user name “testingftp.txt”.



```
root@ubuntu: /home/group4
File Edit View Search Terminal Help
root@ubuntu:/home/group4# ls -l /home/ftpusers/ajim
total 276
-rw-r--r-- 1 ftpuser ftpgroup 150460 Sep 23 09:11 'logical design.png'
-rw-r--r-- 1 ftpuser ftpgroup 128670 Sep 23 09:11 'physical design.png'
-rw-r--r-- 1 root    root      0 Nov 29 23:32 test.text
root@ubuntu:/home/group4# touch /home/ftpusers/ajim/testingftp.txt
root@ubuntu:/home/group4# ls -l /home/ftpusers/ajim
total 276
-rw-r--r-- 1 ftpuser ftpgroup 150460 Sep 23 09:11 'logical design.png'
-rw-r--r-- 1 ftpuser ftpgroup 128670 Sep 23 09:11 'physical design.png'
-rw-r--r-- 1 root    root      0 Dis 11 15:17 testingftp.txt
-rw-r--r-- 1 root    root      0 Nov 29 23:32 test.text
root@ubuntu:/home/group4#
```

Figure 6.2.26.2: The new file in the ftp user that have been created.

Testing on the client

Step 1: Open the WinSCP application to access the ftp user via client. And log in.

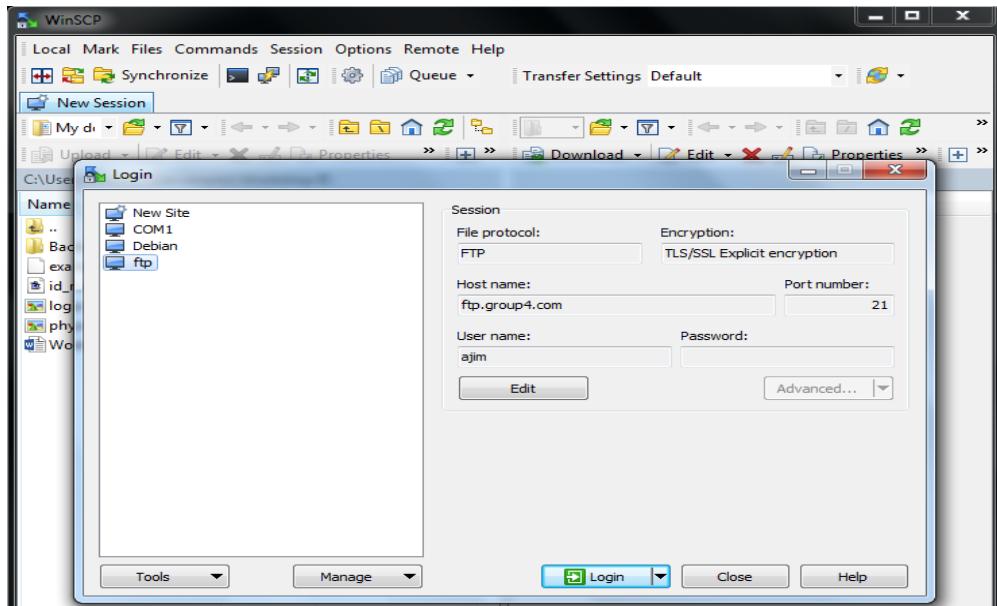


Figure 6.2.26.3: The dashboard of the log in user.

Step 2: Enter the password and wait to connect.

