



**FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY**

**BITC & BITZ 2018/2019 SESSION**

**WORKSHOP 2 (BITU 3923)**

**GROUP 10**

**PROJECT TITLE: PROXY SERVER**

**FINAL REPORT**

**PREPARED BY:**

No.	Name	Matric No.
1.	MUHAMMAD NUQMAN SIDDIQI BIN MOHAMAD AKHIR	B031610049
2.	NOOR NABILAH BINTI NORDIN	B031720020
3.	NURZANNAH NADATUL SAADIAH BINTI IRWAN	B031610046
4.	HUD BIN ABDUL RAZAKEK	B031610032
5.	NURUL NAJLAA BINTI AHMAD ARIFFIN	B031710075
6.	ZARINA ARIFAH BINTI AFRIZON	B031610155
7.	TENG WEI XIAN	B031610131
8.	NUR FARHANA BINTI DARKASEH	B031610415
9.	KABELAN P. MANICKAVELU	B031610411

**SUPERVISED BY**

**EN. NOR AZMAN BIN MAT ARIF (M)**

**DR. OTHMAN BIN MOHD (S)**

**EN. MOHD HAKIM BIN ABDUL HAMID (S)**

**EVALUATED BY**

**DR. SHEIKH FAISAL ABDUL LATIP**

## **ACKNOWLEDGEMENT**

First and foremost, we would like to thank our project supervisor, En Nor Azman Bin Mat Arif and our co-supervisor Dr. Othman Bin Mohd and En. Mohd Hakim Bin Abdul Hamid for their valuable guidance and advice that lead us to finish all their services in Workshop 2. Three of them inspired us greatly to work in team for this project. Their willingness to motivate us contributed tremendously to our project. We also would like to thank them for showing us some examples that are related to the services in our project which helped us to understand our project better. Besides that, they also taught us that we must think out of the box from our comfort zone and try to make our services better and great. All of this guidance helped us to complete our project on time. We would also like to thank our evaluator for this workshop, Dr. Shekh Faisal bin Abdul Latip for taking their time to evaluate us. This evaluation gave us a deeper understanding of our services and what we must add to our service to make it better than we already have.

We also would like to thank the authority of University Teknikal Malaysia Melaka (UTeM) for providing us with good environment and facilities to complete this project. Finally, an honorable mention goes to families and friends for their understandings and supports for us in completing this project. With the help of everyone that was mentioned above, we were able to overcome many problems that occurred during the Workshop 2 and we were able to complete our project successfully on time.

## **ABSTRACT**

In this Workshop 2 project, we must define, implement and manage tasks which start from selecting a leader to lead this project from the beginning until the end of this project. A task has been given to each member and we create a schedule for the task to finish on time and who will do what service. It is very important to manage and organizes every task given in order to avoid any problems and error later. Our main objective in this Workshop II is for this project to be successful and able to go through the obstacles and challenges faced while completing the task given. Next our objective also is to have deeper understanding about the service on how it works, and we are grateful to experience this as it helped us to be more prepared in our industrial training. Our group had decided to use Windows Server 2012 R2, Fedora server 2 and Ubuntu server. We chose this server operating system because it has many benefits. Our group also was assigned to set up 30 services listed. The 30 services listed are DNS (IPv4 & IPv6), Linux Email Server, DHCP, Secured FTP, Routing & NAT, Access, Control List (ACL), Samba, VLAN, IPv6 Web (IPv6 Web test run from neighboring group), Proxy Server, Radius Server for Network Accounting, Network Management System, Security Hardening, Security Policy, Authentication using radius server, User authentication and authorization, Firewall for router (ACL), Remote login using SSH, Server hardening, Harden Linux server, Harden Fedora server, Harden Windows server, Harden web server, Authentication user by integrating AD with Linux, Installation IDS (port mirror), IPSec between server and client, Samba Security Services, Port Security, STP Security, VLAN security. During the Workshop II, we faced several problems but still managed to overcome it and make this project in time and successfully completed the services.

## **ABSTRAK**

Dalam Projek Bengkel 2 ini, kita harus menentukan, melaksanakan dan menguruskan tugas-tugas yang telah diberikan. Kami bermula dengan memilih seorang pemimpin untuk mengetuai projek ini dari awal hingga ke akhir projek bengkel 2 ini. Setiap ahli kumpulan telah dibahagikan dengan tugas secara sama rata dan sebuah jadual telah dihasilkan di mana jadual itu digunakan untuk memastikan bahasa tugas itu disiapkan dalam masa yang ditetapkamn. Setiap tugas harus diuruskan dengan sebaik mungkin untuk mengelakkan daripada menimbulkan sebarang masalah dan kesilapan. Objektif utama Bengkel 2 ini adalah untuk melaksanakan projek ini dengan jayanya dan untuk mengatasi sebarang halangan dan cabaran yang dihadapi semasa menyelesaika tugasan tang diberikan sepangjang semester ini. Selain itu, mendapatkan pemahaman mengenai servis-servis yang perlu ada di setiap rangkaian komputer juga merupakan salah satu objektif bengkel ini. Kami sangat berterima kasih kepada pengalaman ini kerana projek ini banyak membantu kami untuk bersedia untuk latihan industry nanti. Kumpulan kami telah membuat keputusan untuk menggunakan Window Server 2012 R2, Fedora Server dan Ubuntu Server. Kami memilih sistem operasi pelayan ini kerana manfaatnya. Kumpulan kami juga telah ditugaskan untuk membekalkan 30 servis kepada rangkaian kami. Antara 30 servis yang disenariakan adalah DNS (IPv4 & IPv6), Linux Email Server, DHCP, Secured FTP, Routing & NAT, Access, Control List (ACL), Samba, VLAN, IPv6 Web (IPv6 Web test run from neighboring group), Proxy Server, Radius Server for Network Accounting, Network Management System, Security Hardening, Security Policy, Authentication using radius server, User authentication and authorization, Firewall for router (ACL), Remote login using SSH, Server hardening, Harden Linux server, Harden Fedora server, Harden Windows server, Harden web server, Authentication user by integrating AD with Linux, Installation IDS (port mirror), IPSec between server and client, Samba Security Services, Port Security, STP Security, VLAN security.

## TABLE OF CONTENT

<b>ACKNOWLEDGEMENT.....</b>	<b>I</b>
<b>ABSTRACT .....</b>	<b>II</b>
<b>ABSTRAK.....</b>	<b>III</b>
<b>TABLE OF CONTENT.....</b>	<b>IV - X</b>
<b>LIST OF FIGURES .....</b>	<b>XI - XXIX</b>
<b>CHAPTER 1.....</b>	<b>1</b>
<b>INTRODUCTION.....</b>	<b>1</b>
1.1 Introduction .....	1
1.2 Objective .....	2
1.3 Project Plan .....	3
1.4 Project Plan / Schedule .....	4
1.5 Conclusion.....	5
<b>CHAPTER 2.....</b>	<b>6</b>
<b>PROJECT REQUIREMENT .....</b>	<b>6</b>
2.1 Introduction .....	6
2.2 Types of Operating System use in the Project.....	6
2.3 Operating System Background.....	6
2.3.1 Window Server 2012 R2.....	6
2.3.2 Ubuntu 16.04 .....	7
2.3.3 Fedora 28 .....	7
2.4 Operating System Justification.....	7
2.4.1 Window Server 2012 R2.....	7
2.4.2 Ubuntu 16.04.....	8

2.4.3 Fedora 28 .....	8
2.5 Hardware Requirement.....	8
2.6 Hardware Justification .....	9
2.6.1 Window Server .....	9
2.6.2 Ubuntu Server .....	9
2.6.3 Fedora Server .....	10
2.6.4 Router .....	10
2.6.5 Switch .....	12
2.6.6 UTP cable.....	12
2.6.7 RJ45 .....	13
2.6.8 Crimping Tool.....	13
2.7 Conclusion .....	14
<b>CHAPTER 3.....</b>	<b>15</b>
<b>DESIGN .....</b>	<b>15</b>
3.1 Introduction .....	15
3.2 Security Policy .....	15
3.2.1 General .....	15
3.3 Logical Security.....	17
3.3.1 Network.....	17
3.4 Operational Security .....	19
3.5 Server Security .....	20
3.6 Network Security .....	22
3.7 Application Security .....	23
3.8 Physical Security .....	29
3.9 Physical Design .....	31

3.10 Logical Design.....	32
2.6.2 IP Addressing Table .....	33
2.6.3 Conclusion.....	34
<b>CHAPTER 4.....</b>	<b>35</b>
<b>SERVICES.....</b>	<b>35</b>
4.1 Overview of Services .....	35
4.1.1 Domain Name System (DNS).....	35
4.1.2 Dynamic Host Configuration Protocol (DHCP).....	35
4.1.3 IPv6 Web with IPv6 Tunnelling .....	35
4.1.4 Inter VLAN and VLSM Addressing.....	36
4.1.5 Secured FTP.....	36
4.1.6 Authentication using radius server.....	36
4.1.7 Routing.....	37
4.1.8 Network Address Translation (NAT) .....	37
4.1.9 Access Control List (ACL) .....	37
4.10 Samba.....	37
4.1.11 Linux Email Server .....	38
4.1.12 Proxy Server.....	38
4.1.13 Web, SSL and Virtual Hosting .....	38
4.1.14 Server Virtualization.....	39
4.1.15 Remote Login Using SSH.....	39
4.1.16 Network Management System.....	39
4.1.17 Port Security.....	40
4.1.18 Linux Server Hardening .....	40
4.1.19 Instrusion Detection System (IDS) .....	40

4.1.20 Security Policy .....	41
4.1.21 Router Hardening.....	41
4.1.22 Window Server Hardening .....	41
4.1.23 Authentication.....	42
4.1.24 IPsec .....	42
4.1.25 Samba Security Services.....	42
4.1.26 Active Directory.....	43
4.1.27 VLAN Security .....	43
4.1.28 Cloud Server .....	43
4.1.29 Media Streaming Center .....	44
4.1.30 Wireless user authentication using Radius server .....	45
4.2 Individual Task.....	46
4.2.1 Service Task (For BITC) .....	46
4.2.2 Service Task (For BITZ) .....	47
<b>CHAPTER 5 .....</b>	<b>49</b>
5.1 Introduction .....	50
5.2 Installation of Service.....	50
5.2.1 DNS (primary and secondary servers) IPv4 & IPv6.....	50
5.2.2 DHCP (IPV4).....	81
5.2.3 DHCP (IPv6).....	87
5.2.4 IPv6 Web with IPv6 Tunneling .....	93
5.2.5 InterVLAN & VLSM Addressing .....	97
5.2.6 Secured FTP.....	99
5.2.7 AAA (Authentication, Authorization and accounting) using Radius .....	102
5.2.8 Routing & Network Address Translation (NAT) .....	119

5.2.9 Access Control List (ACL) .....	120
5.2.10 Samba.....	121
5.2.11 Linux Email Server.....	123
5.2.12 Proxy Server.....	138
5.2.13 Web, SSL & Virtual Hosting .....	142
5.2.14 Server Virtualization.....	163
5.2.15 Wireless Authentication using Radius Server.....	170
5.2.16 Remote Login using SSH.....	176
5.2.17 Network Management System.....	183
5.2.18 Port Security.....	186
5.2.19 Linux Server Hardening.....	189
5.2.20 Intrusion Detection System (IDS) & Port Mirror .....	210
5.2.21 Security Policy .....	224
5.2.22 Router Hardening.....	224
5.2.23 Window Server Hardening .....	225
5.2.24 Authentication user by Integrating AD users with Linux .....	263
5.2.25 IPSec for remote employee .....	267
5.2.26 Samba Security Services.....	274
5.2.27 Active Directory.....	276
5.2.28 VLAN Security .....	288
5.2.29 Cloud Server .....	290
5.2.30 Media Streaming Server .....	294
<b>CHAPTER 6.....</b>	<b>297</b>
6.1 Introduction .....	298
6.2 Service Testing .....	298

6.2.1 DNS (primary and secondary servers) IPv4 & IPv6.....	298
6.2.2 DHCP (IPV4).....	301
6.2.3 DHCP (IPv6).....	304
6.2.4 IPv6 Web with IPv6 Tunneling .....	305
6.2.5 Secured FTP.....	306
6.2.6 Routing & Network Address Translation (NAT) .....	308
6.2.7 Access Control List (ACL) .....	309
6.2.8 Samba.....	311
6.2.9 Linux Email Server .....	319
6.2.10 Proxy Server.....	323
6.2.11 Web, SSL & Virtual Hosting .....	325
6.2.12 Server Virtualization.....	328
6.2.13 Wireless Authentication using Radius Server.....	329
6.2.14 Remote Login using SSH.....	361
6.2.15 Network Management System.....	369
6.2.16 Port Security.....	375
6.2.17 Linux Server Hardening.....	377
6.2.18 Intrusion Detection System (IDS) & Port Mirror .....	381
6.2.19 Router Hardening.....	387
6.2.20 Window Server Hardening .....	388
6.2.21 Authentication user by Integrating AD users with Linux.....	390
6.2.22 IPSec for remote employee .....	393
6.2.23 Samba Security Services.....	399
6.2.24 Active Directory.....	401
6.2.25 VLAN Security .....	403

6.2.26 Cloud Server .....	404
6.2.27 Media Streaming Server .....	405
<b>CHAPTER 7 .....</b>	<b>407</b>
<b>CONCLUSION .....</b>	<b>407</b>
7.1 Introduction .....	407
7.2 Project Advantages .....	408
7.3 Project Disadvantages .....	408
7.4 Project Limitation.....	409
7.5 Conclusion.....	409

## LIST OF FIGURES

Figure 2.6.4: Cisco Integrated Service Router.....	11
Figure 2.6.5: Cisco Catalyst 2960 Switch.....	12
Figure 2.6.6: UTP cable .....	12
Figure 5.2.1.1: Open Server Manager and Administrative Tool .....	50
Figure 5.2.1.2: Check the DNS Server for installation .....	51
Figure 5.2.1.2.1: Right click on Forward Lookup Zone and select New.....	52
Figure 5.2.1.2.2: Click Next.....	53
Figure 5.2.1.2.3: Choose Primary zone and Click Next .....	53
Figure 5.2.1.2.3: Insert the zone name with group1.com then Click Next .....	54
Figure 5.2.1.2.4: Choose “Allow both non secure and secure dynamic” .....	54
Figure 5.2.1.2.15: Click Finish to create IPv4 Forward Lookup Zone .....	55
Figure 5.2.1.2.15: Right click on the Forward Lookup Zone and choose .....	55
Figure 5.2.1.2.5: Insert the name and IP address for Windows .....	56
Figure 5.2.1.3.1: Right click on Reverse Lookup Zone and select New Zone .....	57
Figure 5.2.1.3.2: Proceed with Next .....	58
Figure 5.2.1.3.2: Choose Primary zone and Next.....	59
Figure 5.2.1.3.3: Choose IPv4 Reverse Lookup Zone then Next .....	60
Figure 5.2.1.3.4: Insert the Network ID which is 192.168.9.130 .....	61
Figure 5.2.1.3.5: Choose “Allow both non secure and secure dynamic updates” .....	61
Figure 5.2.1.3.6: Click Finish to Create IPv4 Reverse Lookup Zone.....	62
Figure 5.2.1.3.7: Right click the IPv4 Reverse Lookup Zone and add New .....	63
Figure 5.2.1.3.8: Add the host IP Address and the host name for windows.....	63
Figure 5.2.1.4.1: Install IP Address version 6 in the Windows Server.....	64
Figure 5.2.1.4.1: Assigned the static IP Address, Subnet-prefix Length and Default Gateway .....	64
Figure 5.2.1.5.1: Right click on the Forward Lookup Zones and choose.....	65
Figure 5.2.1.5.2: Click Next.....	65
Figure 5.2.1.5.3: Choose Primary zone and Click Next .....	66
Figure 5.2.1.5.4: Checked the "To all DNS Servers running on domain controllers in this domain: group10.com".....	66
Figure 5.2.1.5.5: Create a new zone name and Click Next.....	67
Figure 5.2.1.5.6: Allow both secure dynamic updates.....	67
Figure 5.2.1.5.7: Click Finish to create IPv6 Forward Lookup Zone for Windows .....	68

Figure 5.2.1.5.8: Right click on the Reverse Lookup Zones and choose New Zone.....	69
Figure 5.2.1.5.9: Click Next.....	70
Figure 5.2.1.5.10: Choose Primary zone and Click Next .....	71
Figure 5.2.1.5.11: Choose IPv6 Reverse Lookup Zone then Click Next.....	71
Figure 5.2.1.5.12: Insert the IPv6 Address Prefix and Click Next .....	72
Figure 5.2.1.5.13: Click Finish to create IPv6 Reverse Lookup Zone for Windows.....	73
Figure 5.2.1.5.14: Insert the host IP address and host name for client to add New Host .....	74
Figure 5.2.1.5.15: Successfully create the new host .....	75
Figure 5.2.3.6.1: Installation bind9 .....	76
Figure 5.2.3.6.2: Edit configuration file .....	76
Figure 5.2.3.7.1: Open Properties .....	77
Figure 5.2.3.7.2: Checked the allow Zone Transfer .....	77
Figure 5.2.3.7.3: checked "Automatic notify" and add Ubuntu IP address .....	78
Figure 5.2.3.8.1: Open Properties .....	79
Figure 5.2.3.8.2: Click Edit button to add IP address Ubuntu Server.....	79
Figure 5.2.3.8.3: Checked "Automatic notify" and add Ubuntu IP address .....	80
Figure 5.2.2.1: show Open DHCP Manager .....	81
Figure 5.2.2.2: show the New Scope Wizard.....	82
Figure 5.2.2.3: show the Name and Description for the New Scope.....	82
Figure 5.2.2.4: show the Configuration of IP Address .....	83
Figure 5.2.2.5: show the Configuration of Exclusions and Delay .....	83
Figure 5.2.2.6: show the Lease Duration that Need to be Set.....	84
Figure 5.2.2.7: show the DHCP Options .....	84
Figure 5.2.2.8: show the Default Gateway Used by Client .....	85
Figure 5.2.2.9: show the Configuration of Domain Name and DNS Servers.....	85
Figure 5.2.2.10: show Scope Activation .....	86
Figure 5.2.3.2: New Scope Wizard .....	87
Figure 5.2.3.2: New Scope Wizard .....	87
Figure 5.2.3.3: DHCP Server .....	88
Figure 5.2.3.4: Network Connection.....	88
Figure 5.2.3.5: Network Connection.....	89
Figure 5.2.3.6: Enable Ipv6.....	89
Figure 5.2.3.7: TCP/IPv6 Properties.....	90
Figure 5.2.3.8: DHCP Servers .....	90

Figure 5.2.3.9: DHCP Servers Configuration Options .....	91
Figure 5.2.3.10: Scope Options.....	91
Figure 5.2.3.11: Wireless client using Ipv6. ....	92
Figure 5.2.3.12: Wired Client using Ipv6. ....	92
Figure 5.2.4.2.1: Properties of webipv6.....	96
Figure 5.2.6.1: Enabling.....	100
Figure 5.2.6.2: Configuration.....	100
Figure 5.2.6.3: Check user .....	101
Figure 5.2.7.1: Server Manager .....	102
Figure 5.2.7.2: Add Roles and Features.....	102
Figure 5.2.7.3: Select server roles.....	103
Figure 5.2.7.4: Installation progress .....	103
Figure 5.2.7.5: Network Policy Server .....	104
Figure 5.2.7.6: Enable NPS.....	104
Figure 5.2.7.7: New radius client.....	105
Figure 5.2.7.8: New network policies.....	106
Figure 5.2.7.9: Policy Name .....	107
Figure 5.2.7.10: Specify Condition.....	107
Figure 5.2.7.11: Check names.....	108
Figure 5.2.7.12: Access permission .....	108
Figure 5.2.7.13: Authentication method .....	109
Figure 5.2.7.15: Configure settings.....	110
Figure 5.2.7.16: Attribute information.....	110
Figure 5.2.7.19: Vendor specific.....	111
Figure 5.2.7.20: Attribute value .....	112
Figure 5.2.7.21: Complete .....	113
Figure 5.2.7.22: Accounting in Network Policy Server.....	113
Figure 5.2.7.23: Introduction in accounting configuration .....	114
Figure 5.2.7.24: Select accounting option .....	114
Figure 5.2.7.25: Configure file logging .....	115
Figure 5.2.7.26: Conclusion.....	115
Figure 5.2.8.1: Configure NAT interface.....	119
Figure 5.2.8.2: Configure static NAT .....	119
Figure 5.2.8.3: Configure static access list .....	119

Figure 5.2.8.4: Create dynamic NAT pool .....	119
Figure 5.2.8.5: Create OSPF routing for NAT.....	119
Figure 5.2.9.1: Server Manager Dashboard.....	120
Figure 5.2.9.2: Server Manager Dashboard .....	120
Figure 5.2.9.3: Server Manager Dashboar .....	120
Figure 5.2.9.4: Server Manager Dashboard .....	120
Figure 5.2.9.5: Server Manager Dashboard .....	120
Figure 5.2.10.1: show Installing Samba Package .....	121
Figure 5.2.10.2: show Open the Port for Samba.....	121
5.2.10.3: Figure show to Enable the Access to Home Directory .....	121
Figure 5.2.10.4: show Add the User with pdbeedit .....	122
Figure 5.2.10.5: show Share the Home Directory for Each User .....	122
5.2.10.6: Figure show the change the permission to 0777 .....	122
Figure 5.2.11.1: Set hostname for Ubuntu Server. ....	123
Figure 5.2.11.2: Check your location time info. ....	123
Figure 5.2.11.3: Check status your time synchronization with your server. ....	124
Figure 5.2.11.4: Set an A record maps a FQDN to an IP address. ....	124
Figure 5.2.11.5: Set an MX record tells other MTAs that your mail server mail.group10.com is responsible for email delivery for your domain. ....	125
Figure 5.2.11.6: Command to run postfix.....	125
Figure 5.2.11.7: Selecting Internet Site. ....	126
Figure 5.2.11.8: Domain name entered.....	126
Figure 5.2.11.9: Show “/etc/postfix/main.cf” file is generated.....	127
Figure 5.2.11.10: Show mail version. ....	127
Figure 5.2.11.11: Netstat show what port is active and listening. ....	127
Figure 5.2.11.12: Run the following command on a separate computer such as your personal computer. ....	128
Figure 5.2.11.13: A pairs of key and certificates created based on RSA encryption 2048 bit.	128
Figure 5.2.11.14: Information that will incorporated into the certificate request.....	128
Figure 5.2.11.15: Edit the master.cf file. ....	129
Figure 5.2.11.16: The above configuration enables the submission daemon of Postfix and requires TLS encryption. ....	129
Figure 5.2.11.17: Edit the main.cf file. ....	129
Figure 5.2.11.18: Edit the TLS parameter as follows. ....	130

Figure 5.2.11.19: Save and close the file. Then reload Postfix.	130
Figure 5.2.11.20: port 587 is now open.	130
Figure 5.2.11.21: Install Dovecot core package and the IMAP daemon package.	131
Figure 5.2.11.22: Add the following line to enable IMAP protocol.	131
Figure 5.2.11.23: Sample output of mail spool directory.	131
Figure 5.2.11.24: Add the following line in the file.	132
Figure 5.2.11.25: Add dovecot to the mail group so that Dovecot can read the INBOX.	132
Figure 5.2.11.26: Edit the authentication config file.	132
Figure 5.2.11.27: Uncomment the following line “ <code>disable_plaintext_auth = yes</code> ”.	132
Figure 5.2.11.28: Add “ <code>auth_username_format = %n</code> ” if you want to use full email address ( <code>username@your-domain.com</code> ) to login.	133
Figure 5.2.11.29: Add “plain login” to use another common authentication mechanism instead of PLAIN authentication mechanism.	133
Figure 5.2.11.30: specify the location of your SSL/TLS cert and private key. Don’t leave out < character.	133
Figure 5.2.11.31: Edit the following file.	134
Figure 5.2.11.32: Change “service auth” section to the following so that Postfix can find the Dovecot authentication server.	134
Figure 5.2.11.33: Edit the below config file.	134
Figure 5.2.11.34: To auto create a folder, simply add the following line in the mailbox section.	135
Figure 5.2.11.35: Restart your dovecot and postfix.	135
Figure 5.2.11.36: make a directory for rainloop.	135
Figure 5.2.11.37: Install curl.	136
Figure 5.2.11.38: Download the latest RainLoop community edition.	136
Figure 5.2.11.39: rainloop directory to /var/www/.	136
Figure 5.2.11.40: Now set web server user (www-data) as the owner.	136
Figure 5.2.11.41: create the virtual host file with the following command.	136
Figure 5.2.11.42: Put the following text into the file.	137
Figure 5.2.11.43: Save and close file, then enable this virtual host and reload apache.	137
Figure 5.2.12.1: Squid Installation Command.	138
Figure 5.2.12.2: Squid Installation Complete.	138
Figure 5.2.12.3: Command to enter squid configuration.	139
Figure 5.2.12.4: Enable http access to all.	139

Figure 5.2.12.5: Now it can block any accessible domain in “block.domain.acl” file .....	140
Figure 5.2.12.6: Command to enter blocked domain file .....	140
Figure 5.2.12.7: Shows website “dummy.group10.com” is in block list.....	141
Figure 5.2.12.8: Restart squid services .....	141
Figure 5.2.13.1: Add Web Server (IIS) role .....	142
Figure 5.2.13.2: Web Server (IIS) features.....	143
Figure 5.2.13.3: Web Server (IIS) role services .....	143
Figure 5.2.13.4: Install Web Server (IIS) .....	144
Figure 5.2.13.5: Opening Progress .....	144
Figure 5.2.13.6: IIS Manager .....	145
Figure 5.2.13.7: Adding Website.....	145
Figure 5.2.13.8: Adding Default Document .....	146
Figure 5.2.13.9: Adding Default Document .....	146
Figure 5.2.13.10: Adding HTML file .....	147
Figure 5.2.13.11: Adding New Zone .....	147
Figure 5.2.13.12: New Zone note .....	148
Figure 5.2.13.13: Choosing Zone Type .....	148
Figure 5.2.13.14: Choosing the AD Zone Replication Scope.....	149
Figure 5.2.13.15: Zone Name .....	149
Figure 5.2.13.16: Choosing the Dynamic Update.....	150
Figure 5.2.13.17: Adding New Host.....	150
Figure 5.2.13.18: It shows that the New Host has been added successfully.....	151
Figure 5.2.13.19: Opening IIS Manager .....	152
Figure 5.2.13.20: Clicking on localhost server and Server Certification.....	153
Figure 5.2.13.21: Choosing server certificate .....	153
Figure 5.2.13.22: Entering details for the certificate .....	154
Figure 5.2.13.23: Adding Website.....	154
Figure 5.2.13.24: Filling information for SSL .....	155
Figure 5.2.13.25: Certificate information .....	156
Figure 5.2.13.26: The SSL website already added.....	157
Figure 5.2.13.27: Opening Progress .....	158
Figure 5.2.13.28: IIS Manager .....	159
Figure 5.2.13.29: Adding Website .....	159
Figure 5.2.13.30: Adding Default Document .....	160

Figure 5.2.13.31: Adding Default Document .....	160
Figure 5.2.13.32: Adding HTML file .....	161
Figure 5.2.13.33: Adding New Host.....	161
Figure 5.2.13.34: It shows that the New Host has been added successfully.....	162
Figure 5.2.14.1: Adding roles and feature .....	163
Figure 5.2.14.2: Choosing the protocol to authenticate live migrations.....	164
Figure 5.2.14.3: Default location for virtual hard disk files .....	164
Figure 5.2.14.4: Confirmation for installation .....	165
Figure 5.2.14.5: Installation process .....	165
Figure 5.2.14.6: Installation finished .....	166
Figure 5.2.14.7: Turning on server .....	166
Figure 5.2.14.8: Hyper-V Manager.....	167
Figure 5.2.14.9: New Virtual Machine Wizard .....	167
Figure 5.2.14.10: Specifying Name .....	168
Figure 5.2.14.11: Choosing the generation for the virtual machine .....	168
Figure 5.2.14.12: Connecting Virtual Hard Disk.....	169
Figure 5.2.14.13: Installing Operating System .....	169
Figure 5.2.15.1 Create new user .....	170
Figure 5.2.15.2 Network Policy Server interface starter .....	170
Figure 5.2.15.3 Select 802.1X Connection Type.....	171
Figure 5.2.15.4 Select 802.1X Connection Type.....	171
Figure 5.2.15.5 Select configure and Authentication Method Type.....	172
Figure 5.2.15.6 Add radius group for this network policy.....	172
Figure 5.2.15.7 Add snap-ins .....	173
Figure 5.2.15.8 Select Certificates snap-in .....	173
Figure 5.2.15.9 Start Certificate Enrollment.....	174
Figure 5.2.15.10 Request Certificate to enroll .....	174
Figure 5.2.15.11 List of certificates .....	175
Figure 5.2.16.1: SSH Configuration on Router .....	176
Figure 5.2.16.2: SSH Configuration on Router .....	176
Figure 5.2.16.3: Check the SSH whether the SSH is on or off.....	177
Figure 5.2.16.4: SSH Configuration on Switch .....	178
Figure 5.2.16.5: SSH Configuration on switch.....	178
Figure 5.2.16.6: Configuration on ubuntu server.....	179

Figure 5.2.16.7: SSH Configuration on ubuntu server .....	180
Figure 5.2.16.8: SSH Configuration on Fedora server .....	180
Figure 5.2.16.9: SSH Configuration on Fedora server .....	181
Figure 5.2.16.10: SSH Configuration on Fedora server .....	181
Figure 5.2.16.11: SSH Configuration on Fedora server .....	182
Figure 5.2.16.12: SSH Configuration on Fedora server .....	182
Figure show Installing the Mariadb Server.....	183
Figure show the Configuration of Settings in Mariadb for Root User .....	183
Figure show the Configuration of Repository for Installing.....	184
Figure show the Configuration of Enable the HTTPD and SNMPD Server .....	184
Figure show the Configuration of the Firewall.....	184
Figure show the Cacti Version 1.1.38 Installation Wizard .....	185
Figure 5.2.18.1: Configure Port for Windows Server.....	186
Figure 5.2.18.2: Configure Port for Fedora Server .....	186
Figure 5.2.18.3: Configure Port for Ubuntu Server .....	187
Figure 5.2.18.4: Configure Port for Client Wired Server .....	187
Figure 5.2.18.5: Configure Port for Client Wired Server .....	188
Figure 5.2.18.6: Assign Error Disable to management.....	188
Figure 5.2.19.1: command to update .....	189
Figure 5.2.19.2: softwares and updates interface.....	189
Figure 5.2.19.3: interface of ubuntu software center .....	190
Figure 5.2.19.4: Command to set the password .....	190
Figure 5.2.19.5: Show the password information .....	191
Figure 5.2.19.6: Command to install library for minimum password .....	191
Figure 5.2.19.7: Edit the configuration file.....	191
Figure 5.2.19.8: Configuration file for minimum passsword .....	192
Figure 5.2.19.9: install nmap .....	192
Figure 5.2.19.10: list of service in ubuntu server .....	193
Figure 5.2.19.11: Command to stop the services.....	194
Figure 5.2.19.12: show port and services .....	194
Figure 5.2.19.13: command to open local configuration .....	195
Figure 5.2.19.14: Edit local configuration .....	195
Figure 5.2.19.15: command to open main configuration .....	195
Figure 5.2.19.16: Edit the main configuration .....	196

Figure 5.2.19.17: command to check status bluetooth.....	196
Figure 5.2.19.18: command to open host configuration .....	196
Figure 5.2.19.19: Before edit the configuration.....	197
Figure 5.2.19.20: After edit the configuration .....	197
Figure 5.2.19.21: update fedora server system .....	198
Figure 5.2.19.22: update process 1 .....	199
Figure 5.2.19.23: update process 2 .....	200
Figure 5.2.19.24: update process 3 .....	201
Figure 5.2.19.25: update process 4 .....	202
Figure 5.2.19.26: update complete.....	203
Figure 5.2.19.27: Password info before edit.....	203
Figure 5.2.19.28:command to edit .....	204
Figure 5.2.19.29: after edit.....	204
Figure 5.2.19.30: command to edit password.....	204
Figure 5.2.19.32: Finish Installing .....	205
Figure 5.2.19.33: View open port .....	206
Figure 5.2.19.34: Port open.....	207
Figure 5.2.19.35: Disable service .....	207
Figure 5.2.19.36: Result .....	208
Figure 5.2.19.37: Bluetooth Status .....	208
Figure 5.2.19.38: Processing .....	209
Figure 5.2.19.39:Command to close .....	209
Figure 5.2.19.1: install update .....	210
Figure 5.2.19.2: install build-essential .....	210
Figure 5.2.19.3: install lippcap-dev .....	210
Figure 5.2.19.4: install libpcre3-dev .....	211
Figure 5.2.19.5: install libdumbnet-dev .....	211
Figure 5.2.19.6: install zlib1g-dev .....	212
Figure 5.2.19.7: install bison flex .....	212
Figure 5.2.19.8: install all dependencies .....	213
Figure 5.2.19.9: install daq-2.0.6 .....	213
Figure 5.2.19.10: extract daq-2.0.6 .....	214
Figure 5.2.19.11: configure make and install in daq-2.0.6 .....	215
Figure 5.2.19.12: Extract snort-2.9.12 .....	216

Figure 5.2.19.13: enable sourefire and make install in Snort-2.9.12 .....	216
Figure 5.2.19.14: Command to update shared library .....	217
Figure 5.2.19.15: Command to craete symlink .....	217
Figure 5.2.19.16: Command to reate user .....	217
Figure 5.2.19.17: Command to create file and set permissions .....	218
Figure 5.2.19.18: Command to create file in rules .....	218
Figure 5.2.19.19: Command to copy configuration .....	218
Figure 5.2.19.20: check the download in extraction snort and daq .....	218
Figure 5.2.19.21: Install community rules .....	219
Figure 5.2.19.22: Extract the download community rules .....	219
Figure 5.2.19.23: Extract to /etc/snort .....	220
Figure 5.2.19.24: download oinkcode of snort .....	220
Figure 5.2.19.25: Command to edit configuration snort .....	220
Figure 5.2.19.26: Edit configuration snort .....	221
Figure 5.2.19.27: Configure the local.rules .....	222
Figure 5.2.19.28: show port mirror setup .....	223
Figure 5.2.19.29: show the int fa0/20 .....	223
Figure 5.2.22.1: Encrypt password on the device .....	224
Figure 5.2.22.2: Setup Password minimal length .....	224
Figure 5.2.22.3: Setup Login Failure .....	224
Figure 5.2.22.4: Password Implementation At Line Console .....	224
Figure 5.2.22.5: Setup Exec-Timeout .....	224
Figure 5.2.23.1: Security Policy Wizard .....	225
Figure 5.2.23.2: Create new security policy .....	226
Figure 5.2.23.3: Enter the DNS's name .....	226
Figure 5.2.23.4: Processing Securing Configuration Database .....	227
Figure 5.2.23.5: Role-Based service configuration .....	227
Figure 5.2.23.6: Select Server Roles .....	228
Figure 5.2.23.7: Select Client Features .....	228
Figure 5.2.23.8: Select Administration and Other Options .....	229
Figure 5.2.23.9: Selected Additional Services .....	229
Figure 5.2.23.10: Handling Unspecified Services .....	230
Figure 5.2.23.11: Confirm Service Changes .....	231
Figure 5.2.23.12: Network Security .....	231

Figure 5.2.23.13: Network Security Rules .....	232
Figure 5.2.23.14: Registry Settings .....	232
Figure 5.2.23.15: Security Signatures .....	233
Figure 5.2.23.16: Require LDAP Signing .....	233
Figure 5.2.23.17: Set Authentication Methods .....	234
Figure 5.2.23.19: Authentication using Domain Accounts .....	235
Figure 5.2.23.20: Registry Setting Summary .....	235
Figure 5.2.23.21: Audit Policy .....	236
Figure 5.2.23.22: System Audit Policy .....	236
Figure 5.2.23.23: Audit Policy Summary .....	237
Figure 5.2.23.24: Saved Security Policy .....	237
Figure 5.2.23.25: Security Policy File Name .....	238
Figure 5.2.23.26: Apply Security Policy .....	238
Figure 5.2.23.27: Processing Security Policy .....	239
Figure 5.2.23.28: Completing the security Configuration Wizard .....	240
Figure 5.2.23.29: Configure Windows Firewall .....	241
Figure 5.2.23.30: Firewall Status .....	241
Figure 5.2.23.31: Customize Settings .....	242
Figure 5.2.23.32: Open Local Security Policy .....	242
Figure 5.2.23.33: Configure the auditing .....	243
Figure 5.2.23.34: Audit account logon events .....	243
Figure 5.2.23.35: Configuration Done .....	244
Figure 5.2.23.36: After auditing .....	244
Figure 5.2.23.37: Display list of shares on the server .....	245
Figure 5.2.23.38: Installation of bit locker .....	245
Figure 5.2.23.39: BitLocker installation .....	246
Figure 5.2.23.40: BitLocker installation .....	246
Figure 5.2.23.41: Add Roles and features .....	247
Figure 5.2.23.42: Configure installation .....	247
Figure 5.2.23.43: Installation progress .....	248
Figure 5.2.23.44: Open windows firewall with Advanced Security .....	249
Figure 5.2.23.45: Firewall status .....	249
Figure 5.2.23.46: Firewall Setting .....	250
Figure 5.2.23.47: Run services msc .....	250

Figure 5.2.23.48: Print Spooler .....	251
Figure 5.2.23.49: Distributed Transaction Coordinator .....	251
Figure 5.2.23.50: KtmRm for Distributed Transaction .....	252
Figure 5.2.23.51: Run services msc .....	253
Figure 5.2.23.52: Windows Error Reporting Service .....	254
Figure 5.2.23.53: Run services msc .....	254
Figure 5.2.23.54: Secure Socket Tunnelling Protocol .....	255
Figure 5.2.23.55: Run services msc .....	255
Figure 5.2.23.56: NetLogon service .....	256
Figure 5.2.23.57: Show open port .....	257
Figure 5.2.23.58: Show open port in HTTP .....	258
Figure 5.2.23.59: Show open port in MSRPC .....	259
Figure 5.2.23.60: Port scanning status .....	260
Figure 5.2.24.1: Download PBIS (Ubuntu) .....	263
Figure 5.2.24.2: Configure PBIS (Ubuntu) .....	263
Figure 5.2.24.3: Execute PBIS (Ubuntu) .....	264
Figure 5.2.24.4: Restart avachi (Ubuntu) .....	264
Figure 5.2.24.5: Join Domain (Ubuntu) .....	264
Figure 5.2.24.6: Restart SSH (Ubuntu) .....	265
Figure 5.2.24.7: Login setting (Ubuntu) .....	265
Figure 5.2.24.8: Login setting 2 (Ubuntu) .....	265
Figure 5.2.24.9: Login setting 3 (Ubuntu) .....	265
Figure 5.2.24.10: Get Kerberos (Fedora) .....	266
Figure 5.2.24.11: DNS settings (Fedora) .....	266
Figure 5.2.24.12: Discover domain (Fedora) .....	266
Figure 5.2.25.1: Installation .....	267
Figure 5.2.25.2: Interface Softether VPN Server Manager .....	268
Figure 5.2.25.3: Configuration VPN Server Manager 1 .....	269
Figure 5.2.25.4: Configuration VPN Server Manager 2 .....	269
Figure 5.2.25.5: Configuration VPN Server Manager 3 .....	270
Figure 5.2.25.6: Configuration VPN Server Manager 4 .....	271
Figure 5.2.25.7: Configuration VPN Server Manager 5 .....	271
Figure 5.2.25.8: Configuration VPN Server Manager 6 .....	272
Figure 5.2.25.9: Configuration VPN Server Manager 8 .....	272

Figure 5.2.25.10: Configuration VPN Server Manager 9 .....	273
Figure 5.2.25.11: Configuration VPN Server Manager 10 .....	273
Figure 5.2.26.1: Samba Configuration .....	274
Figure 5.2.27.1: Add Active Directory to Server Manager .....	276
Figure 5.2.27.2: AD Installation .....	277
Figure 5.2.27.3: Role-based AD Installation .....	277
Figure 5.2.27.4: Select server for AD .....	278
Figure 5.2.27.5: AD Domain Services .....	278
Figure 5.2.27.6: Add AD features required for AD .....	279
Figure 5.2.27.7: Add additional services for AD .....	279
Figure 5.2.27.8: Add additional features for AD .....	280
Figure 5.2.27.9: Confirm AD installation .....	280
Figure 5.2.27.10: Installing AD to Server Manager .....	281
Figure 5.2.27.11: Confirmation for AD installation .....	281
Figure 5.2.27.12:AD Installation progress .....	281
Figure 5.2.27.13: Finishing AD installation .....	282
Figure 5.2.27.14: Finished AD installation .....	282
Figure 5.2.27.15: Server Manager Dashboard .....	283
Figure 5.2.27.16: Active Directory Users and Computers Window .....	283
Figure 5.2.27.17: User Information .....	284
Figure 5.2.27.18: User Password Information .....	284
Figure 5.2.27.19: User details confirmation .....	285
Figure 5.2.27.20: Create new group .....	285
Figure 5.2.27.21: Group Details .....	286
Figure 5.2.27.22: Group Properties .....	286
Figure 5.2.27.23: Add members to group .....	287
Figure 5.2.27.24: User search .....	287
Figure 5.2.27.25: Group user members .....	288
Figure 5.2.28.3: Change status .....	289
Figure 5.2.28.4: Assign Port to VLAN .....	290
Figure 5.2.29.1: Login in root .....	290
Figure 5.2.29.2: Update the System .....	291
Figure 5.2.29.3: Installation Lamp-server I .....	291
Figure 5.2.29.4: Installation Lamp-server II .....	292

Figure 5.2.29.5: Installation PHP Extension .....	292
Figure 5.2.29.6: Installation another part of PHP Extension .....	292
Figure 5.2.29.7: Installation of NextCloud .....	293
Figure 5.2.29.8: Unzip the package .....	293
Figure 5.2.29.10: Edit the permission of the folder .....	293
Figure 5.2.29.11: Configuring MariaDB for Nextcloud .....	294
Figure 5.2.30.1: Subsonic Downloads Page .....	295
Figure 5.2.30.2: Subsonic Download .....	295
Figure 5.2.30.3: Subsonic Installation .....	296
Figure 5.2.30.4: Subsonic Web Page .....	296
Figure 6.2.1 nslookup 192.168.9.130 .....	298
Figure 6.2.2: Stop DNS Service .....	299
Figure 6.2.3: drive.group10.com is accessible .....	299
Figure 6.2.4: https://web.group10.com is accessible .....	300
Figure 6.2.5: http://web.group10.com is accessible .....	300
Figure 6.2.6 show the DHCP is Enable in the CMD .....	301
Figure 6.2.7 show create New Wizard Scope in the DHCP Manager .....	302
Figure 6.2.8 show Name and Description for the New Scope Wizard .....	302
Figure 6.2.9 show the Configuration of IP Address Range .....	303
Figure 6.2.10 show the DHCP have been Set .....	303
Figure 6.2.11: Wireless client using Ipv6. ....	304
Figure 6.2.12: Wired Client using Ipv6. ....	304
Figure 6.2.13 Homepage of neighboring ipv6 .....	305
Figure 6.2.14 test cmd at client .....	306
Figure 6.2.15 test using FileZila .....	306
Figure 6.2.16 Wireshark monitoring .....	307
Figure 6.2.17 Ping public ip address neighbor from Router. ....	308
Figure 6.2.18 NAT mapping table. ....	308
Figure 6.2.19 NAT neighbor services .....	309
Figure 6.2.20 SSH blocked .....	309
Figure 6.2.21 Web blocked .....	310
Figure 6.2.22 show directory files for Samba and Restart Samba .....	311
Figure 6.2.23 authentication restarting samba .....	311
Figure 6.2.24 show the Locations of the Shared Folders .....	312

Figure 6.2.25 show the Locations of the HighAuth Folder .....	312
Figure 6.2.26 show Connection to Server in Ubuntu .....	313
Figure 6.2.27 show the Folder in the Ubuntu .....	313
Figure 6.2.28 show the file in the Shared Folder .....	314
Figure 6.2.29 show Folder Fail to Open .....	314
Figure 6.2.30 Password Required to Open Folder .....	315
Figure 6.2.31 show the IP Address for Windows to Open .....	315
Figure 6.2.32 show the Folder in the Windows Server .....	315
Figure 6.2.33 show Folder of HighAuthority .....	316
Figure 6.2.34 show File inside the Share Folder .....	316
Figure 6.2.35 show File inside the HighAuthority Folder .....	317
Figure 6.2.36 show the IP Address for the Windows to Open .....	318
Figure 6.2.37 show Folder in the Windows Client .....	318
Figure 6.2.38 show the File can be seen in the Share Folder .....	318
Figure 6.2.39 show that Folder HighAuthority cannot be accessed .....	319
Figure 6.2.40: Linux Mail interface .....	319
Figure 6.2.41: Login Interface. ....	320
Figure 6.2.42: User Interface .....	320
Figure 6.2.43: Create new message .....	321
Figure 6.2.44: Compose mail to other user group10@group10.com by pressing send button .....	321
Figure 6.2.45: check your sent inbox to make sure message is sent. ....	322
Figure 6.2.46: Login other user .....	322
Figure 6.2.47: check inbox .....	322
Figure 6.2.48: message/attachment was sent. ....	322
Figure 6.2.49: Internet Browser setting .....	323
Figure 6.2.50: Proxy Setting. ....	323
Figure 6.2.51: Proxy Menu setup. ....	324
Figure 6.2.52: dummy.group10.com had been blocked by proxy. ....	324
Figure 6.2.53 It shows the Website has been added successfully .....	325
Figure 6.2.54: Showing the Web is already secured .....	325
Figure 6.2.54: Security Exception. ....	326
Figure 6.2.55: Show the Website. ....	326
Figure 6.2.56: It shows the Website has been added successfully .....	327

Figure 6.2.57: Hyper-V Manager .....	328
Figure 6.2.58: Installing Ubuntu .....	328
Figure 6.2.58: Ubuntu is running .....	329
Figure 6.2.59 Active Directory Interfaces .....	331
Figure 6.2.60 Wireless Properties .....	332
Figure 6.2.61 Configure AP .....	333
Figure 6.2.62 Run and configure mmc .....	333
Figure 6.2.63 New Console .....	334
Figure 6.2.64 Add/Remove Snap-in .....	335
Figure 6.2.65 Add on console root .....	335
Figure 6.2.66 Duplicate Template .....	336
Figure 6.2.67 Properties of New Template .....	337
Figure 6.2.13.10 Properties of New Template (continue) .....	338
Figure 6.2.68 Properties of New Template (continue) .....	339
Figure 6.2.69 Security New Template .....	340
Figure 6.2.70 Security New Template (continue) .....	341
Figure 6.2.71 Certification Authority .....	342
Figure 6.2.71 Certification Authority .....	343
Figure 6.2.73 Success add into Certificate Templates .....	344
Figure 6.2.74 Request New Certificate .....	344
Figure 6.2.75 Before enroll certificate .....	345
Figure 6.2.76 Show request certificates .....	346
Figure 6.2.77 Radius Authentication .....	346
Figure 6.2.78 Configure certificate properties (continue) .....	347
Figure 6.2.79 Installation Page .....	348
Figure 6.2.80 Network Policy Server .....	349
Figure 6.2.81 Configure Network Policy Server .....	350
Figure 6.2.82 New RADIUS Client .....	351
Figure 6.2.83 Select EAP type which is PEAP .....	352
Figure 6.2.84 Configure 802.1X .....	353
Figure 6.2.85 Friendly Name which is WirelessG10 is Radius Server .....	354
Figure 6.2.86 Secure Wireless Connection .....	355
Figure 6.2.87 Export Wireless Radius Certificate .....	356
Figure 6.2.88 Export Wireless Radius Certificate (continue) .....	357

Figure 6.2.89 Export Wireless Radius Certificate (continue) .....	358
Figure 6.2.90 Certificate Export Wizard .....	359
Figure 6.2.91 Completing the Certificate Export Wizard .....	360
Figure 6.2.92 SSH testing on Router .....	361
Figure 6.2.93 SSH testing on Router .....	362
Figure 6.2.94 SSH testing on Router .....	362
Figure 6.2.95 SSH testing on Router .....	363
Figure 6.2.96 SSH testing on Switch .....	363
Figure 6.2.97 SSH testing on fedora server .....	364
Figure 6.2.98 SSH testing on ubuntu .....	364
Figure 6.2.99 check status on ubuntu server .....	365
Figure 6.2.100 log in fedora server using SSH on ubuntuserver .....	365
Figure 6.2.101 create folder in fedora server using SSH on ubuntuserver .....	366
Figure 6.2.102 folder successfully created .....	366
Figure 6.2.103 file successfully created .....	366
Figure 6.2.104 to start the service ssh .....	367
Figure 6.2.105 open ubuntu server with ssh .....	367
Figure 6.2.106 create the new folder .....	368
Figure 6.2.107 insert any word in text file .....	368
Figure 6.2.108 check the created file at PC ubuntu server .....	368
Figure 6.2.109 to check word in text file .....	369
Figure 6.2.110 show Login Page to Cacti .....	370
Figure 6.2.111 show the Main Page of Cacti .....	370
Figure 6.2.112 show the Device Connected to Cacti .....	371
Figure 6.2.113 show Cacti Logs .....	371
Figure 6.2.114 show Default Tree Graph for Linux .....	372
Figure 6.2.115 show graph of Linux .....	372
Figure 6.2.116 show graph of Windows Client .....	373
Figure 6.2.117 show graph of Windows Server .....	373
Figure 6.2.118 show graph of Switch .....	374
Figure 6.2.119 To display Mac Address .....	375
Figure 6.2.120 To display the Secure port .....	375
Figure 6.2.121 To display port security information .....	376
Figure 6.2.122 To display port security information .....	376

Figure 6.2.123 system update .....	377
Figure 6.2.124 To display port have disable .....	378
Figure 6.2.125 To display password information .....	378
Figure 6.2.126 check status bluetooth .....	378
Figure 6.2.127 To display password information .....	379
Figure 6.2.128 To display status bluetooth .....	379
Figure 6.2.129 port scanning .....	380
Figure 6.2.130 run command check status snort .....	381
Figure 6.2.131 Check veryfying of snort .....	381
Figure 6.2.131 Test the configuration file .....	382
Figure 6.2.132 Test snort .....	382
Figure 6.2.133 Run Snort in Console mode .....	383
Figure 6.2.144 Check test Detection ICMP .....	384
Figure 6.2.145 Check Detection HTTP .....	385
Figure 6.2.146 Check Detection SSH .....	385
Figure 6.2.147 Command to check the save log file .....	386
Figure 6.2.148 Password Encryptions Router .....	387
Figure 6.2.149 Password Minimal Length Router .....	387
Figure 6.2.150 Login Failure Router .....	387
Figure 6.2.151 Password implementation at line console .....	387
Figure 6.2.152 Execution timeout for 3 minutes Router .....	387
Figure 6.2.153 Port scanning status .....	388
Figure 6.2.154: Login page (Ubuntu) .....	390
Figure 6.2.155: Change to Active Directory user (Ubuntu) .....	391
Figure 6.2. 156: Join Active Directory (Fedora) .....	391
Figure 6.2. 157: Check Active Directory group (Fedora) .....	391
Figure 6.2. 158: Change to Active Directory (Fedora) .....	391
Figure 6.2.159: Window Server Active Directory Users and Computers .....	392
Figure 6.2.160: Set up a new connection .....	393
Figure 6.2. 161: Set up a new connection 2 .....	393
Figure 6.2. 162: Set up a new connection 3 .....	394
Figure 6.2. 163: Set up a new connection 4 .....	394
Figure 6.2. 164 Login to VPN .....	395
Figure 6.2.165: VPN show connected .....	396

Figure 6.2. 166: Try to ping Window Server .....	396
Figure 6.2. 167: Set up a new connection without internet. ....	397
Figure 6.2. 168: Set up a new connection without internet to another island. ....	398
Figure 6.2. 169: On Window 192.168.9.2 .....	399
Figure 6.2.170: On Window 192.168.9.2 .....	399
Figure 6.2. 171: On Window 192.168.9.2 .....	400
Figure 6.2. 172: On Window 192.168.9.66 .....	400
Figure 6.2. 173: System Properties Information .....	401
Figure 6.2. 174: Computer Name/Domain Changes .....	401
Figure 6.2. 174: Username and Password authentication for AD .....	402
Figure 6.2. 175: Restart computer .....	402
Figure 6.2. 176: List of VLAN .....	403
Figure 6.2. 177: Homepage of drive.group10.com .....	404
Figure 6.2. 178: List of there file stored inside the cloud server .....	404
Figure 6.2. 179: Subsonic Login Page .....	405
Figure 6.2. 180: Subsonic Setting Page .....	405
Figure 6.2. 181: Subsonic Homepage .....	406

## **CHAPTER 1**

### **INTRODUCTION**

#### **1.1 Introduction**

For starter, BITU 3923 known as Workshop II is a subject that must be taken by each third year Bachelor Degree students as a platform to enhance knowledge and prepare students before undergo their Final Year Project and their Industrial Training. During Workshop II, students are able to work in the group and the students required to analyze and design the network infrastructure, install and manage the network services infrastructure, and also to maintain and control the network services infrastructure.