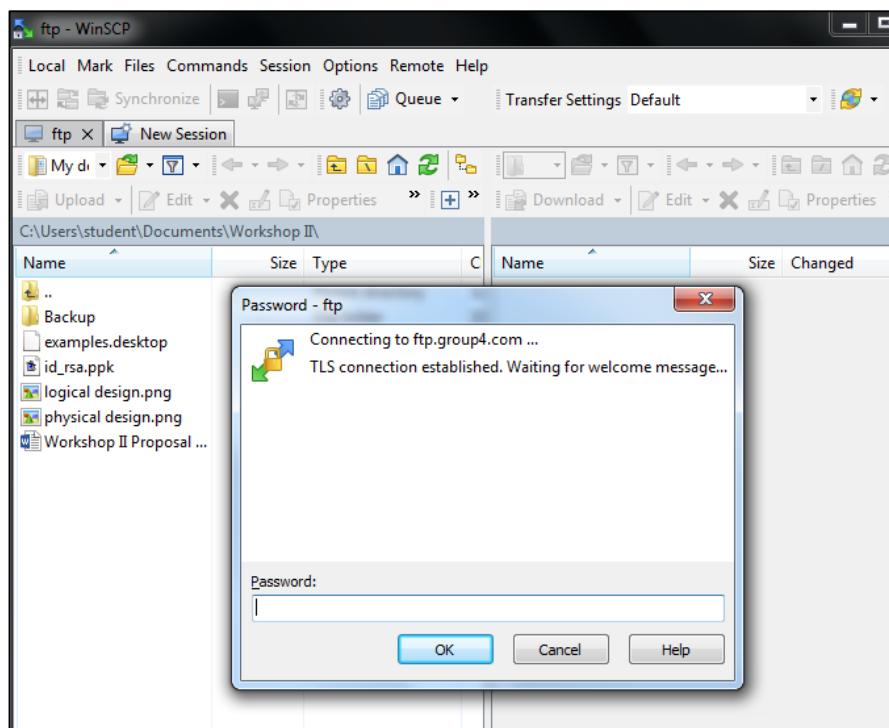


Figure 6.2.26.4: The entry password dashboard in client interface.

Step 3: After successful log in, client will view the dashboard of the remote and the client.

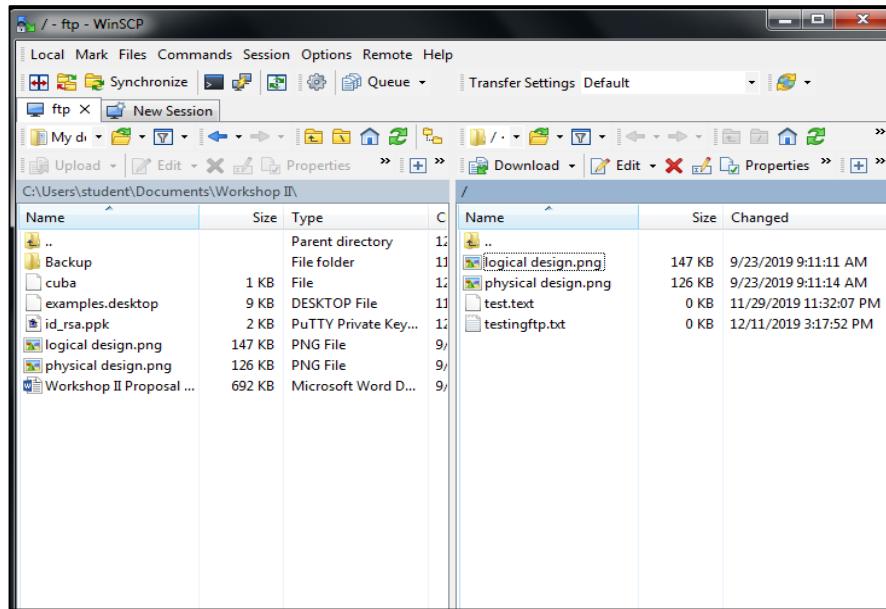


Figure 6.2.26.5: The client and remote dashboard interface.

Step 4: Drag the testing file to the client site for sharing. And the file will be shared.

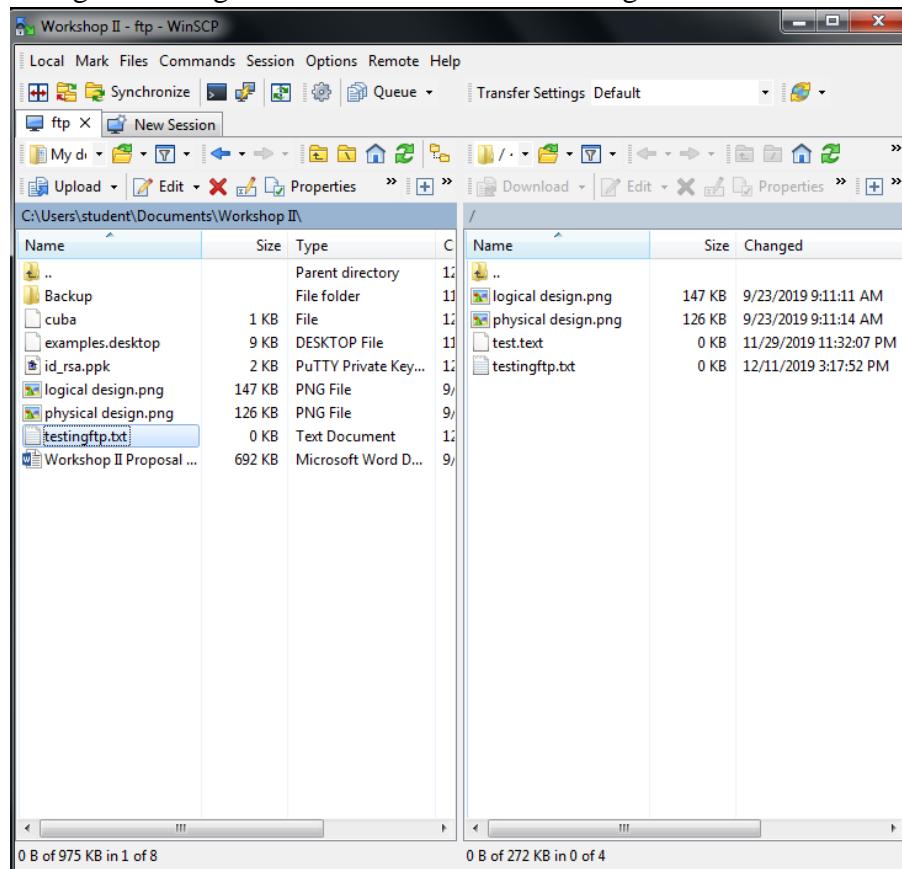


Figure 6.2.26.6: The client is successful transfer the file from the ftp remote.

6.2.27 Access Control List

Step 1: Testing SSH by starting new session on putty and apply ip address for Debian server(10.1.1.130)

```
RtGroup3(config-ext-nacl)#do sh access-list
Standard IP access list NAT
    10 permit 192.168.3.192, wildcard bits 0.0.0.7 (14 matches)
    20 permit 192.168.3.200, wildcard bits 0.0.0.7 (14 matches)
    30 permit 192.168.3.208, wildcard bits 0.0.0.7 (80 matches)
    40 permit 192.168.3.0, wildcard bits 0.0.0.127 (251 matches)
    50 permit 192.168.3.128, wildcard bits 0.0.0.63
Extended IP access list ACL-GROUP4
    10 deny tcp 192.168.3.0 0.0.0.127 10.1.1.128 0.0.0.15 eq 22 (17 matches)
    30 deny tcp 192.168.3.0 0.0.0.127 host 10.1.1.129 eq telnet (7 matches)
    40 deny tcp 192.168.3.0 0.0.0.127 host 10.1.1.131 eq ftp (77 matches)
    60 deny icmp 192.168.3.0 0.0.0.127 host 10.1.1.130 echo (4 matches)
    70 permit ip any any (380 matches)
Extended IP access list IPSEC-ACL
    10 permit gre host 113.114.115.2 host 113.114.115.1 (560010 matches)
```