This project also train students critically to work in a group and discuss the problems arise toward solving and produce conclusion. Skills of solving problems are critically needed in the actual environment in industry which emphasize a good team worker and actual critical thinking. The students are needed to gather all previous skills and knowledge combined it with new skills and knowledge to lead this project to success.

The students are divided into group of 9 members consisting of 6 BITC students and 3 of BITZ students. Students in the group are required to develop a project based on their majoring. The equipment provided to students are three servers (1 Windows and 2 Linux Distro), one network interface card, one router (2 FastEthernet) and one manageable switch. Other equipment are 15 meters long UTP cable, 12 RJ-45 connectors and one set of crimping tool.

Each group must propose and implement its own network services adequate to 18 services or configuration of BITC students and 12 services or configuration of BITZ students. Each group must use different operating systems such as Window server, Ubuntu server and Fedora server. Configuration and test by the students must be carried out using the CLI (Command Line Interface).

## **1.2 Objective**

The objective for the Workshop 2 is to develop a network system by using different operating systems in LAN and WAN connection and develop understanding of problem solving techniques to solve a particular problem or services. Then to fulfill the requirement of subject BITU3923. Besides that, the objectives of the network development are:

- To design network infrastructure by using the available tool.
- To be able to implement designated network services.
- To be able to install and integrate network services infrastructure to suit environment.
- To be able to maintain and control the network services infrastructure.
- To implement network services that are certainly secured

### 1.3 Project Plan

Task Name	Week
Project Proposal	Week 1-2
Installation Server	Week 2
VLAN, IPv6 Transition Mechanism, DNS, DHCP, Active Directory	Week 2-5
Progress Report 1	Week 2-5
IPv6 Web, IPv6 Web SSL and Virtual Hosting	Week 2-5
Proxy Server, Linux Email Server, VLAN Security	Week 2-5
IPv4 Web, IPv4 Web SSL and Virtual Hosting, User Authentication and authorization	Week 2-5
Authentication user by Integrating AD with Linux, STP Security	Week 2-5
Radius Server for Network Accounting, Network Management System (service)	Week 2-5
Authentication using Radius Server, Wireless user authentication using Radius server, Secured FTP	Week 2-5
Remote Login using SSH, Harden Linux Server, Harden Windows Server	Week 2-5
Harden Web Server, Security Policy, Samba, Samba Security Services	Week 2-5
Progress Report 2	Week 6-10
IPsec between Server and User, Port Security, IDS	Week 6-10
Video, Poster	Week 6-10
Port Mirror, Firewall for router (ACL), Routing and NAT	Week 6-10
Inter-group Integration	Week 6-10
Progress Report 3	Week 11-12
Final Report	Week 14
Presentation (Poster and Video)	Week 14

*Table 1.3.1: project plan*

#### **1.4 Project Plan / Schedule**

No.	Handle by	Task
1.	Muhammad Nuqman Siddiqi Bin Mohamad Akhir Hud Bin Abdul Razakek Zarina Arifah Binti Afrizon Nur Farhana Binti Darkaseh Noor Nabilah Binti Nordin Teng Wei Xian Nurul Najlaa Binti Ahmad Ariffin Nurzannah Nadatul Saadiah Binti Irwan Kabelan P. Manickavelu	Writing Report and Proposal
2.	Muhammad Nuqman Siddiqi Bin Mohamad Akhir Hud Bin Abdul Razakek Zarina Arifah Binti Afrizon Nur Farhana Binti Darkaseh Noor Nabilah Binti Nordin Teng Wei Xian Nurul Najlaa Binti Ahmad Ariffin Nurzannah Nadatul Saadiah Binti Irwan Kabelan P. Manickavelu	Hardware Preparation
3.	Muhammad Nuqman Siddiqi Bin Mohamad Akhir Hud Bin Abdul Razakek Zarina Arifah Binti Afrizon Nur Farhana Binti Darkaseh Noor Nabilah Binti Nordin Teng Wei Xian Nurul Najlaa Binti Ahmad Ariffin Nurzannah Nadatul Saadiah Binti Irwan Kabelan P. Manickavelu	Operating system Installation

4.	Muhammad Nuqman Siddiqi Bin Mohamad Akhir Hud Bin Abdul Razakek Zarina Arifah Binti Afrizon Nur Farhana Binti Darkaseh Noor Nabilah Binti Nordin Teng Wei Xian Nurul Najlaa Binti Ahmad Ariffin Nurzannah Nadatul Saadiah Binti Irwan Kabelan P. Manickavelu	Network Setup and Configuration
----	--	---------------------------------

## 1.5 Conclusion

Upon the completion of workshop II, we are able to install, configure, set up, monitor and maintain a complete network given the necessary network equipment and services. We are also exposed to different operating system environment. We should be able to design our own network and maintain a good network environment. Moreover, we will learn to build up a crucial security system to secure and protect the network from being attacked and compromised. Besides, we will be able to apply teamwork and project management skills in the future. All of these are the basic requirements that prepare us for the real working environment. In addition, we can apply our knowledge we gained in class through practical and find out our weaknesses and improve them. Finally, we can gain extra knowledge, experience and confidence to face the future challenges in final year project and industrial training.

## **CHAPTER 2**

### **PROJECT REQUIREMENT**

#### **2.1 Introduction**

In this workshop, we have been provided with the equipment which are three servers, 1 Cisco 2811 router (2 Fast Ethernet), one Cisco 2960 manageable switch, 15 meters UTP cable, 12 pieces of RJ45 and one set crimping tool.

By using the equipment above, we are required to design, set up, maintain and monitor a network environment with basic server applications and fundamental services. 18 network services and 12 security services are required to implement in the network infrastructure.

We are also required to use different operating system for servers. The operating systems used in the servers are Windows Server 2012 R2, Ubuntu Server 16.04 and Fedora 28. We will explain our selection in next section.

#### **2.2 Types of Operating System**

We choose the most popular operating system in the industry to get ourselves familiar for future career. Among these OSs, the most popular ones are Windows and UNIX. (W3Tech, 2015) Therefore, we choose Windows Server 2012 R2, Ubuntu 16.04 and Fedora 28.

#### **2.3 Operating System Background**

##### **2.3.1 Windows Server 2012 R2**

Windows Server 2012 R2 is a release of Microsoft Windows server line of operating system in 2012. It is the successor to Windows Server 2008. Like Windows Vista, Windows Server 2012 R2 is built on the Windows NT 6.0 kernel. The main features of Windows Server 2012 R2 including server core, active directory roles, Windows Power Shell (Command Line Shell) and terminal services and so on.

### **2.3.2 Ubuntu 16.04**

Ubuntu is a Debian-based Linux operating system for personal computers, tablets and smartphones, where Ubuntu Touch edition is used; and also runs network servers, usually with the Ubuntu Server edition, either on physical or virtual servers. Ubuntu 16.04 runs on all major architectures – x86, x86-64, ARM v7, ARM64, POWER8 and IBM System z mainframes via LinuxONE. (Ubuntu.com, 2016)

### **2.3.3 Fedora 28**

Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project and sponsored by Red Hat. Fedora contains software distributed under a free and open-source license and aims to be on the leading edge of such technologies.

## **2.4 Operating System Justification**

### **2.4.1 Windows Server 2012 R2**

Windows Server 2012 R2 has been selected as one of the platform used in Workshop 2. It comes with solid functions and enhancements in network management, virtualizing desktop infrastructure, storage, access and information protection, the web and application platform, and more. This operating system are able to perform IP address management that involves centralized management, monitoring, and auditing of IP address spaces and corresponding infrastructure servers on a network. In this case, it used for the management and monitoring of Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) servers. It also implementing the next generation of Active Directory Domain Services Simplified Administration, and is the most radical domain re-envisioning since Windows server 2000.

### **2.4.2 Ubuntu Server**

Ubuntu is the most popular open source operating system software among Linux distros based on Debian. Ubuntu is free to use architecture and always up to date with security fixes, beneficial for low risk and high impact bug fixes and conservative. Ubuntu provide 3 different edition which is Ubuntu Desktop for personal user, Ubuntu Server for cloud and server, and finally Ubuntu Core for IoT devices and robots. In this scenario Ubuntu Server were selected. It will be implemented with Linux Email Server, Secured FTP; with authentication and encryption, Web, SSL and Virtual Hosting and AAA (Authentication, Authorization, and Accounting) using Radius. The Ubuntu server will be secured by Linux Server hardening.

### **2.4.3 Fedora Server**

Fedora Server is a short-lifecycle, community-supported server operating system that enables seasoned system administrators, experienced with any OS, to make use of the very latest technologies available in the open source community. Fedora Server can manage your system simply with Cockpit's powerful, modern interface. Besides, it can view and monitor system performance and status, and deploy and manage container-based services. The use of Fedora Server for this project is installing the Network Management System and Proxy Server

## **2.5 Hardware Requirement**

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

## 2.6 Hardware Justification

### 2.6.1 Windows Server

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

*Table 2.6.1: Hardware Specification of Windows Server*

### 2.6.2 Ubuntu Server

Brand	Dell Optiplex 7010
CPU	Intel Core i5-3470 @3.20GHz
RAM	4GB 1600MHz DDR3 SDRAM
HDD	160GB 7200rpm HDD
Display adapter	Intel HD Graphics 4000 Dynamic Video Memory Technology 5.0

*Table 2.6.2: Hardware Specification of Ubuntu Server*

### 2.6.3 Fedora Server

Brand	HP xw6600 Workstation
CPU	Intel Xeon 5450 @2.00GHz
RAM	2GB 1600MHz DDR3 SDRAM
HDD	160GB 7200rpm HDD
Display adapter	Intel HD Graphics 4000 Dynamic Video Memory Technology 5.0

*Table 2.6.3: Hardware Specification of Fedora Server*

### 2.6.4 Router

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

The Cisco 2811 Integrated Services Router provides the following support:

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

Security:

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

Voice:

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



*Figure 2.6.4: Cisco Integrated Service Router*

## 2.6.5 Switch

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



*Figure 2.6.5: Cisco Catalyst 2960 Switch*

## 2.6.6 UTP cable

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



*Figure 2.6.6: UTP cable*

### **2.6.7 RJ45**

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



*Figure 2.6.7: RJ45 Connector*

### **2.6.8 Crimping Tool**

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

A cable tester is also provided to ensure the cable is functional.

## **2.7 Conclusion**

As the conclusion, before installing Operating System, one should ensure that the computer meet the requirements. It can be complicated to integrate three different types of Operating System with 30 different services and configuration in a network infrastructure. We have to consider the compatibility and performance of the server and decide which service belong to which server. We also have to minimize the effect to the network if one of the hardware is down. After all these consideration, we would expect a secured network infrastructure with good performance and minimum downtime.

## **CHAPTER 3**

## **DESIGN**

### **3.1 Introduction**

In this Workshop II, we must define, design, implement and manage network services. Every group need to implement their own network design which is needed to be applied in real device. Stated in the requirement, that needs us to design network that include three different servers, one CISCO router, one CISCO switch and a client host for the design. Our group already design the network that have two client that from internal and external. We have been supplied with RJ-45, UTP cable, console cable and a set of crimping tools. We also required using different operating system to set the network environment. The NOS we choose to install into HP platform is Window Server 2012 R2, Linux Fedora 28 and DELL platform for Linux Ubuntu 16.04 LTS.

### **3.2 Security Policy**

#### **3.2.1 General**

- Objective**

Workshop 2 Group 10 Security Policy created to minimize the impact of security incidents. This policy also aims to facilitate the sharing of information between two groups. This can only be achieved by ensuring that all the assets are protected.

The main objective of the Workshop 2 Group 10 Security Policy is as follows:

- To ensure the smooth operation between two groups and minimize the damage or destruction;
- Protect the interests of all parties that rely on information from the system the impact of any failure or weakness in terms of confidentiality, integrity, availability, validity of the information and communication.
- Preventing the misuse or theft of assets Group 10.

- **Policy Statement**

Security is defined as a state that is free from threats and risks acceptable. Security policy is an ongoing process. It involves periodic activities that must be performed from time to time to ensure safety because of the threats and vulnerabilities are constantly changing.

There are four (4) basic components, Workshop 2 Group 10 Security Policy:

- a. Protecting official information from unauthorized access lawful authority;
- b. Ensure that any information is accurate and complete;
- c. Ensuring the availability of information when needed by the user;
- d. Ensure access to only authorized users or revenue information from legitimate sources

- **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.

- a. All user-level and system-level passwords must follow format of a password with minimum combination 6 characters contain letter and numbers containing at least three number (for example, from 0-9).
- b. Where possible, users must not use the same password for various network Group 8 access needs.
- c. Passwords must not be inserted into email messages or other forms of electronic communication.
- d. Passwords must not be revealed over the phone to anyone.
- e. Do not hint at the format of a password (for example, "my family name").
- f. 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.

- g. Do not use the "Remember Password" feature of applications (for example, web browsers).
- h. All system-level passwords (for example, root, enable, administration accounts, and so on) must be changed on at least a quarterly basis.
- I. All user-level passwords (for example web, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every four months.
- II. Password cracking or guessing may be performed on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Guidelines.

- **Email Policy**

- a. All use of email must be consistent with policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
- b. Our email account should be used primarily related purposes; personal communication is permitted on a limited basis, but non-related uses are prohibited.
- c. All data contained within an email message or an attachment must be secured according to the Data Protection Standard.
- d. Users are prohibited from automatically forwarding email to a third party email system. Individual messages which are forwarded by the user must not contain confidential or above information.
- e. Using a reasonable amount of resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from an email account is prohibited.

### **3.3 Logical Security**

#### **3.3.1 Network**

- **Infrastructure**

Network infrastructure shall be maintained by Systems Administration team leader. These will include cabling information, physical port configuration details, expected/allowed

data flow directions, and any further pertinent information, as applicable. When any changes is made it should be updated and revise it.

- **External connectivity**

Only such services as are required for normal operation should be visible externally systems and servers which do not require access to the Internet for their normal operation must not be granted that access. If such access becomes temporarily necessary for an authorized administrative task, such access may be granted under the procedures of the SM and must be reported and logged.

- **Intrusion detection**

Logs should be examined regularly (by manual or automatic means) for unusual patterns and/or traffic; Anomalies should be investigated as they are discovered and should be reported to appropriate personnel in near real time (e.g. text message, email) and investigated as soon as possible.

Suspicious activity which may indicate an actual system intrusion or compromise should trigger the incident response protocol.

- **Operating System**

Any operating system used for critical server machines must be available under an OSI approved open source software license.

- **Disk Encryption**

Any operating system used for critical server machines must support software full disk or disk volume encryption, and this encryption option must be enabled for all relevant disks/volumes when the operating system is first installed on the machine.

- **Operating configuration**

Servers must enable only the operating system functions required to support the necessary services. Options and packages chosen at OS install shall be documented, and

newly installed systems must be inspected to ensure that only required services are active, and their functionality is limited through configuration options.

Any required application software must follow similar techniques to ensure minimal exposure footprint. Documentation for installing and configuring servers with the appropriate software packages and configurations will be maintained by the System Administrators.

- **Patching**

Software used on production servers must be kept current with respect to patches affecting software security. Patch application must be approved by the Systems Administration team leader, fully documented in the logs and documentation.

- **Application**

Requests for ad hoc queries over the application database for business or similar purposes must be approved by the Arbitrator.

- **Access control**

All access to critical data and services shall be controlled and logged.

- **Application Access**

General access for Members shall be provided via a dedicated application. General features are made available according to Assurance Points and similar methods controlled in the software system.

### **3.4 Operational Security**

- **System administration**

Primary Systems Administration tasks shall be conducted fewer than four eyes principle. These shall include backup performance verification, software patch application, account creation and deletion, and hardware maintenance.

- **Privileged accounts and passphrases**

Access to privileged accounts (root and user via SSH or console) must be strictly controlled. Passphrases and SSH private keys used for entering into the systems will be kept private.

- **Authorized users**

Only Systems Administrators designated are authorized to access accounts. Systems Administration team leader may temporarily permit Software Assessors access to the application via SSH in order to do advanced debugging, or as specifically directed by the Arbitrator.

- **Access to Systems**

All access is secured, logged and monitored

- **Changing**

The procedure for changing passphrases and SSH keys shall be documented.

- **Required staff response time**

Response times should be documented for Disaster Recovery planning.

- **Change management procedures**

All changes made to system configuration must be recorded and reported in regular summaries to the organization.

## **3.5 Server Security**

### **General Requirements**

- **Server security policy**

- a. All internal servers deployed at network Group 8 owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment.

- b. Services and applications that will not be used must be disabled where practical.
- c. Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.
- d. Trust relationships between systems are a security risk, and their use should be avoided.  
Do not use a trust relationship when some other method of communication is sufficient.
- e. Always use standard security principles of least required access to perform a function.
- f. If a methodology for secure channel connection is available privileged access must be performed over secure channels example encrypted network connections using SSH or IPSec.
- g. Servers should be physically located in an access-controlled environment.
- h. All security-related events on critical or sensitive systems must be logged as follows:
  - I. Weekly full backups of logs will be retained for at least 1 month.
  - II. Monthly full backups will be retained for a minimum of 1 years.

- **Software Installation Policy**

- a. Software must be selected from an approved software list, maintained by the Information Technology department, unless no selection on the list meets the requester's need.
- b. The Information Technology Department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

- **Information Logging Standard**

- a. All systems that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions shall record and retain audit-logging information
- b. Logs shall be created whenever any of the following activities are requested to be performed by the system:
  - i. Create, read, update, or delete confidential information, including confidential authentication information such as passwords.

- ii. User authentication and authorization for activities such as user login and logout.
- iii. Adding a new user or group, changing user privilege levels, and user password changes.
- iv. Detection of suspicious/malicious activity such as from an Intrusion Detection System (IDS).

### **3.6 Network Security**

- **Router and Switch Security Policy**

- a. Routers and switches must use RADIUS for all user authentications.
- b. The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device's support organization.
- c. All routing updates shall be done using secure routing updates.
- d. Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.
- e. Access control lists for transiting the device are to be added as business needs arise.

- **Remote Access Policy**

- a. It is the responsibility of Group 8 with remote access privileges to Group 8's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to our network
- b. General access to the Internet for recreational use through our network is strictly limited to our group member (hereafter referred to as "Authorized Users"). When accessing

- our network from a personal computer, Authorized Users are responsible for preventing access to any of our computer resources or data by non-Authorized Users.
- c. Performance of illegal activities through the network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access.
  - d. Secure remote access must be strictly controlled with encryption and strong pass-phrases.
  - e. While using an our owned computer to remotely connect to corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.
  - f. All hosts that are connected to internal networks via remote access must use the most up-to-date anti-virus software this includes personal computers. Third party connections must comply with requirements.
  - g. Personal equipment used to connect to networks must meet the requirements of our owned equipment for remote access as stated in the Hardware and Software Configuration Standards for Remote Access to Our Networks.

### **3.7 Application Security**

- **Hardening Services Policy**

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

- i. **Harden Window Server**

- a. Password must have at least 8 character including numbers, symbols and words to produce strong password and also must be renewed after 42 day.
- b. Disable unnecessary services such as Print Spooler.

- c. Enable necessary services such as DNS Client.

- ii. Harden Linux Ubuntu Server**

- a. Password must have at least 8 character including numbers, symbols and words to produce strong password.
- b. Password must be renewed after 4 month.
- c. Disable unnecessary services such as CUPS service using IPP.

- iii. Harden Fedora Server**

- a. Password must have at least 8 character including numbers, symbols and words to produce strong password.
- b. Password must be renewed after 3 month.
- c. Disable unnecessary services such as CUPS service using IPP.

- Access Security**

- a. There a log of all access to the server (entry code records, and video surveillance) for any access to the server
- b. The server access governed by firewall appliances and software.
- c. Web server hardening
  - i. Enable authentication
  - ii. Configure authorization rules
  - iii. Configure server certificates
  - iv. Configure secure socket layer
  - v. Add windows authorization on webpage

- **File system Permissions**

For Linux Servers, are permissions on key security files such as /etc/passwd or /etc/shadow set in accordance with best practice in harden.

- **DNS Service Policy**

- All DNS servers in your network perform standard DNS resolution.
- All DNS servers permit zone transfers to any server.
- All DNS servers are configured to listen on all of their IP addresses.
- User Datagram Protocol (UDP) and TCP/IP port 53 is open on the firewall for network for both source and destination addresses.
- All DNS servers limit zone transfers to servers listed in the records in their zones.
- DNS servers are configured to listen on specified IP addresses.
- Secure dynamic update is allowed for all DNS zones.

- **VLAN Service Policy**

- Vlan security is applied to create external Vlan for managing switch.
- VLAN must have at least one active member port for a service policy to be configured on.
- The TCAM must have enough free entries to configure the service policy on the VLAN.

- **Proxy Server Service Policy**

- Users can conceal their true IP address from the accessed service, and this sometimes used to abuse or interrupt that service.
- Ensuring appropriate types of authorization are used to access the service and potentially by only allowing certain clients to access the proxy based on IPs
- Port used for proxy server is 8080 and we will block Youtube and all social media.

- **Linux Email Server Service Policy**

Email server serves as an electronic post office for email. Mail exchanged across networks is passed between mail servers that run specially designed software.

- a. Emails are sent using SMTP protocol, while email can be retrieved using IMAP or POP3 protocol.
- b. The server use localhost SMTP port 25 connection and localhost imap and pop3 port 110 connection.

- **Secure Shell Service Policy**

- a. Secure Shell (SSH) is a protocol for secure remote login and other secure network services over an insecure network.
- b. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.

- **Authentication using Radius Server Service Policy**

- a. Communication between a **Network Access Server (NAS)** from server to client.
- b. RADIUS server is based on the **User Datagram Protocol (UDP)**.
- c. RADIUS protocol is considered a connectionless service.
- d. RADIUS is a client/server protocol.
- e. It is provided with the username and original password given by the user.
- f. Make the **router** or **switch** as RADIUS host.
- g. The Access-Request packet contains the username, encrypted password, NAS IP address, and port.
- h. A user login consists of a query (**Access-Request**) from the NAS to the RADIUS server and a corresponding response (**Access-Accept or Access-Reject**) from the server.
- i. RADIUS was done using UDP port number 1645 or 1812 for authentication port.
- j. Can support **PPP** or **PAP** or **CHAP** or **UNIX login**, and other authentication mechanisms.

- i. PAP: Password Authentication Protocol. The username is sent in the clear, and the password is optionally encrypted. PAP is normally used with MAB, and some devices use PAP for Web authentications. We recommend you enable this for the MAB rule only and disable PAP for any authentication rules for real authentications.
  - ii. The check box for Detect PAP as Host Lookup allows PAP authentications to access the internal endpoints database. Without this check box selected, MAB would not work.
  - iii. CHAP: Challenge Handshake Authentication Protocol. The username and password are encrypted using a challenge sent from the server. CHAP is not often used with network access; however, some vendors send MAB using CHAP instead of PAP.
  - iv. The check box for Detect CHAP as Host Lookup allows CHAP authentications to access the internal endpoints database. Without this check box selected, MAB does not work.
- 
- **User authentication & authorization Service Policy**
    - a. Communication between a **Network Access Server (NAS)** from server to client.
    - b. RADIUS server is based on the **User Datagram Protocol (UDP)**.
    - c. RADIUS protocol is considered a connectionless service.
    - d. RADIUS is a client/server protocol.
    - e. RADIUS was done using UDP port number **1645** or **1812** for **authentication port** & **1646** or **1813** for **accounting port**.
    - f. **User authentication** is provided with the **username** and original **password** given by the user.
    - g. **User authorization** is the privilege of the user entered in the router.
      - i. **Privilege** is special advantage or right possessed by an individual or group and it has level 0-15
      - ii. **Privilege level 1:** Provides the lowest EXEC mode user privileges and allows only user-level commands available at the router> prompt.

- iii. **Privilege level 15:** The highest level. It includes all enable-level commands at the router# prompt.

- **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. Enable disk quotas
- f. Logon time restriction
- g. Restrict access by IP
- h. Audit logon events
- i. Enable account lockout and account lockout threshold

- **Virtual private network (VPN) Service Policy**

- a. Unauthorized user are not allowed to access internal network
- b. VPN should be use as one time authentication
- c. Only one tunnelling connection is allowed
- d. VPN gateway should be set up by network operational group
- e. VPN user should be auto-disconnected after some time of inactivity
- f. Only info sec-approved VPN clients may be used

- **Domain Name System**

In this Workshop 2, domain name system (DNS) servers translate names suitable for use by people such as group8.com into network addresses 192.168.9.130 for IP v4 and [2007:facc:2::0] for IP v6 address suitable for use by computers.

- **Samba**

- a. Samba is a freeware program that allows end users to access and use files, printers, and other commonly shared resources on a company's intranet or on the Internet.
- b. Samba is often referred to as a network file system and can be installed on a variety of operating system platforms, including: Linux, most common UNIX platforms, Open VMS, and OS/2. In this Workshop 2, we run Samba on Fedora platform which enable to share folder among networks.

- **Samba Security**

In this session, we apply several methods for authentication of clients. There are: -

- a. User-level authentication

Verifies user and their password to allow them access to the folder that we were shared.

Create several username and password that can access to the server.

- b. Host-based Protection

Use hosts allow and hosts deny command to access server from a specific range of networks.

In this part, we allowed network from VLAN Clients and VLAN Windows Server may access to Samba server.

### **3.8 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

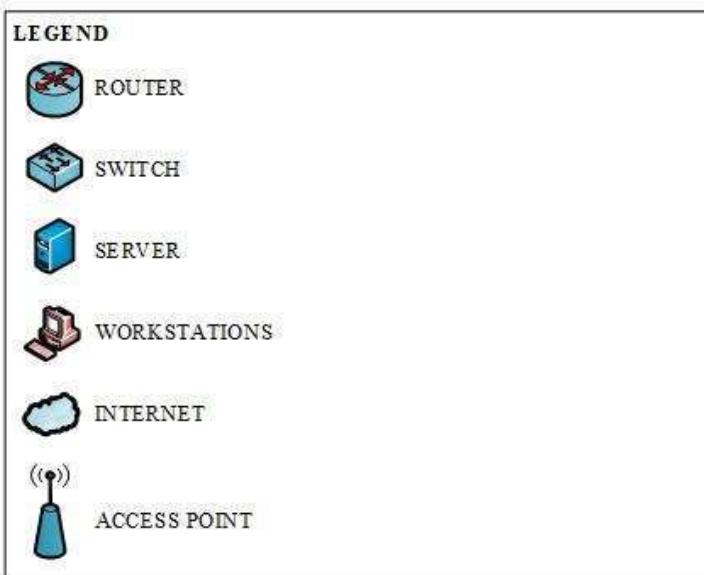
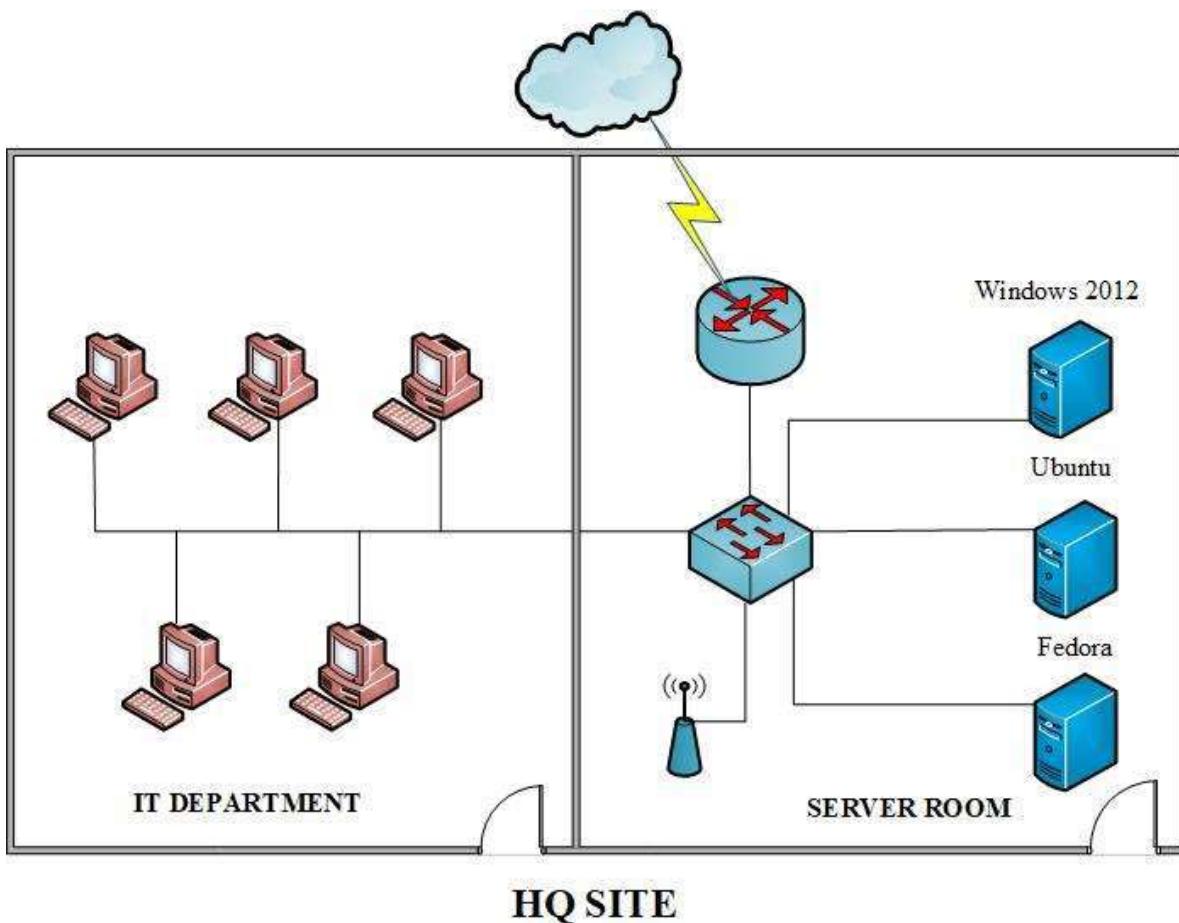
- Provisioning

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

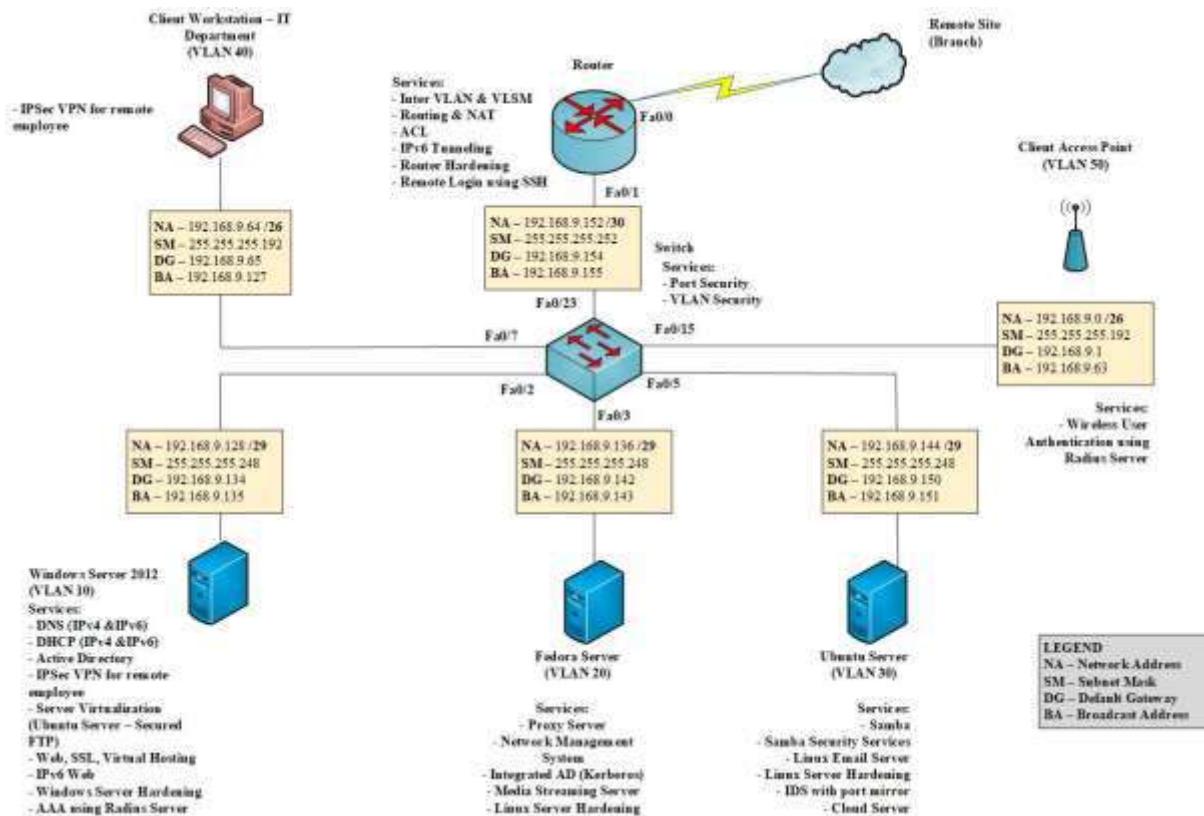
### 3. Physical access

- In accordance with the principle of dual control, at least two persons authorized for access must be on site at the same time for physical access to be granted.
- 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).

### 3.9 Physical Design



### 3.10 Logical Design



### 3.10.1 IP Addressing Table

<b>Subnet</b>	<b>Network Address</b>	<b>CIDR</b>	<b>Subnet Mask</b>	<b>IP Range</b>	<b>Broadcast Address</b>
VLAN 50	192.168.9.0	/26	255.255.255.192	192.168.9.1 - 192.168.9.62	192.168.9.63
VLAN 40	192.168.9.64	/26	255.255.255.192	192.168.9.65 - 192.168.9.126	192.168.9.127
VLAN 10	192.168.9.128	/29	255.255.255.248	192.168.9.129 - 192.168.9.134 (Hyper-V 192.168.9.131)	192.168.9.135
VLAN 20	192.168.9.136	/29	255.255.255.248	192.168.9.137 - 192.168.9.142	192.168.9.143
VLAN 30	192.168.9.144	/29	255.255.255.248	192.168.9.145 - 192.168.9.150	192.168.9.151
ROUTER & SWITCH VLAN 5	192.168.9.152	/30	255.255.255.252	192.168.9.153 (Router) - 192.168.9.154 (Switch)	192.168.9.155

<b>Name</b>	<b>Network Address</b>	<b>Default Gateway</b>	<b>IP Address</b>	<b>CIDR</b>
Windows Server	2007:facc:2::0	2007:facc:2::1	2007:facc:2::2	/64
Fedora Server	2007:facc:3::0	2007:facc:3::1	2007:facc:3::2	/64
Ubuntu Server	2007:facc:4::0	2007:facc:4::1	2007:facc:4::2	/64
Client_Wired	2007:facc:5::0	2007:facc:5::1	2007:facc:5::2	/64
Client_AP	2007:facc:6::0	2007:facc:6::1	2007:facc:6::2	/64
Router			2007:facc:100::1	/64

### **3.11 Conclusion**

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

## **Chapter 4.**

### **Services**

#### **4.1 Overview of Services**

##### **4.1.1 Domain Name System (DNS)**

DNS is a service that translates domain names to its respective IP address and vice versa. This is necessary because, although domain names are easy for people to remember, computers or machines, access websites or network resources based on IP addresses. The server in the network will be the authoritative DNS server for the domain used in the project to provide name resolution.

##### **4.1.2 Dynamic Host Configuration Protocol (DHCP)**

DHCP (Dynamic Host Configuration Protocol) is a service that provides **reliable IP address configuration and reduced network administration for clients to access the 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. Besides, any modification to the IP address of the router and DNS servers can be implemented easily.

##### **4.1.3 IPv6 Web with IPv6 Tunneling**

Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic. It is intended to replace the widely used Internet Protocol version 4 (IPv4). IPv6 Web service is required in this project to allow host running latest Layer 3 protocol; IPv6 to access the web server's content. The technical basis for tunneling, or encapsulating IPv6 packets in IPv4 packets, is outlined in RFC 4213. When the Internet backbone was IPv4 only one of the frequently used tunneling protocols was 6to4.[52] Teredo tunneling was also frequently used for integrating IPv6 LANs with the IPv4 Internet backbone. Teredo is outlined in RFC 4380 and allows IPv6 local area networks to tunnel over IPv4 networks, by encapsulating IPv6 packets within UDP. The Teredo

relay is an IPv6 router that mediates between a Teredo server and the native IPv6 network.

#### **4.1.4 Inter VLAN and VLSM Addressing**

InterVLAN routing can be defined as a way to forward traffic between different VLAN by implementing a router in the network. VLANs logically segment the switch into different subnets, when a router is connected to the switch, an administrator can configure the router to forward the traffic between the various VLANs configured on the switch. The user nodes in the VLANs forwards traffic to the router which then forwards the traffic to the destination network regardless of the VLAN configured on the switch.

#### **4.1.5 Secured FTP**

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

#### **4.1.6 Authentication using radius server**

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

#### **4.1.7 Routing**

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.

#### **4.1.8 Network Address Translation (NAT)**

Network Address Translation is the act of translating an address from one to another within the packet. A router that acts as intermediary between networks performs the NAT function. One network is designated the inside network and the other is the outside. The local inside network addresses maps to one or more global outside IP addresses and unmaps the global IP addresses on incoming packets back into local IP addresses. This helps ensure security since each outgoing or incoming request must go through a translation process that also offers the opportunity to qualify or authenticate the request or match it to a previous request. Moreover, NAT allows network clients with private IP to communicate with public network such as the internet.

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

The Access Control List (ACL) is used for filtering traffic based on a given filtering criteria on a router or switch interface. Based on the conditions supplied by the ACL, a packet is allowed or blocked from further movement. The filtering can be made through IP address and also TCP port. The usage of ACL allows only certain network traffic to get in or out of the network.

### **4.10 Samba**

Samba is an Open Source suite that provides file and print services to all manner of SMB/CIFS (Server Message Block/ Common Internet File System) clients. Samba is freely available under the GNU General Public License and provides interoperability between Linux/Unix servers and Windows-based clients. Samba allows Windows to share files and printer on UNIX host and also vice versa. This

software is essential in this project because it offers seamless resource sharing across the network comprising of host with different platform.

#### **4.1.11 Linux Email Server**

Message transfer agent software that transfers electronic mail messages from one computer to another using a client–server application architecture. An MTA implements both the client (sending) and server (receiving) portions of the Simple Mail Transfer Protocol.

The major functions of an MTA are:

- Accepting messages originating from the user agent and forwarding them to their destination (other user agents).
- Receiving all messages that are transmitted from other user agents for further transmission.
- Keeping track of each and every activity and analyzing and storing the recipient list to perform future routing functions.
- Sending auto-responses about non-delivery when a message does not reach its intended destination.

#### **4.1.12 Proxy Server**

A proxy server is a computer that acts as a gateway between a local network and a larger-scale network such as the Internet. 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.

#### **4.1.13 Web, SSL and Virtual Hosting**

SSL stands for Secure Sockets Layer. It is a standard security technology for forming an encrypted connection between a server and a client. It is commonly used in a web server and browser is security protocol that allows confidential information to be transmitted securely. The secure connection is made by using

certificates and SSL Certificate has a pair of public and private key that work together to establish an encrypted connection.

#### **4.1.14 Server Virtualization**

Server virtualization is the masking of server resources, including the number and identity of individual physical servers, processors, and operating systems, from server users. The server administrator uses a software application to divide one physical server into multiple isolated virtual environments. The virtual environments are sometimes called virtual private servers, but they are also known as guests, instances, containers or emulations. There are three popular approaches to server virtualization: the virtual machine model, the paravirtual machine model, and virtualization at the operating system (OS) layer.

#### **4.1.15 Remote Login Using SSH**

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

#### **4.1.16 Network Management System**

A network management system (NMS) is an application or set of applications that lets network engineers manage a network's independent components inside a bigger network management framework and performs several key functions. An NMS identifies, configures, monitors, updates and troubleshoots network devices -- both wired and wireless -- in an enterprise network. A system management control application then displays the performance data collected from each network component, allowing network engineers to make changes as needed.

#### **4.1.17 Port Security**

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

#### **4.1.18 Linux Server Hardening**

One of the myths about Linux is that it is secure, as it is not susceptible to viruses or other forms of malware. This is partially true, as Linux uses the foundations of the original UNIX operating system. Processes are separated and a normal user is restricted in what he or she can do on the system. Still, Linux is not perfectly secure by default. One of the reasons is the Linux distributions that package the GNU/Linux kernel and the related software. They have to choose between usability, performance, and security. Linux server hardening are used to improve the security level of a system, we take different types of measures. This could be the removal of an existing system service or uninstall some software components. System hardening is the process of doing the right things. The goal is to enhance the security level of the system. There are many aspects to securing a system properly. Yet, the basics are similar for most operating systems. So the system hardening process for Linux desktop and servers is that that special.

#### **4.1.19 Instruction Detection System (IDS)**

An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any malicious activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources, and uses alarm filtering techniques to distinguish malicious activity from false alarms.

#### **4.1.20 Security Policy**

Security policy should keep the malicious users out and also exert control over potential risky users within your organization. The first step in creating a policy is to understand what information and services are available (and to which users), what the potential is for damage and whether any protection is already in place to prevent misuse. In addition, the security policy should dictate a hierarchy of access permissions; that is, grant users access only to what is necessary for the completion of their work.

#### **4.1.21 Router Hardening**

For most enterprise LANs, the router has become one of the most critical security appliances in use. Configured properly, it can keep all but the most determined bad guys out, and if you want, it can even keep the good guys in. But an improperly configured router is only marginally better than having no security in place at all.

#### **4.1.22 Window Server Hardening**

Windows Server hardening involves identifying and remediating security vulnerabilities. Few steps to hardening window server are:

- Organizational Security
- Windows Server Preparation
- Windows Server Installation
- User Account Security Hardening
- Network Security Configuration

#### **4.1.23 Authentication**

Authentication is the process of determining whether someone or something is who or what it declares itself to be. When a potential subscriber accesses an authentication server, a username and password may be the only identifying data required. In a more sophisticated system called Kerberos, the subscriber must request and receive an encrypted security token that can be used to access a particular service. RADIUS (Remote Authentication Dial-In User Service) is a commonly used authentication method. TACACS+ (Terminal Access Controller Access Control System Plus) is similar to RADIUS but is used with Unix networks. RADIUS employs UDP (User Datagram Protocol) and TACACS+ employs TCP (Transmission Control Protocol).

#### **4.1.24 IPsec**

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. 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. It allows you to add IP restrictions, and TCP/UDP level encryption to applications which may not otherwise support it. Provide message confidentiality by encrypting all of the data sent between two computers. Also, provide message integrity between two computers (without encrypting data).

#### **4.1.25 Samba Security Services**

There are only two types of security modes for Samba, share-level and user-level, which are collectively known as security levels. Share-level security can only be implemented in one way, while user-level security can be implemented in one of four different ways. The different ways of implementing a security level are called security modes.

#### **4.1.26 Active Directory**

Active Directory Domain Services is Microsoft's Directory Server. It provides authentication and authorization mechanisms as well as a framework within which other related services can be deployed (AD Certificate Services, AD Federated Services, etc). It is an LDAP compliant database that contains objects. The most commonly used objects are users, computers, and groups. These objects can be organized into organizational units (OUs) by any number of logical or business needs. Group Policy Objects (GPOs) can then be linked to OUs to centralize the settings for various users or computers across an organization.

#### **4.1.27 VLAN Security**

VLANs segment a network, creating multiple broadcast domains, they effectively allow traffic from the broadcast domains to remain isolated while increasing the network's bandwidth, availability and security. Most managed switches are VLAN-capable, but this doesn't mean that they all perform the job equally well. The market has been flooded by thousands of switches that seem to do the job, but special consideration must be taken before making a purchase. A switch in a VLAN-enabled network needs to do a lot more than just switch packets between its ports.

#### **4.1.28 Cloud Server**

A cloud server is primarily an Infrastructure as a Service (IaaS) based cloud service model. There are two types of cloud server: logical and physical. A cloud server is logical when it is delivered through server virtualization. In this delivery model, the physical server is logically distributed into two or more logical servers, each of which has a separate OS, user interface and apps, although they share physical components from the underlying physical server. Whereas the physical cloud server is also accessed through the Internet remotely, it isn't shared or distributed. This is commonly known as a dedicated cloud server.

#### **4.1.29 Media Streaming Center**

Subsonic is a web-based media streaming tool which lets you play, share, search and access radio stations and offers whole lot of other features. It allows to stream music on-the-go, which works great when you want to play different genres in different locations. Once configured and set up, your media collection can be accessed from web or from any mobile phone. Yes, they have separate apps for both iPhone and Android. It is developed to handle gigantic music collection, even though it is optimized for MP3 streaming yet supports almost every audio and video format. On first time usage, its system tray icon will prompt you to configure settings to get started. Just open Subsonic web application and you'll get a complete control panel with awesome collection of features to begin with. Select music folders, themes, default language, etc. Furthermore, it lets you authorize users with appropriate rights to create and share music library. With transcoder plugins you can easily convert and stream any audio formats on real-time. You can also select bitrates of music streams and let it work as podcast receiver.

#### **4.1.30 Wireless user authentication using Radius server (AD user account/Mac Address)**

WPA2-Enterprise with 802.1x authentication can be used to authenticate users or computers in a domain. The supplicant (wireless client) authenticates against the RADIUS server (authentication server) using an EAP method configured on the RADIUS server. The gateway APs (authenticator) role is to send authentication messages between the supplicant and authentication server. This means the RADIUS server is responsible for authenticating users. APs perform EAPOL exchanges between the supplicant and convert these to RADIUS Access-requests messages, which are sent to the RADIUS server's IP address and UDP port specified in Dashboard. Gateway APs need to receive a RADIUS Access-accept message from the RADIUS server in order to grant the supplicant access to the network. For best performance, it is recommended to have the RADIUS server and gateway APs located within the same layer-2 broadcast domain to avoid firewall, routing, or authentication delays. Keep in mind the AP is not responsible for authenticating wireless clients and acts as an intermediary between clients and the RADIUS server.

## **4.2 INDIVIDUAL TASK**

### **4.2.1 SERVICES TASK (FOR BITC)**

No.	Handle by	Services
1.	MUHAMMAD NUQMAN SIDDIQI BIN MOHAMAD AKHIR	1. Server Virtualization ( <b>Main</b> ) 2. Proxy Server 3. Web, SSL & Virtual Hosting
2.	HUD BIN ABDUL RAZAKEK	1. Active Directory ( <b>Main</b> ) 2. Routing & Network Address Translating NAT 3. Access Control List (ACL)
3.	ZARINA ARIFAH BINTI AFRIZON	1. DNS ( <b>Main</b> ) 2. Cloud Server 3. IPv6 Web with IPv6 Tunneling
4.	NUR FARHANA BINTI DARKASEH	1. AAA (Authentication, Authorization, and Accounting) using Radius ( <b>Main</b> ) 2. Inter VLAN 3. Secured FTP

5.	NOOR NABILAH BINTI NORDIN	<ul style="list-style-type: none"> <li>1. NMS Network Management System <b>(Main)</b></li> <li>2. DHCP (IPv4)</li> <li>3. Samba</li> </ul>
6.	KABELAN P. MANICKAVELU	<ul style="list-style-type: none"> <li>1. Linux Email Server <b>(Main)</b></li> <li>2. Media Streaming Server</li> <li>3. DHCP (IPv6)</li> </ul>

## 9.2 SERVICES TASK (FOR BITZ)

No.	Handle by	Services
1.	TENG WEI XIAN	<ul style="list-style-type: none"> <li>1. IPSec VPN for remote employees <b>(Main)</b></li> <li>2. VLAN Security</li> <li>3. Samba Security Services</li> <li>4. Authentication user by integrating AD with Linux</li> </ul>

2.	NURUL NAJLAA BINTI AHMAD ARIFFIN	<ol style="list-style-type: none"> <li>1. Wireless user authentication using Radius server (AD user account/Mac Address) (<b>Main</b>)</li> <li>2. Security Policy</li> <li>3. Router Hardening</li> <li>4. Windows Server hardening</li> </ol>
3.	NURZANNAH NADATUL SAADIAH BINTI IRWAN	<ol style="list-style-type: none"> <li>1. IDS with port mirror (<b>Main</b>)</li> <li>2. Remote login using SSH</li> <li>3. Port Security</li> <li>4. Linux Server hardening</li> </ol>

## **Chapter 5**

### **Installation and Configuration**

## 5.1 Introduction

In this chapter present the installation and the configuration of the services which we had installed and configured in our Workshop 2. All services had been installed and configured to integrate network services infrastructure to suit the network environment and security policies that have been set. We used different operating system such as Window Server 2012 R2, Ubuntu 16.04, Fedora 28 and Window 10.

## 5.2 Installation of Services

### 5.2.1 DNS (primary and secondary servers) IPv4 & IPv6

The figures show the installation of DNS (Domain Name System) for IPv4 and IPv6 step-by-step.