Figure 6.2.27.1: Testing SSH

Step 2: Testing for icmp by ping Debian server because deny Debian only

```
C:\Users\students>ping 10.1.1.130

Pinging 10.1.1.130 with 32 bytes of data:
Reply from 192.168.3.1: Destination net unreachable.

Ping statistics for 10.1.1.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

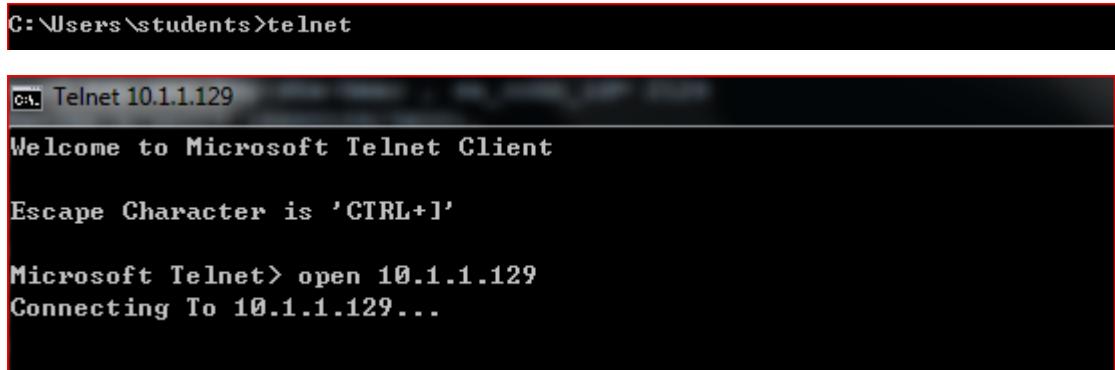
Figure 6.2.27.2: Testing icmp

Step 3: Matches on icmp increase

```
RtGroup3(config-ext-nacl)#do sh access-list
Standard IP access list NAT
    10 permit 192.168.3.192, wildcard bits 0.0.0.7 (14 matches)
    20 permit 192.168.3.200, wildcard bits 0.0.0.7 (14 matches)
    30 permit 192.168.3.208, wildcard bits 0.0.0.7 (80 matches)
    40 permit 192.168.3.0, wildcard bits 0.0.0.127 (251 matches)
    50 permit 192.168.3.128, wildcard bits 0.0.0.63
Extended IP access list ACL-GROUP4
    10 deny tcp 192.168.3.0 0.0.0.127 10.1.1.128 0.0.0.15 eq 22 (18 matches)
    30 deny tcp 192.168.3.0 0.0.0.127 host 10.1.1.129 eq telnet (7 matches)
    40 deny tcp 192.168.3.0 0.0.0.127 host 10.1.1.131 eq ftp (77 matches)
    60 deny icmp 192.168.3.0 0.0.0.127 host 10.1.1.130 echo (8 matches)
    70 permit ip any any (496 matches)
Extended IP access list IPSEC-ACL
    10 permit gre host 113.114.115.2 host 113.114.115.1 (560155 matches)
```

Figure 6.2.27.3: Matches on icmp increase

Step 4: Test for telnet



C:\> Telnet 10.1.1.129
 Welcome to Microsoft Telnet Client
 Escape Character is 'CTRL+]'
 Microsoft Telnet> open 10.1.1.129
 Connecting To 10.1.1.129...

Figure 6.2.27.4: Testing telnet

Step 5: Show access list to see the matches for telnet