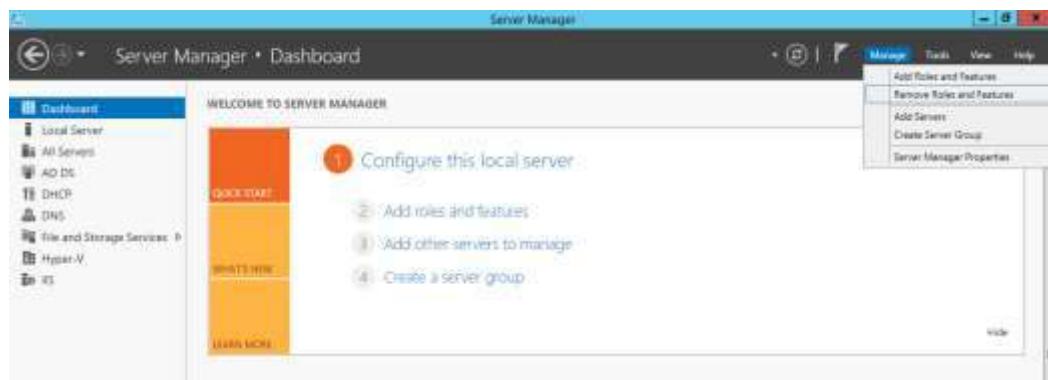
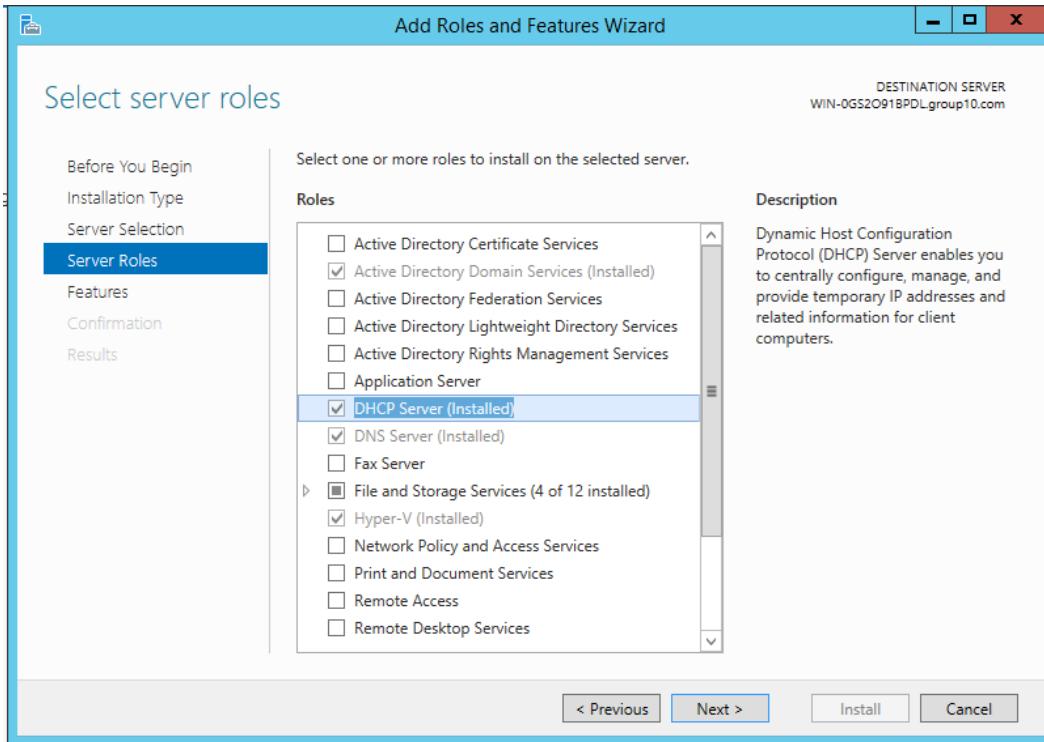


Figure 5.2.1.1: Open Server Manager and Administrative Tool



*Figure 5.2.1.2: Check the DNS Server for installation*

After finish the installation DNS, first creates the IPv4 Forward Lookup Zone. Normal DNS queries are forward lookup queries; they request the IP address that corresponds to a fully qualified domain name. While A reverse lookup is the opposite of a forward lookup. It returns the fully qualified domain of a host based on its IP address. The step had show as below

### 5.2.1.2 Create IPv4 Forward Lookup Zone

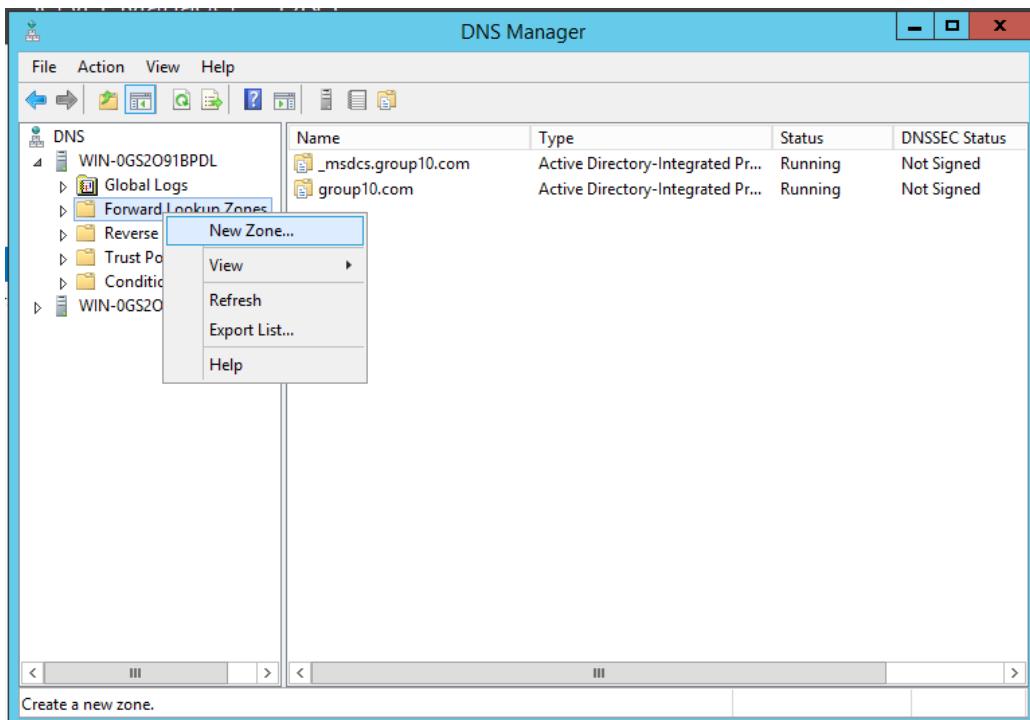
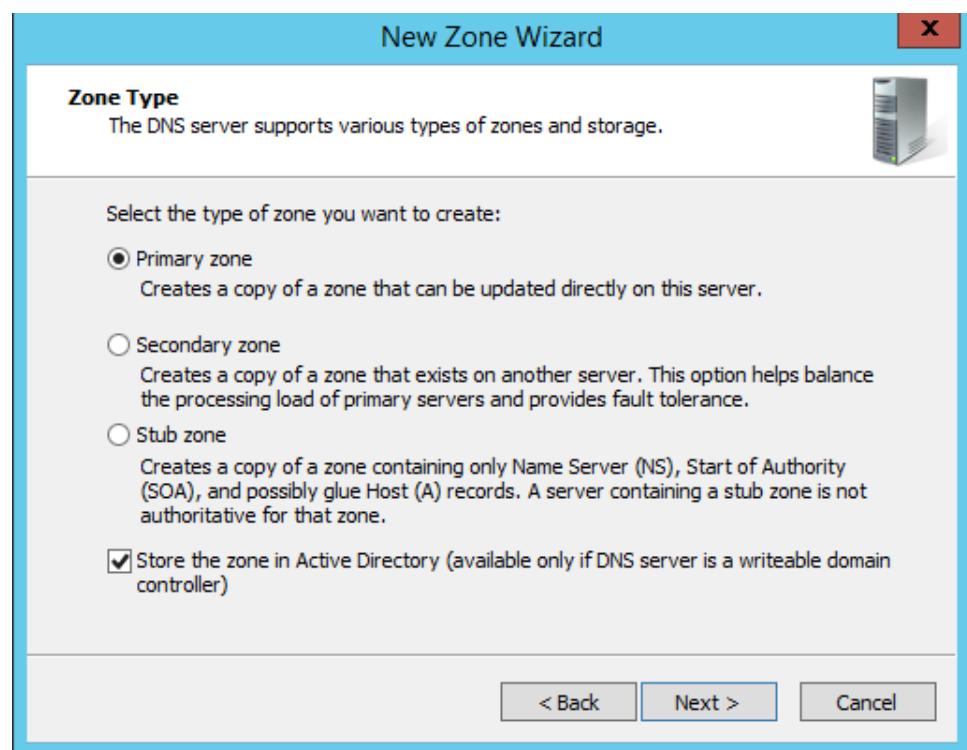


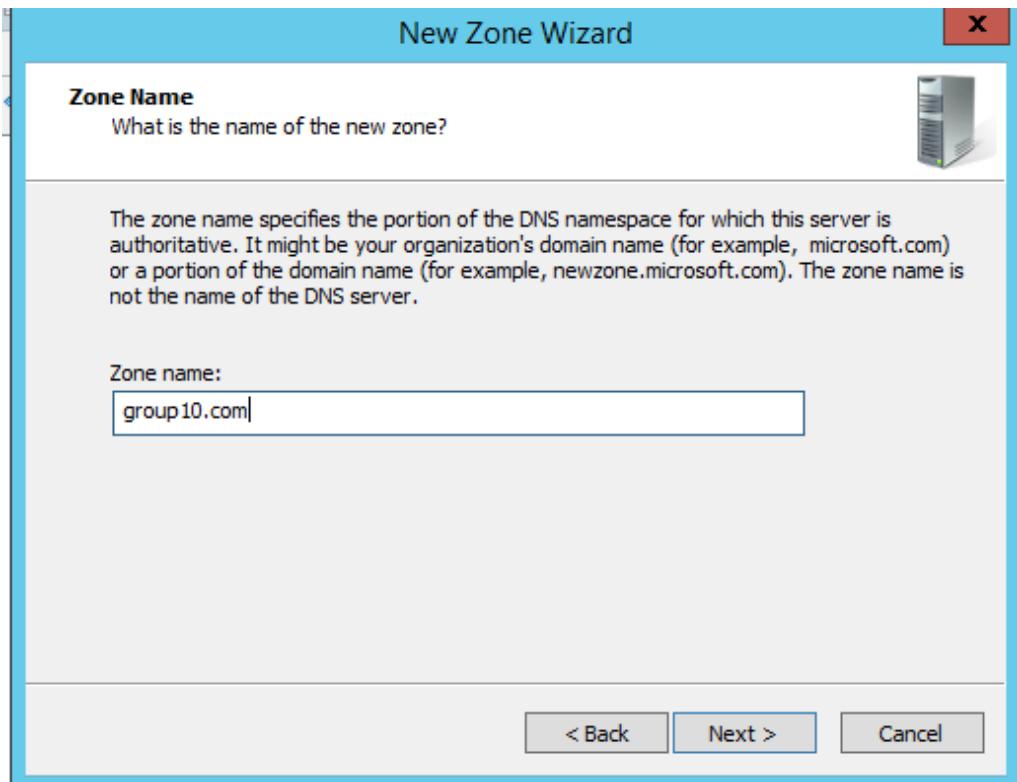
Figure 5.2.1.2.1: Right click on Forward Lookup Zone and select New



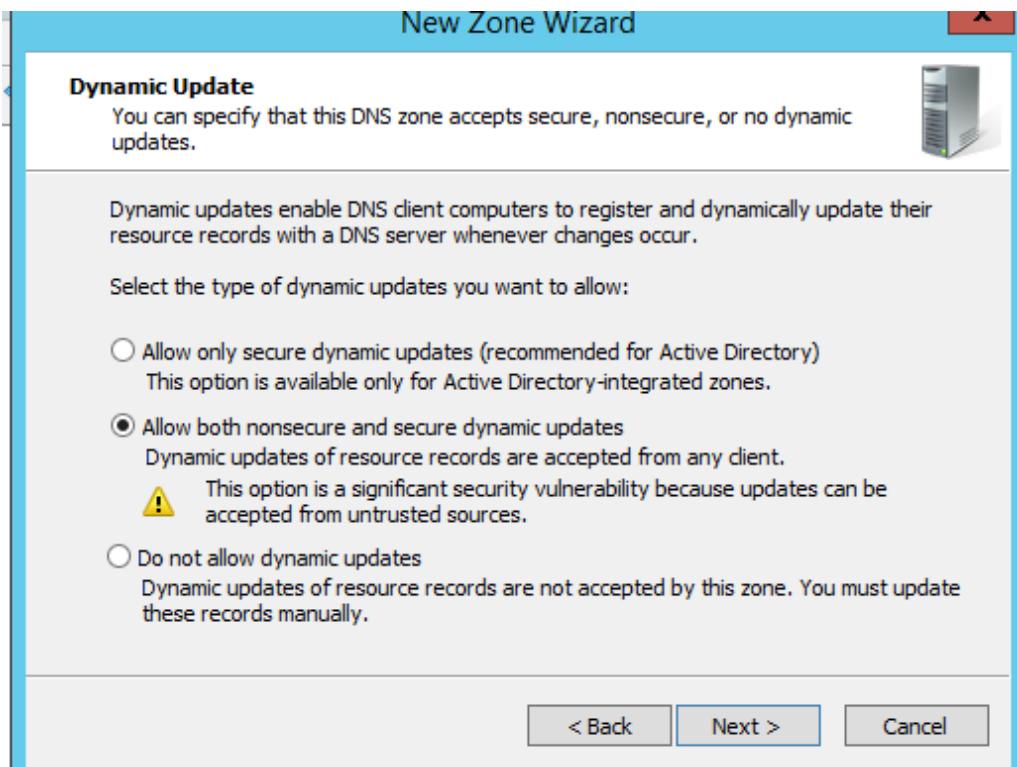
*5.2.1.2.2: Click Next*



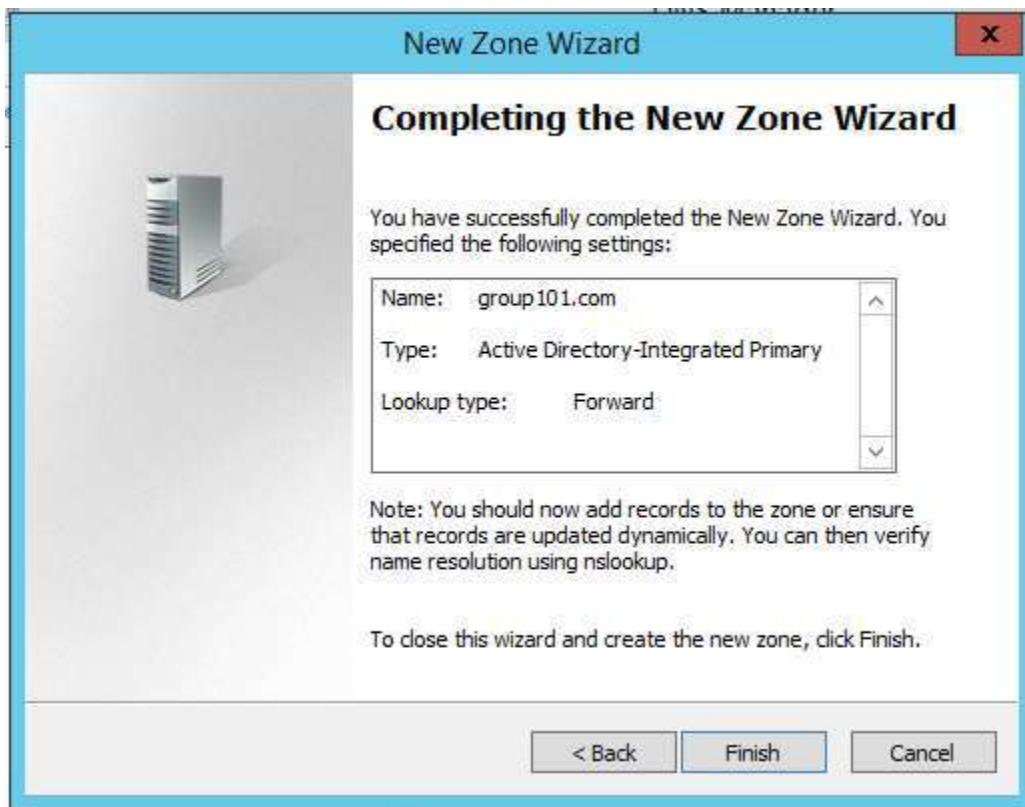
*5.2.1.2.3: Choose Primary zone and Click Next*



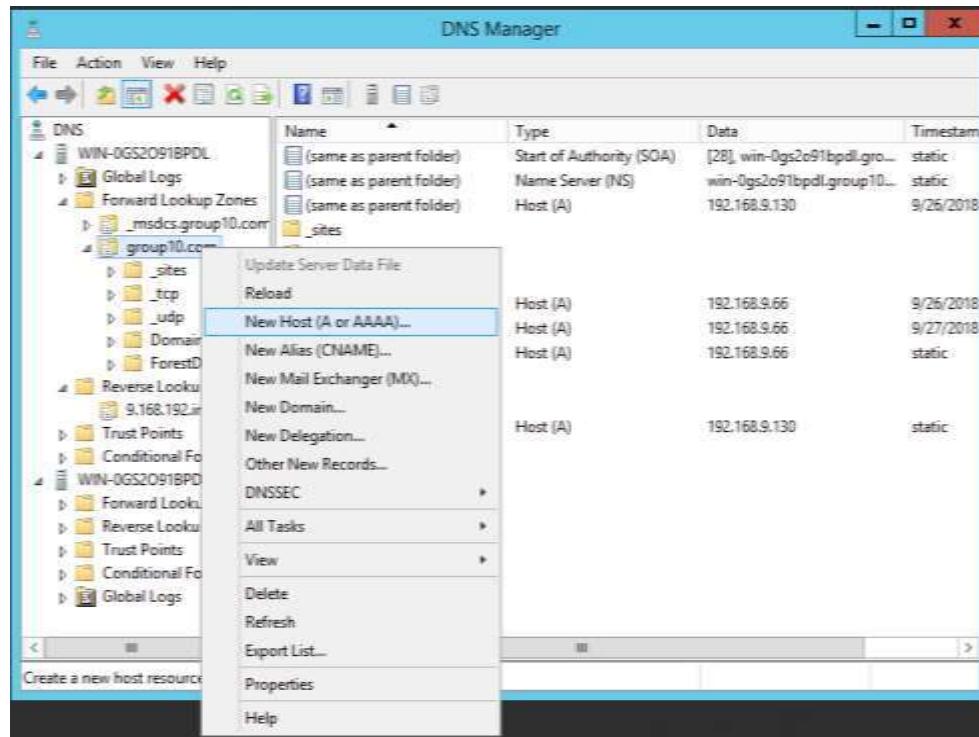
*5.2.1.2.3: Insert the zone name with group10.com then Click Next*



*5.2.1.2.4: Choose "Allow both non secure and secure dynamic"*



#### *5.2.1.2.15: Click Finish to create IPv4 Forward Lookup Zone*



#### *5.2.1.2.15: Right click on the Forward Lookup Zone and choose*

New Host X

Name (uses parent domain name if blank):  
windows

Fully qualified domain name (FQDN):  
windows.group10.com.

IP address:  
192.168.9.130

Create associated pointer (PTR) record

Allow any authenticated user to update DNS records with the same owner name

Add Host Cancel

*5.2.1.2.5: Insert the name and IP address for Windows*

After IPv4 Reverse Lookup Zone creates successfully, then create the IPv4 Forward Lookup Zone.

### 5.2.1.3 *Create IPv4 Reverse Lookup Zone*

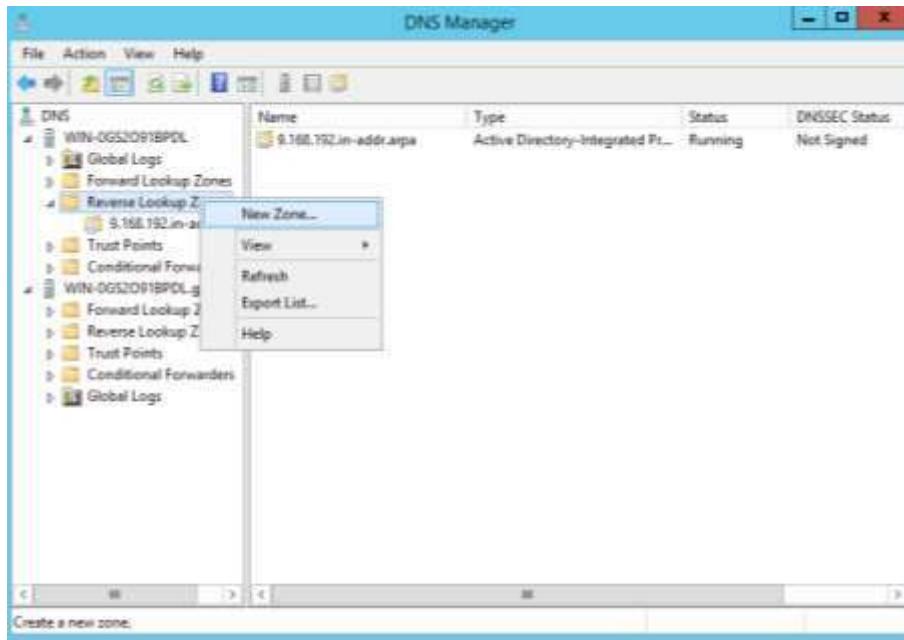
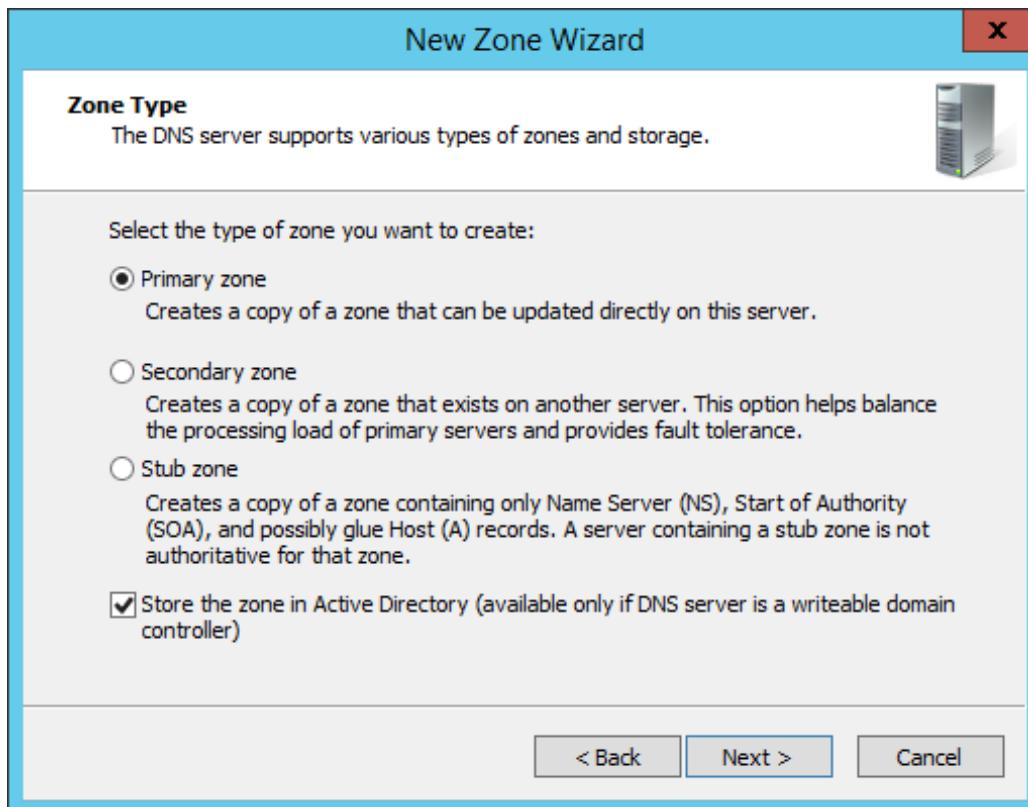


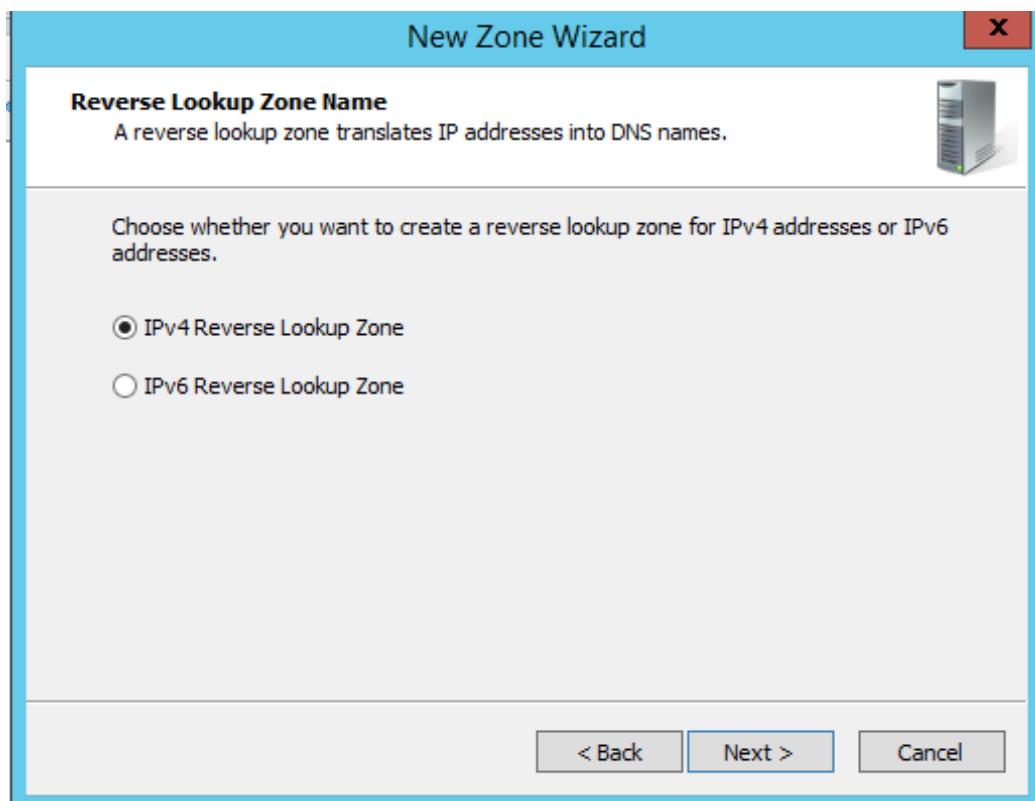
Figure 5.2.1.3.1: Right click on Reverse Lookup Zone and select New Zone



*Figure 5.2.1.3.2: Proceed with Next*



*Figure 5.2.1.3.2: Choose Primary zone and Next*



*Figure 5.2.1.3.3: Choose IPv4 Reverse Lookup Zone then Next*

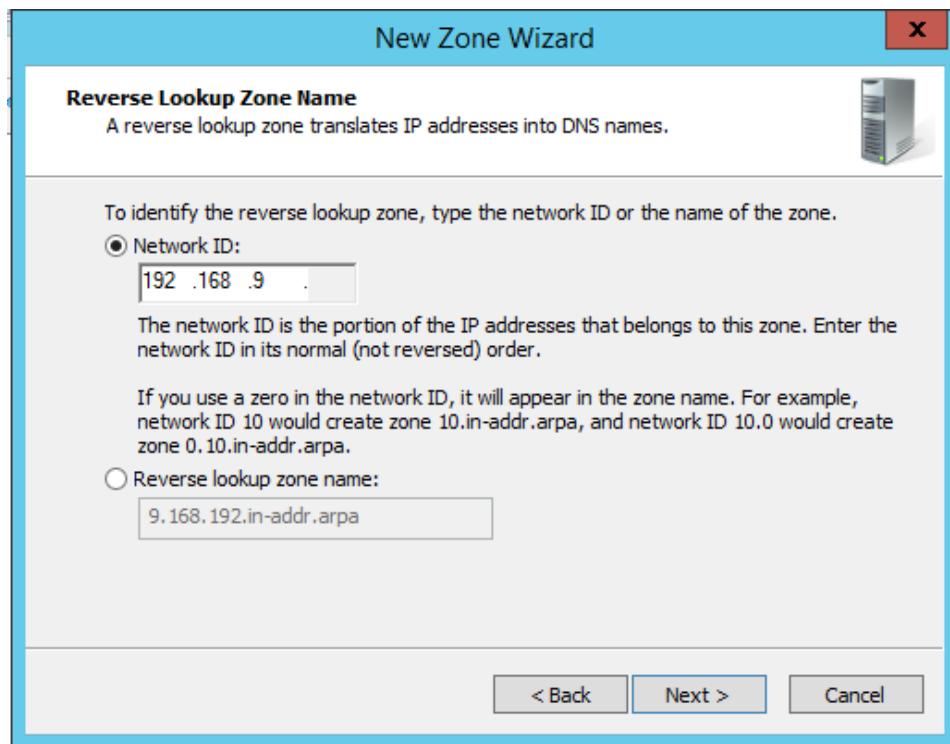


Figure 5.2.1.3.4: Insert the Network ID which is 192.168.9.130

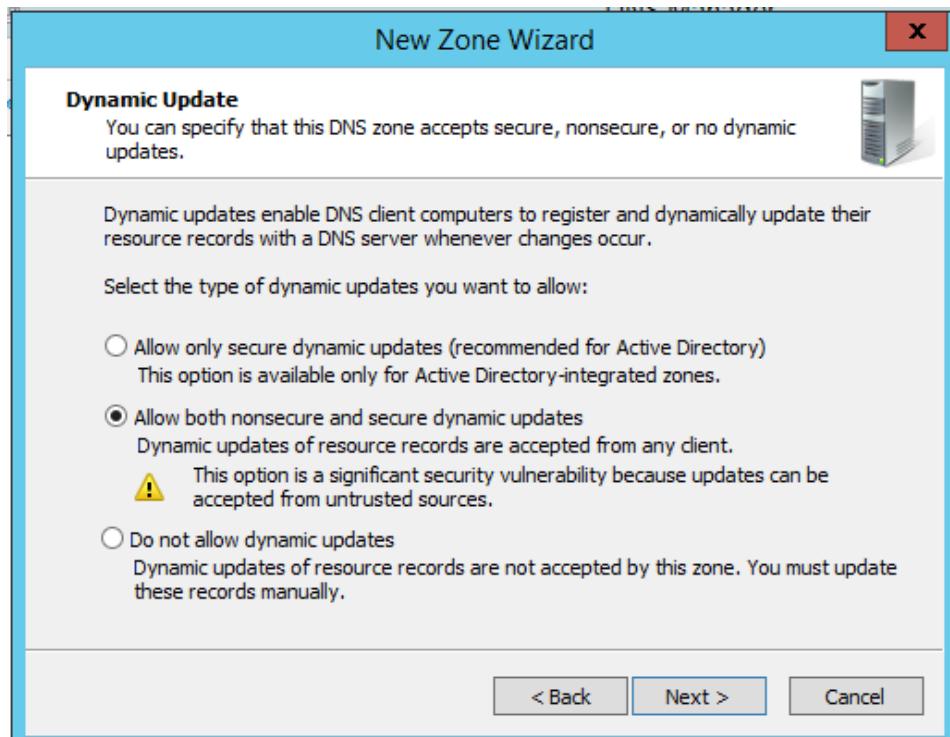


Figure 5.2.1.3.5: Choose “Allow both non secure and secure dynamic updates”



*Figure 5.2.1.3.6: Click Finish to Create IPv4 Reverse Lookup Zone*

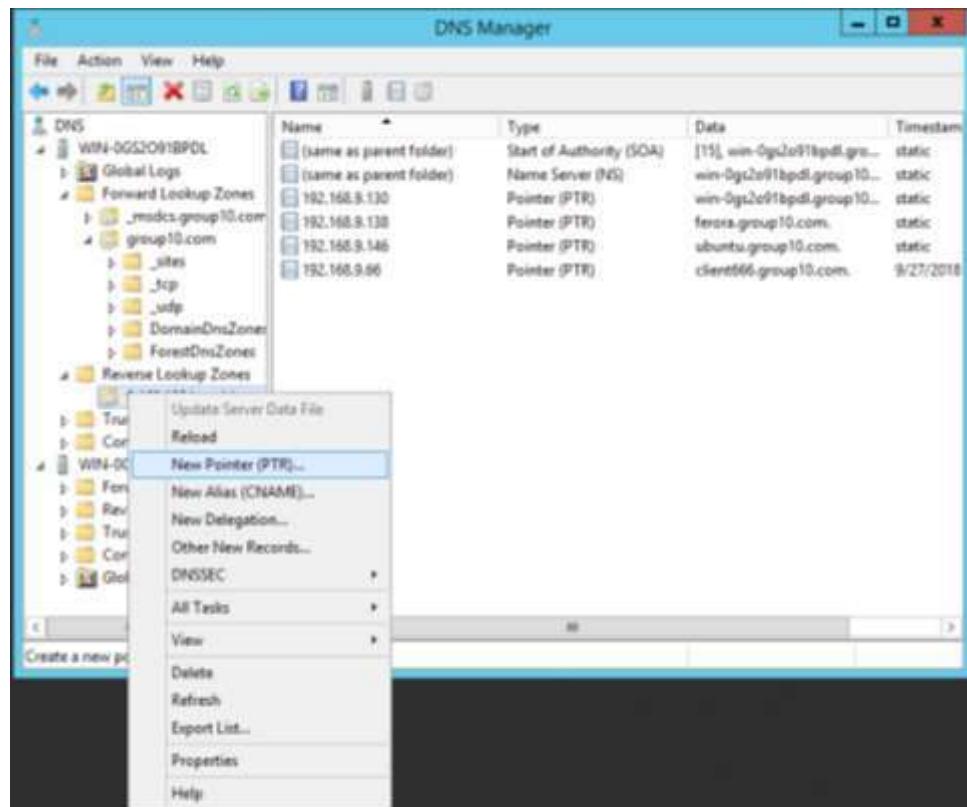


Figure 5.2.1.3.7: Right click the IPv4 Reverse Lookup Zone and add New

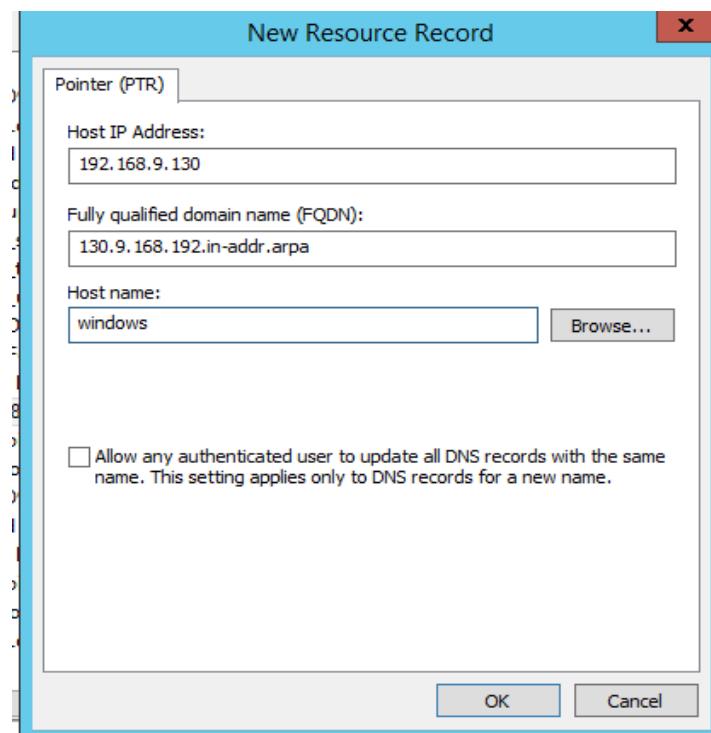


Figure 5.2.1.3.8: Add the host IP Address and the host name for windows

The forward look up zone had been configured successfully. Now create the Forward Lookup Zone and Reverse Lookup Zone for IPv6 address.

#### 5.2.1.4 Create IPv6 Reverse Lookup Zone

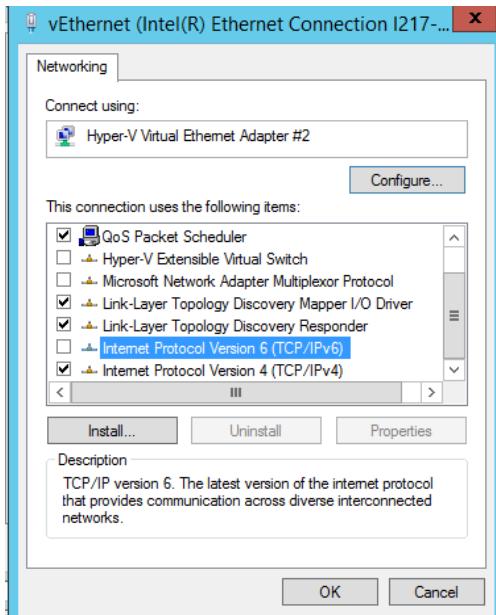


Figure 5.2.1.4.1: Install IP Address version 6 in the Windows Server

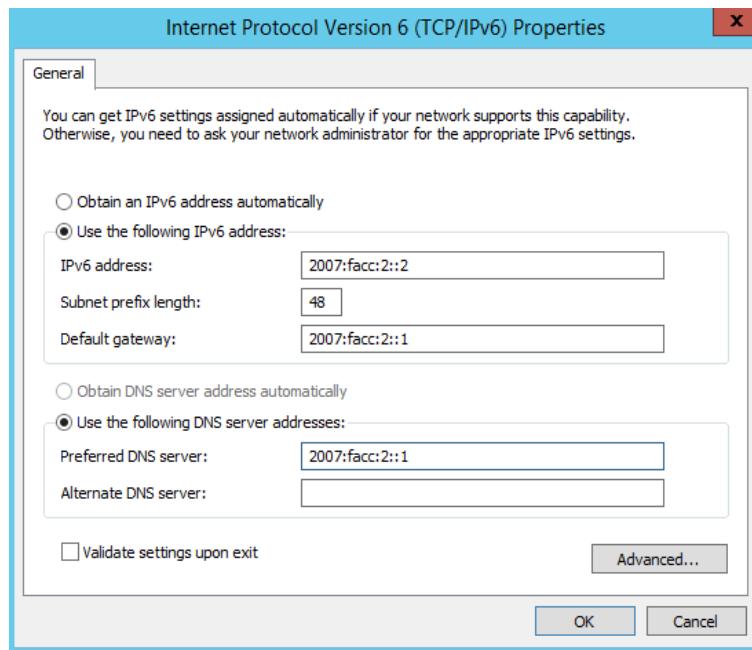


Figure 5.2.1.4.1: Assigned the static IP Address, Subnet-prefix Length and Default Gateway

### 5.2.1.5 Create IPv6 Forward Lookup Zone

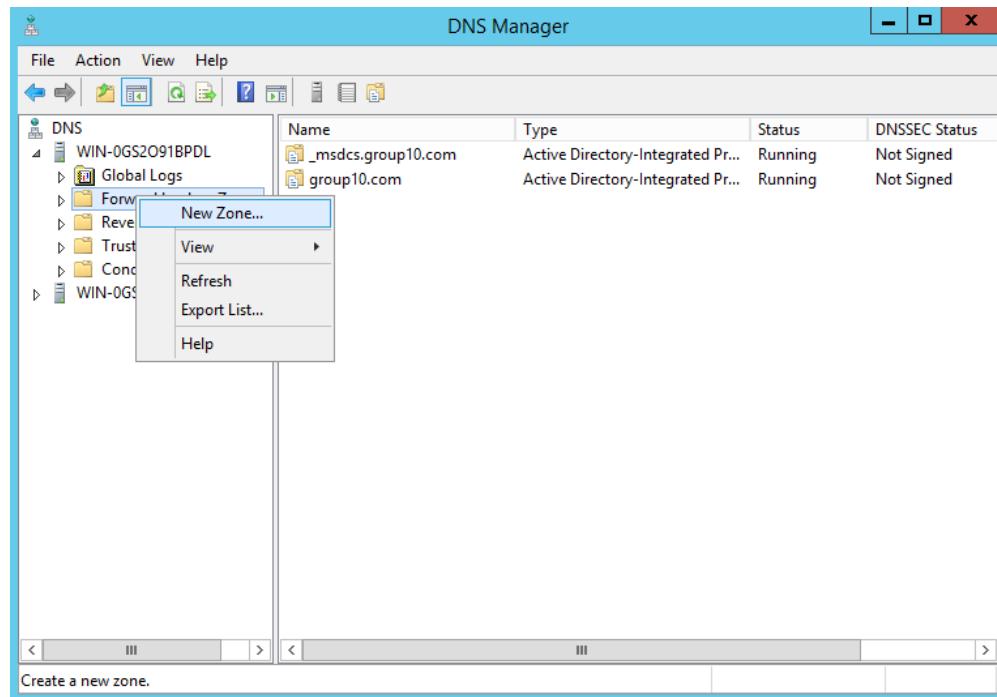


Figure 5.2.1.5.1: Right click on the Forward Lookup Zones and choose



Figure 5.2.1.5.2: Click Next

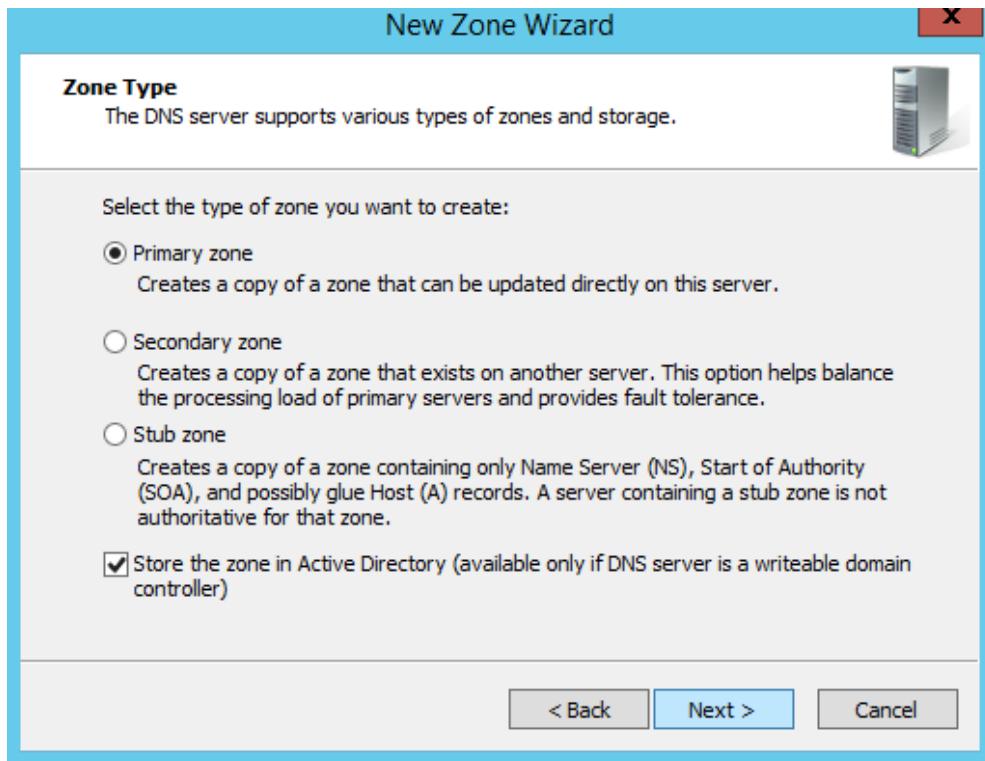


Figure 5.2.1.5.3: Choose Primary zone and Click Next

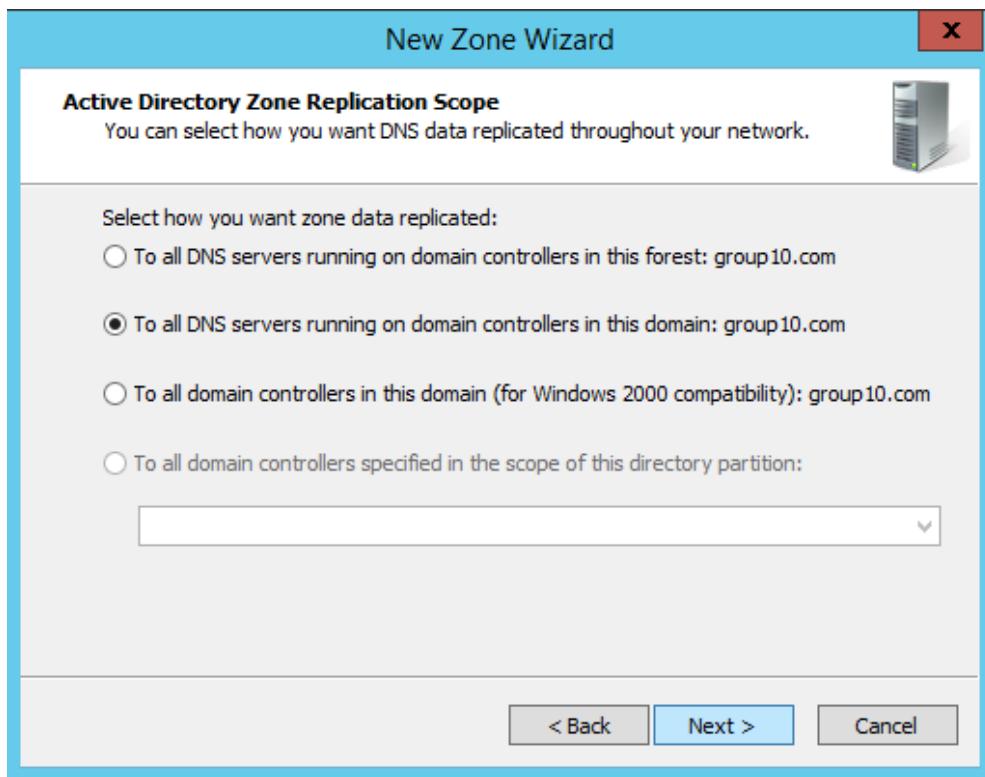


Figure 5.2.1.5.4: Checked the 'To all DNS Servers running on domain controllers in this domain: group10.com'



Figure 5.2.1.5.5: Create a new zone name and Click Next

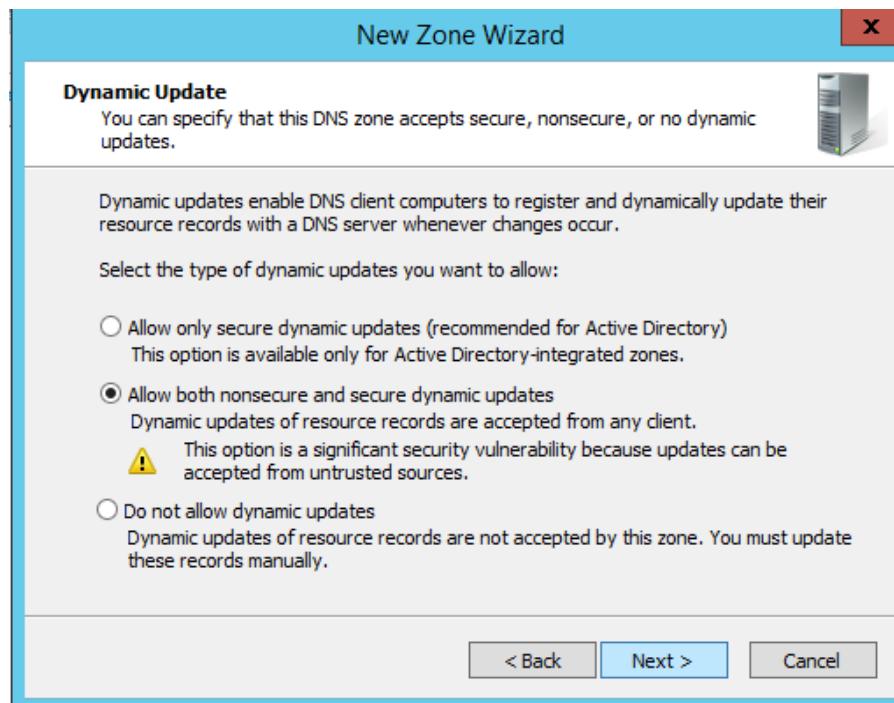
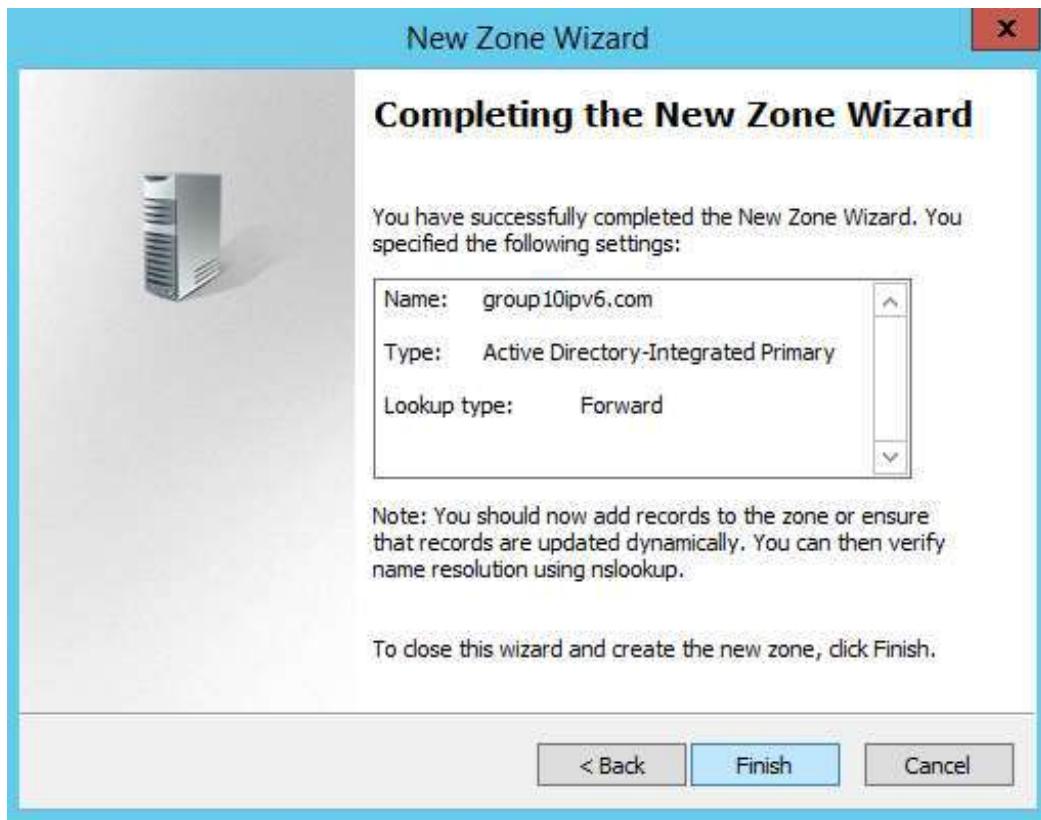


Figure 5.2.1.5.6: Allow both secure dynamic updates



*Figure 5.2.1.5.7: Click Finish to create IPv6 Forward Lookup Zone for Windows*

#### 5.2.3.4 Create IPv6 Reverse Lookup Zone

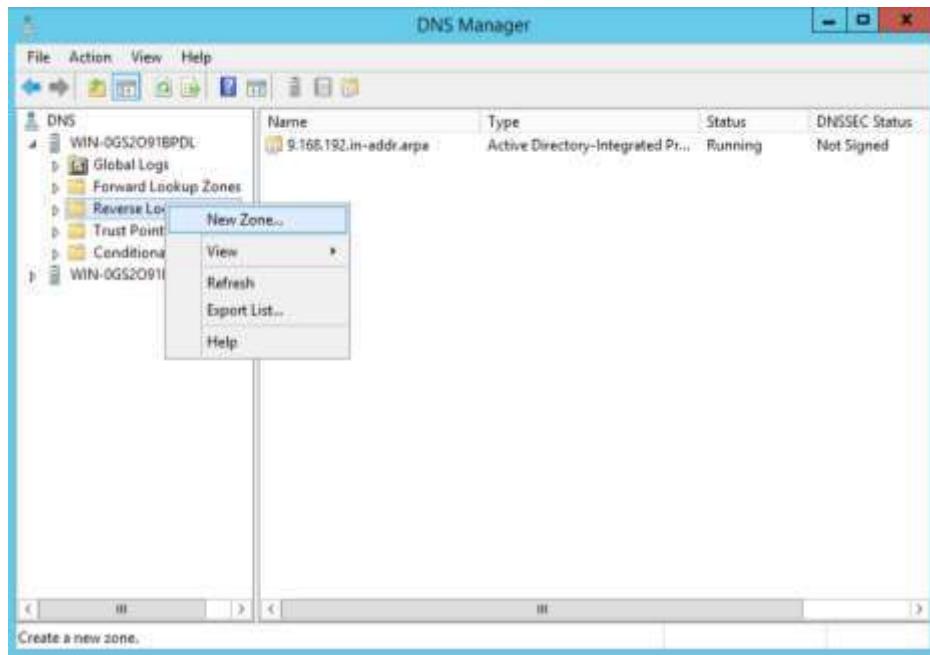


Figure 5.2.1.5.8: Right click on the Reverse Lookup Zones and choose New Zone



*Figure 5.2.1.5.9: Click Next*

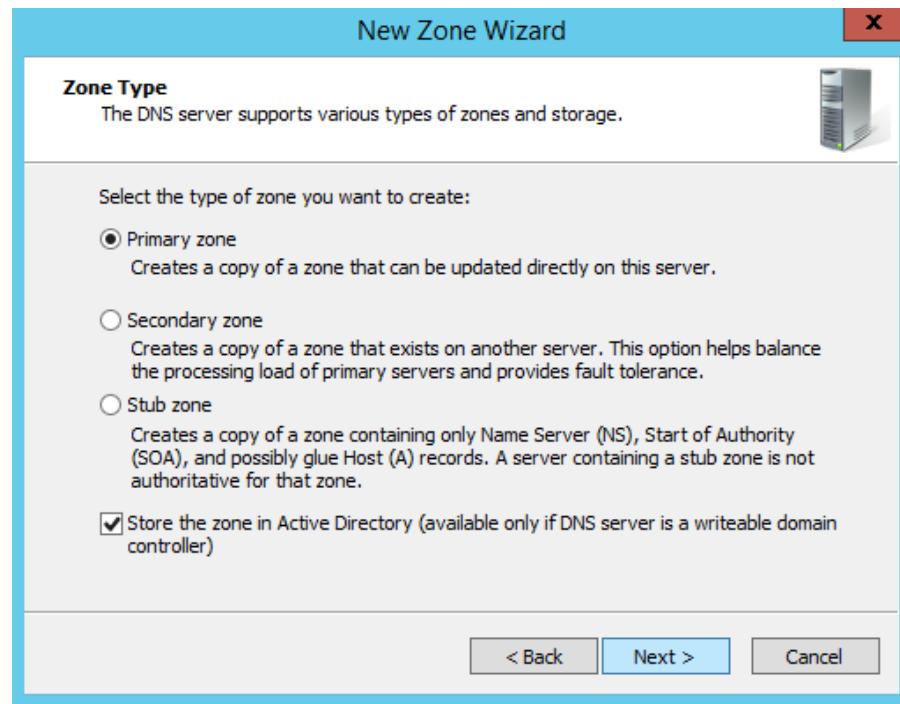


Figure 5.2.1.5.10: Choose Primary zone and Click Next

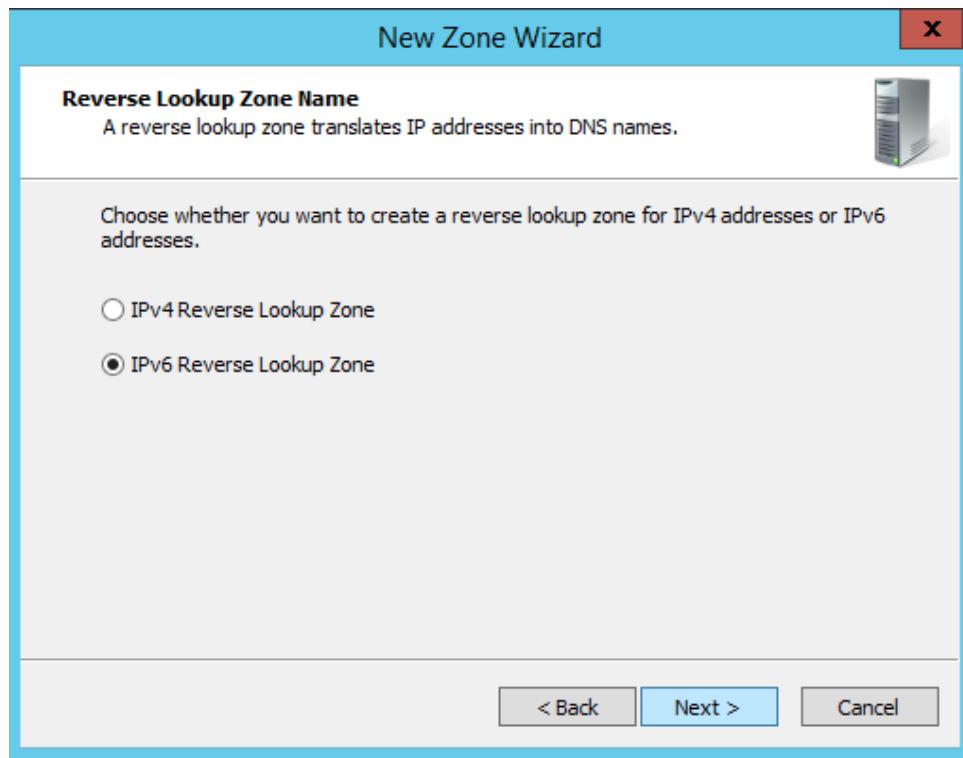
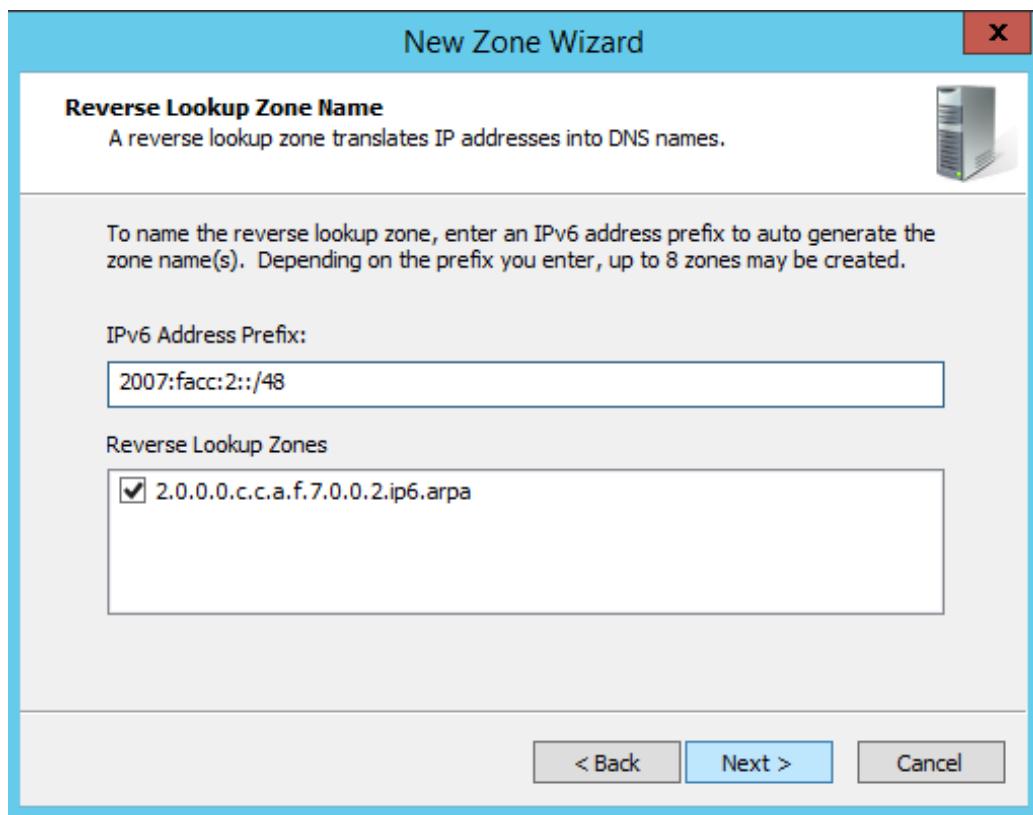
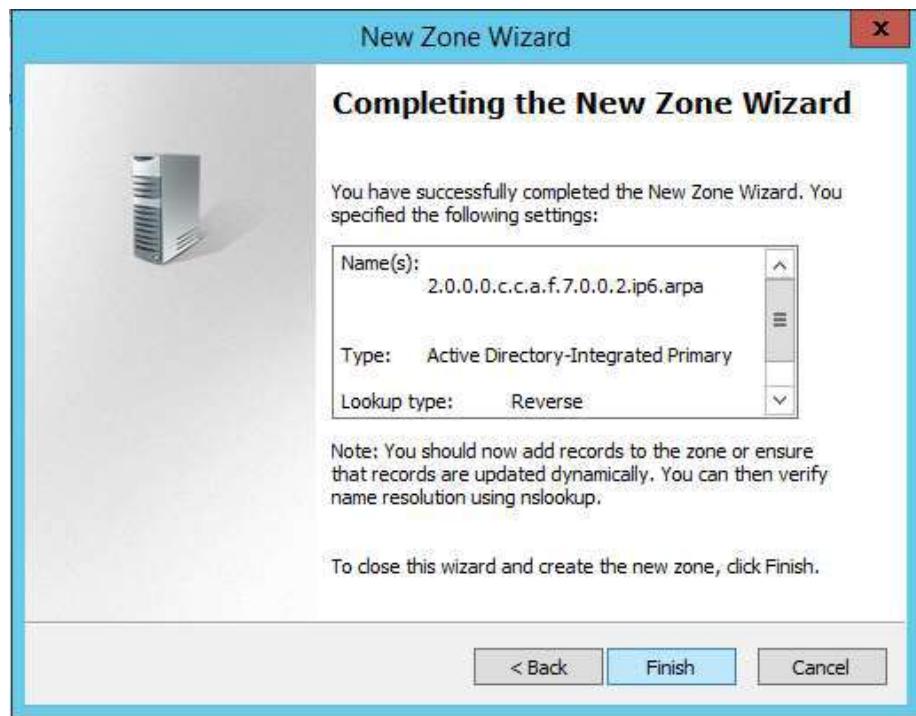