```
RtGroup3(config-ext-nacl)#do sh access-list
Standard IP access list NAT
  10 permit 192.168.3.192, wildcard bits 0.0.0.7 (14 matches)
  20 permit 192.168.3.200, wildcard bits 0.0.0.7 (14 matches)
  30 permit 192.168.3.208, wildcard bits 0.0.0.7 (80 matches)
  40 permit 192.168.3.0, wildcard bits 0.0.0.127 (251 matches)
  50 permit 192.168.3.128, wildcard bits 0.0.0.63
Extended IP access list ACL-GROUP4
  10 deny tcp 192.168.3.0 0.0.0.127 10.1.1.128 0.0.0.15 eq 22 (18 matches)
  30 deny tcp 192.168.3.0 0.0.0.127 host 10.1.1.129 eq telnet (9 matches)
  40 deny tcp 192.168.3.0 0.0.0.127 host 10.1.1.131 eq ftp (77 matches)
  60 deny icmp 192.168.3.0 0.0.0.127 host 10.1.1.130 echo (8 matches)
  70 permit ip any any (514 matches)
Extended IP access list IPSEC-ACL
  10 permit gre host 113.114.115.2 host 113.114.115.1 (560194 matches)
```

Figure 6.2.27.5: Matches on telnet increase

Step 6: Test on <ftp://10.1.1.131>

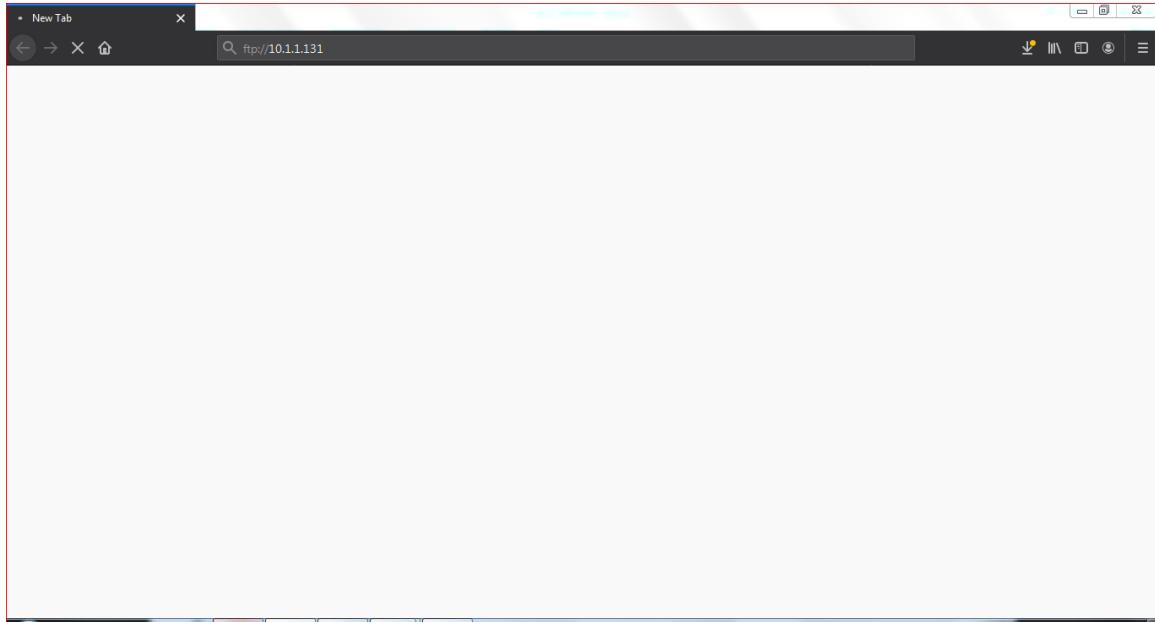


Figure 6.2.27.6: Testing ftp

Step 7: Show access list to see the matches for ftp

```
RtGroup3(config-ext-nacl)#do sh access-list
Standard IP access list NAT
    10 permit 192.168.3.192, wildcard bits 0.0.0.7 (14 matches)
    20 permit 192.168.3.200, wildcard bits 0.0.0.7 (14 matches)
    30 permit 192.168.3.208, wildcard bits 0.0.0.7 (80 matches)
    40 permit 192.168.3.0, wildcard bits 0.0.0.127 (251 matches)
    50 permit 192.168.3.128, wildcard bits 0.0.0.63
Extended IP access list ACL-GROUP4
    10 deny tcp 192.168.3.0 0.0.0.127 10.1.1.128 0.0.0.15 eq 22 (18 matches)
    30 deny tcp 192.168.3.0 0.0.0.127 host 10.1.1.129 eq telnet (10 matches)
    40 deny tcp 192.168.3.0 0.0.0.127 host 10.1.1.131 eq ftp (79 matches)
    60 deny icmp 192.168.3.0 0.0.0.127 host 10.1.1.130 echo (8 matches)
    70 permit ip any any (525 matches)
Extended IP access list IPSEC-ACL
    10 permit gre host 113.114.115.2 host 113.114.115.1 (560234 matches)
```

Figure 6.2.27.7: Matches on ftp increase

Step 8: do wr command for saving all the command

```
RtGroup3(config-ext-nacl)#do wr
Building configuration...
[OK]
```

Figure 6.2.27.8: Saving configuration

6.2.28 IPv6 Tunnel and IPv6 Web Testing

Step 1: Open website on remote site and view remote address of the website

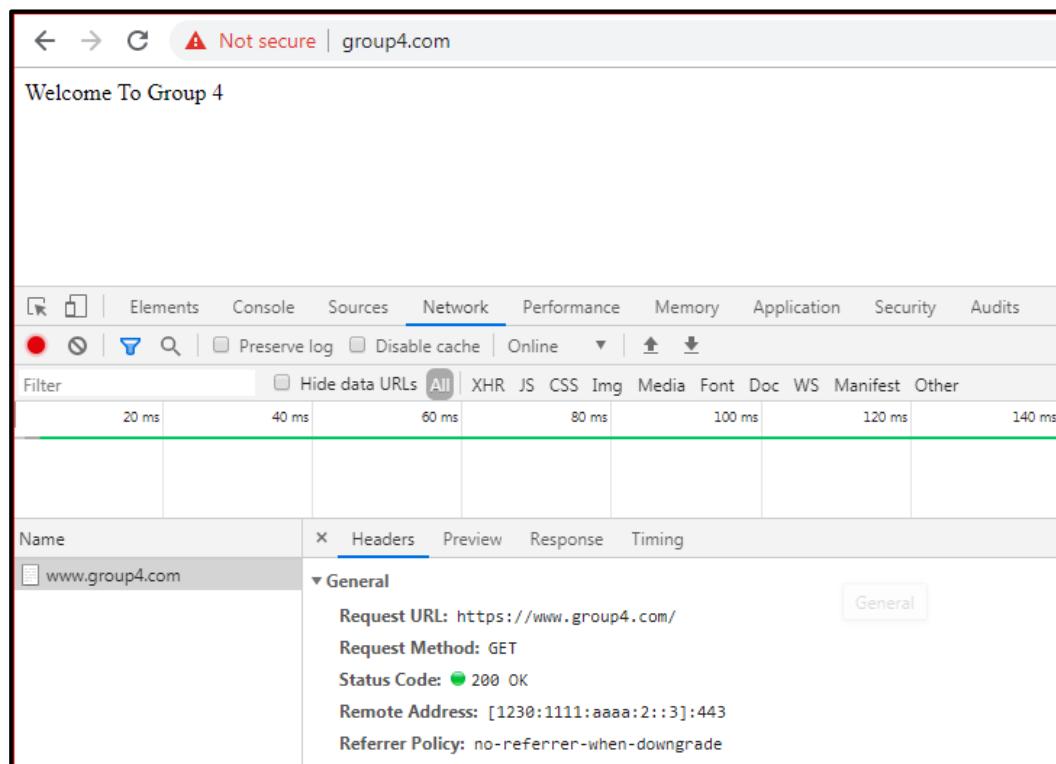


Figure 6.2.28.1: group4.com website with IPv6 Address

Step 2: Interface tunnel in “UP” condition for both site

```
R4(config)#do sh ip int br
Interface          IP-Address      OK? Method Status       Protocol
FastEthernet0/0    200.200.200.1   YES NVRAM up        down
FastEthernet0/0.10 unassigned      YES unset up        down
FastEthernet0/1    unassigned      YES NVRAM up        up
FastEthernet0/1.10 10.1.1.126    YES NVRAM up        up
FastEthernet0/1.20 10.1.1.142    YES NVRAM up        up
Serial0/2/0        unassigned      YES NVRAM down     down
Serial0/2/1        113.114.115.1 YES NVRAM up        up
NVI0              unassigned      NO  unset up        up
Loopback1         1.1.1.1       YES NVRAM up        up
Tunnel0            2.2.2.1       YES NVRAM up        up
R4(config)#[
```

Figure 6.2.28.2: Tunnel0 status

Step 3: Ping tunnel IP address on remote site