Figure 5.2.1.5.11: Choose IPv6 Reverse Lookup Zone then Click Next



*Figure 5.2.1.5.12: Insert the IPv6 Address Prefix and Click Next*



*Figure 5.2.1.5.13: Click Finish to create IPv6 Reverse Lookup Zone for Windows*

New Host X

Name (uses parent domain name if blank):

Fully qualified domain name (FQDN):

IP address:

Create associated pointer (PTR) record

Allow any authenticated user to update DNS records with the same owner name

Add Host Cancel

*Figure 5.2.1.5.14: Insert the host IP address and host name for client to add New Host*

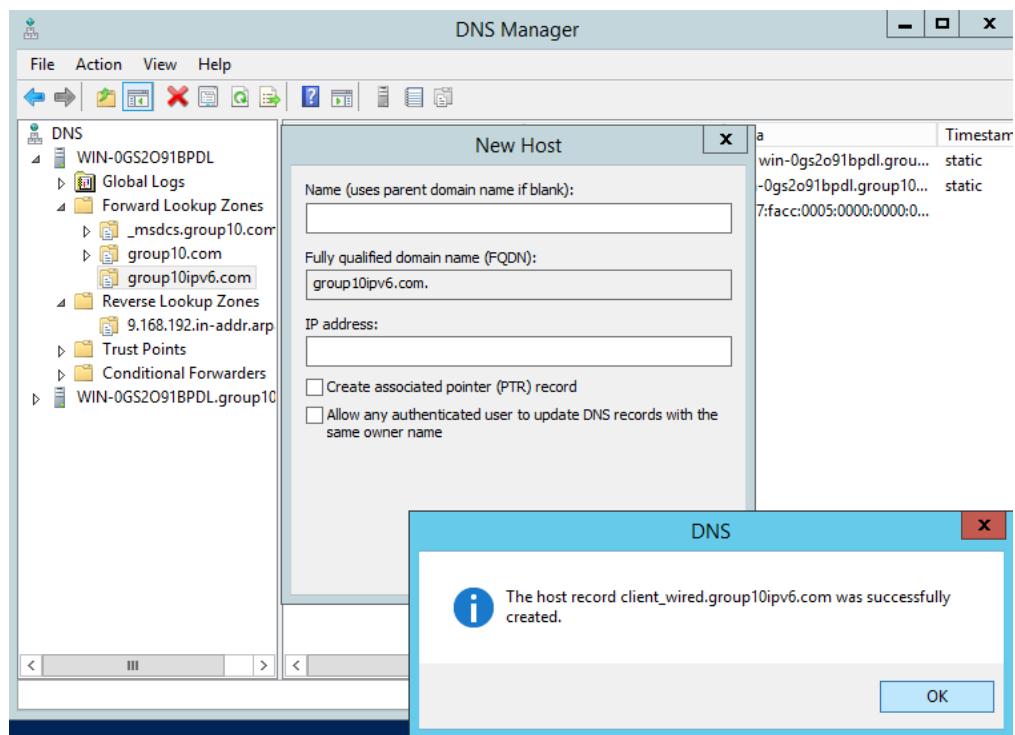


Figure 5.2.1.5.15: Successfully create the new host

Secondary server contain read-only copies of the zone file, and they get their info from a primary server in a communication known as a zone transfer. This means, Secondary DNS will take care of all queries to access DNS server if primary DNS is down or having a problem.

#### 5.2.3.6 Configuration Secondary DNS

Step 1: Installation BIND9 Service inside Ubuntu Server.

```
group10@group10:~$ sudo -l
[sudo] password for group10:
root@group10:~# sudo apt-get install bind9
Reading package lists... Done
Building dependency tree
Reading state information... Done
bind9 is already the newest version (1:9.10.3.dfsg.P4-Ubuntu1.11).
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
```

Figure 5.2.3.6.1: Installation bind9

Step 2: Add this line inside configuration file “/etc/bind/named.conf.default-zones”

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

// prime the server with knowledge of the root servers:
zone "." {
    type hint;
    file "/etc/bind/db.root";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912.
zone "localhost" {
    type master;
    file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
    type master;
    file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
    type master;
    file "/etc/bind/db.0";
};

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

zone "group10.com" {
    type slave;
    masters {192.168.9.130;};
    file "/var/cache/bind/db.group10.com";
};

zone "9.168.192.in-addr.arpa" {
    type slave;
    masters{192.168.9.130;};
    file "/var/cache/bind/db.9.168.192";
};
```

Figure 5.2.3.6.2: Edit configuration file

### 5.2.3.7 Forward zone Secondary DNS

Step 1: Right click on Forward Zone in and open Properties.

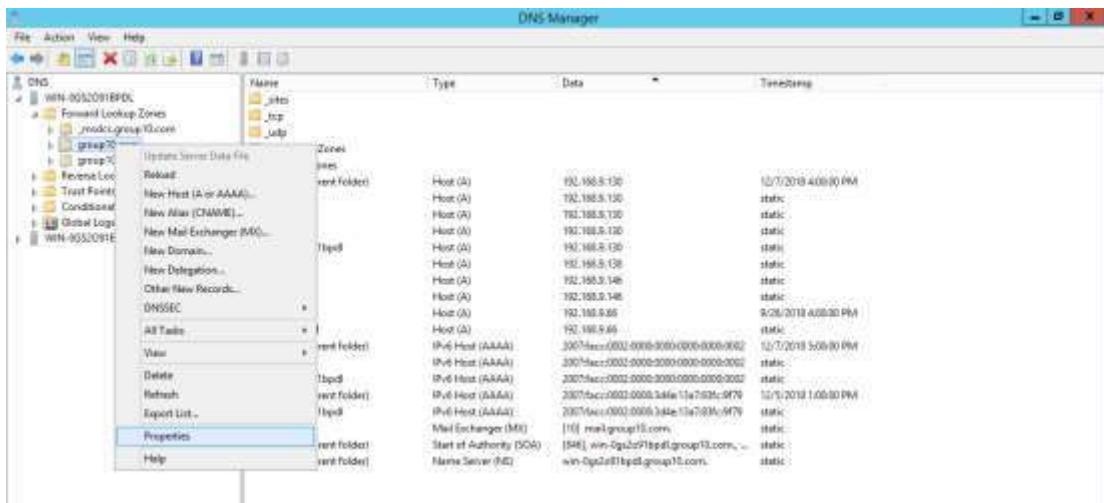


Figure 5.2.3.7.1: Open Properties

Step 2: Checked the “allow Zone Transfer” and Click Edit button to add the IP Address of the Ubuntu Sever

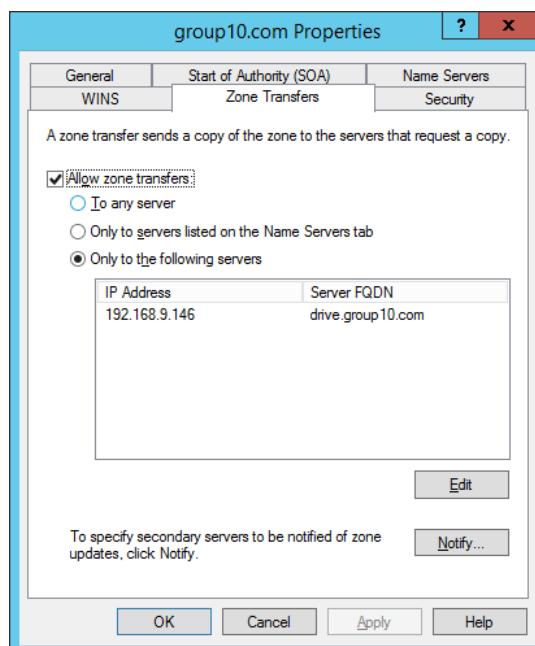
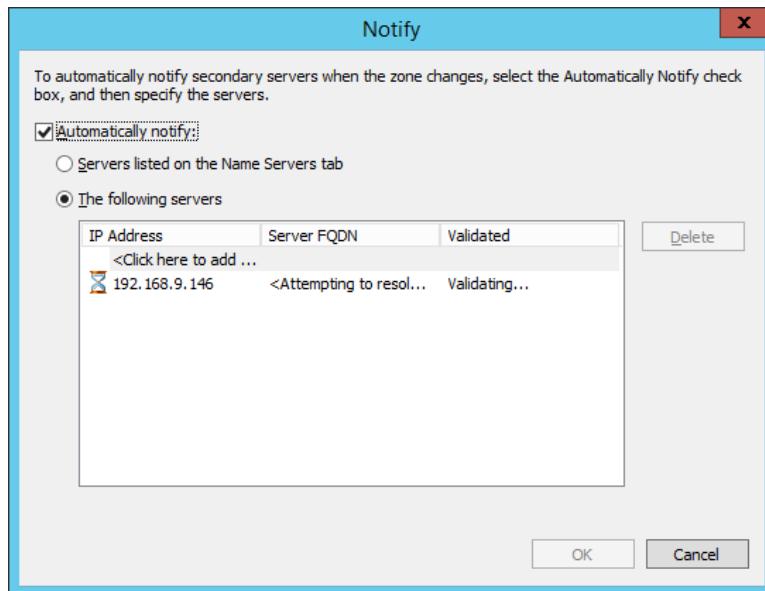


Figure 5.2.3.7.2: Checked the allow Zone Transfer

Step 3: Click on Notify button and add IP Address od Ubuntu server again, which it will notify Ubuntu Server as backup DNS Server, also called as Secondary DNS



*Figure 5.2.3.7.3: checked "Automatic notify" and add Ubuntu IP address*

### 5.2.3.8 Reverse zone Secondary DNS

Step 1: Right click on Reverse Zone in and open Properties.

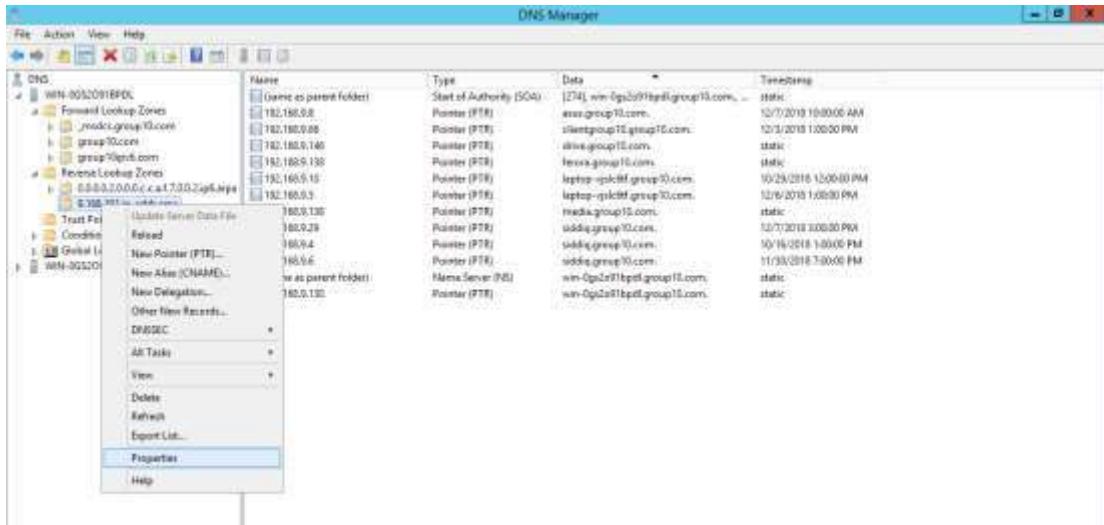


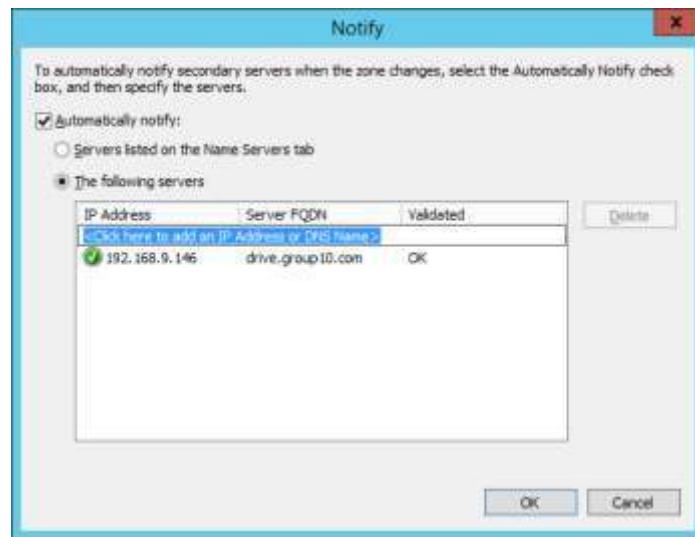
Figure 5.2.3.8.1: Open Properties

Step 2: Go to Zone Transfer tab, Check the “Allow zone transfer” and add IP address of Ubuntu Sever after click Edit button.



Figure 5.2.3.8.2: Click Edit button to add IP address Ubuntu Server

Step 3: Click on Notify button and add IP Address od Ubuntu server again, which it will notify Ubuntu Server as backup DNS Server, also called as Secondary DNS



*Figure 5.2.3.8.3: Checked "Automatic notify" and add Ubuntu IP address*

## 5.2.2 DHCP (IPV4)

### Dynamic Host Configuration Protocol (DHCP) IPv4

The DHCP is a network protocol used to assign IP address and provide configuration information such as servers, desktop or devices, so they can communicate on a network using the Internet Protocol.

1. Open the DHCP Manager

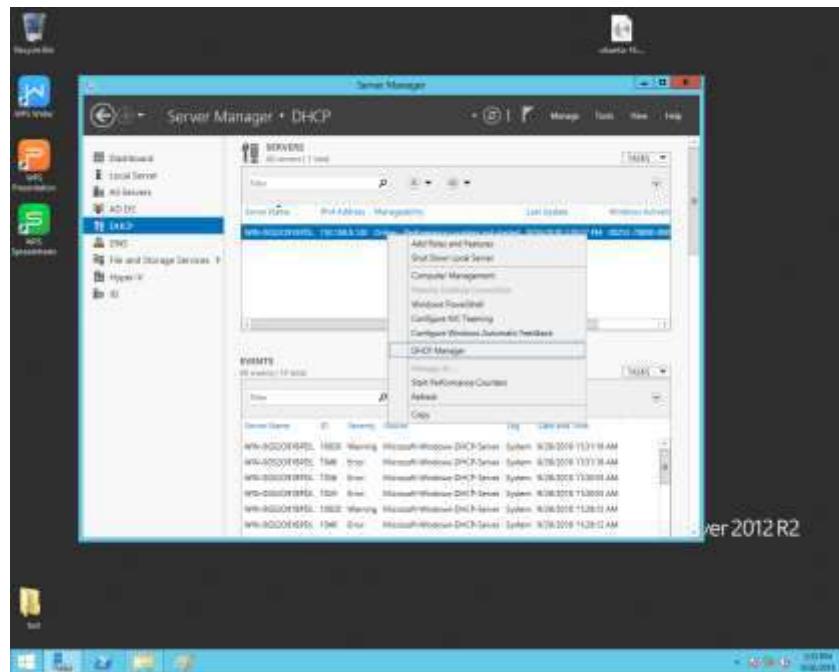
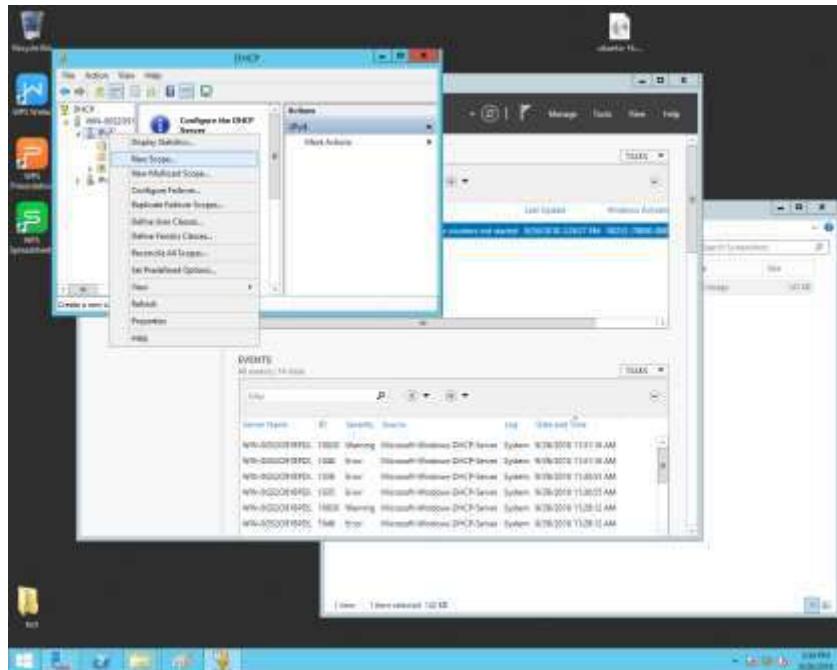


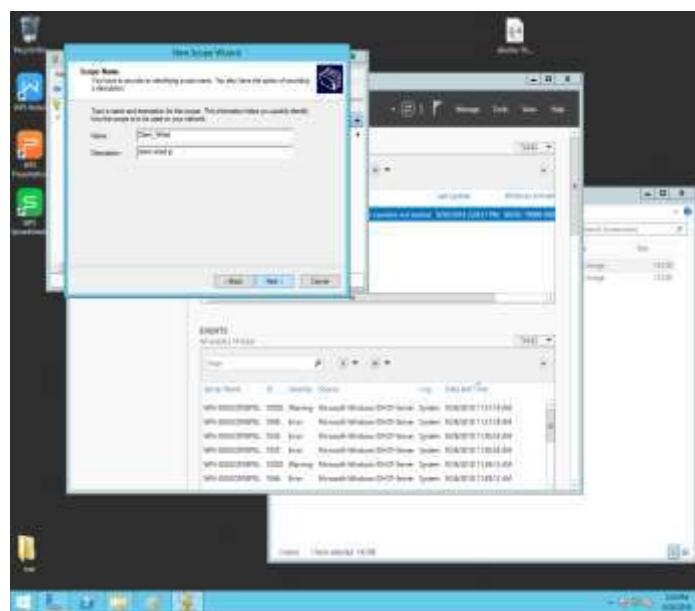
Figure 5.2.2.1: show Open DHCP Manager

- Right click on the Ipv4 and click on the new scope



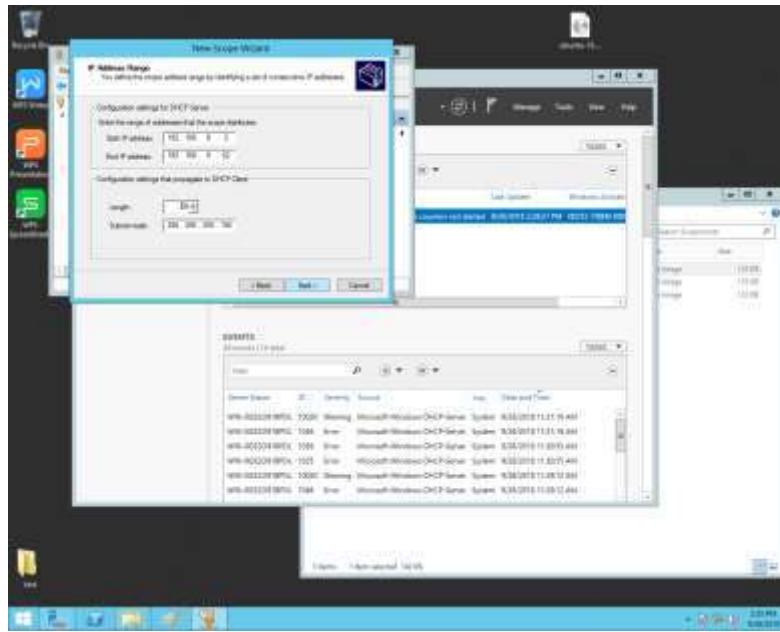
*Figure 5.2.2.2: show the New Scope Wizard*

- Add the name and the description into the new scope wizard in order to create the DHCP



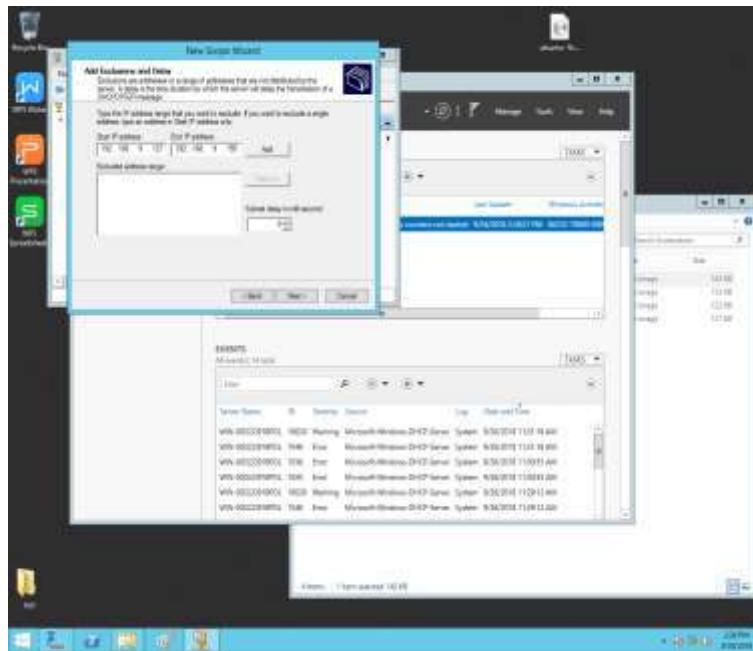
*Figure 5.2.2.3: show the Name and Description for the New Scope*

- Configure the IP Address Range by entering the start IP address, end IP address, length and the subnet mask for the IP



*Figure 5.2.2.4: show the Configuration of IP Address*

- Configure the exclusions and delay for the new scope wizard



*Figure 5.2.2.5: show the Configuration of Exclusions and Delay*

- Set the lease duration for scope leases when distributed by this server

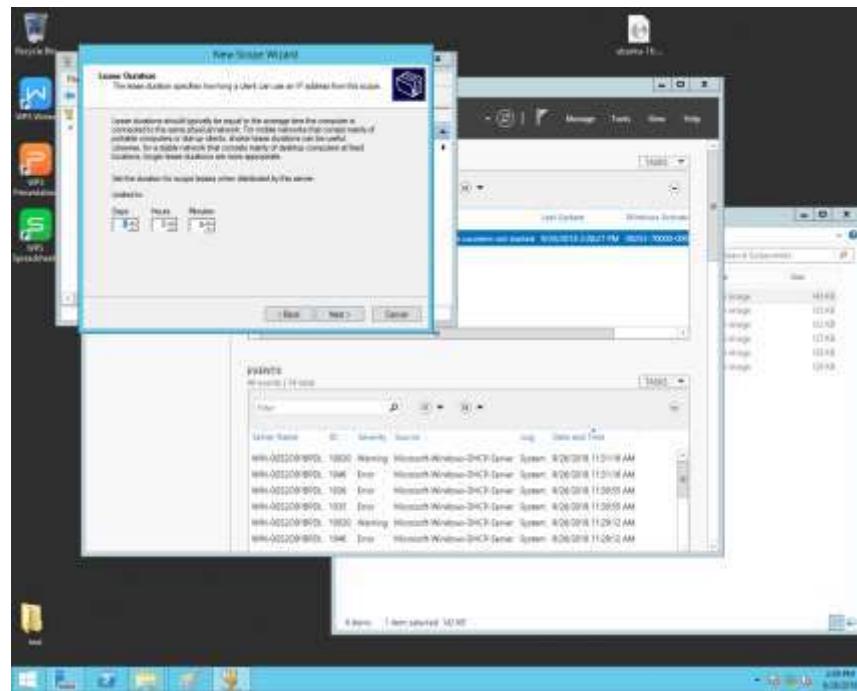


Figure 5.2.2.6: show the Lease Duration that Need to be Set

- Configure the DHCP options for the scope

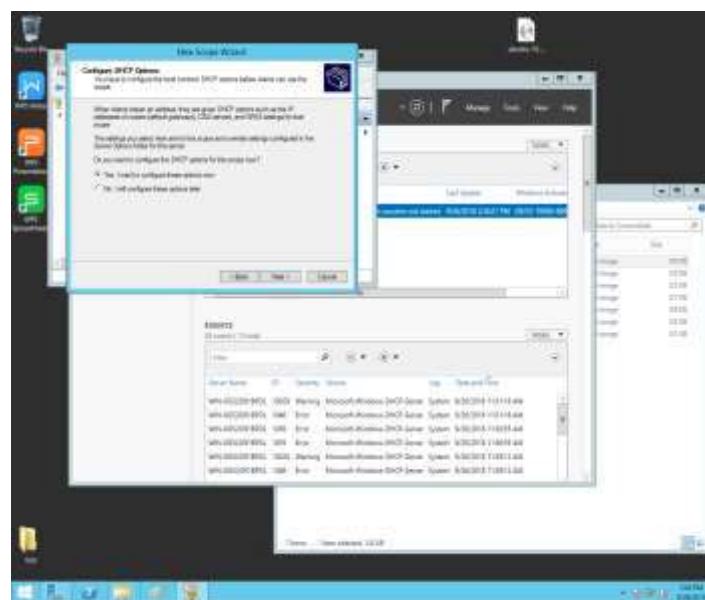


Figure 5.2.2.7: show the DHCP Options

8. Configure the Router (Default Gateway) used by client

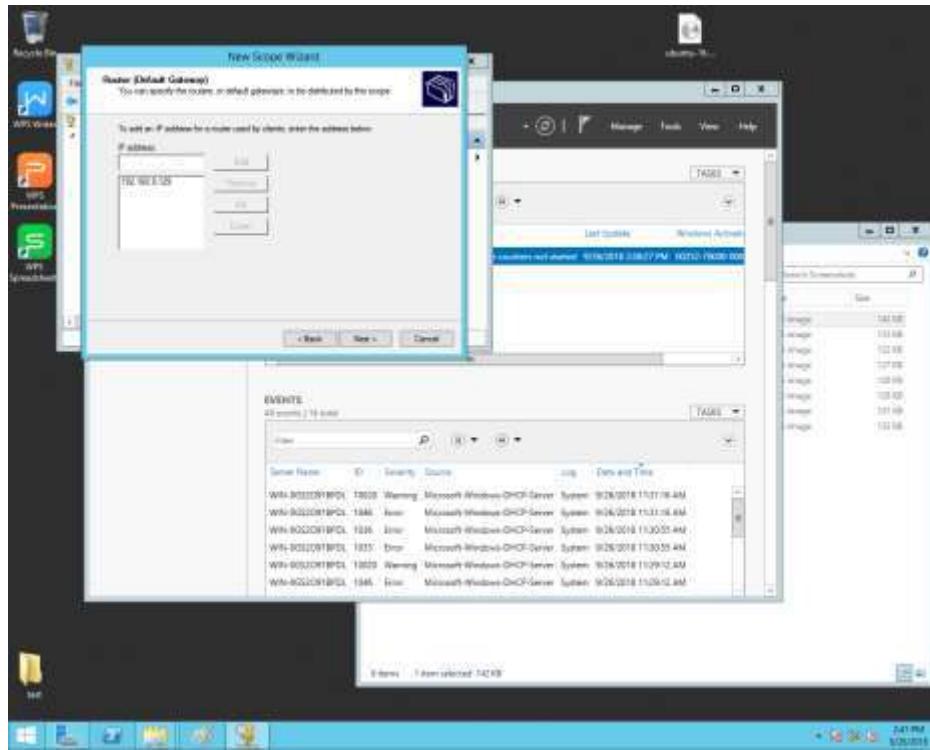


Figure 5.2.2.8: show the Default Gateway Used by Client

9. Configure the domain name and DNS servers

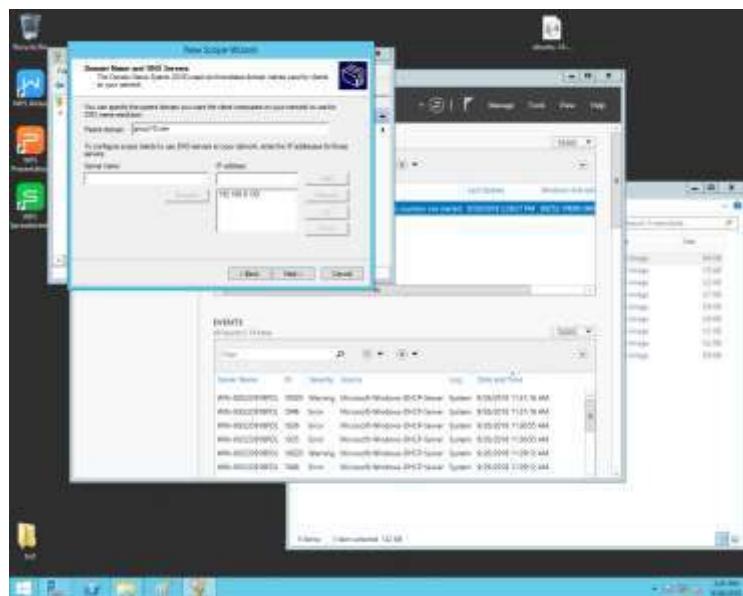


Figure 5.2.2.9: show the Configuration of Domain Name and DNS Servers

## 10. Activating the new scope wizard

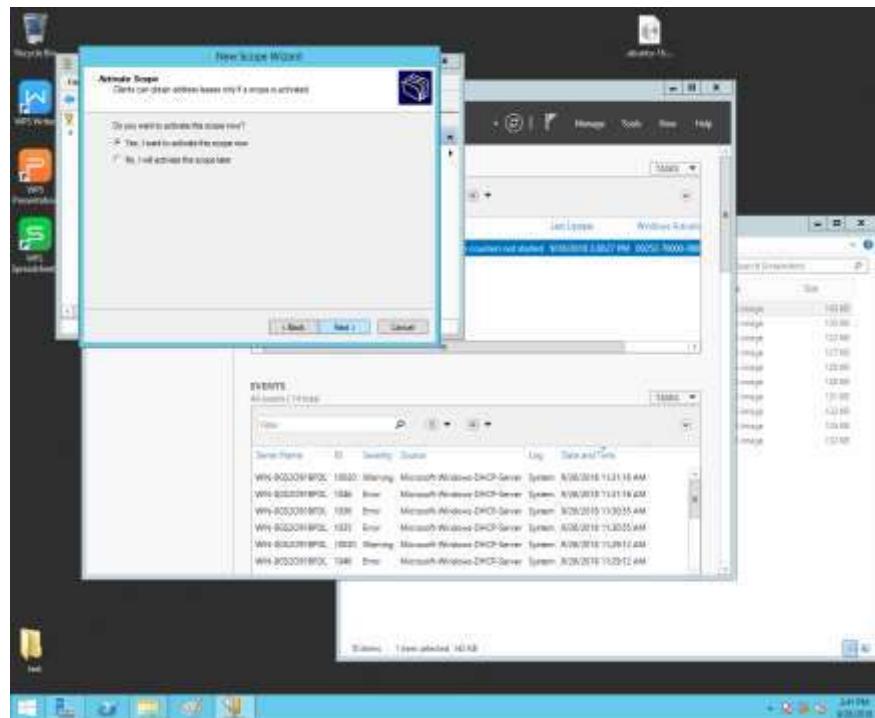


Figure 5.2.2.10: show Scope Activation

### 5.2.3 DHCP (IPV6)

**Step 1:** Click Start Menu> Server Manager. After that choose Add Roles and follow the wizard by selecting DHCP Server and click Next button.

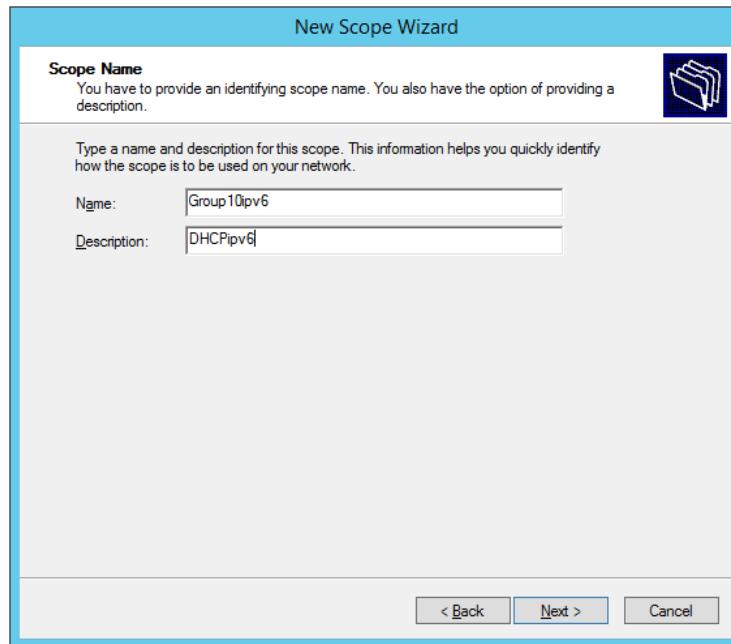


Figure 5.2.3.1: New Scope Wizard

**Step 2:** Enter the IPv6 address. Click Next Button until it Finish.



Figure 5.2.3.2: New Scope Wizard

**Step 3:** Expand the IPv6 and there new Scope has been created

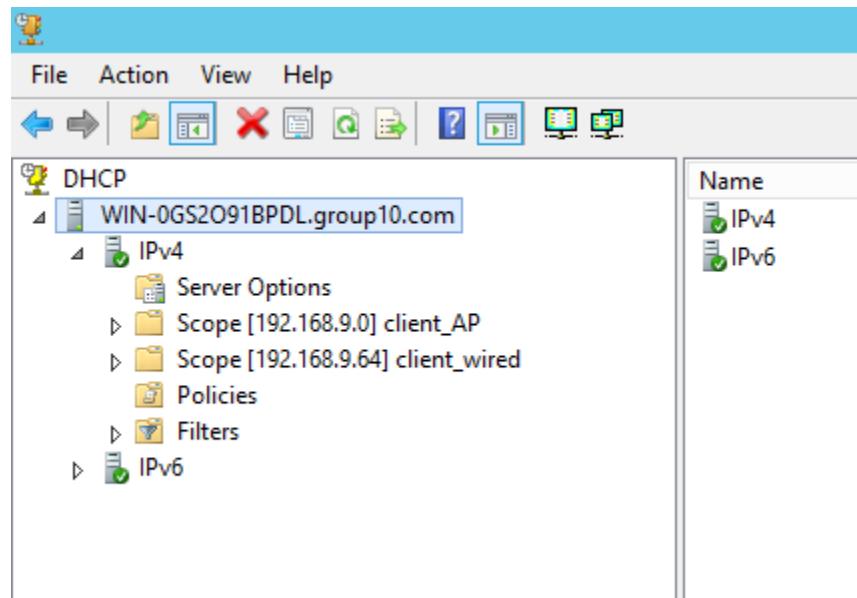


Figure 5.2.3.3: DHCP Server

**Step 4:** Open network connection and select network used by switch.

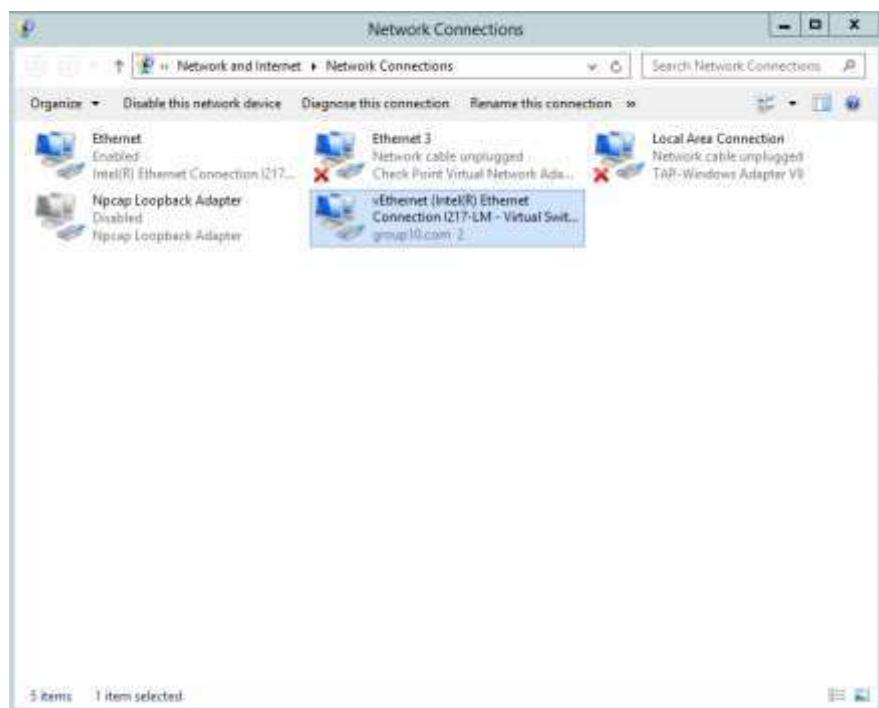
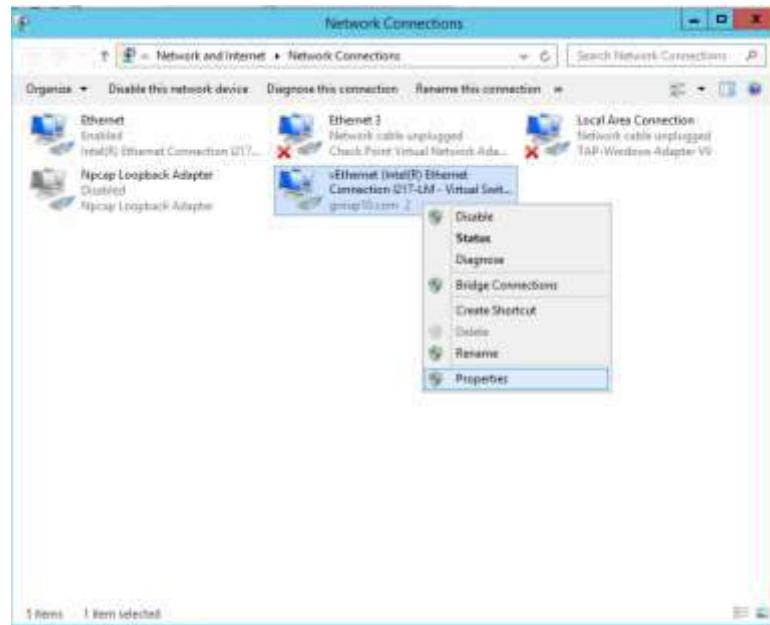


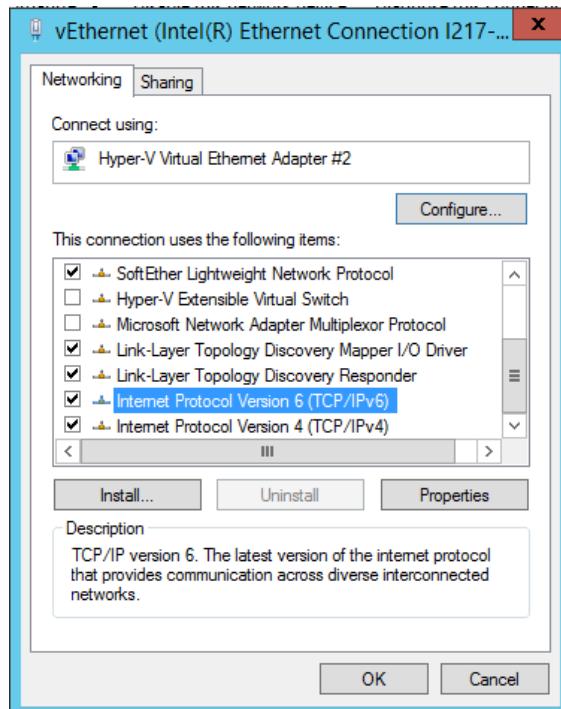
Figure 5.2.3.4: Network Connection

**Step 5:** Click right click and select Properties.



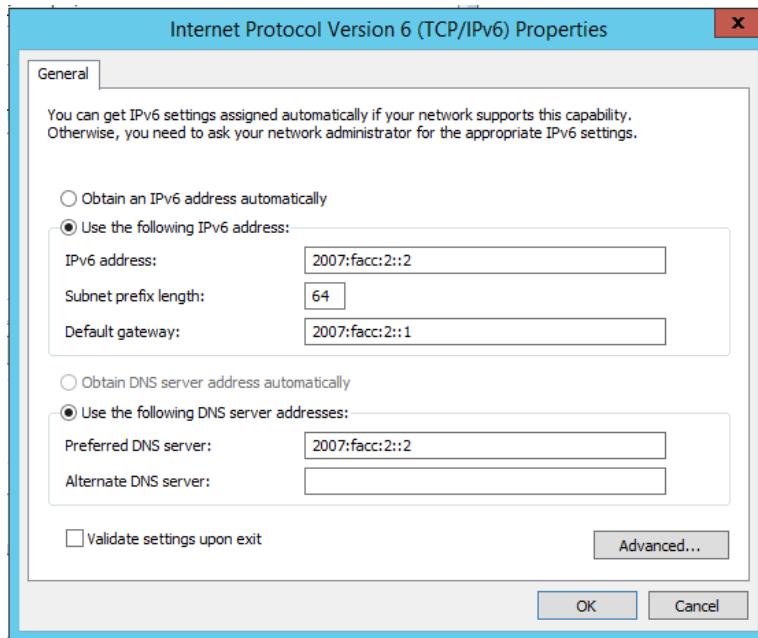
*Figure 5.2.3.5: Network Connection*

**Step 6:** Click the TCP/IPv6 to be ticked then click Properties.



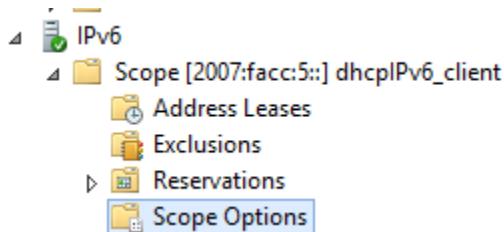
*Figure 5.2.3.6: Enable Ipv6*

**Step 7:** Enter the IPv6 ip address



*Figure 5.2.3.7: TCP/IPv6 Properties*

**Step 8:** Select scope option at the IPv6 DHCP server.



*Figure 5.2.3.8: DHCP Servers*

**Step 9:** Click Right Click on Scope Options

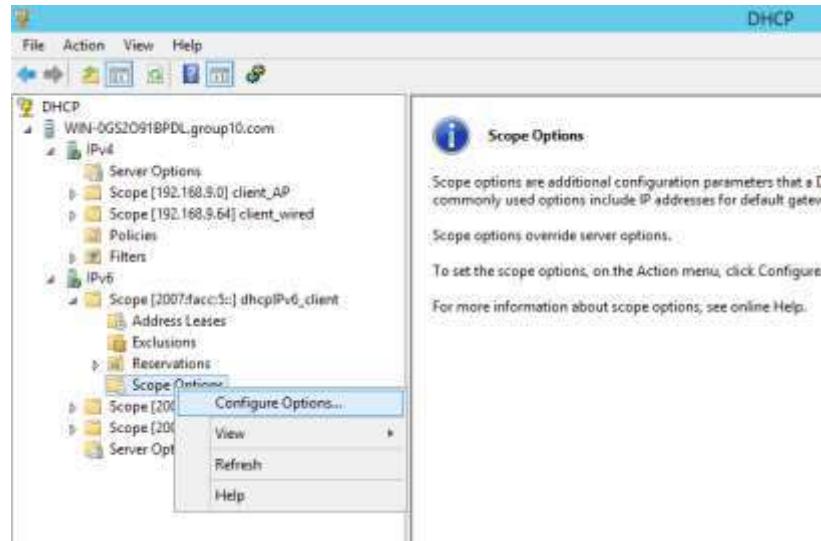


Figure 5.2.3.9: DHCP Servers Configuration Options

**Step 10:** In General make sure DNS of IPv6 ticked then click OK

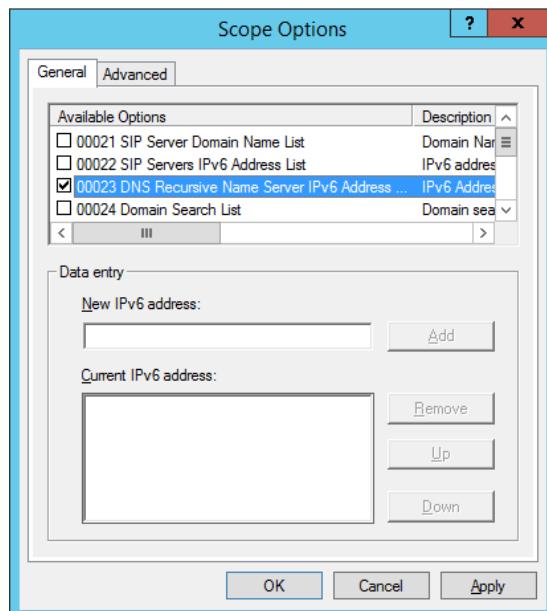


Figure 5.2.3.10: Scope Options

DHCP							
	Client IPv6 Address	Name	Lease Expiration	IID	Type	Unique ID	Description
WIN-0GS2O91BPD\group10.com	2007:facc:60:182::	SIDDIQ	12/21/2018 3:37:22 PM	49845447	IANA	000100012...	
IPv6	2007:facc:60:5e7::	ssus	12/19/2018 10:31:38 AM	190064414	IANA	000100012...	
Scope [2007:facc:5c:] dhcpIPv6_	2007:facc:60:62b::	LAPTOP-VISLC6TF	12/21/2018 5:12:59 PM	527753151	IANA	000100011...	
Address Leases	2007:facc:60:c71::	SIDDIQ	12/12/2018 7:58:03 PM	53894445	IANA	000100012...	
Exclusions							
Reservations							
Scope Options							
Scope [2007:facc:f1:] dhcpIPv6_							
Address Leases							
Exclusions							
Reservations							
Scope Options							
Scope [2007:facc:7:] client							
Server Options							

Figure 5.2.3.11: Wireless client using Ipv6.

DHCP							
	Client IPv6 Address	Name	Lease Expiration	IID	Type	Unique ID	Description
WIN-0GS2O91BPD\group10.com	2007:facc:50:714::	UserHud\group10.c...	12/21/2018 4:20:19 PM	90439786	IANA	000100012...	
IPv6							
Scope [2007:facc:5c:] dhcpIPv6_							
Address Leases							
Exclusions							
Reservations							
Scope Options							
Scope [2007:facc:6c:] dhcpIPv6_							
Address Leases							
Exclusions							
Reservations							
Scope Options							
Scope [2007:facc:7c:] client							
Server Options							

Figure 5.2.3.12: Wired Client using Ipv6.

## 5.2.4 IPV6 Web with IPV6 Tunneling

### 5.2.4.1 IPv6 Tunnelling

To configure 6to4 tunnelling, we first need to create a tunnel interface on each dual-stack edge router. There are three key components relevant to ipv6ip:

- The tunnel mode (ipv6ip)
- The tunnel source (IPv6)
- The 6to4 IPv6 address (within 2002::/16)

Step 1: On our router, we create the tunnel interface, configure it as ipv6ip, and specify its cloud-facing IPv6 interface as the tunnel source:

```
R1(config)# interface tunnel0
R1(config-if)# tunnel mode ipv6ip
R1(config-if)# tunnel source 200.200.200.9
R1(config-if)# tunnel destination 200.200.208.3
```

Step 2: Determine the IPv6 address of the tunnel interface

```
R1(config-if)# ipv6 enable
R1(config-if)# ipv6 address 2018:0909:1010:0910::2/48
```

Step 3: With OSPFv3, just as with the other IPv6 routing protocols, the interfaces and therefore the networks attached to them are configured directly on the interface in interface configuration mode.