```
R4(config)#do ping 1230:1111:aaaa:3::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1230:1111:AAAA:3::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms
R4(config)#[
```

Figure 6.2.28.3: Ping status success

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 for testing. All testing are successful tested.

CHAPTER 7: CONCLUSION

7.1 Introduction

All task given finish and meet the due date. Implementation of this Workshop 2 starts from selecting group leader for lead this subject from beginning until end. Each group member has been given the services until done. It is important to manage the services to avoid error to other services.

Workshop 2 is prerequisite for student before ongoing industrial training. This Workshop 2 related to subject Computer Organization and Architecture, Operating System, Local Area Network, Internet Technology, Network Analysis and Design, Wide Area Network and Network Project Management.

Besides, it provides and exchanged knowledge between network and security students. Students can get more knowledge after exploring about their services. Lot of things to be studied for set up, installing, configuration and troubleshoot for all services that implement in Workshop 2.

7.2 Project Advantages

By doing this project, it gives more experiences and can be used on the workplace. So, the advantages are:

- Learned how to overcome any problems that occur when configuration
- Helps student enhance their soft skills
- Gained more knowledge about network and security services
- Improved communication skills between network and security students
- Gives environment for the real work
- Make student manage their time to complete all services given

7.3 Project Disadvantages

There are some disadvantages during do this subject which are:

- Students lack of knowledge about some services
- Network equipment are not in good condition

7.4 Project Limitation

Due to this limitation, this project need to adapt and work harder to succeed. These limitations are:

- The network can be implement in wired environment
- Equipment that provided to each group are not in good condition
- Project involved only for 3 servers

7.5 Conclusion

Last but not least, we are able to set up and configure network using network equipment provided. In Workshop 2, there are 3 different servers that are being used to complete this project which is Windows Server, Debian and Ubuntu. We are able to design and maintaining for a good condition. In addition, we learn to build up crucial security system such as Server Hardening, Port Security, and Access Control List (ACL) to secure and protect the network being access by unauthorized access. So, this Workshop 2 done by applying the knowledge that we have learned from Computer Organization and Architecture, Operating System, Local Area Network, Internet Technology, Network Analysis and Design and Wide Area Network.

In conclusion, this Workshop 2 may help students to prepare for work in real job environment or industrial training. We have managed to complete all the tasks given. We grateful and appreciate to our supervisor for guiding us until it successful complete besides gain lots of new knowledge.

REFERENCES

- Kamalakannan Srinivasan* (2015, July). End-to-end steps for configuring Active Directory Kerberos authentication. Retrieved from <https://docs.bmc.com/docs/sso90/end-to-end-steps-for-configuring-active-directory-kerberos-authentication-474057067.html>
- Karim Budzar (February, 2019). How to Configure DHCP Server on Windows Server 2012 R2. Retrieved from <https://www faqforge com/windows/configure-dhcp-server-windows-server-2012-r2/>