```
R1(config-if)# ipv6 router ospf 4
R1(config-if)# router-id 2.2.2.2
R1(config-if)# redistribute static
```

Step 4: List the static route of the neighbouring IP addresses.

```
ipv6 route 2001:db8:1234:f010::2/64 tunnel0
```

```
ipv6 route 2001:db8:1234:f020::2/64 tunnel0
```

```
ipv6 route 2001:db8:1234:f030::2/64 tunnel0
```

```
ipv6 route 2001:db8:1234:f101::/64 tunnel0
```

```
ipv6 route 2001:db8:1234:f102::/64 tunnel0
```

Step 5: Remember to apply ospf protocol on your intervlan too, so neighbouring host can access the IPv6 Web

```
interface fe0/1.10
ipv6 enable
ipv6 ospf 4 area 0
exit
interface fe0/1.20
ipv6 enable
ipv6 ospf 4 area 0
exit
interface fe0/1.30
ipv6 enable
ipv6 ospf 4 area 0
exit
interface fe0/1.40
ipv6 enable
```

#### 5.2.4.2 IPv6 Web

IPv6 website is created through virtual hosting. Virtual hosting is used to enable the web server to host multiple website in the server.

Add new host website in DNS Setting as ***webipv6.group10.com*** and use the IPv6 2007:facc:2::2

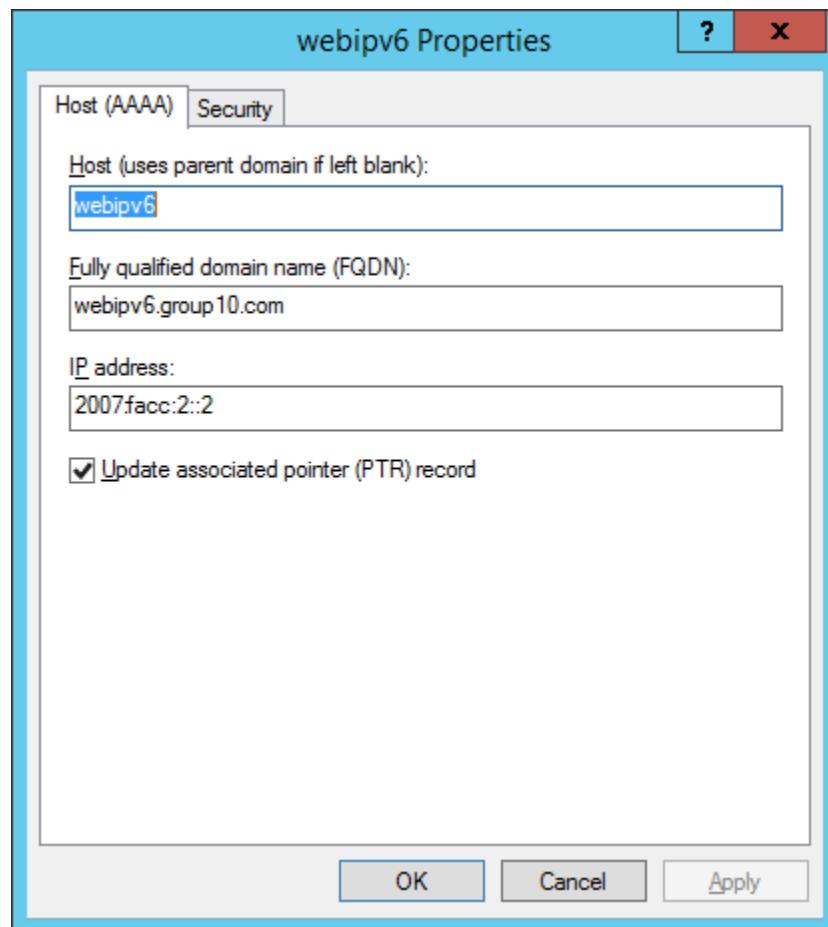


Figure 5.2.4.2.1: Properties of webipv6

## 5.2.5 InterVLAN

**Step 1 :** reset router to format factory

**Step 2 :** type the following command

**Step 3 :** interVLAN 5

```
#int fa0/1.5  
#encapsulation dot1q 5  
#ip add 192.198.9.153 255.255.252
```

**Step 4 :** interVLAN 10

```
#int fa0/1.10  
#encapsulation dot1q 10  
#ip add 192.198.9.129 255.255.255.248
```

**Step 5 :** interVLAN 20

```
#int fa0/1.20  
#encapsulation dot1q 20  
#ip add 192.198.9.137 255.255.255.248
```

**Step 6 :** interVLAN 30

```
#int fa0/1.30  
#encapsulation dot1q 30
```

```
#ip add 192.198.9.145 255.255.255.248
```

**Step 7 : interVLAN 40**

```
#int fa0/1.40  
#encapsulation dot1q 40  
#ip add 192.198.9.65 255.255.255.192
```

**Step 8 : interVLAN 50**

```
#int fa0/1.50  
#encapsulation dot1q 50  
#ip add 192.198.9.1 255.255.255.192
```

**Step 9 : save**

```
#int fa0/1  
  
#no shut
```

## 5.2.6 Secured FTP

### Secure file transfer protocol

Step 1: install vsftpd

```
Group10@group10:-Virtual-Machine:~$ sudo apt-get install vsftpd
```

Step 2: to begin the configuration, open the vsftpd.conf file by command

```
Group10@group10:-Virtual-Machine:~$ sudo su
```

```
Group10@group10:-Virtual-Machine:/home/group10# nano /etc/vsftpd.conf
```

Step 3: to apply all the setting, just inster the command :

```
Group10@group10:-Virtual-Machine:/home/group10# service vsftpd start
```

Step 1: install openssh server

```
Group10@group10:~$ sudo apt install openssh server
```

Step 2 : After installing, the commands below can be used to stop, start and enable the service to always start up when the server boots...

```
Group10@group10:~$ sudo systemctl stop ssh.service
```

```
Group10@group10:~$ sudo systemctl start ssh.service
```

```
Group10@group10:~$ sudo systemctl enable ssh.service
```

Step 3: add the # before the first line, then add the highlighted line just below it to enable SFTP.... This will change the subsystem to internal-sftp only

```
#Subsystem sftp /usr/lib/openssh/sftp-server
Subsystem sftp internal-sftp
# Set this to 'yes' to enable user authentication account processing
```

*Figure 5.2.6.1: Enabling*

Step 4: add the lines below at the end of the file

```
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication. Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
UsePAM yes

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

*Figure 5.2.6.2: Configuration*

Step 5 : create group to test sftp named sftp users

```
Group10@group10:~$ sudo groupadd sftp_users
```

Step 6 : add user and take the user into the group

```
Group10@group10:~$ sudo usermo -aG sftp_users fana
```

```
Group10@group10:~$ sudo usermo -aG sftp_users group10
```

Step 7 : Check user

```
group10@group10-Virtual-Machine: ~
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for fana
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] Y
group10@group10-Virtual-Machine:~$ su fana
Password:
fana@group10-Virtual-Machine:/home/group10$ sudo su
[sudo] password for fana:
fana is not in the sudoers file. This incident will be reported.
fana@group10-Virtual-Machine:/home/group10$ exit
exit
group10@group10-Virtual-Machine:~$ sudo usermod -aG sftp_users fana
group10@group10-Virtual-Machine:~$ sftp fana@192.168.9.131
fana@192.168.9.131's password:
Connected to 192.168.9.131.
sftp> ls
fana    group10    nukeman
sftp> █
```

*Figure 5.2.6.3: Check user*

## 5.2.7 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**.

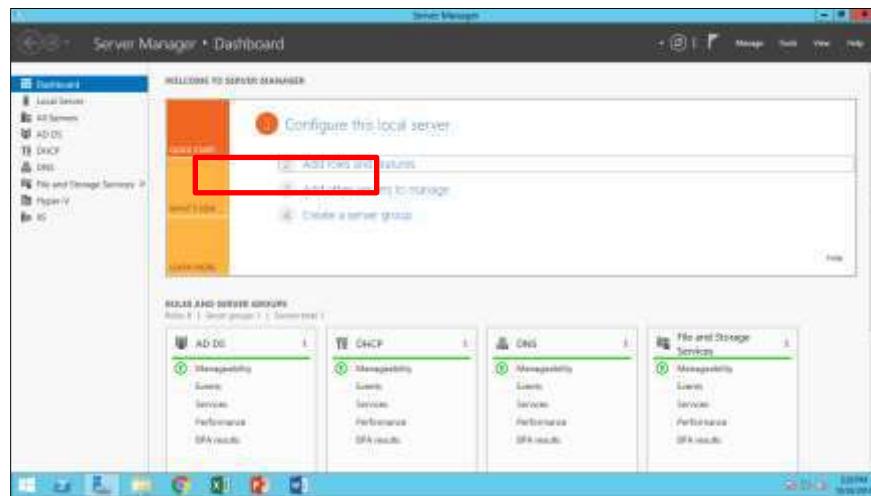


Figure 5.2.7.1: Server Manager

**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**.

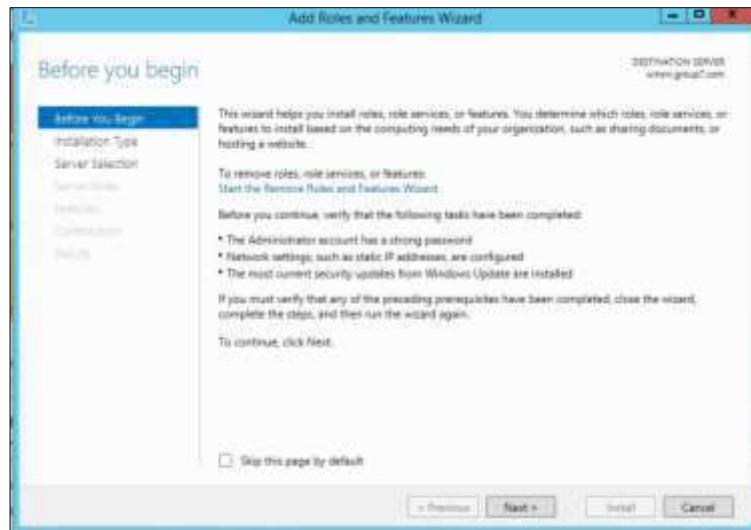


Figure 5.2.7.2: Add Roles and Features

**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.

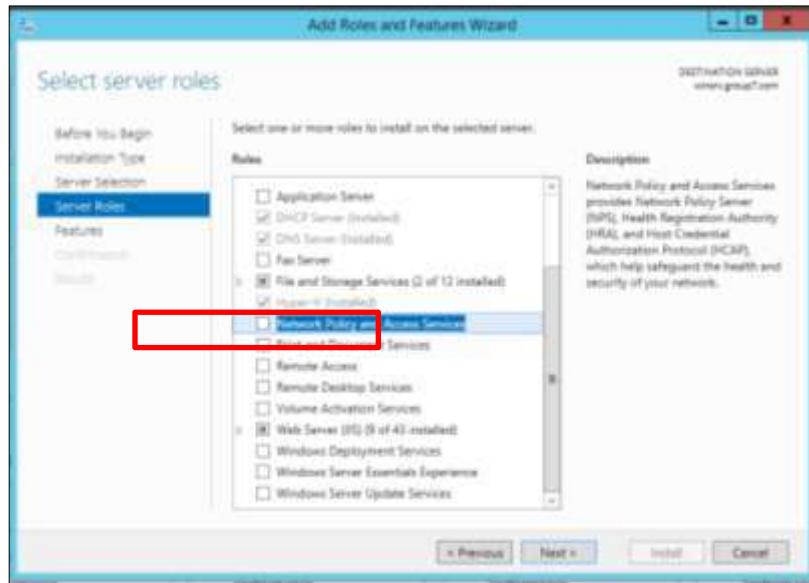


Figure 5.2.7.3: Select server roles

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

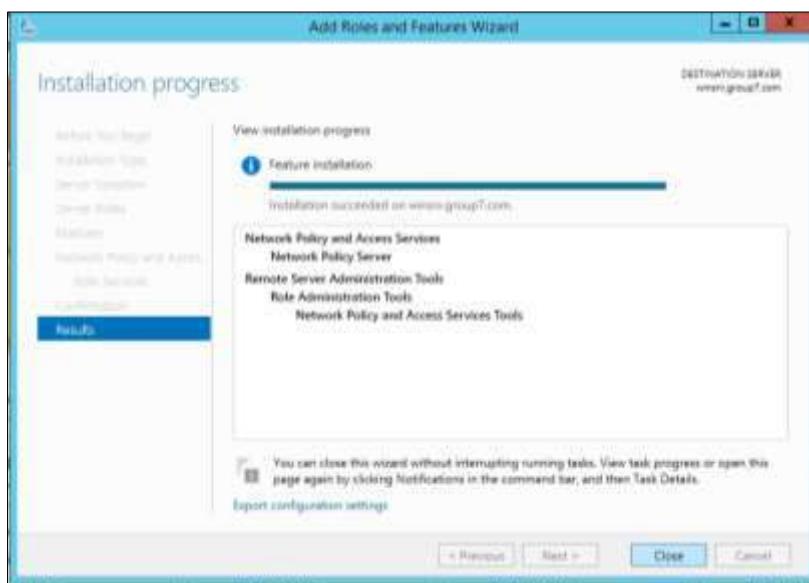


Figure 5.2.7.4: Installation progress

**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.

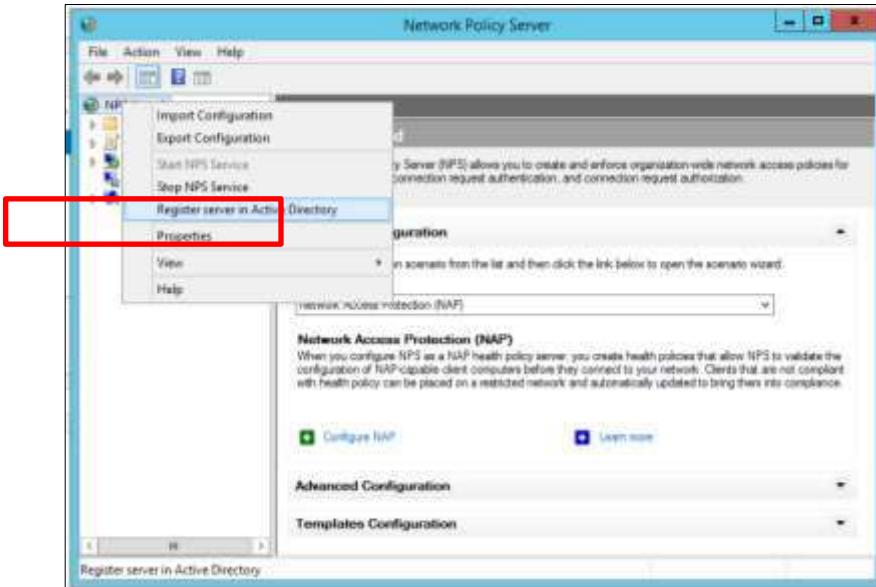


Figure 5.2.7.5: Network Policy Server

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

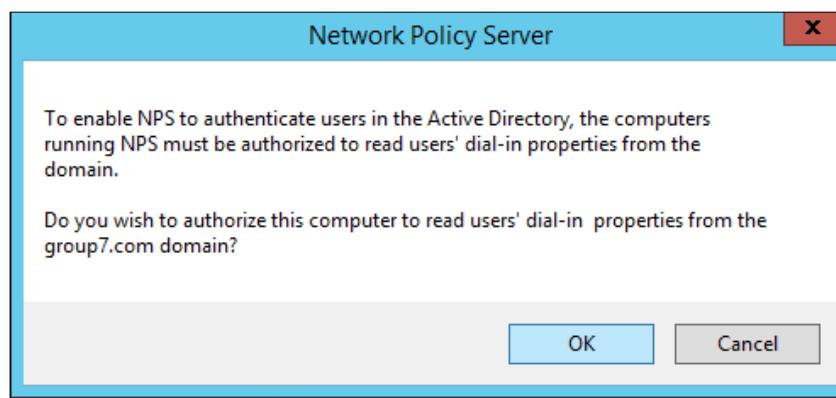


Figure 5.2.7.6: Enable NPS

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

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



*Figure 5.2.7.7: New radius client*

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

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

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

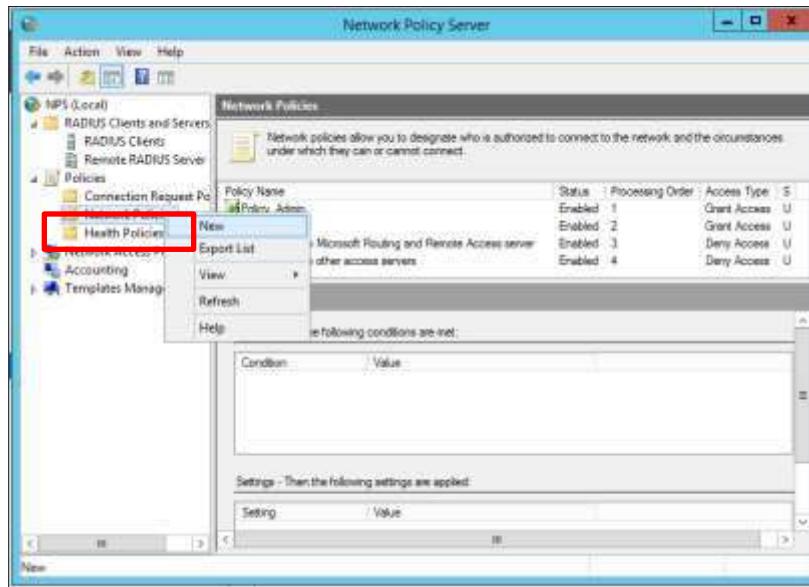
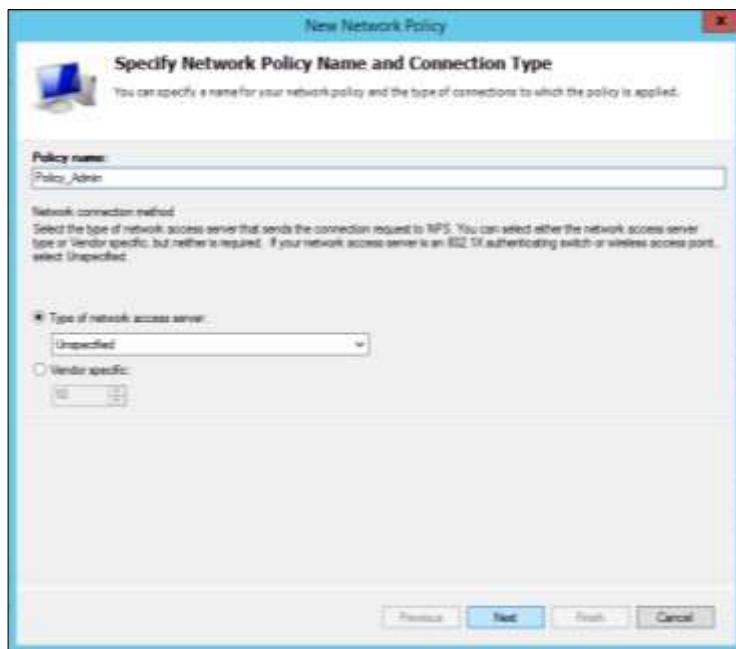


Figure 5.2.7.8: New network policies

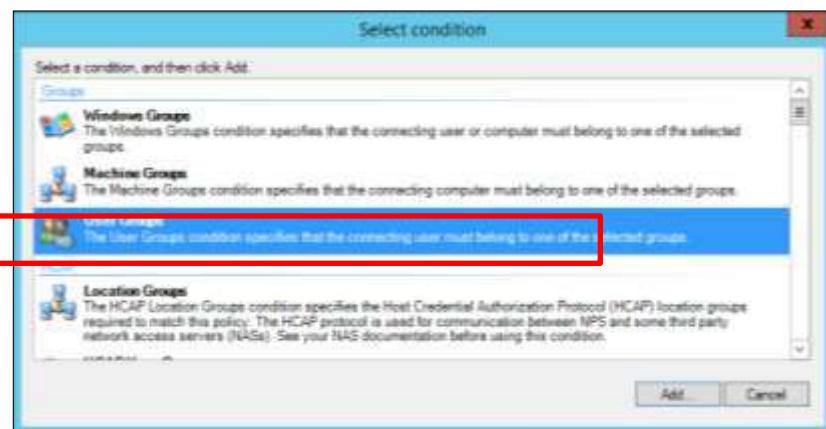
**Step 10:** Enter the Policy Name and click **next**.



*Figure 5.2.7.9: Policy Name*

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

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



*Figure 5.2.7.10: Specify Condition*

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

**Step 13:** Enter the object name to select > type “AAA” > click Check Names. Then, choose Group10User and click OK.

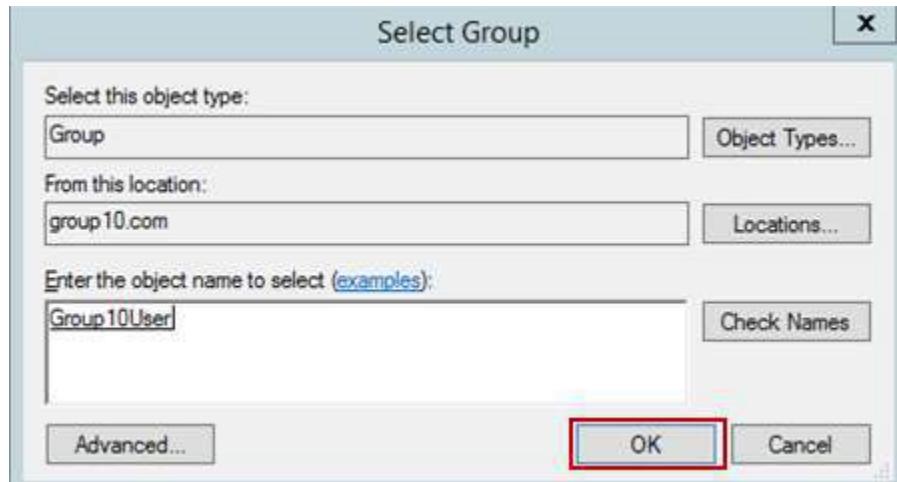


Figure 5.2.7.11: Check names

**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.

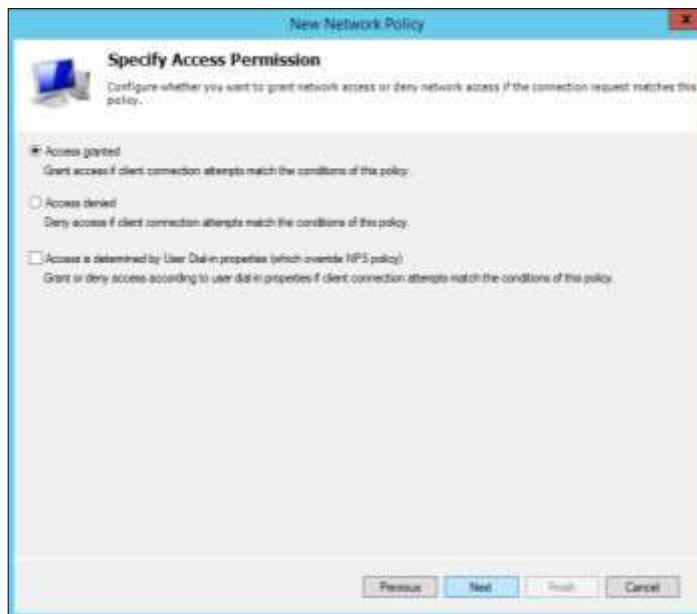


Figure 5.2.7.12: Access permission

**Step 15:** On Configuration Authentication Methods, tick on Unencrypted authentication (PAP, SPAP), and Encrypted authentication. Proceed to Next. When Connection Request Policy windows appear, click no.

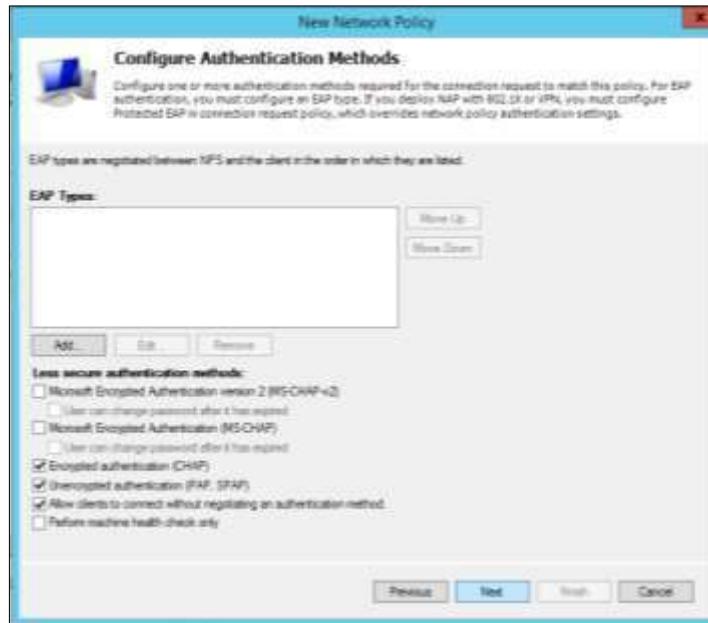


Figure 5.2.7.13: Authentication method

**Step 16: Configure Constraint** page, proceed to Next.

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

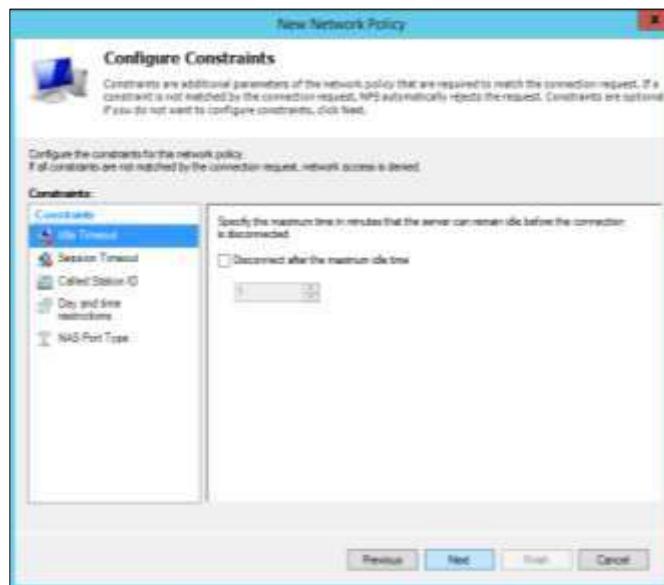


Figure 5.2.7.14: Configure constraint

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

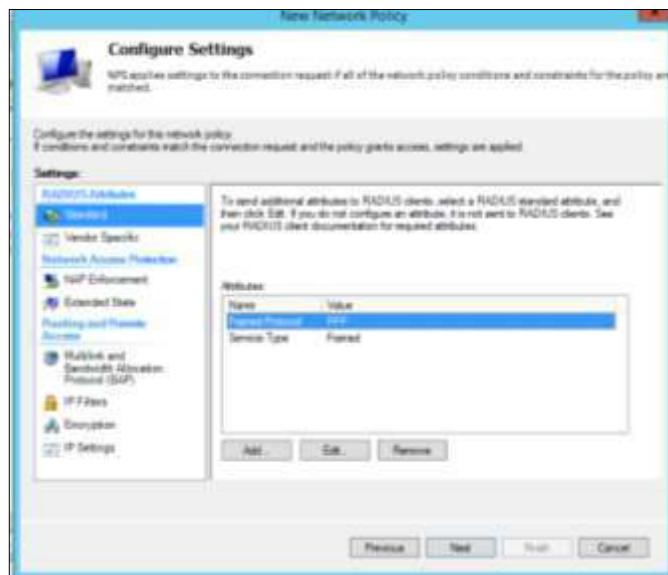


Figure 5.2.7.15: Configure settings

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

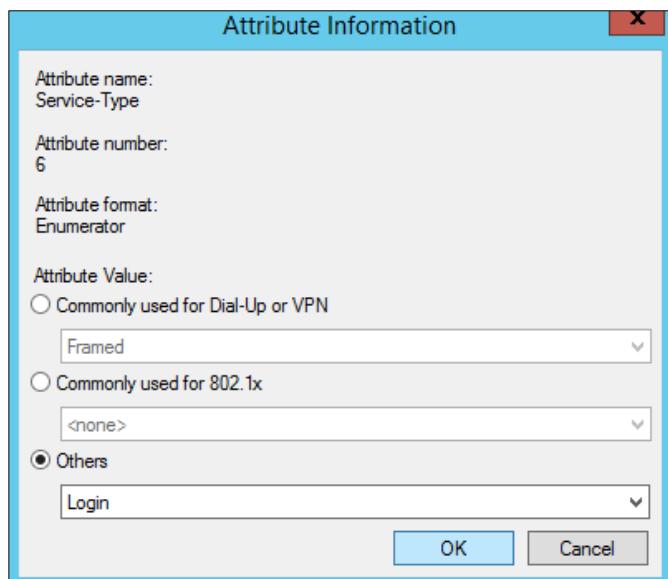


Figure 5.2.7.16: Attribute information

**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.

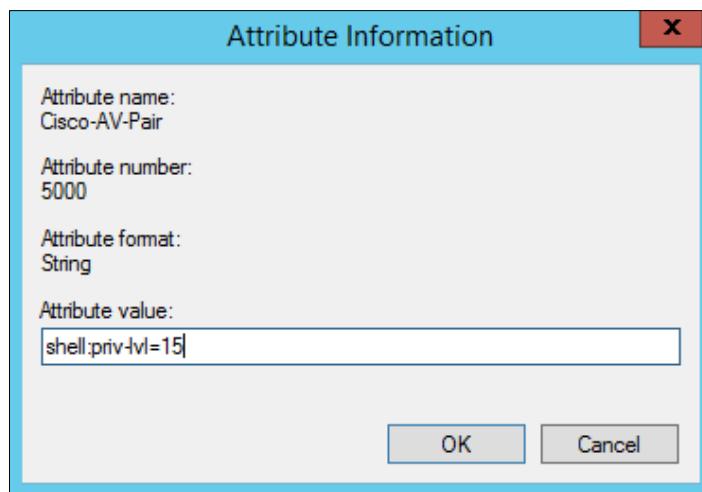


*Figure 5.2.7.19: Vendor specific*

**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.

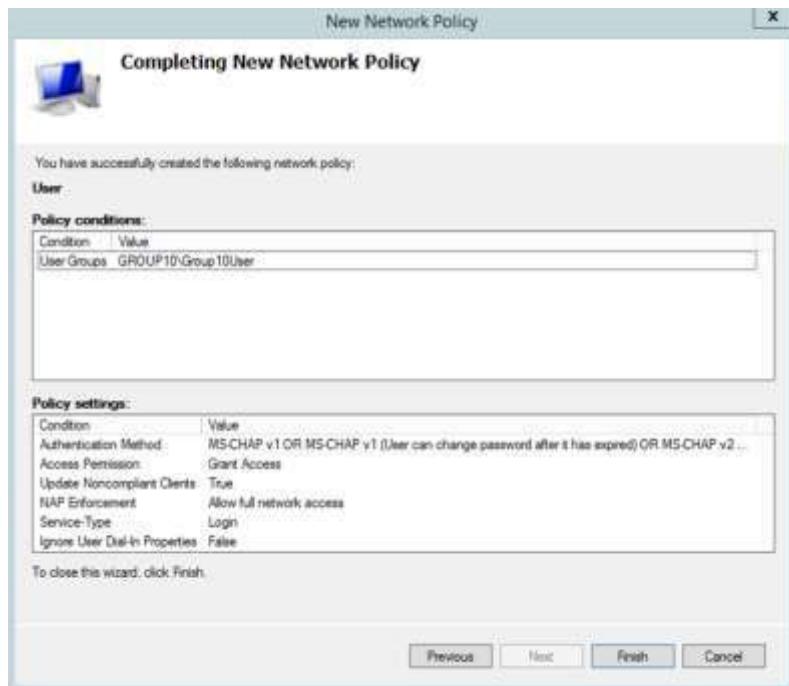
- privilege level 1 = non-privileged (prompt is router>), the default level for logging in
- privilege level 15 = privileged (prompt is router#), the level after going into enable mode
- privilege level 0 = seldom used, but includes 5 commands: disable, enable, exit, help, and logout



*Figure 5.2.7.20: Attribute value*

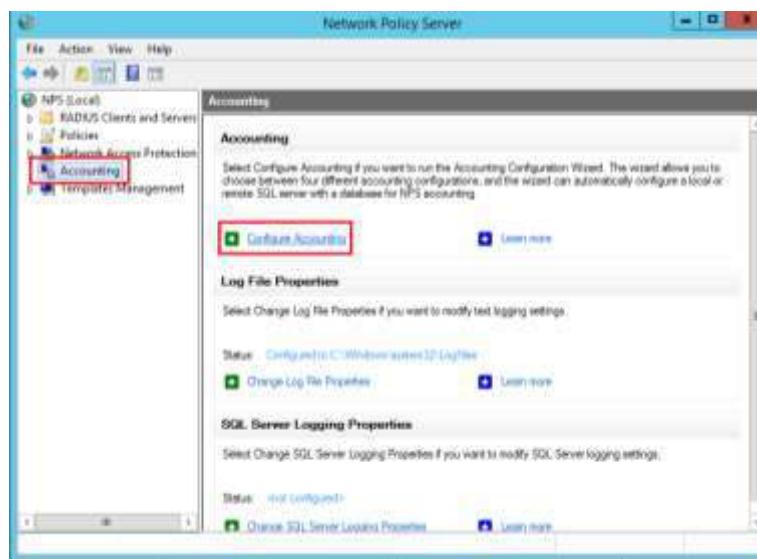
**Step 21:** In **Completing New Network Policy**, it will displays that successfully created the network policy, Click **Finish**. Then your network policy is created.

Successful created network policy



*Figure 5.2.7.21: Complete*

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



*Figure 5.2.7.22: Accounting in Network Policy Server*

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

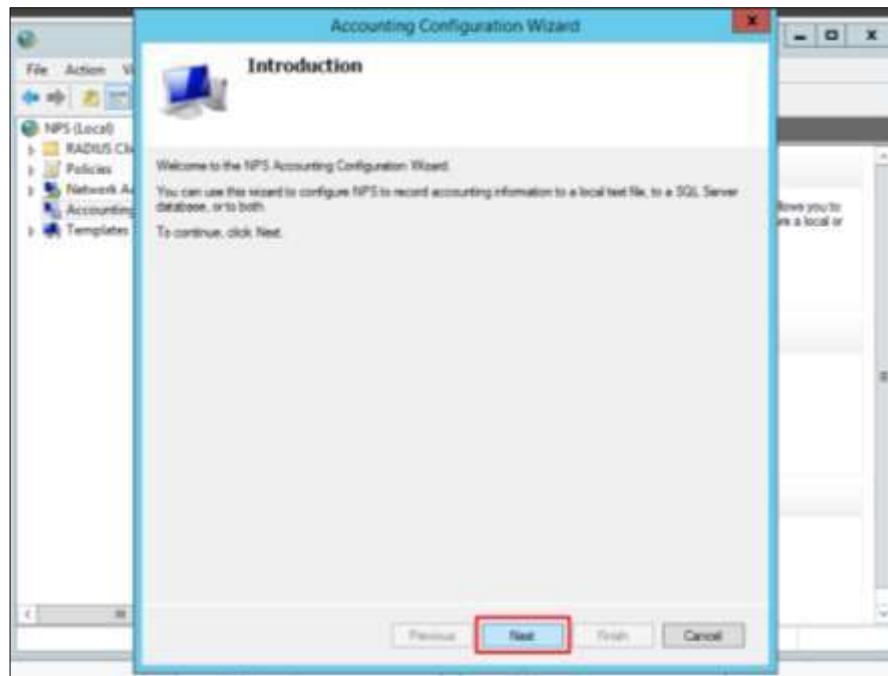


Figure 5.2.7.23: Introduction in accounting configuration

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

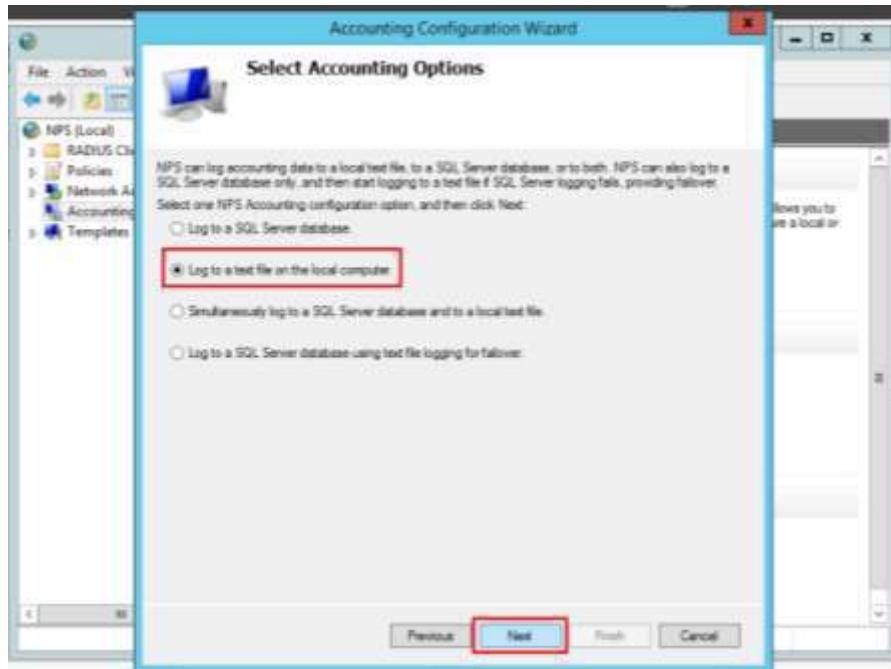


Figure 5.2.7.24: Select accounting option

**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.

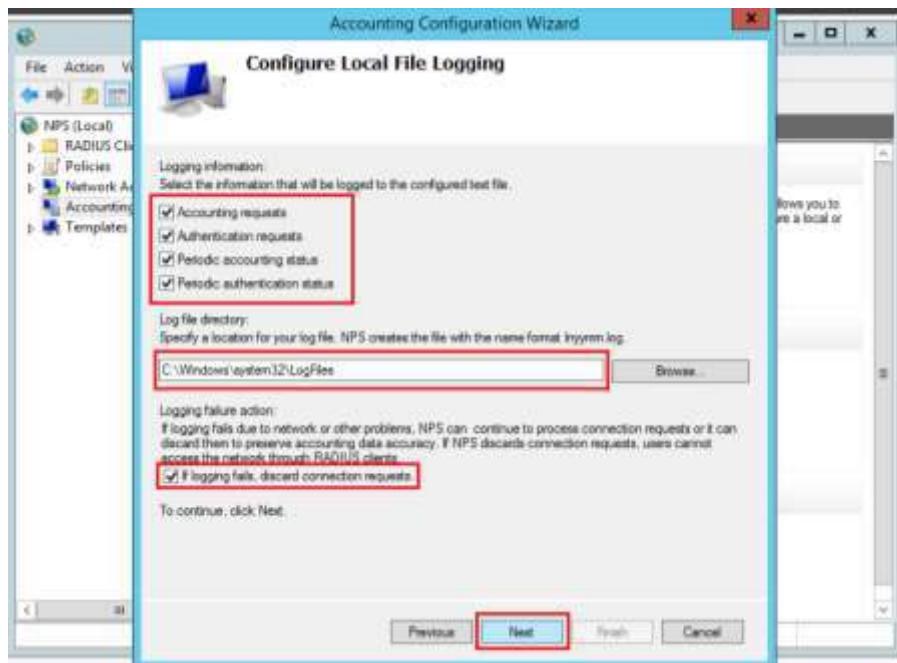


Figure 5.2.7.25: Configure file logging

**Step 26:** In the Conclusion page, click Close.

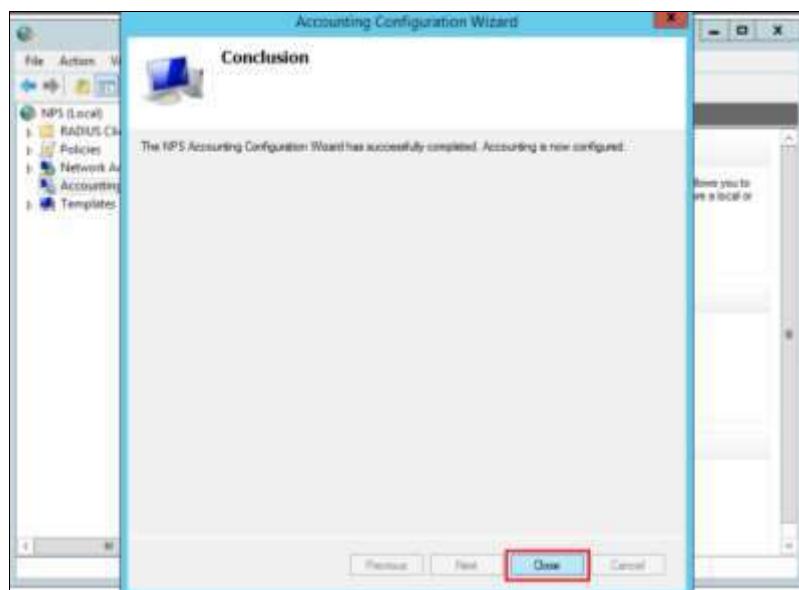


Figure 5.2.7.26: Conclusion

## AUTHENTICATION USING RADIUS SERVER

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

```
Router(config)# config t  
Router(config)# aaa new-model  
Router(config)# aaa group server radius RAD  
Router(config-in-rad)# server-private 192.168.9.130 auth-port 1645 acct-port  
1646 key Abc123  
Router(config-in-rad)# exit  
Router(config)# aaa authentication login default group RAD local  
Router(config)# aaa authorization exec default group RAD local if-  
authenticated  
Router(config)# aaa authorization console
```

Configuration in putty for aaa new model

```
Login as : group10  
Password : enter your password  
Group10-RT#en  
Group10-RT#config t  
Group10-RT(config)#aaa new  
Group10-RT(config)#aaa new-model
```

Configuration in putty for authentication

```
Group10-RT(config)#aaa authentication login default group radius local-case  
Group10-RT(config)#aaa authentication login vty group radius local-case  
Group10-RT(config)#aaa authentication enable default group radius local if  
Group10-RT(config)##$zation exec default group radius local if-authenticated
```

Configuration in putty for server name

```
Group10-RT(config)#aaa accounting system default start-stop group radius  
Group10-RT(config)#aaa group server radius RAD1  
Group10-RT(config-sg-radius)#server name SERVER1  
Group10-RT(config-sg-radius)#server name SERVER2
```

```
Group10-RT(config-sg-radius)#exit  
Group10-RT(config)#radius server SERVER1  
Group10-RT(config-radius-server)#key Abc123  
Group10-RT(config-sg-radius)#exit
```

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

## 5.2.8 Routing & Network Address Translation (NAT)

### Routing Configuration

Routing and NAT protocol used must be the same with the neighbor's routing protocol to allow the communication between both islands.

Step 1: Configure the interface on f0/0 as the inside NAT interface and enter the IP Address for the router.

```
group10router(config)#int f0/0
group10router(config-if)#ip address 200.200.208.1 255.255.255.240
group10router(config-if)#ip nat outside
group10router(config-if)#exit
```

*Figure 5.2.8.1: Configure NAT interface*

Step 2: Configure the static NAT translation for each of your machines.

```
group10router(config)#static source static 192.168.0.130 200.200.208.2
group10router(config)#static source static 192.168.0.190 200.200.208.3
group10router(config)#static source static 192.168.0.130 200.200.208.4
group10router(config)#ip nat inside source static 192.168.0.130 200.200.208.5
```

*Figure 5.2.8.2: Configure static NAT*

Step 3: Configure a static access list to define the addresses to be translated.

```
group10router(config)#access-list 1 permit 192.168.0.0 0.0.0.255
```

*Figure 5.2.8.3: Configure static access list*

Step 4: Enter the command listed in the figure below to configure the dynamic NAT address pool for the router.

```
group10router(config)#ip nat inside source list 1 pool S10-Pool
group10router(config)#
group10router(config)#200.200.208.1 200.200.208.7 netmask 255.255.255.240
```

*Figure 5.2.8.4: Create dynamic NAT pool*

Step 5: Enable OSPF routing and enters router configuration mode. Defines an interface on which OSPF runs and defines the area ID for the interface.

```
group10router(config)#router ospf 1
group10router(config-router)#router-id 1.1.1.1
group10router(config-router)#network 192.168.0.0 0.0.0.255 area 0
group10router(config-router)#network 200.200.208.0 0.0.0.255 area 0
group10router(config-router)#exit
```

*Figure 5.2.8.5: Create OSPF routing for NAT*

## 5.2.9 Access Control List (ACL)

Cisco provides basic traffic filtering capabilities with access control lists (also referred to as access list). Access list can be configured for all routed network protocols (IP, AppleTalk, and so on) to filter the packets of those protocols as the packets pass through a router.

Extended ACLs are used in our case rather than standard ACLs because they provide a greater range of control.

### Create Access Control List (ACL)

Step 1: Create an Extended ACL list for the router named access-list 110.

```
group1@router(config)#ip access-list extended 110
```

*Figure 5.2.9.1: Server Manager Dashboard*

Step 2: Create a rule of statement to block ftp-data and ftp services.

```
access-list 110 deny    tcp any 200.200.208.0 0.0.0.15 eq ftp-data  
access-list 110 deny    tcp any 200.200.208.0 0.0.0.15 eq ftp
```

*Figure 5.2.9.2: Server Manager Dashboard*

Step 3: Create a rule of statement to block access to port 22 which is SSH.

```
access-list 110 deny    tcp any 200.200.208.0 0.0.0.15 eq 22
```

*Figure 5.2.9.3: Server Manager Dashboard*

Step 4: Create a rule of statement to block www services.

```
access-list 110 deny    tcp any host 200.200.208.2 eq www  
access-list 110 deny    tcp any host 200.200.208.4 eq www
```

*Figure 5.2.9.4: Server Manager Dashboard*

Step 4: Create a rule of statement to allow ip address from neighbor router.

```
access-list 110 permit ip any any
```

*Figure 5.2.9.5: Server Manager Dashboard*

### 5.2.10 Samba

Samba is a popular freeware program that allows end users to access and use files, printers and other commonly shared resources on a company's intranet or on the internet.

1. First, install the samba package.

```
[group10@localhost ~]$ sudo dnf install -y samba
[sudo] password for group10:
Last metadata expiration check: 0:52:59 ago on Thu 27 Sep 2018 01:19:07 PM EDT.
Package samba-2:4.8.5-0.fc28.x86_64 is already installed, skipping.
Dependencies resolved.
Nothing to do.
Complete!
[group10@localhost ~]$
```

*Figure 5.2.10.1: show Installing Samba Package*

2. Second, open the port using service file or firewall-cmd

```
[group10@localhost ~]$ sudo firewall-cmd --add-service=samba --permanent
success
[group10@localhost ~]$ sudo firewall-cmd --reload
sudo: firewall-cmd: command not found
[group10@localhost ~]$ sudo firewall-cmd --reload
success
```

*Figure 5.2.10.2: show Open the Port for Samba*

3. Third, enable the access to home directory without samba\_share\_t label

```
[group10@localhost ~]$ sudo setsebool -P samba_enable_home_dirs on
[sudo] password for group10:
```

*5.2.10.3: Figure show to Enable the Access to Home Directory*

- Fourth, add the user access to samba using pdredit. The user must be exists in the Fedora.  
If the user to be added by pdredit does not exist, add the user using useradd

The user is already exists so adds <user> with pdredit

```
[group10@localhost ~]$ sudo pdredit -a group10
new password:
retype new password:
Unix username:      group10
NT username:
Account Flags:      [U      ]
User SID:           S-1-5-21-3616446171-107019852-3001921453-1000
Primary Group SID: S-1-5-21-3616446171-107019852-3001921453-513
Full Name:          Group10
Home Directory:    \\localhost\group10
HomeDir Drive:
Logon Script:
Profile Path:      \\localhost\group10\profile
Domain:            LOCALHOST
Account desc:
Workstations:
Munged dial:
Logon time:         0
Logoff time:        Wed, 06 Feb 2036 10:00:39 EST
Kickoff time:       Wed, 06 Feb 2036 10:00:39 EST
Password last set: Thu, 27 Sep 2018 14:24:52 EDT
Password can change: Thu, 27 Sep 2018 14:24:52 EDT
Password must change: never
Last bad password : 0
Bad password count : 0
Logon hours        : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

*Figure 5.2.10.4: show Add the User with pdredit*

- Fifth, share the home directory for each user and share directory with multiple user.  
Reboot smb and nmb after editing smb.conf.

```
[group10@localhost ~]$ sudo systemctl restart smb nmb
[group10@localhost ~]$
```

*Figure 5.2.10.5: show Share the Home Directory for Each User*

- Lastly, change /var/lib/share's permission to 0777.

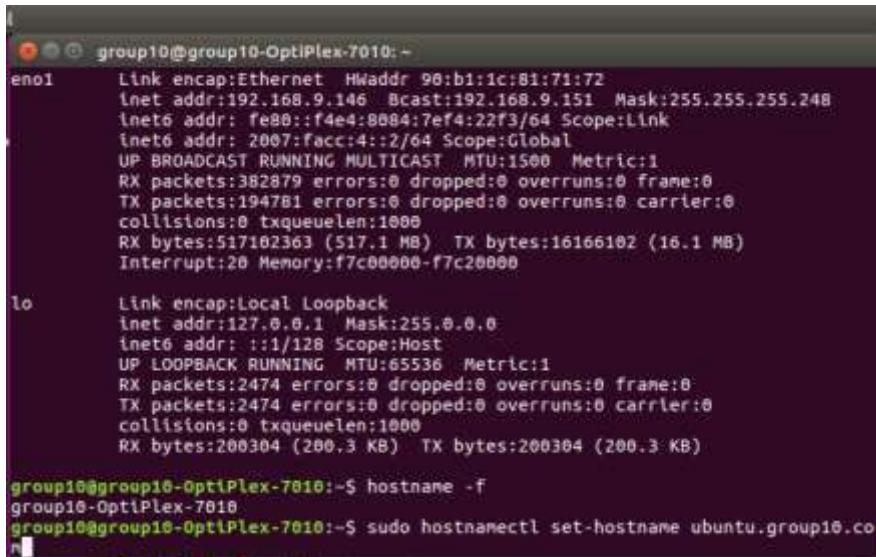
```
[group10@localhost ~]$ sudo mkdir /var/lib/share
mkdir: cannot create directory '/var/lib/share': File exists
[group10@localhost ~]$ sudo chmod 0777 /var/lib/share
```

*5.2.10.6: Figure show the change the permission to 0777*

### 5.2.11 Linux Email Server

Setup RainLoop Webmail on Ubuntu Server.

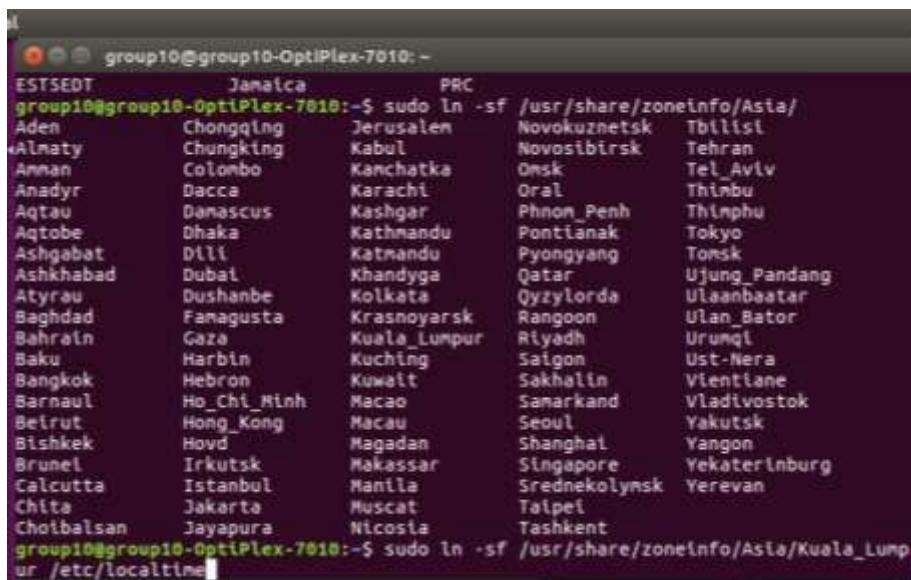
Step 1: Set a correct Hostname for Ubuntu Server.