- Cisco Support (October, 2018). Configure Commonly Used IP ACLs. Retrieved from <https://www.cisco.com/c/en/us/support/docs/ip/access-lists/26448-ACLsamples.html>
- Rahul (May, 2016). How to Install Zabbix Agent in Windows System. Retrieved from <https://tecadmin.net/install-zabbix-agent-windows-system/>
- Aaron Kili (October, 2018). How to Setup Central Logging Server with Rsyslog in Linux. Retrieved from <https://www.tecmint.com/install-rsyslog-centralized-logging-in-centos-ubuntu/>
- Cisco Support (July, 2016). LAN-to-LAN IPsec Tunnel between Two Routers Configuration Example. Retrieved from <https://www.cisco.com/c/en/us/support/docs/routers/1700-series-modular-access-routers/71462-rtr-l2l-ipsec-split.html>
- Chandan Kumar (June, 2019). A practical guide to secure and harden Apache HTTP Server. Retrieved from <https://geekflare.com/apache-web-server-hardening-security/>
- Linuxine (January, 2019). How to Install and Configure Zabbix on Debian 9 Linux. Retrieved from <https://linuxize.com/post/how-to-install-and-configure-zabbix-on-debian-9/>
- [Margaret Rouse](#). Active Directory. Retrieved from <https://searchwindowsserver.techtarget.com/definition/Active-Directory>

Cisco Systems, Inc(2012).IPv6 Implementation Guide, Cisco IOS Release 15.2M&T.

Retrieved from <https://www.cisco.com/c/en/us/td/docs/ios>

xml/ios/ipv6/configuration/15-2mt/ipv6-15-2mt-book/ip6-tunnel.html

Henry Benjamin (May,2002). CCNP Routing Studies: Basic Open Shortest Path

First. Retrieved from

<http://www.ciscopress.com/articles/article.asp?p=26919&seqNum=3>

APPENDIX

Action / Week	1	2	3	4	5	6	7	8	9	10	11	12	13	14
<ul style="list-style-type: none"> ● Briefing on Workshop 2. ● Discussion of division individual task. 														
<ul style="list-style-type: none"> ● Collect/setup hardware. ● Installing Operating System ● Design network topology (logical & physical). ● Assign IP addresses. ● Writing proposal report and submit for approval. 														
<ul style="list-style-type: none"> ● Testing Services. ● Project Progress I 														
<ul style="list-style-type: none"> ● Project progress II 														
<ul style="list-style-type: none"> ● Project progress III & Complete Service. 														
<ul style="list-style-type: none"> ● Preparing Video & Poster. 														
<ul style="list-style-type: none"> ● Final Demonstration of Workshop II exhibition with Supervisor & Evaluator. 														
<ul style="list-style-type: none"> ● Final report, Peer Assessment Report and Log Book Submission 														

APPENDIX(VLSM Addressing and IP table)

Network	Broadcast	Subnet Mask	VLAN
10.1.1.128	10.1.1.143	255.255.255.240	10
1230:1111:AAAA:1::	-	/64	
10.1.1.0	10.1.1.127	255.255.255.128	20
1230:1111:AAAA:2::	-	/64	
113.114.115.0	113.114.115.7	255.255.255.248	
1230:1111:AAAA:3::	-	/64	

Device	Interface	IP Address	Subnet Mask	Default Gateway	VLAN
R4	Serial 0/0	113.114.115.1	255.255.255.248	-	-
	Tun0	1230:1111:AAAA:3::1	/64		-
	Fa 0/1.10	10.1.1.142	255.255.255.240		1
		1230:1111:AAAA:1::FFE	/64		0
	Fa 0/1.20	10.1.1.126	255.255.255.128		2
		1230:1111:AAAA:2::FFE	/64		0
SW	VLAN 10	10.1.1.141	255.255.255.240	-	1
		1230:1111:AAAA:2::FFD	/64		0
WINSVR	Eth0	10.1.1.129	255.255.255.240	10.1.1.142	1
		1230:1111:AAAA:1::1	/64	1230:1111:AAAA:1::FFFE	
DEBIAN	Eth0	10.1.1.130	255.255.255.240	10.1.1.142	

		1230:1111: AAAA:2::2	/64	1230:1111:AAAA: 2::FFFE	1 0
UBUNTU	Eth0	10.1.1.131	255.255.255.240	10.1.1.142	1 0
		1230:1111: AAAA:2::3	/64	1230:1111:AAAA: 2::FFFE	
WAP	Eth0	10.1.1.1	255.255.255.128	-	2 0
		1230:1111: AAAA:2::1	/64		
CLIENT1	Eth0	DHCP	255.255.255.192	172.1.1.78	2 0