```
group10@group10-OptiPlex-7010:~  
en0      Link encap:Ethernet HWaddr 90:b1:1c:81:71:72  
          inet addr:192.168.9.146 Bcast:192.168.9.151 Mask:255.255.255.248  
          inet6 addr: fe80::f4e4:8084%7ef4:22f3/64 Scope:Link  
          inet6 addr: 2007:facci:4::2/64 Scope:Global  
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
          RX packets:382879 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:194781 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:517182363 (517.1 MB) TX bytes:16166182 (16.1 MB)  
          Interrupt:20 Memory:f7c00000-f7c20000  
  
lo      Link encap:Local Loopback  
          inet addr:127.0.0.1 Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING MTU:65536 Metric:1  
          RX packets:2474 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:2474 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:200304 (200.3 KB) TX bytes:200304 (200.3 KB)  
  
group10@group10-OptiPlex-7010:~$ hostname -f  
group10-OptiPlex-7010  
group10@group10-OptiPlex-7010:~$ sudo hostnamectl set-hostname ubuntu.group10.co  
n
```

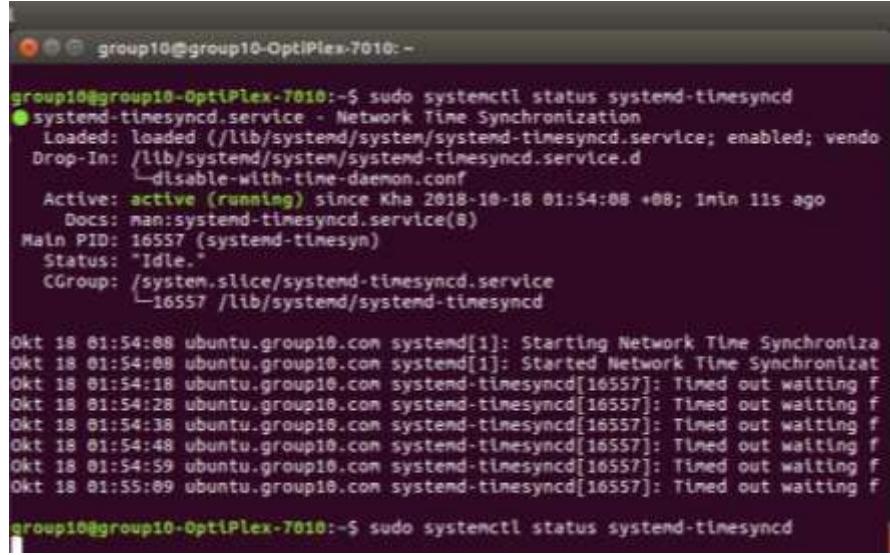
Figure 5.2.11.1: Set hostname for Ubuntu Server.

Step 2: Set System Time



```
EST5EDT    Jamaica      PRC  
group10@group10-OptiPlex-7010:~$ sudo ln -sf /usr/share/zoneinfo/Asia/  
Aden      Chongqing   Jerusalem Novokuznetsk Tbilisi  
Almaty    Chungking   Kabul     Novosibirsk Tehran  
Annan     Colombo     Kathchaka Omsk      Tel_Aviv  
Anadyr    Dacca       Karachi   Oral      Thimbu  
Aqttau    Damascus    Kashgar  Phnom_Penh Thimphu  
Aqtobe    Dhaka       Kathmandu Pontianak Tokyo  
Ashgabat  Dill        Katmandu Pyongyang Tomsk  
Ashkhabad Dubai      Khandya Qatar    Ujung_Pandang  
Atyrau    Dushanbe    Kolkata  Qyzylorda Ulaanbaatar  
Baghdad   Fanagusta   Krasnoyarsk Rangoon  Ulan_Bator  
Bahrain  Gaza        Kuala_Lumpur Riyadh Urumqi  
Baku      Harbin      Kuching   Saigon  Ust-Nera  
Bangkok   Hebron     Kuwait    Sakhalin Vientiane  
Barnaul   Ho_Chi_Minh Macao    Samarkand Vladivostok  
Beirut    Hong_Kong   Macau    Seoul   Yakutsk  
Bishkek   Hovd        Magadan  Shanghai Yangon  
Brunel    Irkutsk    Makassar Singapore Yekaterinburg  
Calcutta  Istanbul   Manila   Srednekolymsk Yerevan  
Chita     Jakarta    Muscat   Taipei  
Choibalsan Jayapura   Nicosia  Tashkent  
group10@group10-OptiPlex-7010:~$ sudo ln -sf /usr/share/zoneinfo/Asia/Kuala_Lumpur /etc/localtime
```

Figure 5.2.11.2: Check your location time info.



```

group10@group10-OptiPlex-7010:~$ sudo systemctl status systemd-timesyncd
● systemd-timesyncd.service - Network Time Synchronization
  Loaded: loaded (/lib/systemd/system/systemd-timesyncd.service; enabled; vendor
  Drop-In: /lib/systemd/system/systemd-timesyncd.service.d
            └─disable-with-time-daemon.conf
  Active: active (running) since Thu 2018-10-18 01:54:08 +08; 1min 11s ago
    Docs: man:systemd-timesyncd.service(8)
   Main PID: 16557 (systemd-timesyncd)
     Status: "Idle."
    CGroup: /system.slice/systemd-timesyncd.service
           └─16557 /lib/systemd/systemd-timesyncd

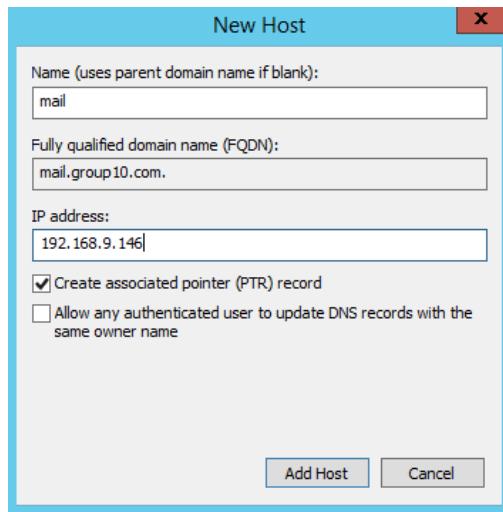
Oct 18 01:54:08 ubuntu.group10.com systemd[1]: Starting Network Time Synchroniza
Oct 18 01:54:08 ubuntu.group10.com systemd[1]: Started Network Time Synchronizat
Oct 18 01:54:18 ubuntu.group10.com systemd-timesyncd[16557]: Timed out waiting f
Oct 18 01:54:28 ubuntu.group10.com systemd-timesyncd[16557]: Timed out waiting f
Oct 18 01:54:38 ubuntu.group10.com systemd-timesyncd[16557]: Timed out waiting f
Oct 18 01:54:48 ubuntu.group10.com systemd-timesyncd[16557]: Timed out waiting f
Oct 18 01:54:59 ubuntu.group10.com systemd-timesyncd[16557]: Timed out waiting f
Oct 18 01:55:09 ubuntu.group10.com systemd-timesyncd[16557]: Timed out waiting f

group10@group10-OptiPlex-7010:~$ sudo systemctl status systemd-timesyncd

```

*Figure 5.2.11.3: Check status your time synchronization with your server.*

Step 3: Set up DNS Records for Your Mail Server in your Windows Server.

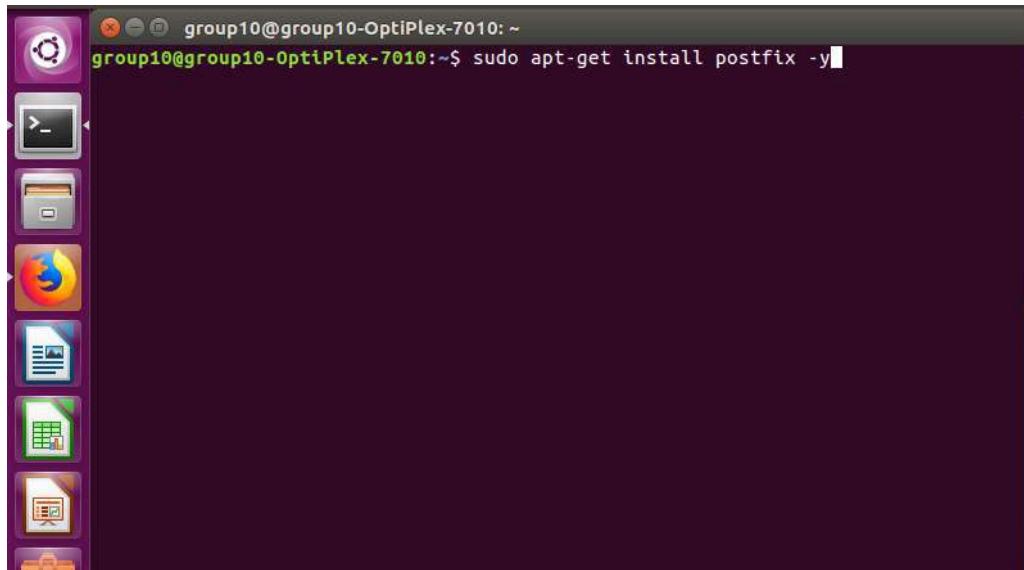


*Figure 5.2.11.4: Set an A record maps a FQDN to an IP address.*



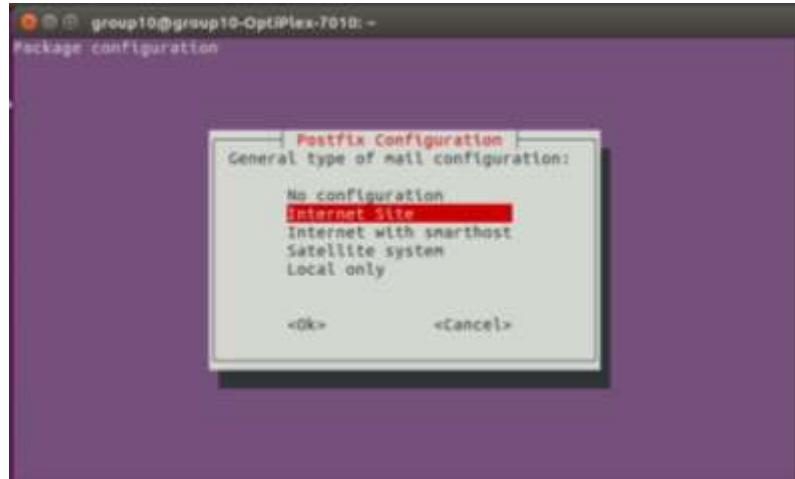
**Figure 5.2.11.5:** Set an MX record tells other MTAs that your mail server mail.group10.com is responsible for email delivery for your domain.

Step 4: Start Installing Postfix. Postfix is a state-of-the-art message transport agent (MTA), aka SMTP server. It's responsible for transporting messages from a mail user agent (MUA or mail client) to a remote SMTP server.



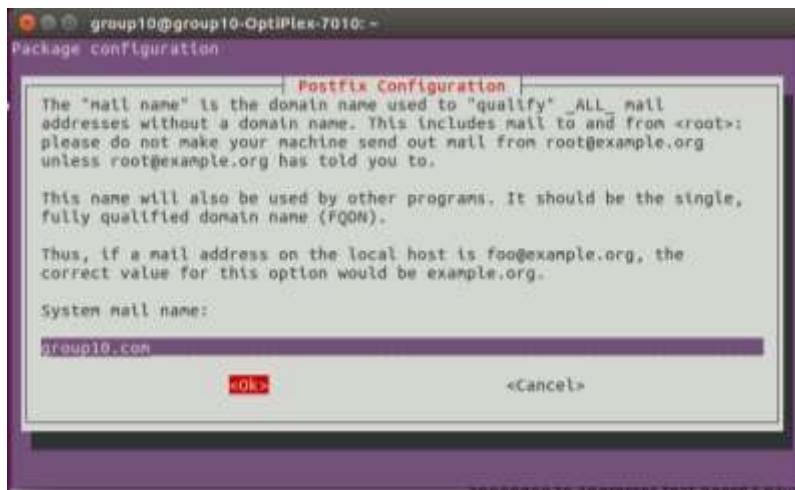
**Figure 5.2.11.6:** Command to run postfix.

Step 5: You will be asked to select a type for mail configuration.



*Figure 5.2.11.7: Selecting Internet Site.*

Step 6: Enter your domain name for the system mail name, i.e. the domain name after @ symbol.  
For example, my email address is [nuqman@group10.com](mailto:nuqman@group10.com)



*Figure 5.2.11.8: Domain name entered.*

Once installed, Postfix will be automatically started and a “/etc/postfix/main.cf” file will be generated.

```

Terminal
group10@group10-OptiPlex-7010:~$ postfix
setting destinations: $myhostname, group10.com, ubuntu.group10.com, localhost.lo
caldomain, localhost
setting relayhost:
+setting mynetworks: 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
setting mailbox_size_limit: 0
setting recipient_delimiter: +
setting inet_interfaces: all
setting inet_protocols: all
/etc/aliases does not exist, creating it.
WARNING: /etc/aliases exists, but does not have a root alias.

Postfix is now set up with a default configuration. If you need to make
changes, edit
/etc/postfix/main.cf (and others) as needed. To view Postfix configuration
values, see postconf(1).

After modifying main.cf, be sure to run '/etc/init.d/postfix reload'.

Running newaliases
Processing triggers for libc-bin (2.23-0ubuntu10) ...
Processing triggers for systemd (229-4ubuntu21.4) ...
Processing triggers for ureadahead (0.100.0-19) ...
Processing triggers for ufw (0.35-0ubuntu2) ...

group10@group10-OptiPlex-7010:~$
```

*Figure 5.2.11.9: Show “/etc/postfix/main.cf” file is generated.*

Now we can check Postfix version with this command:

```
group10@group10-OptiPlex-7010:~$ sudo postconf mail_version
mail_version = 3.1.0
```

*Figure 5.2.11.10: Show mail version.*

The netstat utility tells us that the Postfix master process is listening on TCP port 25.

```
group10@group10-OptiPlex-7010:~$ sudo netstat -lnpt
sudo: unable to resolve host ubuntu.group10.com: Connection timed out
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
PID/Program name
tcp      0      0 127.0.1.1:53              0.0.0.0:*
5715/dnsmasq
tcp      0      0 127.0.0.1:631             0.0.0.0:*
15830/cupsd
tcp      0      0 0.0.0.0:25              0.0.0.0:*
18439/master
tcp6     0      0 ::1:631                 ::*:*
15830/cupsd
tcp6     0      0 ::::25                  ::*:*
18439/master
```

*Figure 5.2.11.11: Netstat show what port is active and listening.*

We can use nmap to scan open ports on our server.

```
group10@group10-OptiPlex-7010:~$ sudo nmap 192.168.9.146
Starting Nmap 7.01 ( https://nmap.org ) at 2018-10-18 03:54 +08
Nmap scan report for 192.168.9.146
Host is up (0.000010s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
25/tcp    open  smtp

Nmap done: 1 IP address (1 host up) scanned in 1.69 seconds
group10@group10-OptiPlex-7010:~$
```

*Figure 5.2.11.12: Run the following command on a separate computer such as your personal computer.*

Step 7: In root, you must generate your own self-signed certificate by running the following command:

```
root@ubuntu:/home/group10
root@ubuntu:/home/group10# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -
keyout /etc/ssl/private/group10.key -out /etc/ssl/certs/group10.pem
```

*Figure 5.2.11.3: A pairs of key and certificates created based on RSA encryption 2048 bit.*

You will need to enter some info such as:

```
root@ubuntu:/home/group10
root@ubuntu:/home/group10# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -
keyout /etc/ssl/private/group10.key -out /etc/ssl/certs/group10.pem
Generating a 2048 bit RSA private key
...+++
.....+++
writing new private key to '/etc/ssl/private/group10.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:MY
State or Province Name (full name) [Some-State]:Melaka
Locality Name (eg, city) []:Durian Tunggal
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Group10
Organizational Unit Name (eg, section) []:Group10
Common Name (e.g. server FQDN or YOUR name) []:group10.com
Email Address []:root@group10.com
root@ubuntu:/home/group10#
```

*Figure 5.2.11.14: Information that will incorporated into the certificate request.*

Step 8: Configuring Postfix. To send emails from a desktop email client, we need to enable the submission service of Postfix so that the email client can submit emails to Postfix SMTP server.



Figure 5.2.11.15: Edit the master.cf file.

In submission section, uncomment or add the following lines. Please allow at least one whitespace (tab or spacebar) before -o.

```
# =====
smtp      inet  n   -     y     -     -          smtpd
#smtp      inet  n   -     y     -     1          postscreen
#smtpd     pass  -   -     y     -     -          smtpd
#dnsblog   unix  -   -     y     -     0          dnsblog
#tlsproxy  unix  -   -     y     -     0          tlsproxy
#submission  inet  n   -     y     -     -          smtpd
-o syslog_name=postfix/submission
-o smtpd_tls_security_level=encrypt
-o smtpd_tls_wrappermode=no
-o smtpd_sasl_auth_enable=yes
-o smtpd_relay_restrictions=permit_sasl_authenticated,reject
-o smtpd_recipient_restrictions=permit_mynetworks,permit_sasl_authenticated,rej$ 
-o smtpd_sasl_type=dovecot
-o smtpd_sasl_path=private/auth

# -o syslog_name=postfix/submission

^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
```

The screenshot shows the 'nano' text editor displaying the '/etc/postfix/master.cf' file. The 'submission' section is highlighted with a yellow background. It contains several configuration options starting with '-o'. The bottom of the screen shows the standard nano key bindings.

Figure 5.2.11.16: The above configuration enables the submission daemon of Postfix and requires TLS encryption.

Step 9: Next, we need to let Postfix know where TLS certificate and private key are. Edit main.cf file.

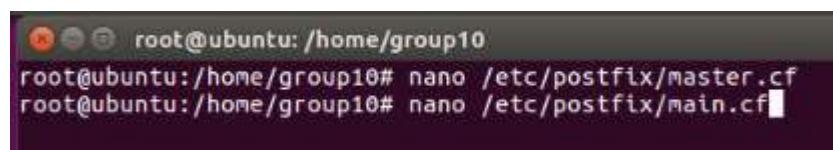


Figure 5.2.11.17: Edit the main.cf file.

```

root@ubuntu:/home/group10
GNU nano 2.5.3           File: /etc/postfix/main.cf          Modified

smtpd_tls_cert_file=/etc/ssl/certs/group10.pem
smtpd_tls_key_file=/etc/ssl/private/group10.key
smtpd_tls_security_level=may
smtpd_tls_protocols = !SSLv2, !SSLv3 !TLSv1
smtpd_tls_loglevel = 1
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache

smtp_tls_security_level = may
smtp_tls_loglevel = 1
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
# information on enabling SSL in the smtp client.

smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_users一会
myhostname = ubuntu.group10.com
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases

^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 5.2.11.18: Edit the TLS parameter as follows.*

```
root@ubuntu:/home/group10# postfix reload
```

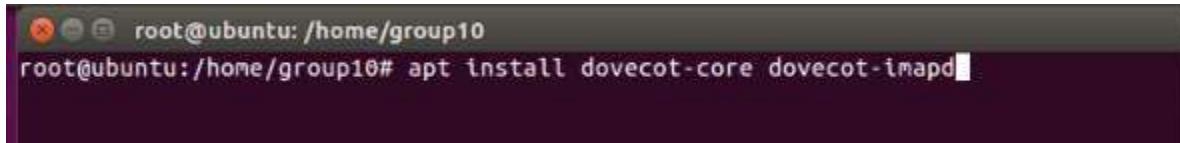
*Figure 5.2.11.19: Save and close the file. Then reload Postfix.*

If you run the following command “netstat -lntp”, you will see:

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
TCP	0	0	127.0.1.1:53	0.0.0.0:*	LISTEN
1054/dnsmasq	0	0	127.0.0.1:631	0.0.0.0:*	LISTEN
3150/cupsd	0	0	0.0.0.0:25	0.0.0.0:*	LISTEN
1599/master	0	0	0.0.0.0:587	0.0.0.0:*	LISTEN
1599/master	0	0	0.0.0.0:587	0.0.0.0:*	LISTEN
tcp6	0	0	:::631	:::*	LISTEN
3150/cupsd	0	0	:::25	:::*	LISTEN
1599/master	0	0	:::587	:::*	LISTEN
1599/master	0	0	:::587	:::*	LISTEN

*Figure 5.2.11.20: port 587 is now open.*

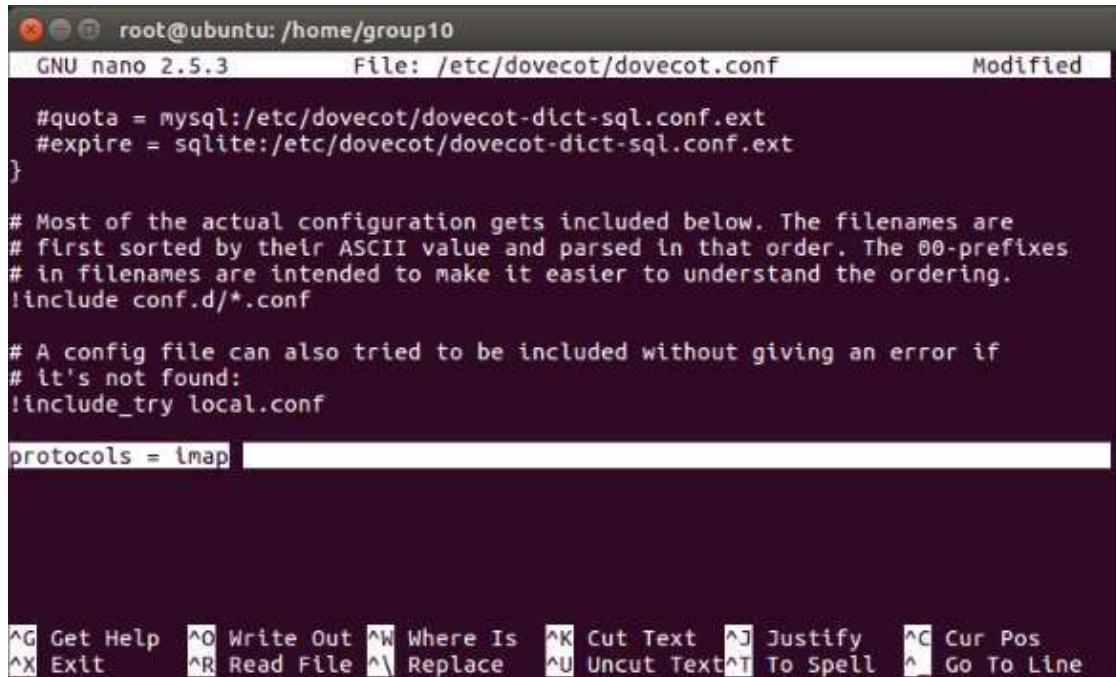
Step 10: Installing Dovecot IMAP Server.



```
root@ubuntu:/home/group10
root@ubuntu:/home/group10# apt install dovecot-core dovecot-imapd
```

Figure 5.2.11.21: Install Dovecot core package and the IMAP daemon package.

Step 11: Configuring Dovecot by editing it in “**dovecot.conf**”.



```
root@ubuntu:/home/group10
GNU nano 2.5.3      File: /etc/dovecot/dovecot.conf      Modified

#quota = mysql:/etc/dovecot/dovecot-dict-sql.conf.ext
#expire = sqlite:/etc/dovecot/dovecot-dict-sql.conf.ext
}

# Most of the actual configuration gets included below. The filenames are
# first sorted by their ASCII value and parsed in that order. The 00-prefixes
# in filenames are intended to make it easier to understand the ordering.
!include conf.d/*.conf

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

protocols = imap
```

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

Figure 5.2.11.22: Add the following line to enable IMAP protocol.

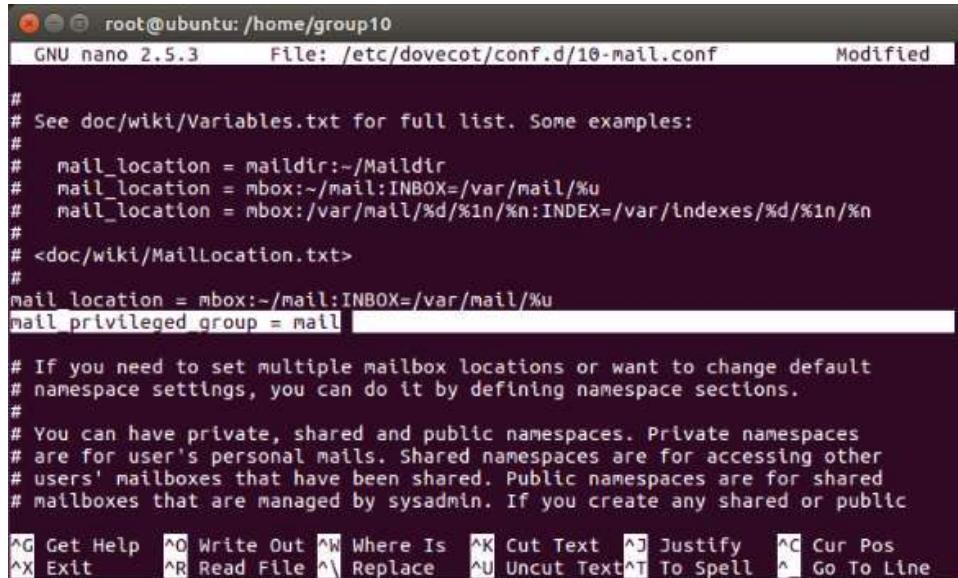
Step 12: Configuring Mailbox Location. Each user’s emails is stored in a single file /var/mail/username.



```
root@ubuntu:/home/group10
root@ubuntu:/home/group10# postconf mail_spool_directory
mail_spool_directory = /var/mail
root@ubuntu:/home/group10#
```

Figure 5.2.11.23: Sample output of mail spool directory.

The config file for mailbox location is **/etc/dovecot/conf.d/10-mail.conf**.



```
root@ubuntu:/home/group10
GNU nano 2.5.3      File: /etc/dovecot/conf.d/10-mail.conf      Modified

#
# See doc/wiki/Variables.txt for full list. Some examples:
#
#   mail_location = maildir:~/Maildir
#   mail_location = mbox:~/mail:INBOX=/var/mail/%u
#   mail_location = mbox:/var/mail/%d/%n/%n:INDEX=/var/indexes/%d/%n/%n
#
# <doc/wiki/MailLocation.txt>
#
mail location = mbox:~/mail:INBOX=/var/mail/%u
mail_privileged_group = mail

#
# If you need to set multiple mailbox locations or want to change default
# namespace settings, you can do it by defining namespace sections.
#
# You can have private, shared and public namespaces. Private namespaces
# are for user's personal mails. Shared namespaces are for accessing other
# users' mailboxes that have been shared. Public namespaces are for shared
# mailboxes that are managed by sysadmin. If you create any shared or public

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

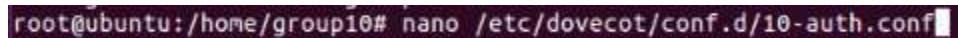
Figure 5.2.11.24: Add the following line in the file.



```
root@ubuntu:/home/group10
root@ubuntu:/home/group10# gpasswd -a dovecot mail
Adding user dovecot to group mail
```

Figure 5.2.11.25: Add dovecot to the mail group so that Dovecot can read the INBOX.

Step 13: Configuring Authentication Mechanism.



```
root@ubuntu:/home/group10# nano /etc/dovecot/conf.d/10-auth.conf
```

Figure 5.2.11.26: Edit the authentication config file.



```
root@ubuntu:/home/group10
GNU nano 2.5.3      File: /etc/dovecot/conf.d/10-auth.conf      Modified

##
## Authentication processes
##

# Disable LOGIN command and all other plaintext authentications unless
# SSL/TLS is used (LOGINDISABLED capability). Note that if the remote IP
# matches the local IP (ie. you're connecting from the same computer), the
# connection is considered secure and plaintext authentication is allowed.
# See also ssl=required setting.
disable_plaintext_auth = yes
```

Figure 5.2.11.27: Uncomment the following line “`disable_plaintext_auth = yes`”.

```

root@ubuntu:/home/group10
GNU nano 2.5.3      File: /etc/dovecot/conf.d/10-auth.conf      Modified

## Authentication processes
##

# Disable LOGIN command and all other plaintext authentications unless
# SSL/TLS is used (LOGINDISABLED capability). Note that if the remote IP
# matches the local IP (ie. you're connecting from the same computer), the
# connection is considered secure and plaintext authentication is allowed.
# See also ssl=required setting.
disable_plaintext_auth = yes
auth_username_format = %n

```

*Figure 5.2.11.28: Add “auth\_username\_format = %n” if you want to use full email address (username@your-domain.com) to login.*

```

root@ubuntu:/home/group10
GNU nano 2.5.3      File: /etc/dovecot/conf.d/10-auth.conf      Modified

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

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

```

*Figure 5.2.11.29: Add “plain login” to use another common authentication mechanism instead of PLAIN authentication mechanism.*

Step 14: Configuring SSL/TLS Encryption. Edit SSL/TLS config file in “/etc/dovecot/conf.d/10-ssl.conf” by changing ssl = no to ssl = required.

```

root@ubuntu:/home/group10
GNU nano 2.5.3      File: /etc/dovecot/conf.d/10-ssl.conf      Modified

## SSL settings
##

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

# PEM encoded X.509 SSL/TLS certificate and private key. They're opened before
# dropping root privileges, so keep the key file unreadable by anyone but
# root. Included doc/mkcert.sh can be used to easily generate self-signed
# certificate, just make sure to update the domains in dovecot-openssl.cnf
ssl_cert = </etc/ssl/certs/group10.pem
ssl_key = </etc/ssl/private/group10.key

# If key file is password protected, give the password here. Alternatively
# give it when starting dovecot with -p parameter. Since this file is often
# world-readable, you may want to place this setting instead to a different
# root owned 6000 file by using ssl_key_password = <path>
ssl_key_password =

# PEM encoded trusted certificate authority. Set this only if you intend to use
# ssl_verify_client_cert=yes. The file should contain the CA certificate(s)
# followed by the matching CRL(s); (e.g. ssl_ca = </etc/ssl/certs/ca.pem>
#ssl_ca =

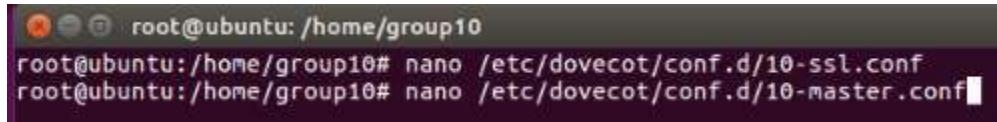
# Require that CRL check succeeds for client certificates.
#ssl_require_crl = yes

# Directory and/or file for trusted SSL CA certificates. These are used only
# for certificate verification.
#ssl_ca_dir =

```

*Figure 5.2.11.30: specify the location of your SSL/TLS cert and private key. Don’t leave out < character.*

Step 15: Configure SASL Authentication Between Postfix and Dovecot.



```
root@ubuntu:/home/group10
root@ubuntu:/home/group10# nano /etc/dovecot/conf.d/10-ssl.conf
root@ubuntu:/home/group10# nano /etc/dovecot/conf.d/10-master.conf
```

Figure 5.2.11.31: Edit the following file.



```
root@ubuntu:/home/group10
GNU nano 2.5.3           File: /etc/dovecot/conf.d/10-master.conf      Modified

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

unix_listener /var/spool/postfix/private/auth {
    mode = 0660
    user = postfix
    group = postfix
}
```

Figure 5.2.11.32: Change “service auth” section to the following so that Postfix can find the Dovecot authentication server.

Step 16: Auto-create Sent and Trash Folder.



```
root@ubuntu:/home/group10
root@ubuntu:/home/group10# nano /etc/dovecot/conf.d/10-ssl.conf
root@ubuntu:/home/group10# nano /etc/dovecot/conf.d/10-master.conf
root@ubuntu:/home/group10# nano /etc/dovecot/conf.d/15-mailboxes.conf
root@ubuntu:/home/group10# nano /etc/dovecot/conf.d/15-mailboxes.conf
```

Figure 5.2.11.33: Edit the below config file.

```

root@ubuntu:/home/group10
GNU nano 2.5.3          File: /etc/dovecot/conf.d/15-mailboxes.conf      Modified

# \Junk    - This mailbox is where messages deemed to be junk mail
# are held.
# \Sent    - This mailbox is used to hold copies of messages that
# have been sent.
# \Trash   - This mailbox is used to hold messages that have been
# deleted.
#
# comment:
# Defines a default comment or note associated with the mailbox. This
# value is accessible through the IMAP METADATA mailbox entries
# "/shared/comment" and "/private/comment". Users with sufficient
# privileges can override the default value for entries with a custom
# value.

# NOTE: Assumes "namespace inbox" has been defined in 10-mail.conf.

namespace inbox {
    # These mailboxes are widely used and could perhaps be created automatically:
    mailbox Drafts {
        special_use = \Drafts
    }
    mailbox Junk {
        special_use = \Junk
    }
    mailbox Trash {
        auto = create
        special_use = \Trash
    }
}

# For \Sent mailboxes there are two widely used names. We'll mark both of

^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 5.2.11.34: To auto create a folder, simply add the following line in the mailbox section.*

```

root@ubuntu:/home/group10
root@ubuntu:/home/group10# systemctl restart dovecot
root@ubuntu:/home/group10# systemctl restart postfix
root@ubuntu:/home/group10# 

```

*Figure 5.2.11.35: Restart your dovecot and postfix.*

Step 17: Download and Install Rainloop Webmail.

```

root@ubuntu:/home/group10/rainloop
root@ubuntu:/home/group10# mkdir rainloop

```

*Figure 5.2.11.36: make a directory for rainloop.*

```
root@ubuntu:/home/group10# cd rainloop
root@ubuntu:/home/group10/rainloop# curl -s http://repository.rainloop.net/installer.php | php
The program 'curl' is currently not installed. You can install it by typing:
apt install curl
root@ubuntu:/home/group10/rainloop# sudo apt install curl
sudo: unable to resolve host ubuntu.group10.com: Connection timed out
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  curl
0 upgraded, 1 newly installed, 0 to remove and 13 not upgraded.
Need to get 138 kB of archives.
After this operation, 339 kB of additional disk space will be used.
Get:1 http://my.archive.ubuntu.com/ubuntu xenial-updates/main amd64 curl amd64 7.47.0-1ubuntu2.9
[138 kB]
Fetched 138 kB in 1s (104 kB/s)
Selecting previously unselected package curl.
(Reading database ... 178967 files and directories currently installed.)
Preparing to unpack .../curl_7.47.0-1ubuntu2.9_amd64.deb ...
Unpacking curl (7.47.0-1ubuntu2.9) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up curl (7.47.0-1ubuntu2.9) ...
You have new mail in /var/mail/root
root@ubuntu:/home/group10/rainloop#
```

Figure 5.2.11.37: Install curl.

```
root@ubuntu:/home/group10/rainloop# curl -s http://repository.rainloop.net/installer.php | php
#!/usr/bin/env php

[RainLoop Webmail Installer]

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

* [Success] Installation is finished!
```

Figure 5.2.11.38: Download the latest RainLoop community edition.

```
root@ubuntu:/home/group10/rainloop# cd ..
root@ubuntu:/home/group10# mv rainloop /var/www/
```

Figure 5.2.11.39: rainloop directory to /var/www/.

```
root@ubuntu:/home/group10# chown www-data:www-data /var/www/rainloop/ -R
```

Figure 5.2.11.40: Now set web server user (www-data) as the owner.

Step 18: Configure Virtual Host for Rainloop.

```
root@ubuntu:/home/group10# nano /etc/apache2/sites-available/rainloop.conf
```

Figure 5.2.11.41: create the virtual host file with the following command.



```
root@ubuntu:/home/group10
GNU nano 2.5.3          File: /etc/apache2/sites-available/rainloop.conf      Modified

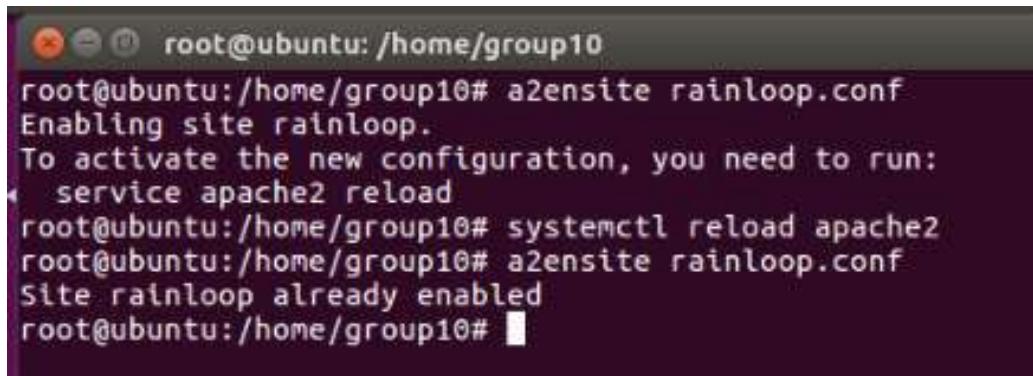
<VirtualHost *:80>
    ServerName ubuntu.group10.com
    DocumentRoot "/var/www/rainloop/"
    ServerAdmin admin@group10.com

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

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

</VirtualHost>
```

Figure 5.2.11.42: Put the following text into the file.



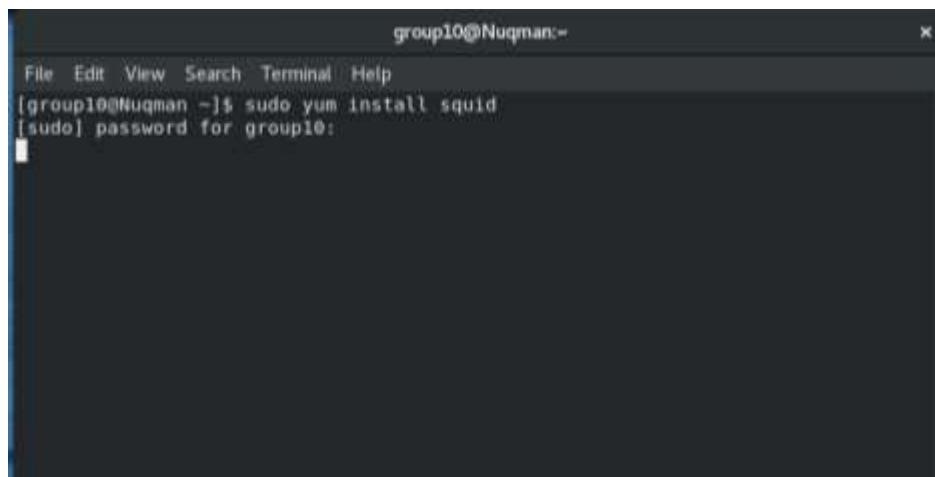
```
root@ubuntu:/home/group10#
root@ubuntu:/home/group10# a2ensite rainloop.conf
Enabling site rainloop.
To activate the new configuration, you need to run:
  service apache2 reload
root@ubuntu:/home/group10# systemctl reload apache2
root@ubuntu:/home/group10# a2ensite rainloop.conf
Site rainloop already enabled
root@ubuntu:/home/group10# █
```

Figure 5.2.11.43: Save and close file, then enable this virtual host and reload apache.

### 5.2.12 Proxy Server on Fedora 28

Proxy is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity.

Step 1: Install squid on your server and wait until it completion

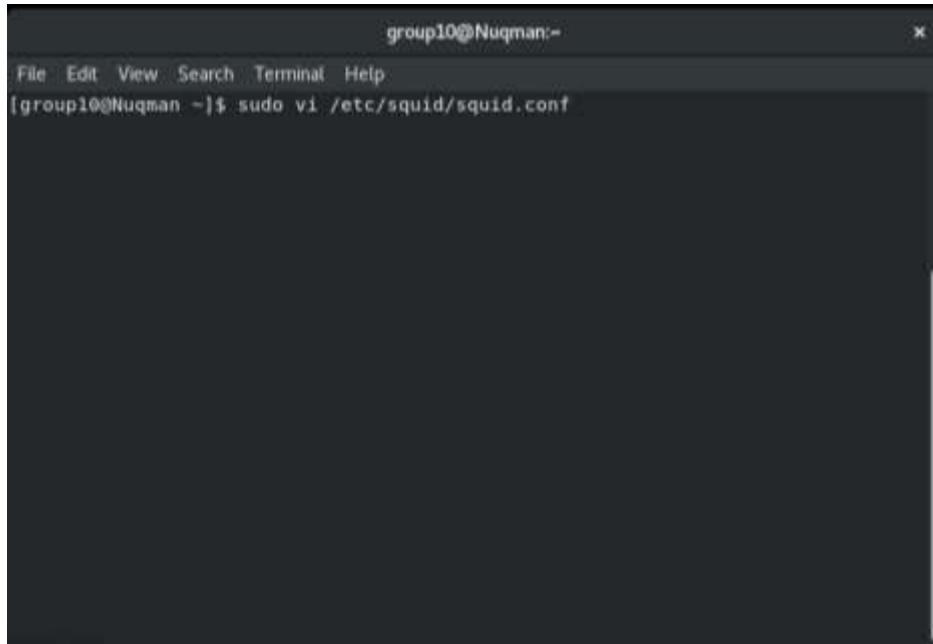


*Figure 5.2.12.1: Squid Installation Command.*

A screenshot of a terminal window showing the output of a yum install command. The output lists various packages being installed, their versions, and their status (e.g., 3/6). It includes packages like perl-Math-BigInt, perl-DBI, libecap, squid, and perl-Digest-SHA. The "Installed:" section shows the packages that have been successfully installed. The message "Complete!" is at the bottom of the output.

*Figure 5.2.12.2: Squid Installation Complete.*

Step 2: Edit file squid in “/etc/squid/squid.conf”. It can either use **vi** or **nano** command.



*Figure 5.2.12.3: Command to enter squid configuration.*

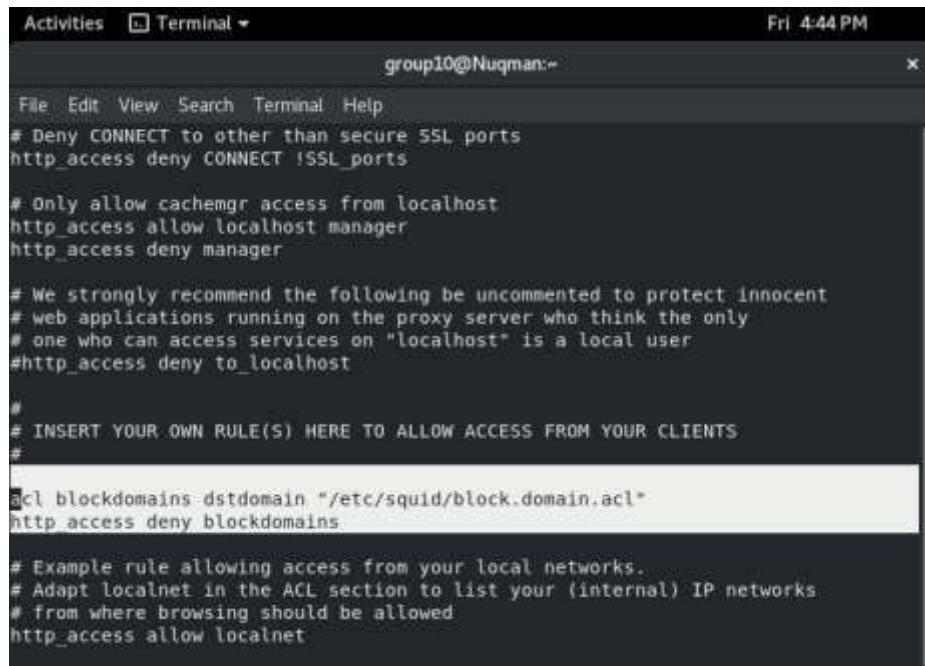
Step 3: Edit and uncomment the comment under “And finally deny all other access to this proxy” with “**http\_access allow all**”.

A screenshot of a terminal window titled "group10@Nuqman:~". The window shows a portion of the "/etc/squid/squid.conf" file. A line of code "http access allow all" is highlighted with a yellow background, indicating it has been uncommented. The rest of the file contains various configuration directives like "acl", "http\_access", and "http\_port".

```
#  
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS  
  
acl blockdomains dstdomain "/etc/squid/block.domain.acl"  
http_access deny blockdomains  
  
# Example rule allowing access from your local networks.  
# Adapt localnet in the ACL section to list your (internal) IP networks  
# from where browsing should be allowed  
http_access allow localnet  
http_access allow localhost  
  
# And finally deny all other access to this proxy  
http access allow all  
  
# Squid normally listens to port 3128  
http_port 3128  
  
# Uncomment and adjust the following to add a disk cache directory.  
#cache_dir ufs /var/spool/squid 100 16 256  
  
# Leave core dumps in the first cache dir
```

*Figure 5.2.12.4: Enable http access to all.*

Step 4: Create file to block wanted domain



```
Activities Terminal Fri 4:44 PM
group10@Nugman:~ 
File Edit View Search Terminal Help
# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager

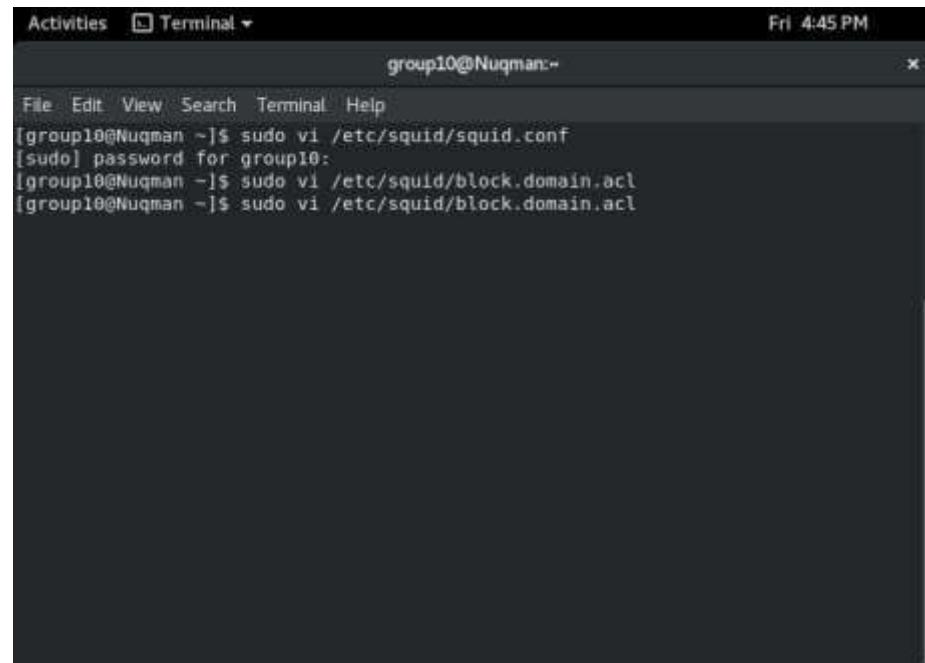
# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
acl blockdomains dstdomain "/etc/squid/block.domain.acl"
http_access deny blockdomains

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

*Figure 5.2.12.5: Now it can block any accessible domain in “block.domain.acl” file.*

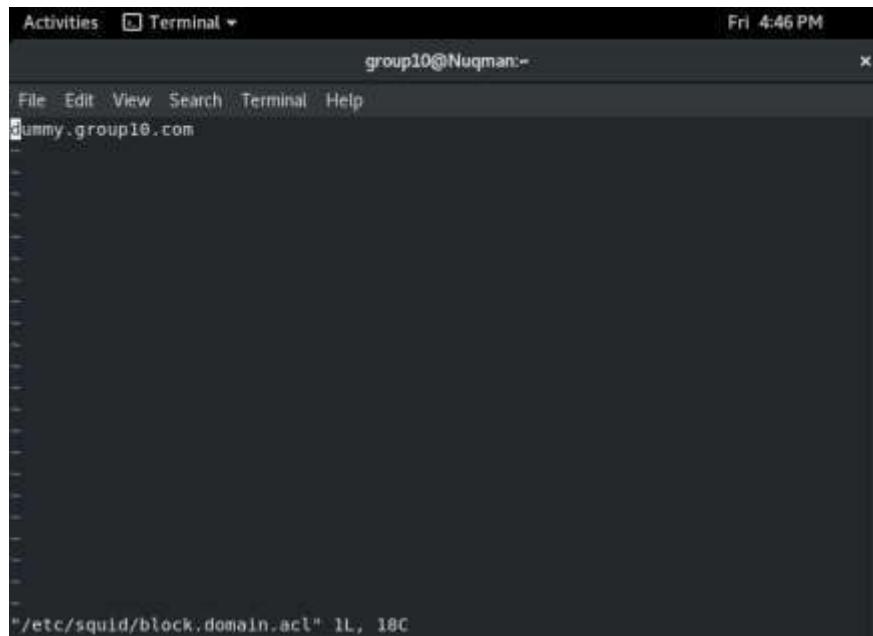
Step 5: Access file “block.domain.acl”



```
Activities Terminal Fri 4:45 PM
group10@Nugman:~ 
File Edit View Search Terminal Help
[group10@Nugman ~]$ sudo vi /etc/squid/squid.conf
[sudo] password for group10:
[group10@Nugman ~]$ sudo vi /etc/squid/block.domain.acl
[group10@Nugman ~]$ sudo vi /etc/squid/block.domain.acl
```

*Figure 5.2.12.6: Command to enter blocked domain file.*

Step 6: Insert any domain you want to block by click “**i**” to insert text. After domain inserted, click button “**esc**”, then write “**:wq**” to save and quit



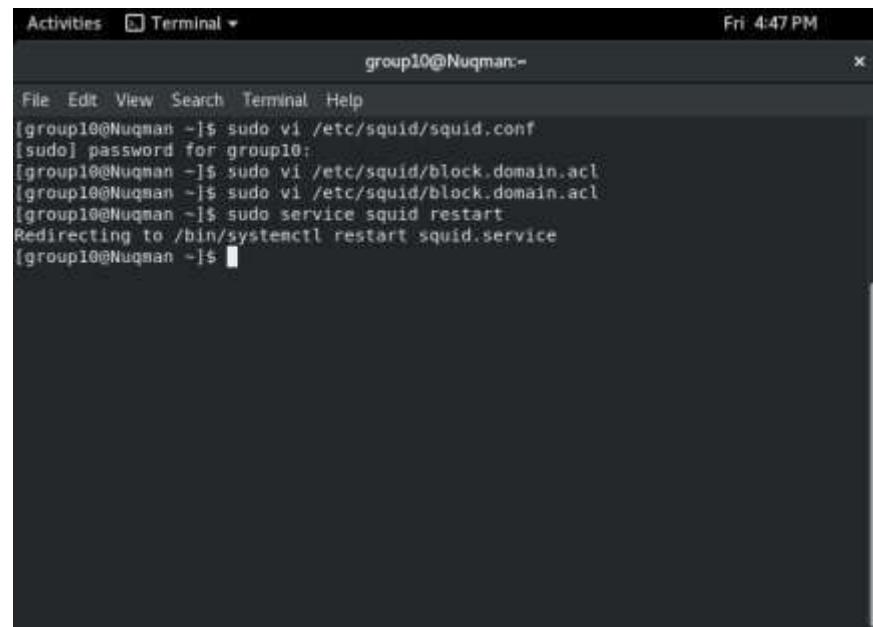
A screenshot of a terminal window titled "Terminal". The window shows a command-line interface with the user "group10@Nuqman:~". The terminal displays the following text:

```
File Edit View Search Terminal Help
dummy.group10.com

"/etc/squid/block.domain.acl" 1L, 18C
```

*Figure 5.2.12.7: Shows website “dummy.group10.com” is in block list.*

Step 7: Now restart the squid services.



A screenshot of a terminal window titled "Terminal". The window shows a command-line interface with the user "group10@Nuqman:~". The terminal displays the following text:

```
File Edit View Search Terminal Help
(group10@Nuqman ~]$ sudo vi /etc/squid/squid.conf
[sudo] password for group10:
[group10@Nuqman ~]$ sudo vi /etc/squid/block.domain.acl
[group10@Nuqman ~]$ sudo vi /etc/squid/block.domain.acl
[group10@Nuqman ~]$ sudo service squid restart
Redirecting to /bin/systemctl restart squid.service
[group10@Nuqman ~]$
```

*Figure 5.2.12.8: Restart squid services.*

## 5.2.13 Web, SSL & Virtual Hosting

### Install Web Server on Windows Server 2012 r2

A website is a collection of publicly accessible, interlinked Web pages that share a single domain name. Websites can be created and maintained by an individual, group, business or organization to serve a variety of purposes. Together, all publicly accessible websites constitute the World Wide Web. A website is also known as a web presence.

Step 1: Add roles on server by select Web Server (IIS) Services

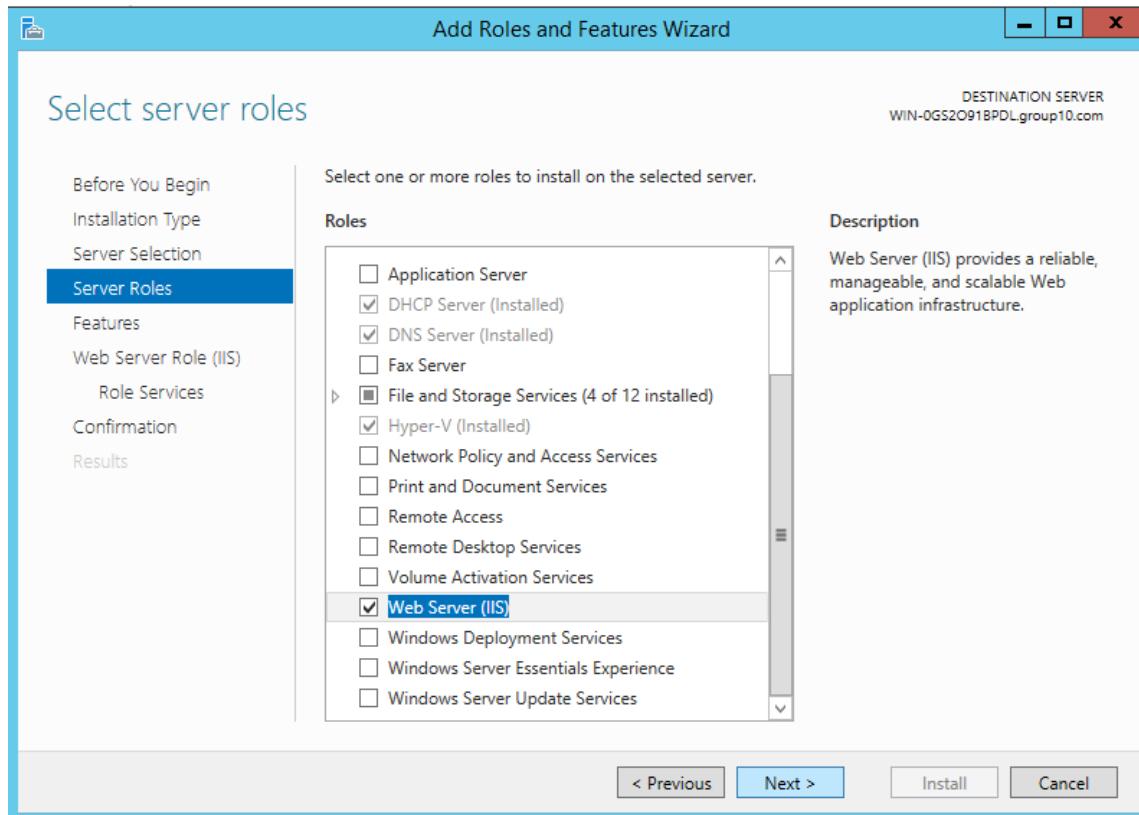


Figure 5.2.13.1: Add Web Server (IIS) role

Step 2: Click on NEXT to proceed with installation

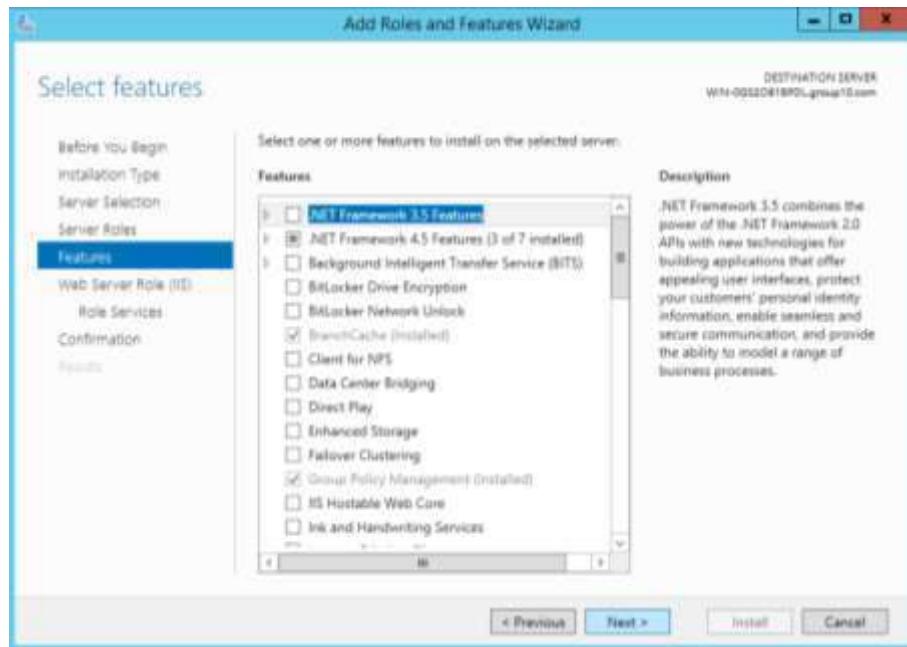


Figure 5.2.13.2: Web Server (IIS) features

Step 3: Check the “IIS Management Console” box under the “Management Tools” and check “IIS 6 WMI Compatibility” box under “IIS 6 Management Compatibility”

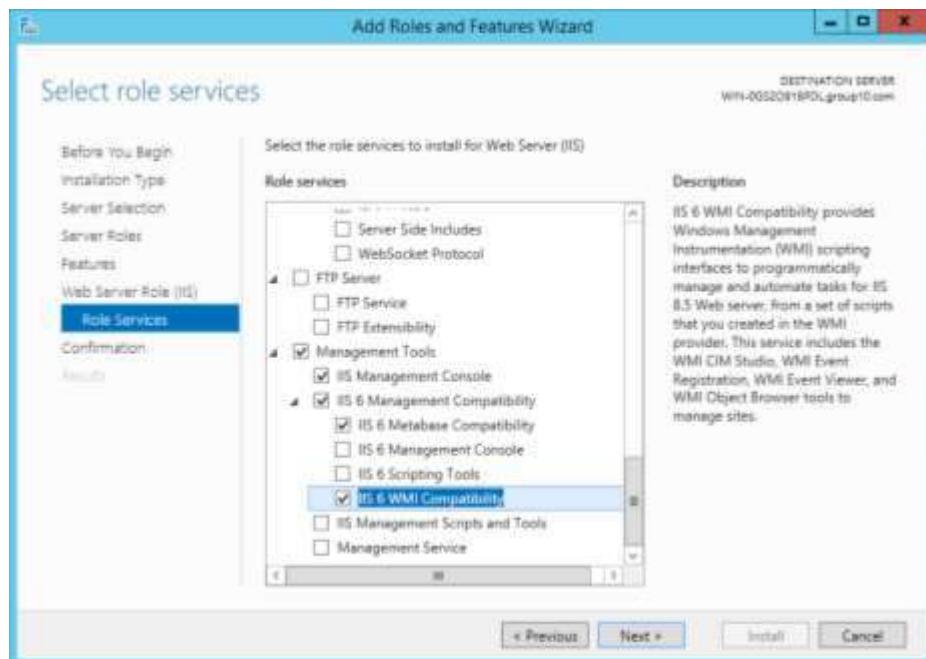
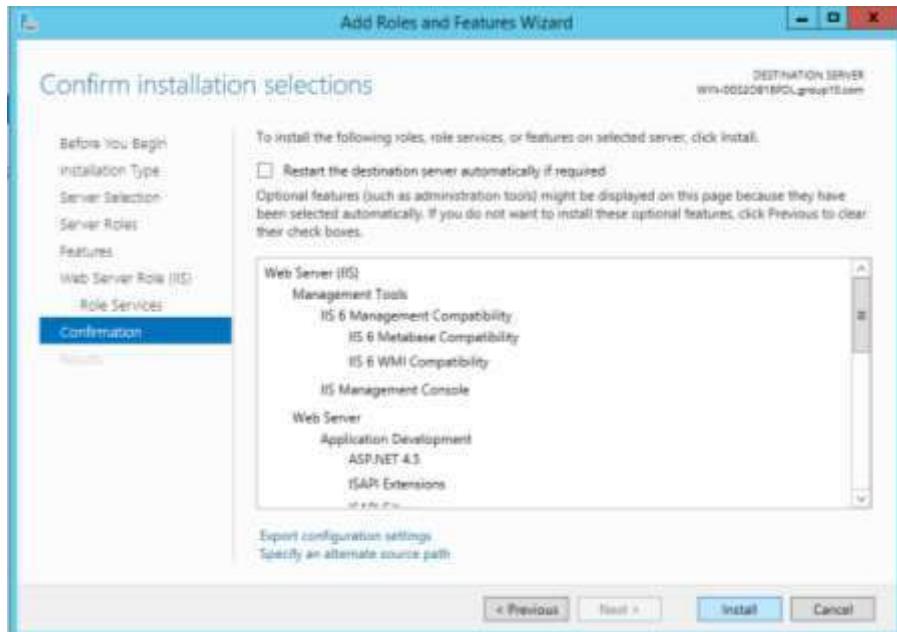


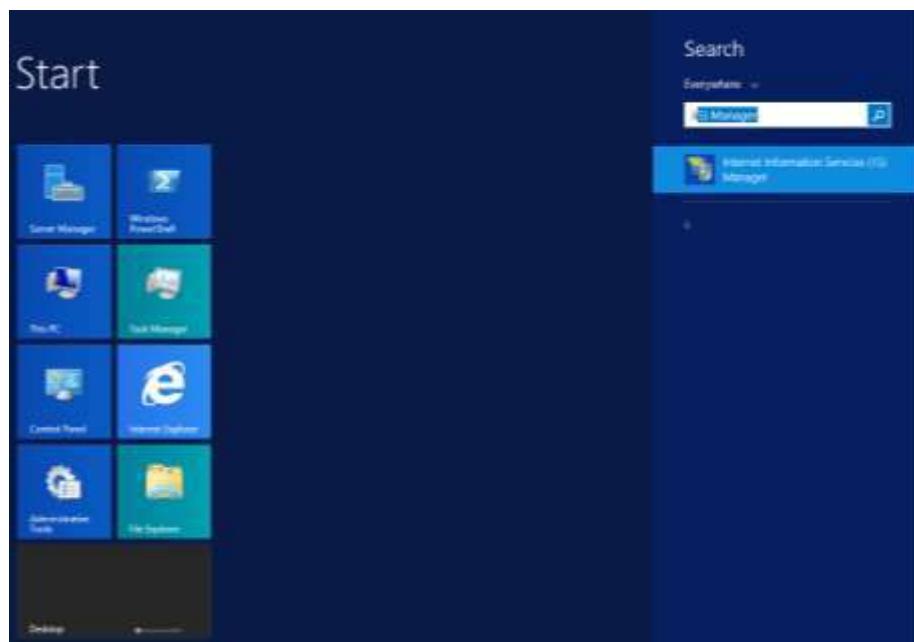
Figure 5.2.13.3: Web Server (IIS) role services

Step 4: Confirm the Installation of Web Server by clicking Install and wait until the installation process finish.



**Figure 5.2.13.4: Install Web Server (IIS)**

Step 5: To open the web server manager, Search IIS Manager in your windows server.



**Figure 5.2.13.5: Opening Progress**

Step 6: Open up the IIS Manager and right click on Sites, then click Add Website.

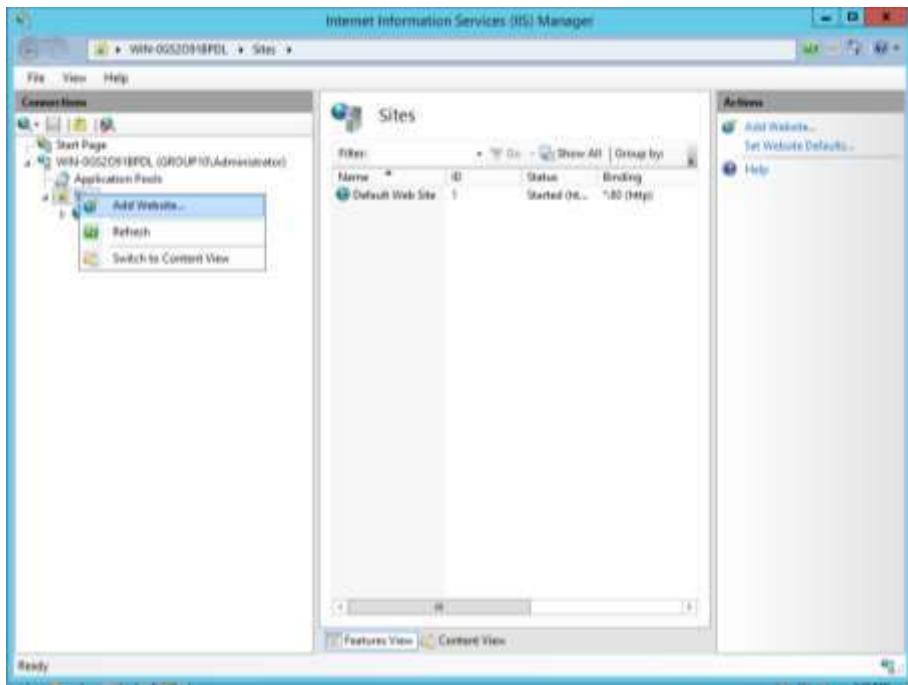


Figure 5.2.13.6: IIS Manager

Step 7: Fill in the Site Name, path and IP address and click OK

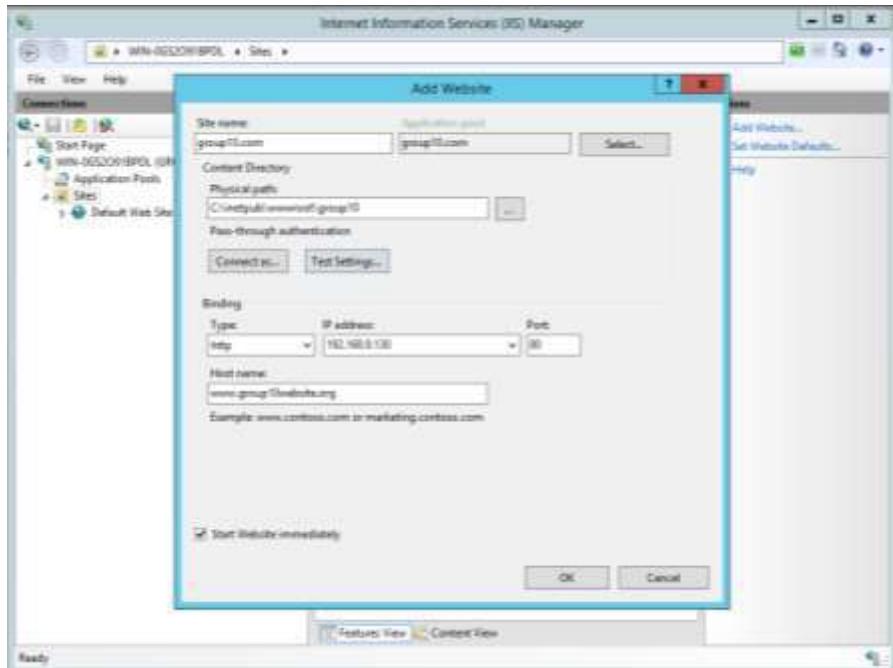


Figure 5.2.13.7: Adding Website

Step 8: At the IIS Manager click on your created website “group10.com” and click on “Default Document”.

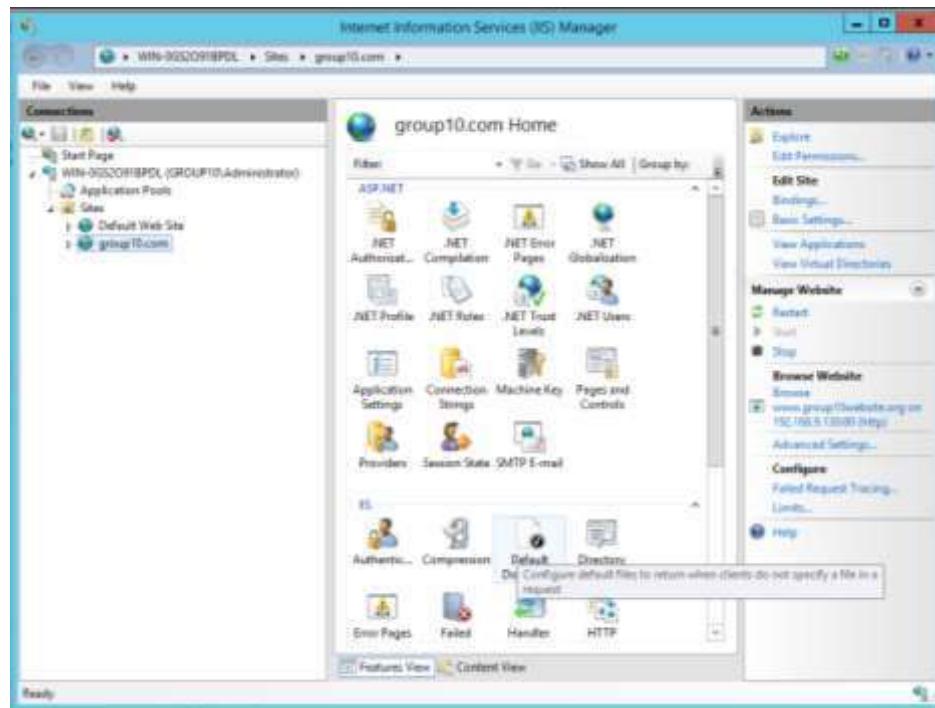


Figure 5.2.13.8: Adding Default Document

Step 9: Click on Add and fill the name for Default Document

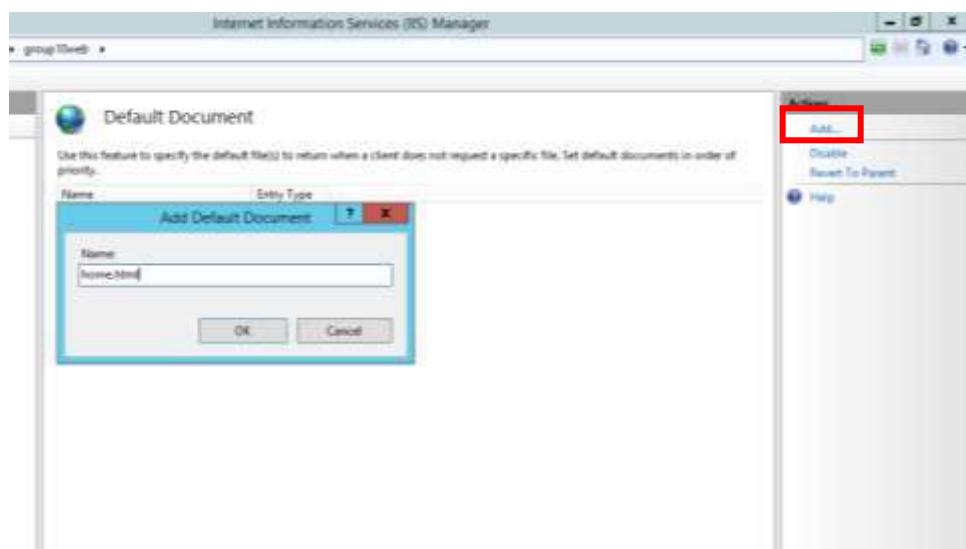


Figure 5.2.13.9: Adding Default Document

Step 10: Open the File Explorer and navigate to ( C:\inetpub\’desired folder’) and create and HTML file for the Website.

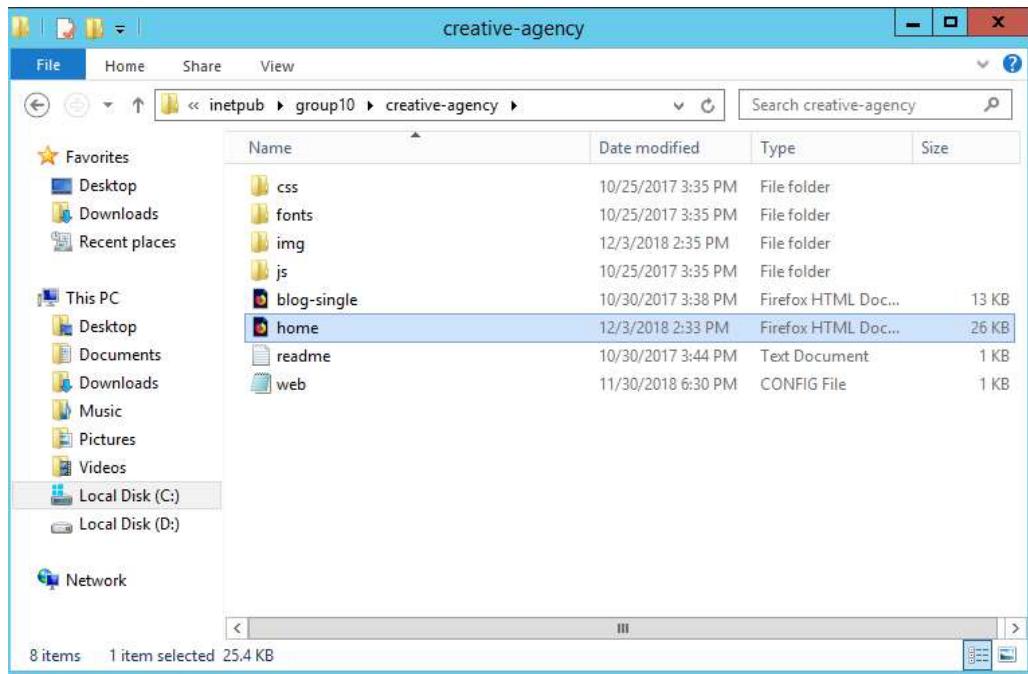


Figure 5.2.13.10: Adding HTML file

Step 11: Open up DNS Manager and click on “Forward Lookup Zone”. Right click to add New Zone

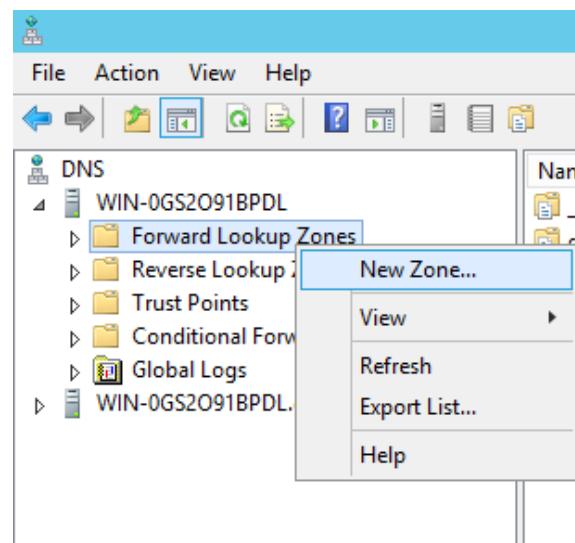


Figure 5.2.13.11: Adding New Zone

Step 12: Click NEXT to proceed with installation



Figure 5.2.13.12: New Zone note

Step 13: Click on 'Primary Zone' for the Zone Type

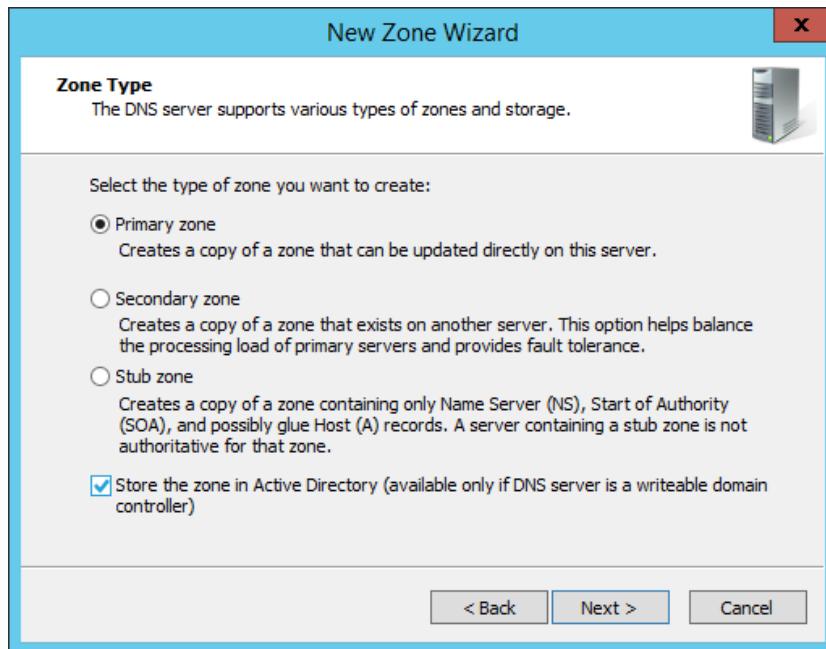
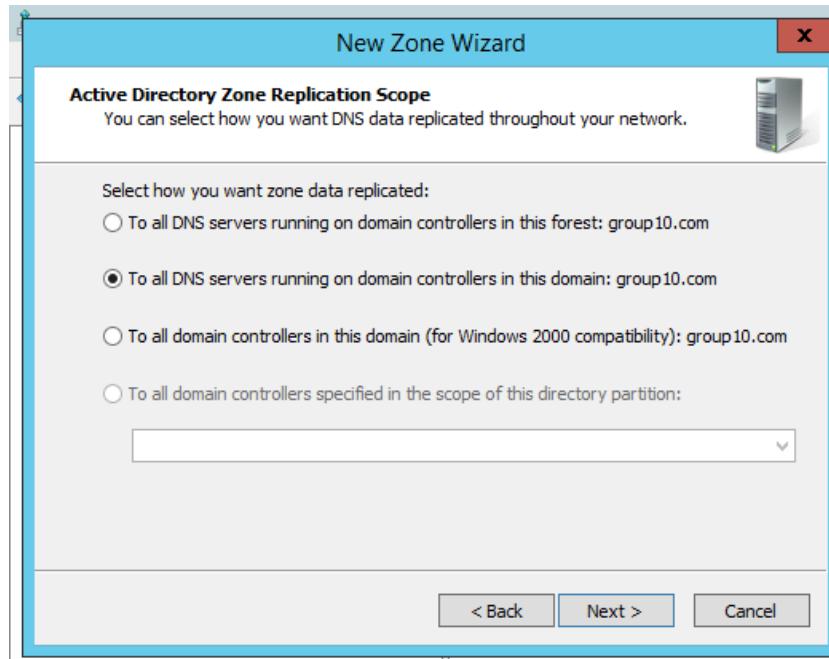


Figure 5.2.13.13: Choosing Zone Type

Step 14: Choose the “To all DNS servers running on domain controllers in this domain: Group10.com” for the AD Directory Zone Replication Scope.



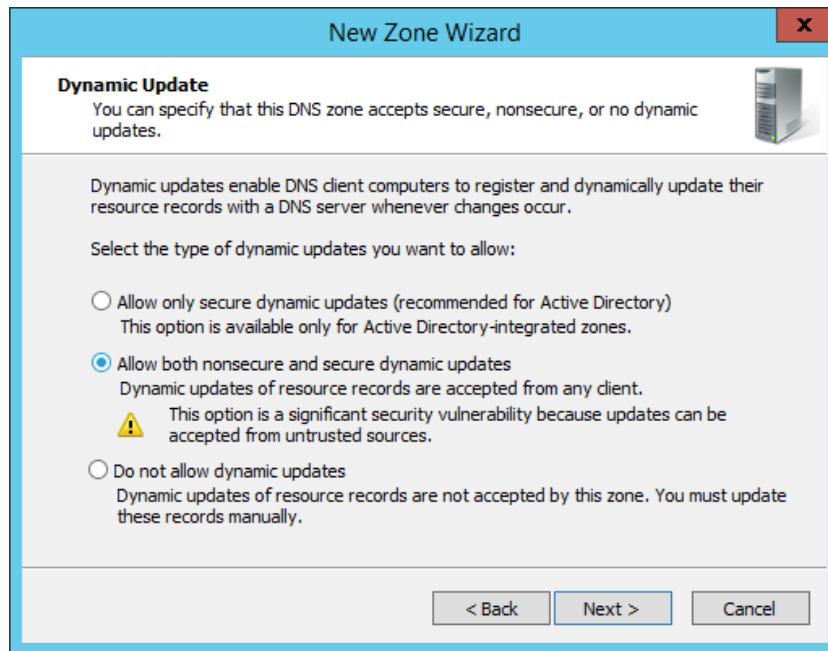
*Figure 5.2.13.14: Choosing the AD Zone Replication Scope*

Step 15: Fill in the name for the Zone name



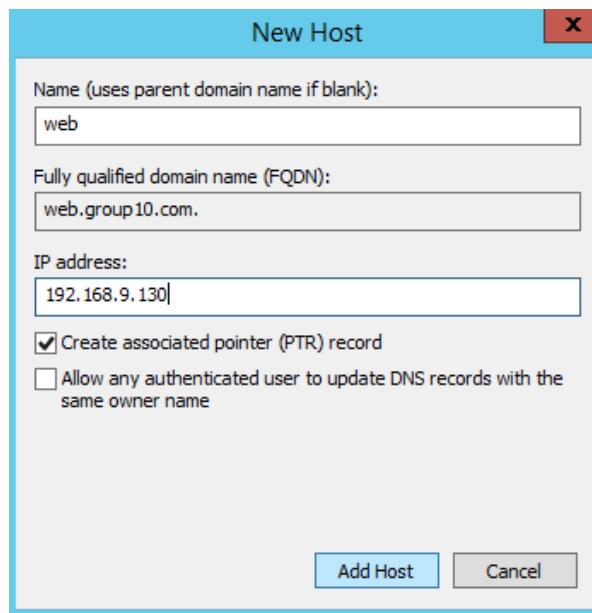
*Figure 5.2.13.15: Zone Name*

Step 16: Click on “Allow both nonsecure and secure dynamic updates” for the Dynamic Update option then click FINISH to complete installation.

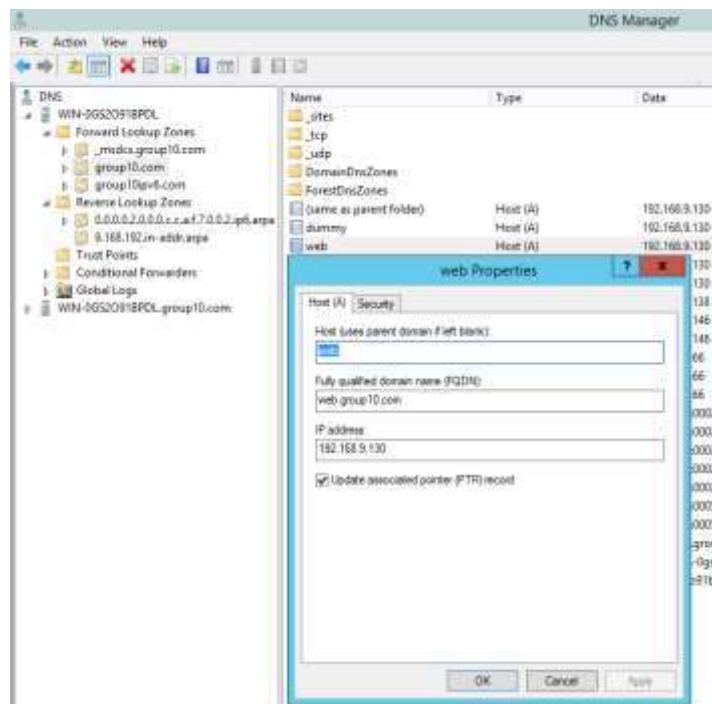


*Figure 5.2.13.16: Choosing the Dynamic Update*

Step 17: Open up DNS Manager and click on “Group10.com”. Then right click and choose “new host A or AAA”. Fill in the Name and IP Address for the new host and click ADD HOST



*Figure 5.2.13.17: Adding New Host*

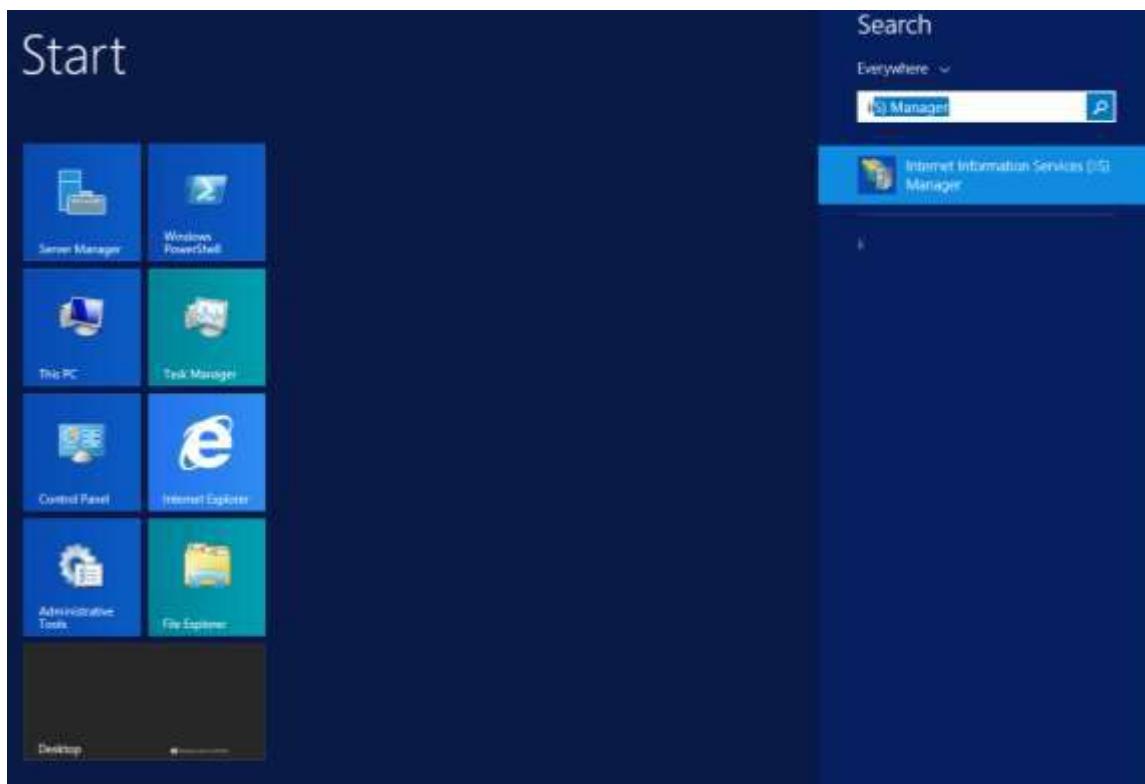


*Figure 5.2.13.18: It shows that the New Host has been added successfully*

## Install Secure Sockets Layer ( SSL ) on Windows Server 2012 r2

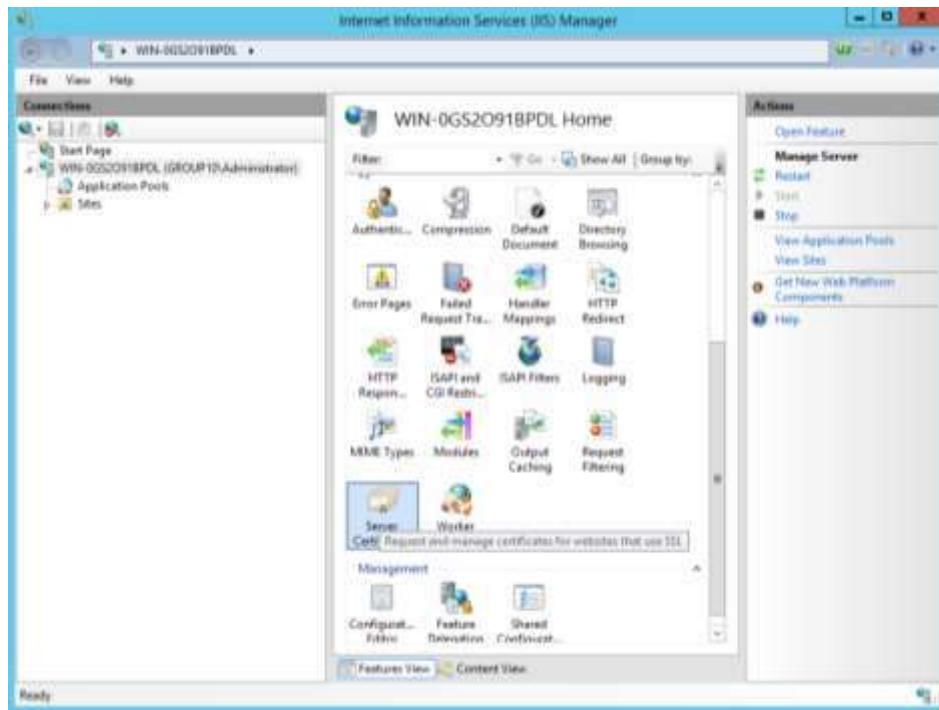
SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.

Step 1: Open up the Internet Information Services ( IIS ) Manager



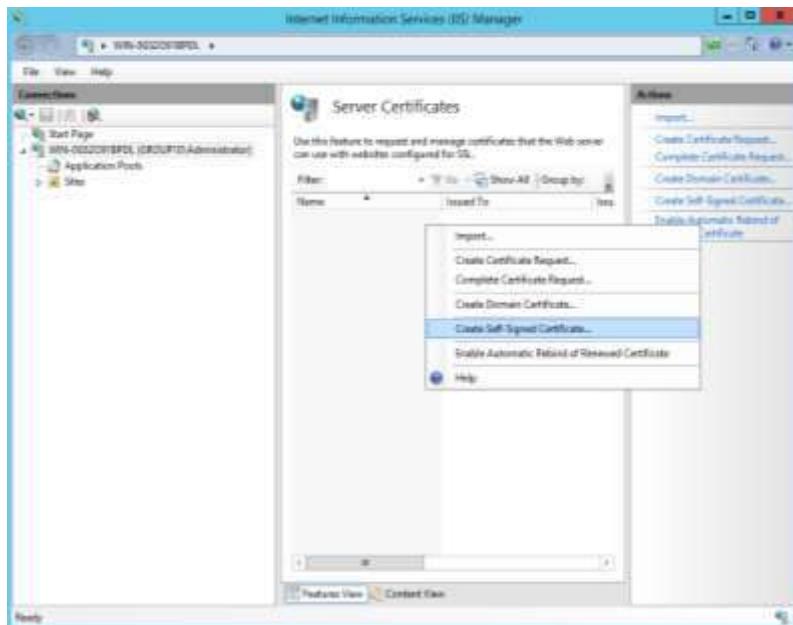
*Figure 5.2.13.19: Opening IIS Manager*

Step 2: Click on localhost server that is “WIN-0GS2O91BPDL (GROUP10\Administrator)” and click on “Server Certification”.



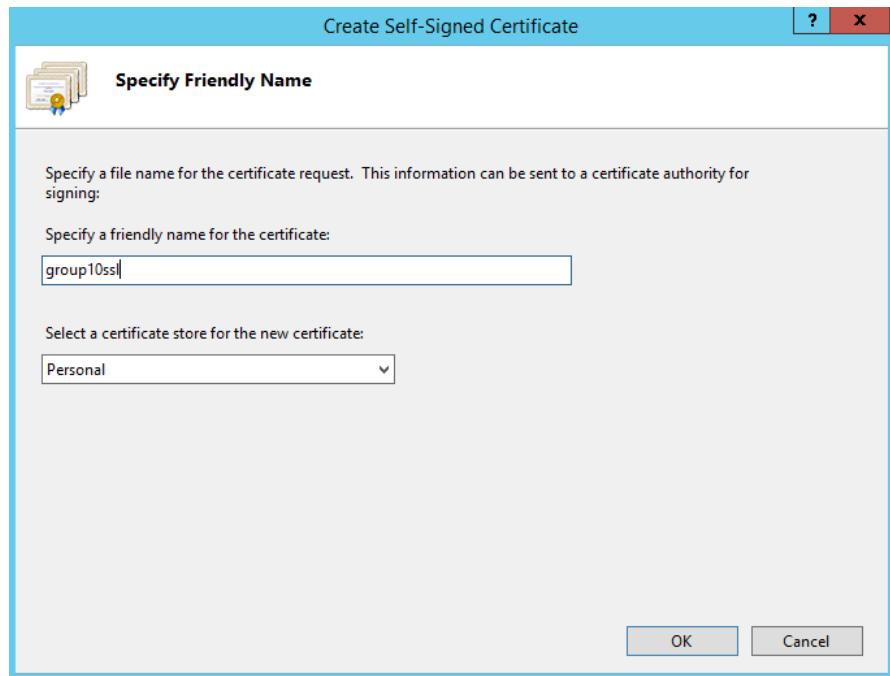
*Figure 5.2.13.20: Clicking on localhost server and Server Certification*

Step 3: Right click on Server Certificates and choose “self-signed certificate”



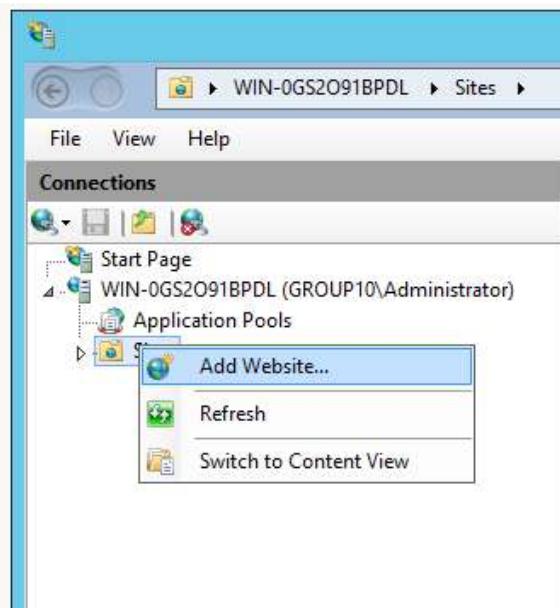
*Figure 5.2.13.21: Choosing server certificate*

Step 4: Enter the name for the certificate and click ‘OK’



*Figure 5.2.13.22: Entering details for the certificate*

Step 5: Click on website then right click and choose ‘Add Website’



*Figure 5.2.13.23: Adding Website*

Step 6: Fill in the Site name, path, and ip address and click ‘OK’

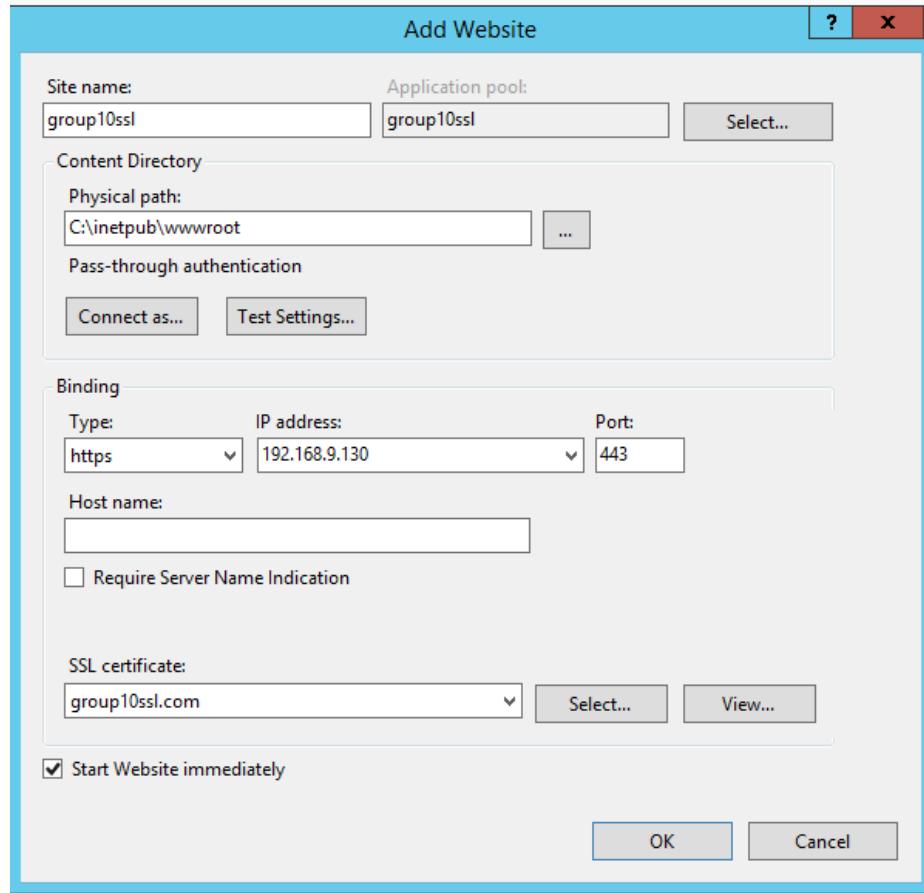


Figure 5.2.13.24: Filling information for SSL

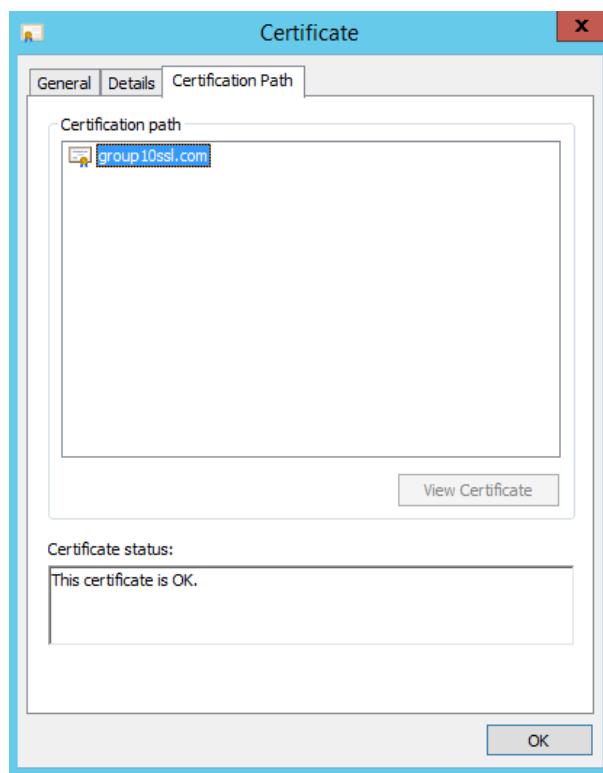
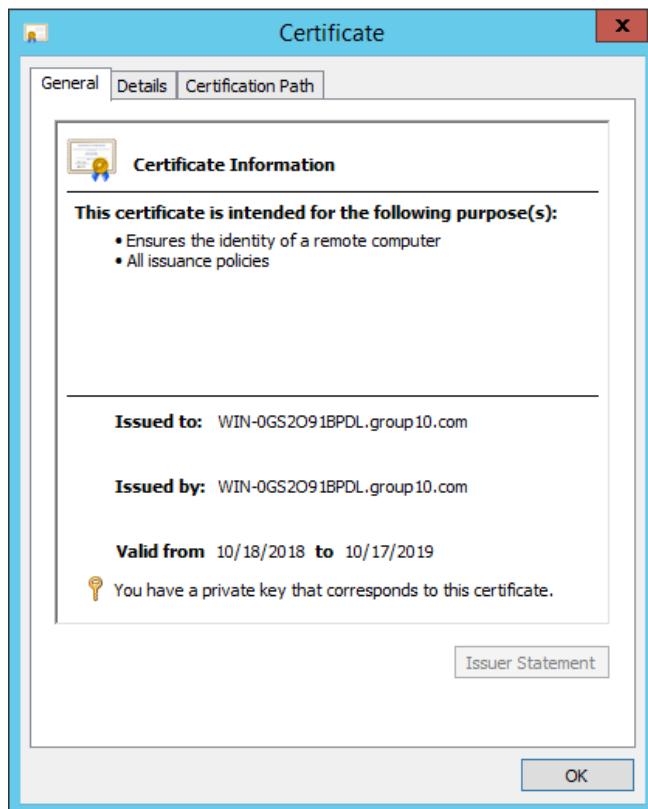


Figure 5.2.13.25: Certificate information

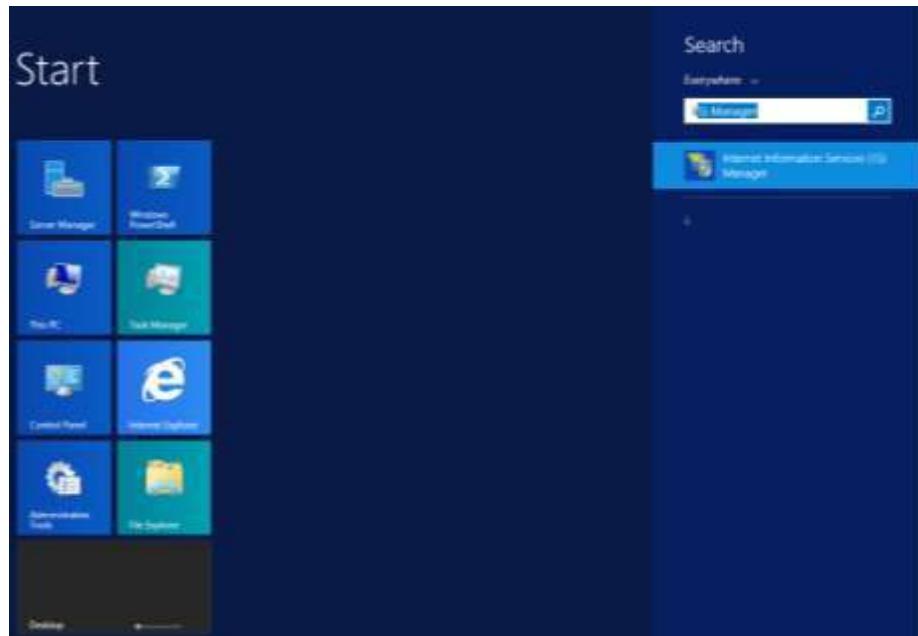
Name	ID	Status	Binding
Default Web Site	1	Started (ht...)	*:80 (http)
group10ssl	2	Started (ht...)	192.168.9.130:443 (I)

*Figure 5.2.13.26: The SSL website already added*

## Install Virtual Hosting Services on Windows Server 2012 r2

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

Step 1: Open the web server manager, Search IIS Manager in your windows server.



*Figure 5.2.13.27: Opening Progress*

Step 2: Open up the IIS Manager and right click on Sites, then click Add Website.

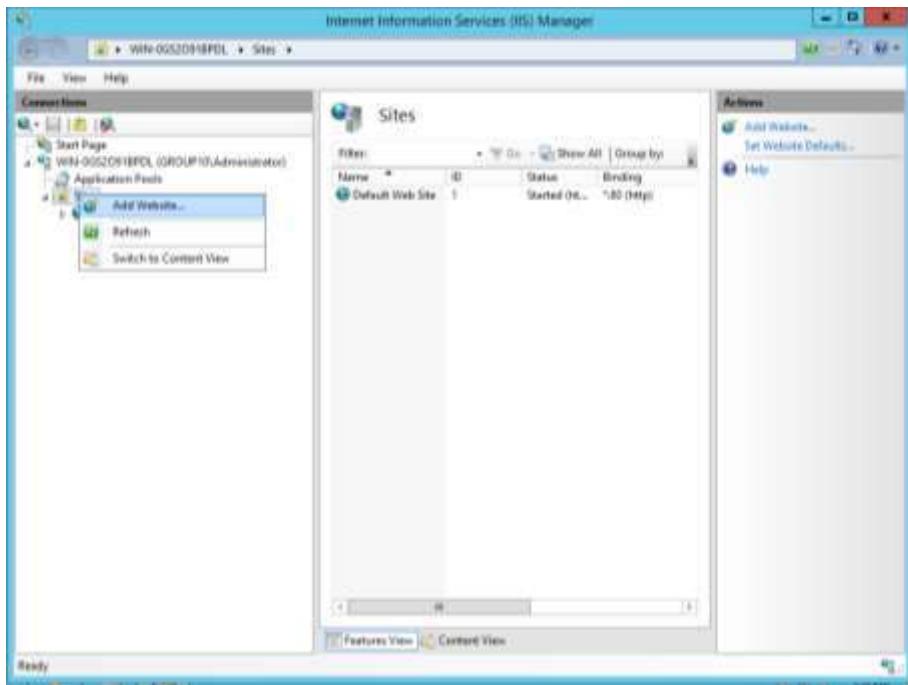


Figure 5.2.13.28: IIS Manager

Step 3: Fill in the Site Name, path and IP address and click OK

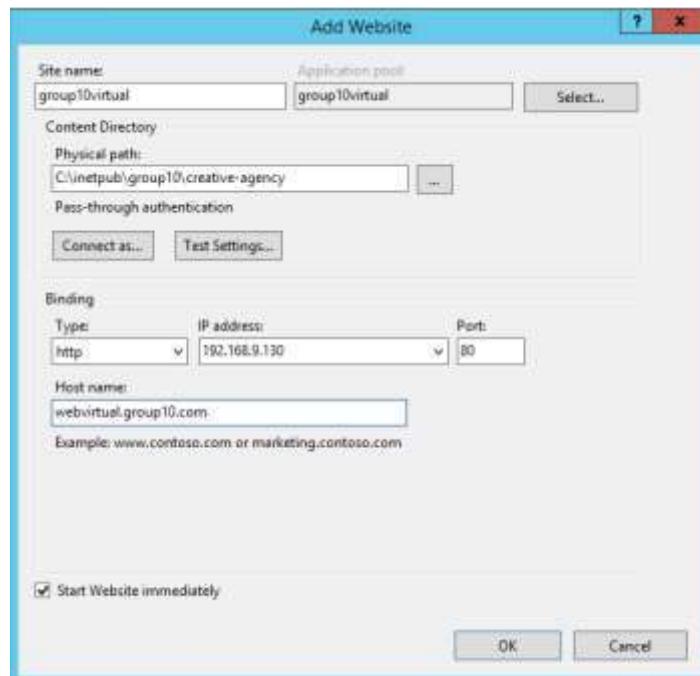


Figure 5.2.13.29: Adding Website

Step 4: At the IIS Manager click on your created website “group10virtual” and click on “Default Document”.

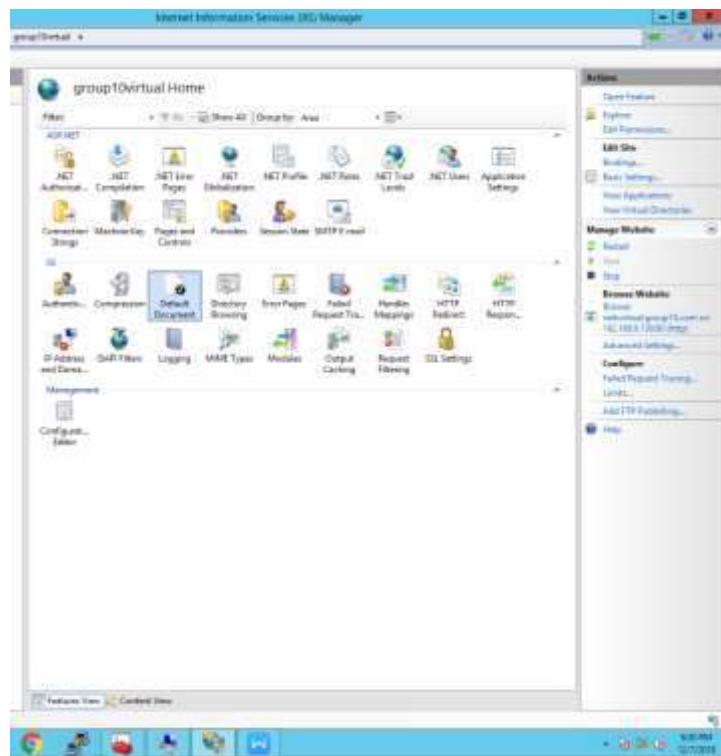


Figure 5.2.13.30: Adding Default Document

Step 5: Click on Add and fill the name for Default Document

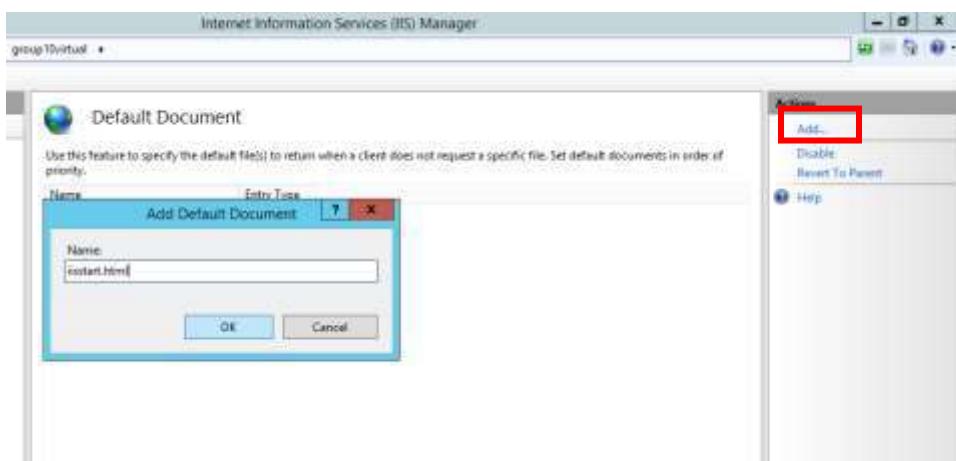


Figure 5.2.13.31: Adding Default Document

Step 6: Open the File Explorer and navigate to (C:\inetpub\’desired folder’) and create and HTML file for the Website.

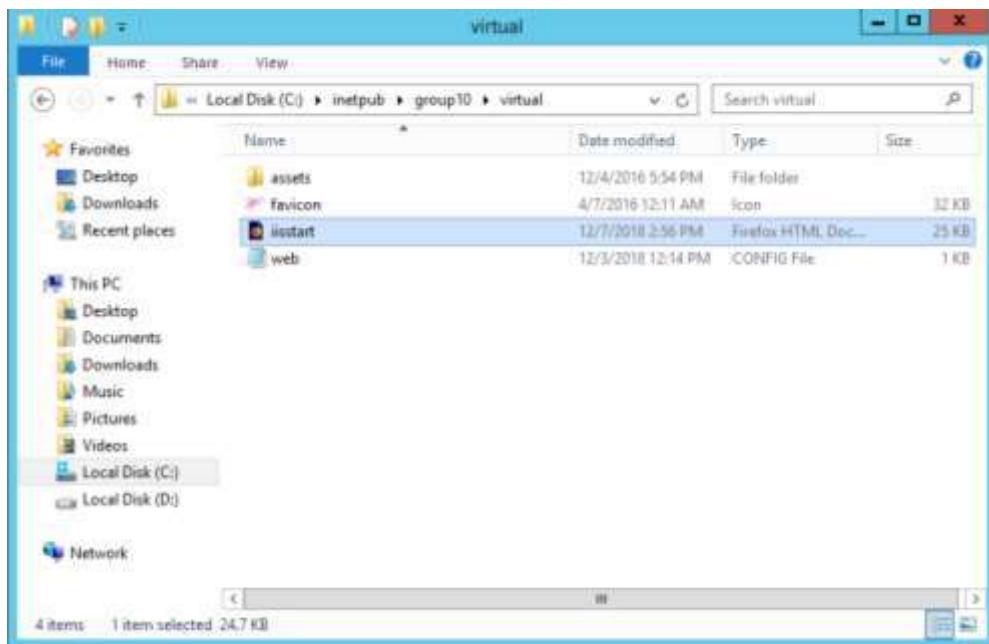


Figure 5.2.13.32: Adding HTML file

Step 7: Open up DNS Manager and click on “Group10.com”. Then right click and choose “new host A or AAA”. Fill in the Name and IP Address for the new host and click ADD HOST

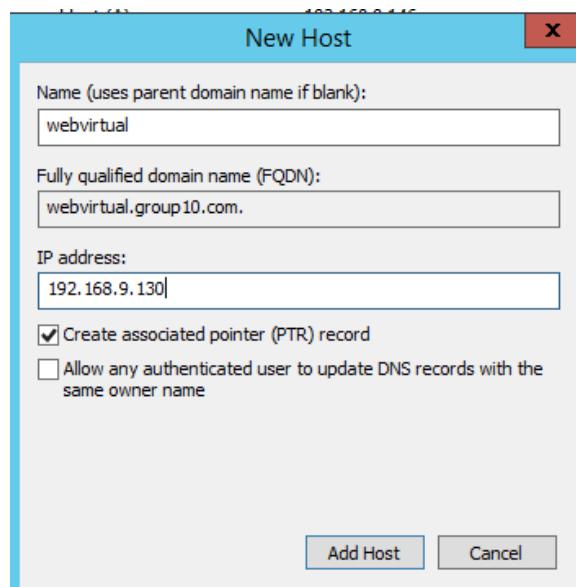


Figure 5.2.13.33: Adding New Host

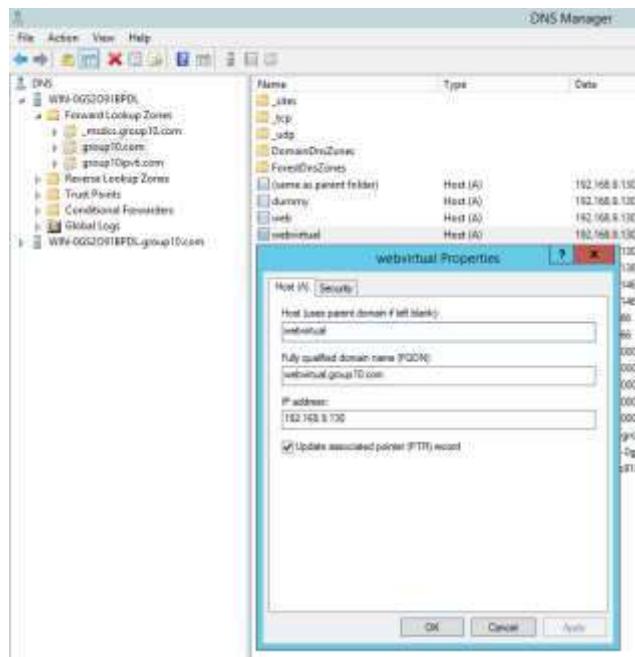


Figure 5.2.13.34: It shows that the New Host has been added successfully

## 5.2.14 Server Virtualization

### Install Hyper-V Virtual Machine on Windows Server 2012

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

Step 1: Add Hyper-v roles and feature in server manager

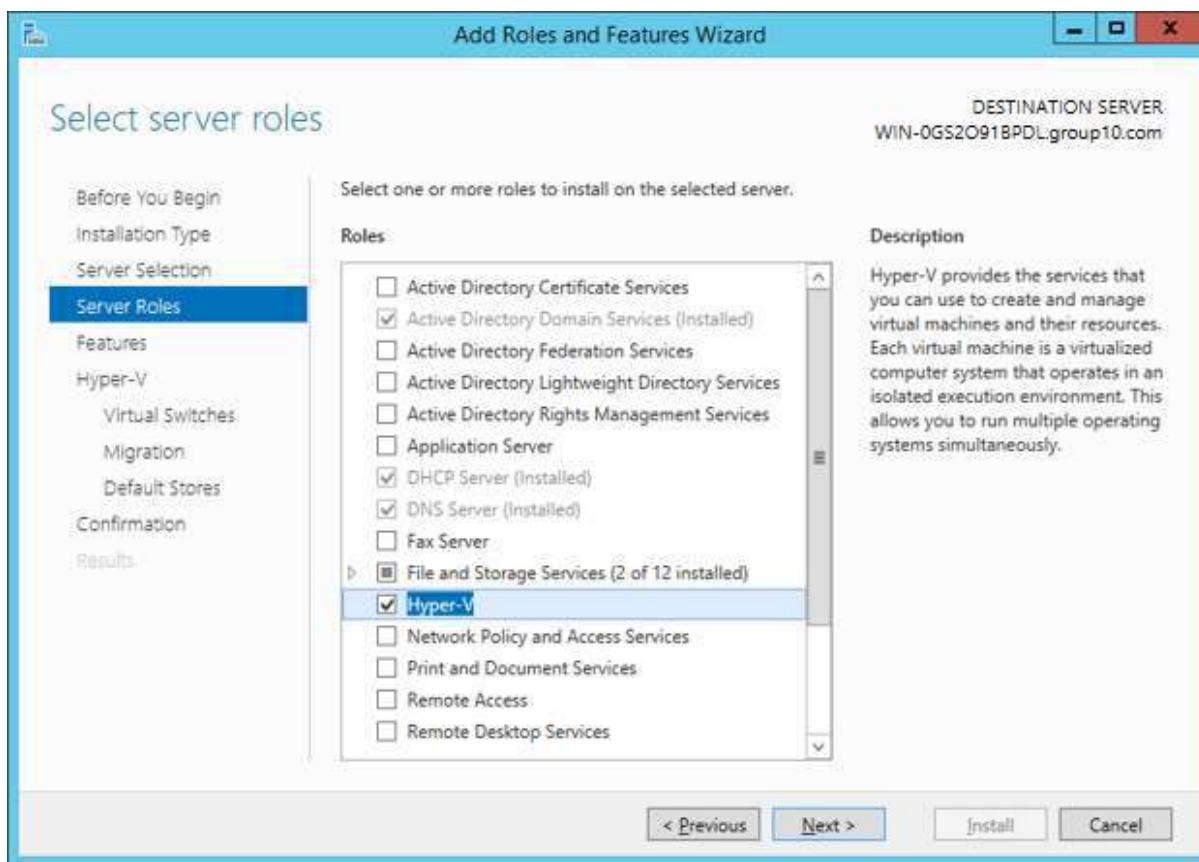
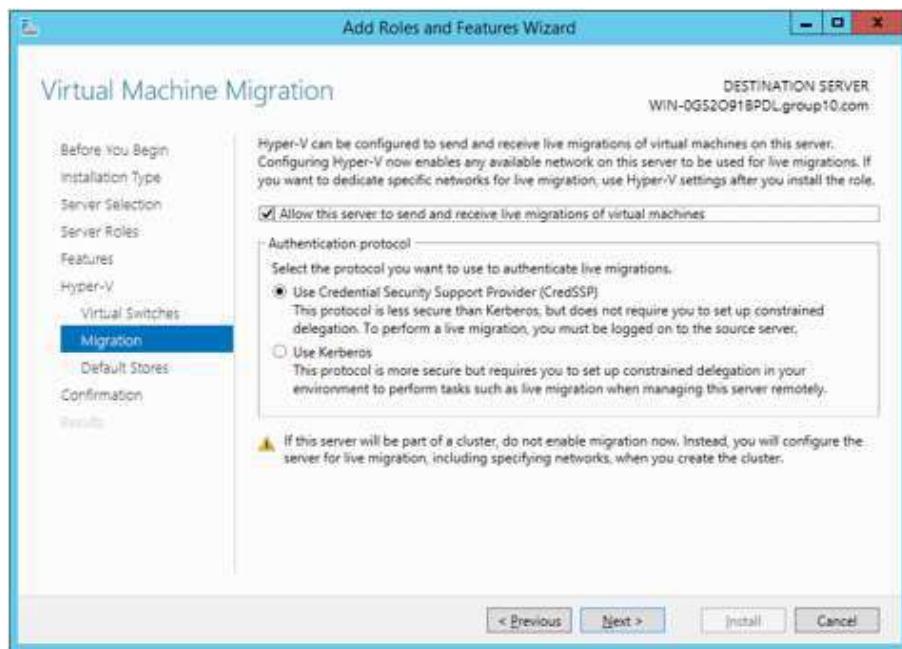


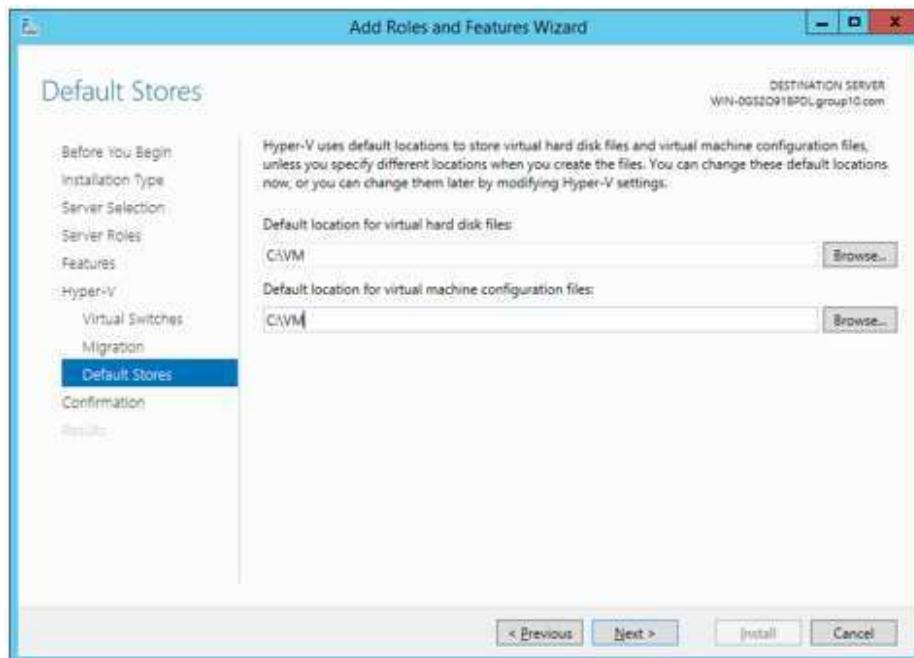
Figure 5.2.14.1: Adding roles and feature

Step 2: Choose the “Use Credential Security Support Provider (CredSSP) and click NEXT



*Figure 5.2.14.2: Choosing the protocol to authenticate live migrations*

Step 3: Insert the location for the virtual hard disk files



*Figure 5.2.14.3: Default location for virtual hard disk files*

Step 4: Click on INSTALL to proceed the installation

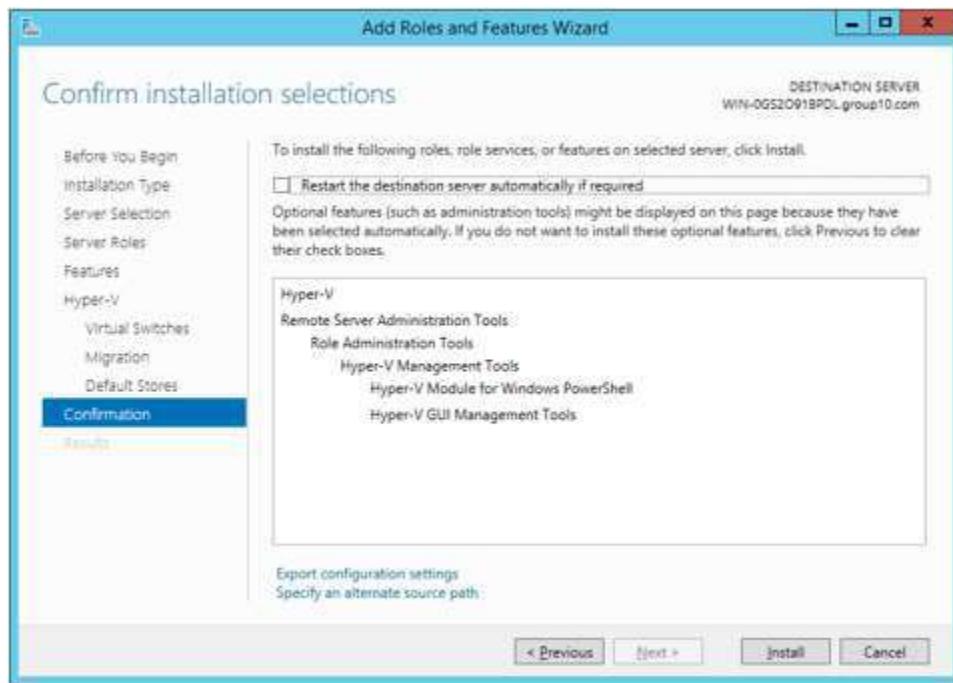


Figure 5.2.14.4: Confirmation for installation

Step 5: Hyper-V is installing

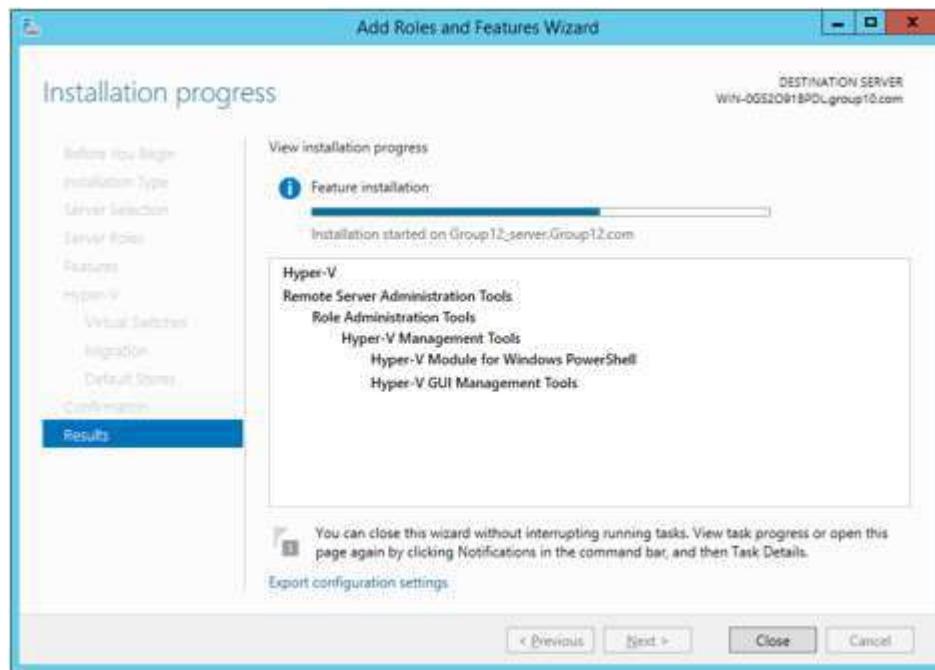
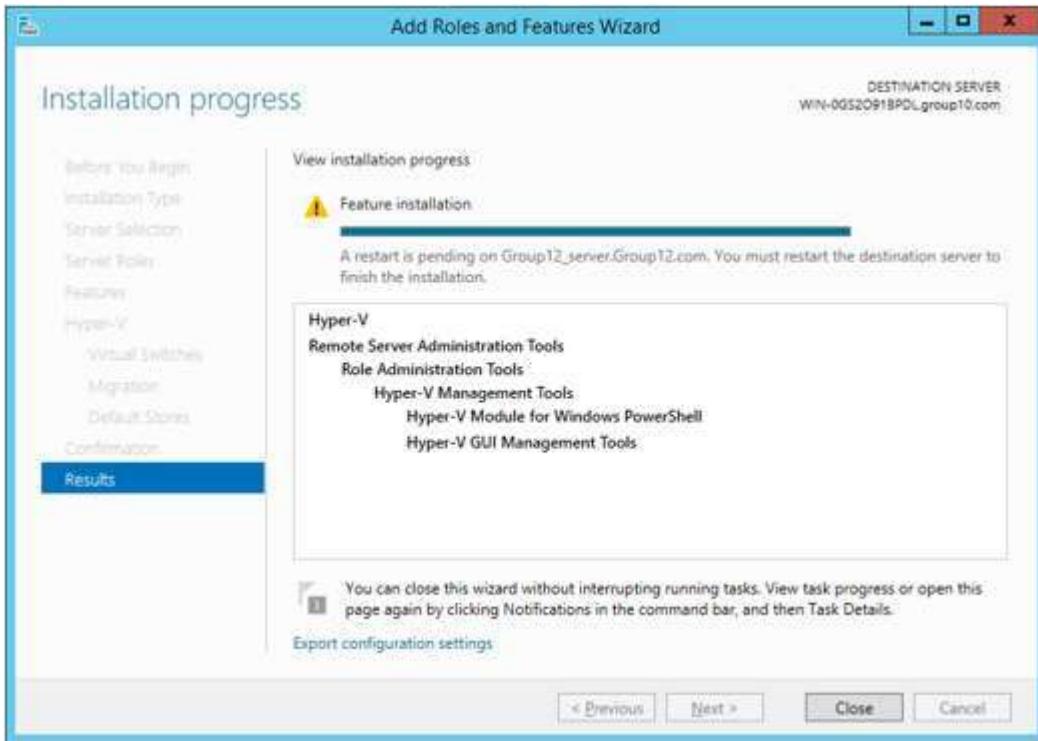


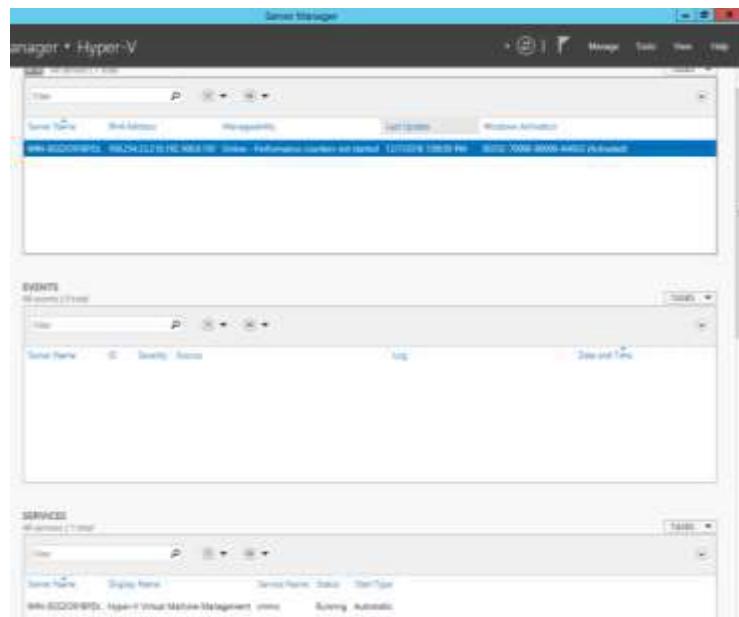
Figure 5.2.14.5: Installation process

Step 6: Once the installation is finished click on CLOSE and restart the server



*Figure 5.2.14.6: Installation finished*

Step 7: Open up the server manager and turn on the counter status of GROUP10\_SERVER



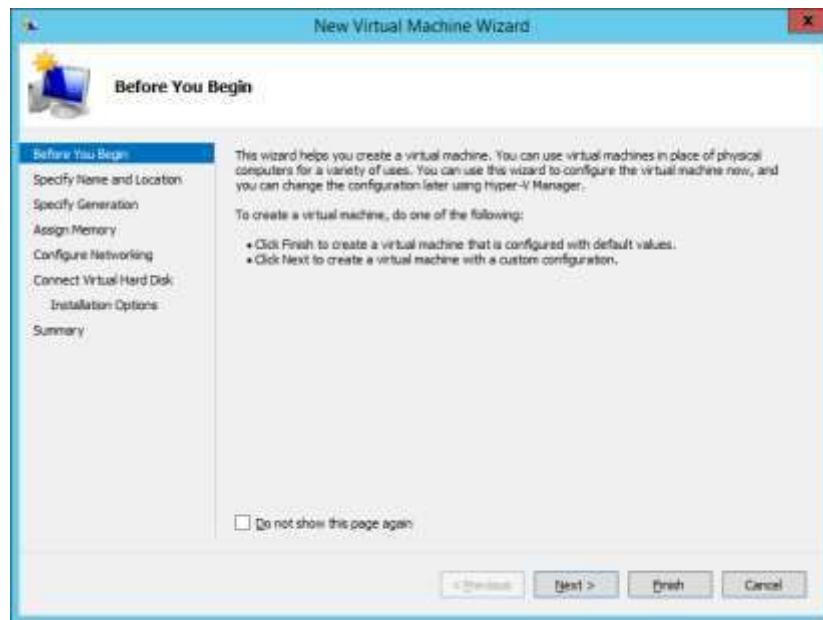
*Figure 5.2.14.7: Turning on server*

Step 8: Open up the Hyper-V Manager



*Figure 5.2.14.8: Hyper-V Manager*

Step 9: Click on “New” to start a new virtual machine and click NEXT



*Figure 5.2.14.9: New Virtual Machine Wizard*

Step 10: Enter the Name for the virtual machine and click NEXT

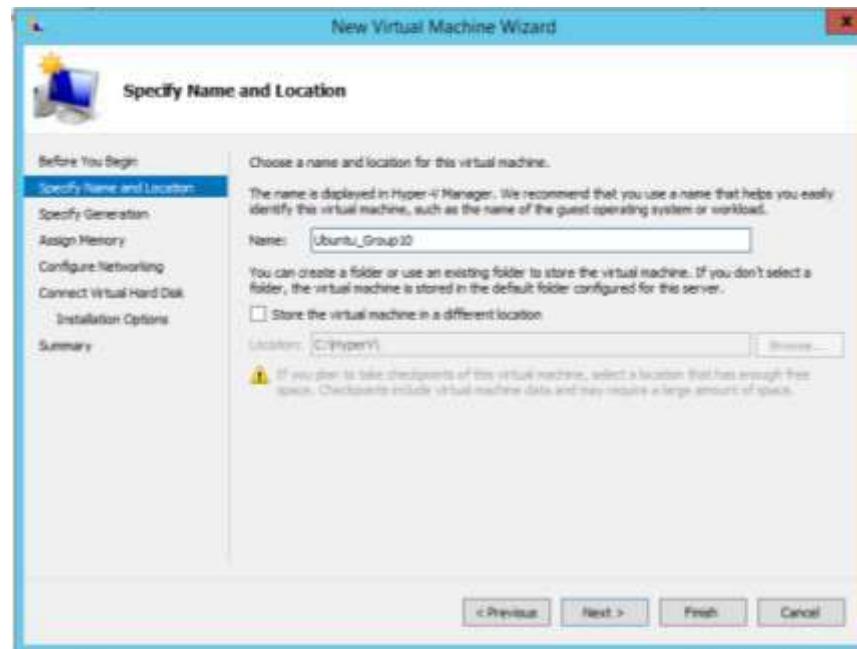


Figure 5.2.14.10: Specifying Name

Step 11: Click on Generation 2 and click NEXT

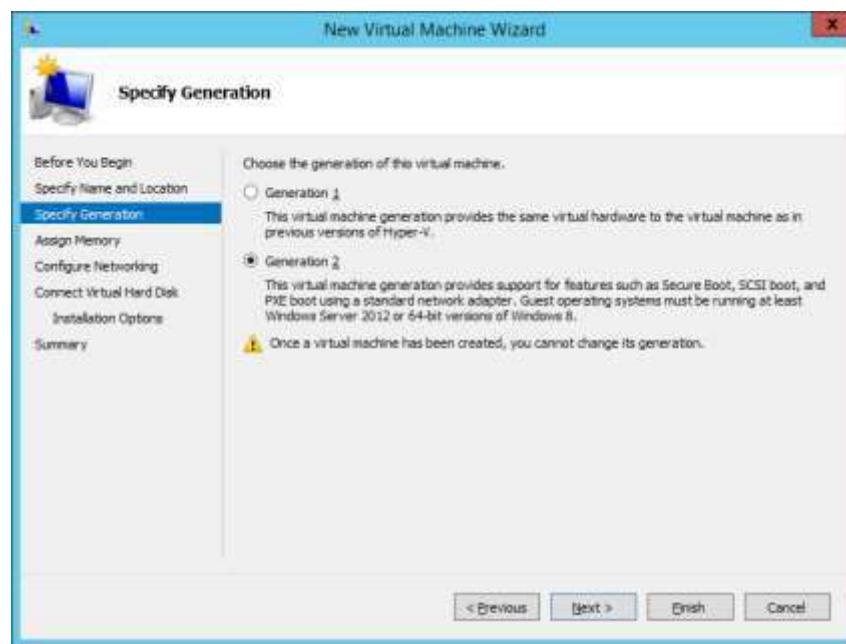


Figure 5.2.14.11: Choosing the generation for the virtual machine

Step 12: Choosing the location and size of the hard disk



Figure 5.2.14.12: Connecting Virtual Hard Disk

Step 13: Installing OS using Ubuntu 16.04 iso, then click finish to complete the installation.

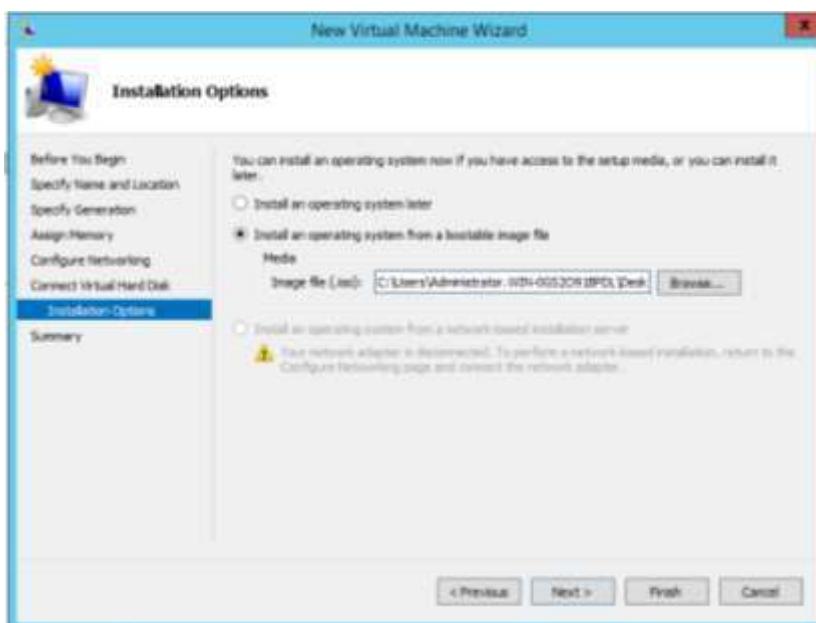
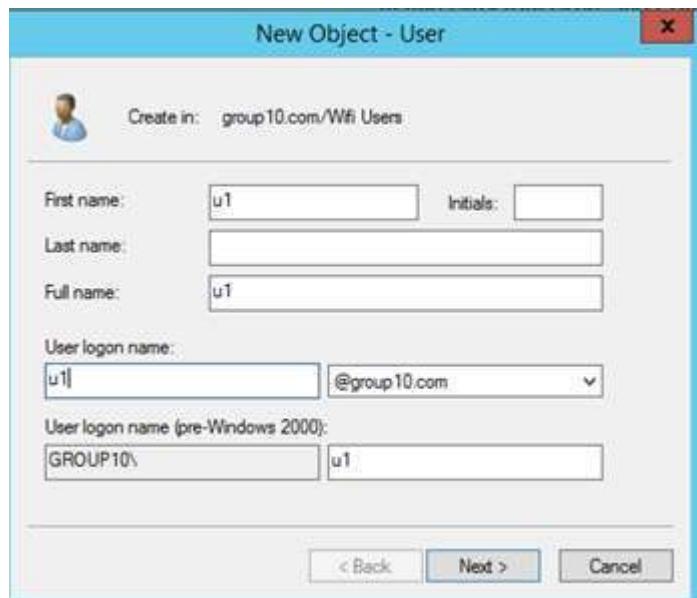


Figure 5.2.14.13: Installing Operating System

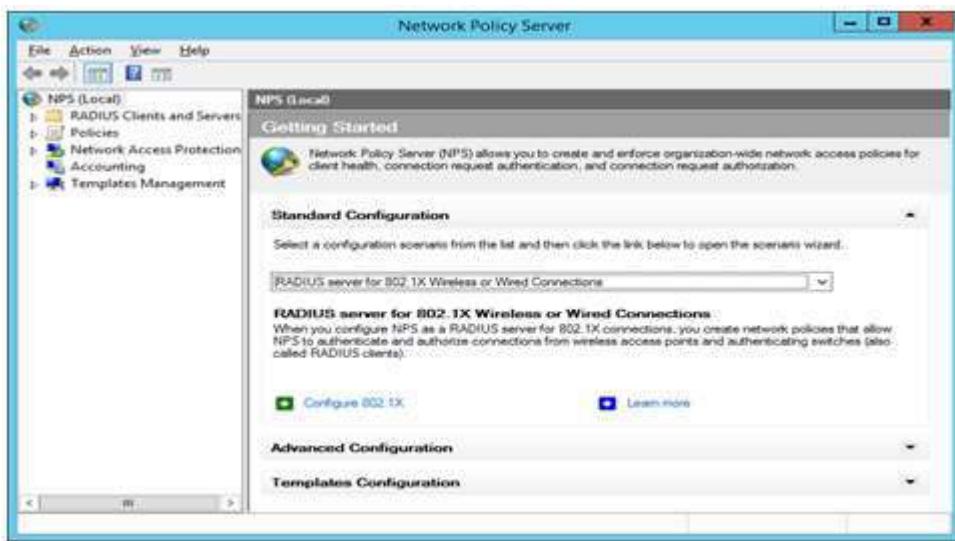
### 5.2.15 Wireless User Authentication using Radius

Step 1: Go to Active Directory and create a new user that can be access



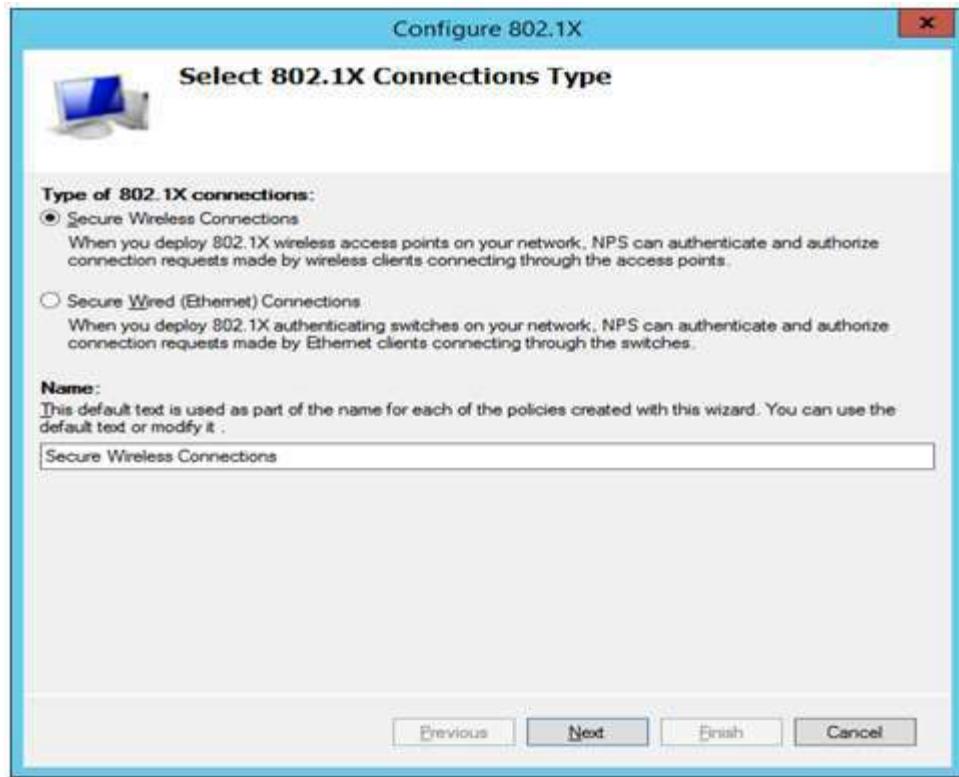
*Figure 5.2.15.1 Create new user*

Step 2: Open network Policy Server to create new radius, for Standard Configuration choose RADIUS server for 802.1X Wireless or Wired Connectors



*Figure 5.2.15.2 Network Policy Server interface starter*

Step 3: For type of 802.1X connections, choose Secure Wireless Connections



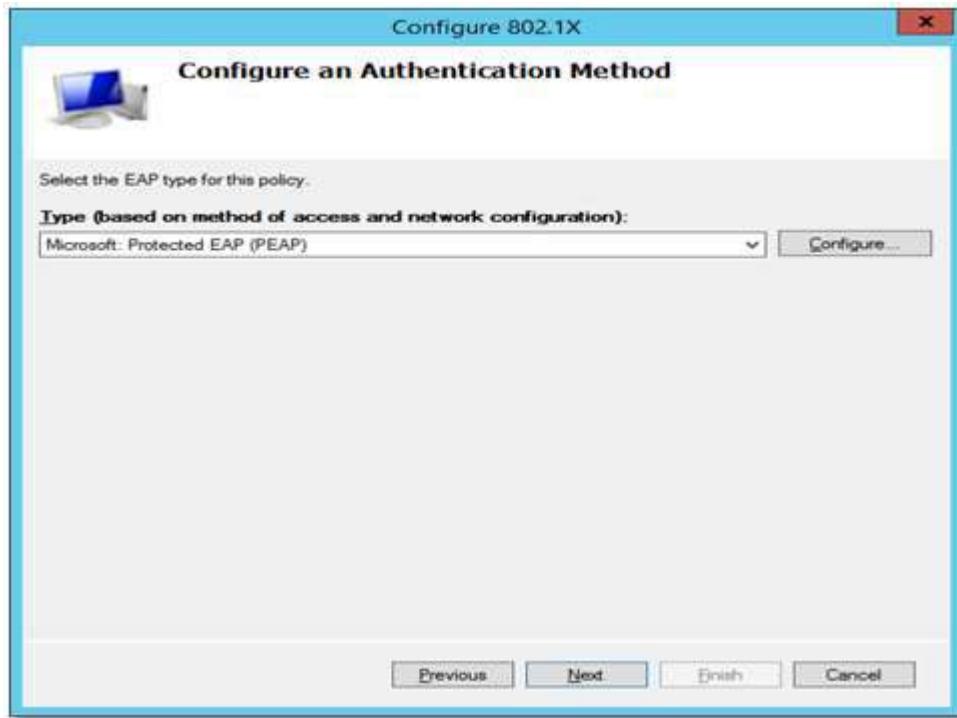
*Figure 5.2.15.3 Select 802.1X Connection Type*

Step 4: Insert the Friendly name, IP address, shared secret (Abc123) and click “OK”.



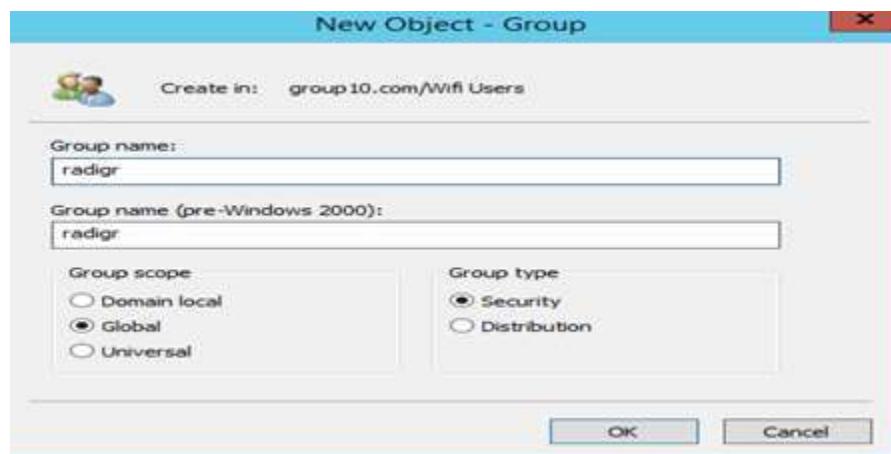
*Figure 5.2.15.4 Select 802.1X Connection Type*

Step 5: In configure and Authentication Method type choose “Microsoft: Protected EAP (PEAP)”.



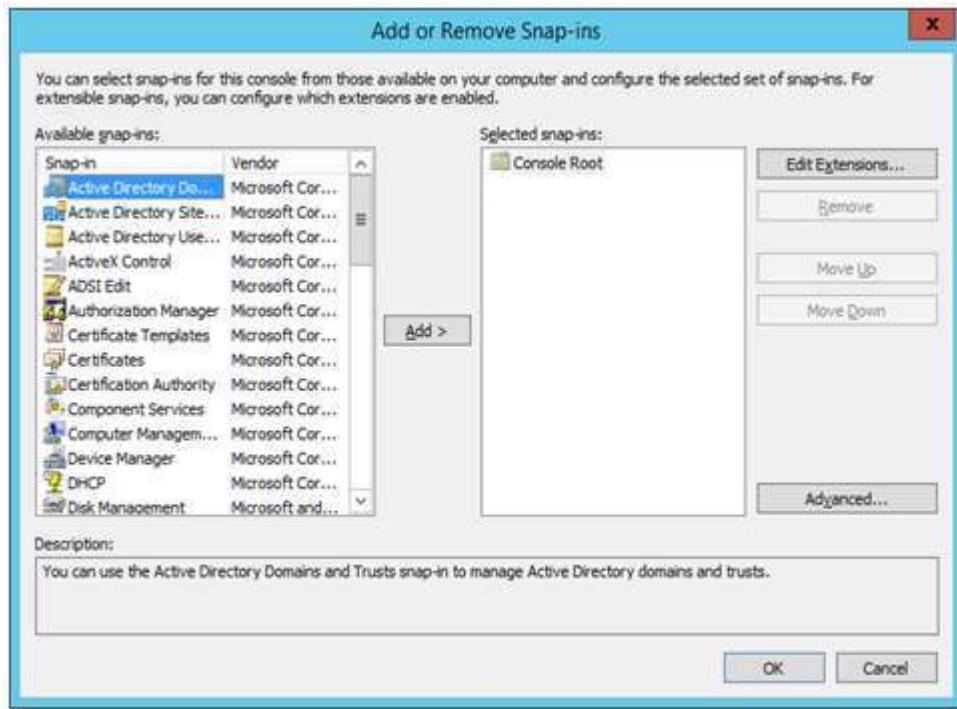
*Figure 5.2.15.5 Select configure and Authentication Method Type*

Step 6: Type “radigr” and check name. (Create “radigr” group and add member that create earlier inside it in Active directory)



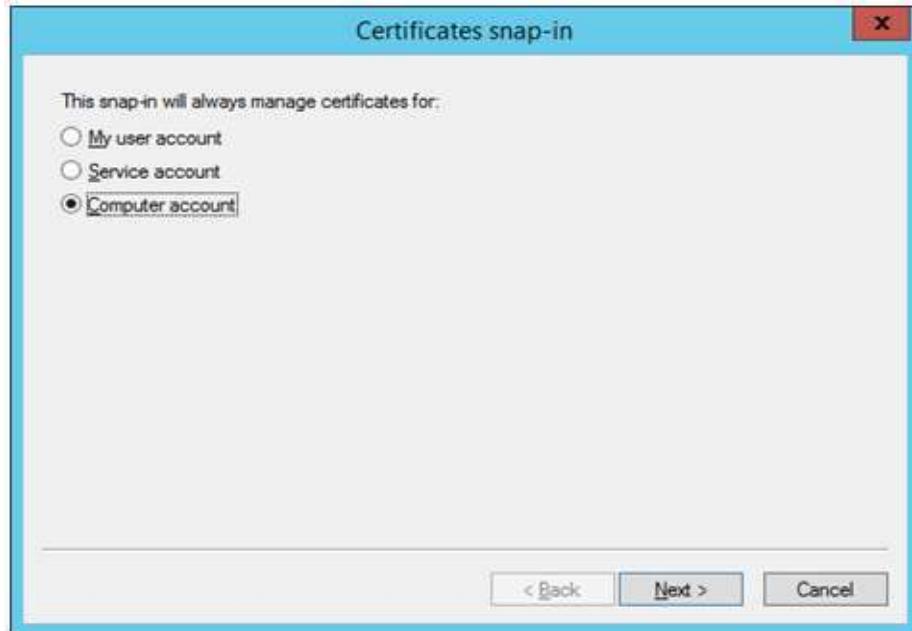
*Figure 5.2.15.6 Add radius group for this network policy*

Step 7: Open console application, click add or remove snap-ins and add certificates.



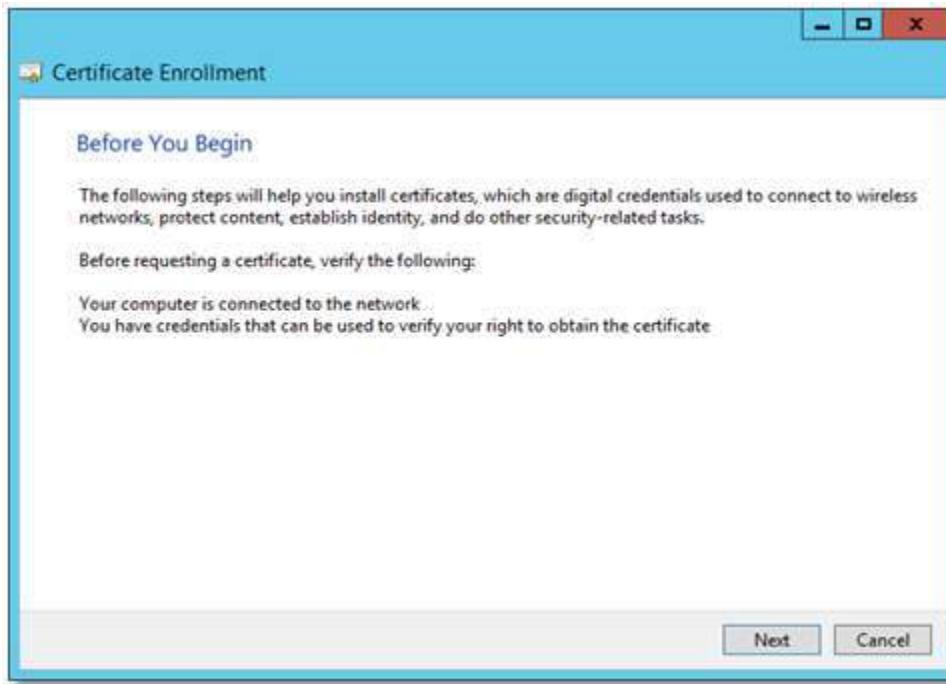
**Figure 5.2.15.7 Add snap-ins**

Step 8: In Certificates snap-in choose computer account.



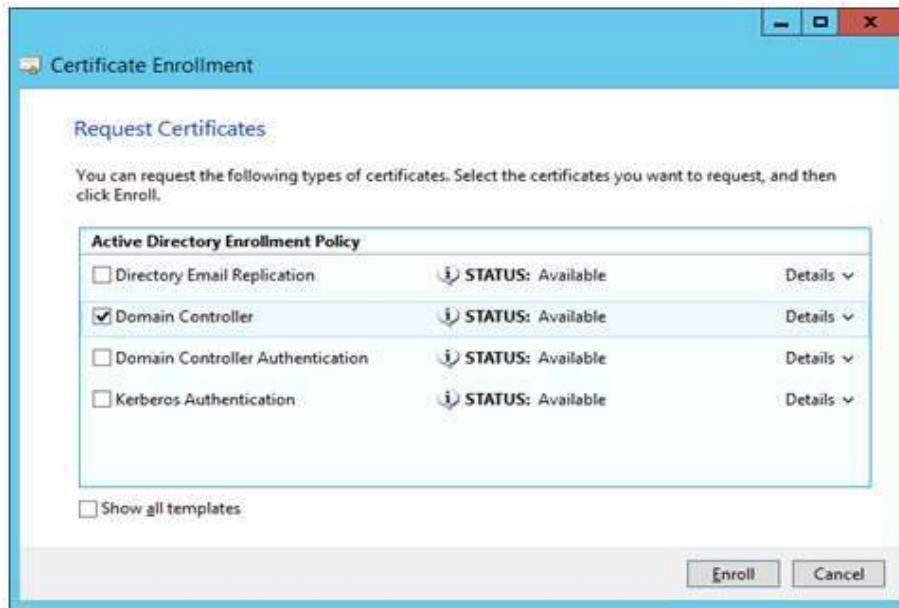
**Figure 5.2.15.8 Select Certificates snap-in**

Step 9: Start Certificate Enrollment by right click console windows



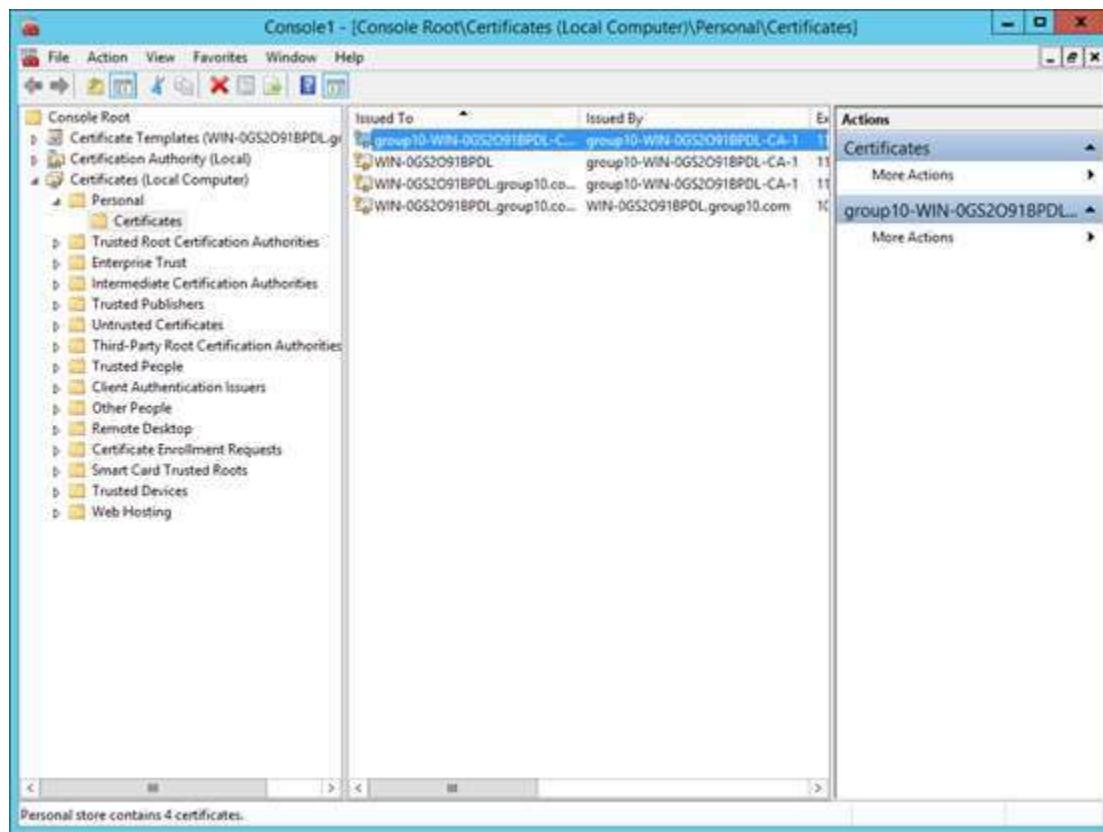
*Figure 5.2.1.5.9 Start Certificate Enrollment*

Step 10: Request “Domain Controller” Certificate to enroll



*Figure 5.2.15.10 Request Certificate to enroll*

Step 11: New Certificate will shown



*Figure 5.2.15.11 List of certificates*

### 5.2.16 Remote Login using SSH

#### Step 1: Configure SSH in Router

A)SSH had been configured through the router by using commands below.

```
group10router(config)#ip domain-name group10.com
group10router(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: group10router.group10.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

group10router(config)#
group10router(config)#
*Jan  1 02:05:12.527: %SSH-5-ENABLED: SSH 1.99 has been enabled
group10router(config)#line vty 0 4
group10router(config-line)#password AAssddl23
group10router(config-line)#transport input ssh
group10router(config-line)#login local
group10router(config-line)#username group10 privilege 15 secret AAssddl23
group10router(config)#exit
group10router#
*Jan  1 02:07:58.359: %SYS-5-CONFIG_I: Configured from console by console
group10router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
group10router(config)#line con 0
group10router(config-line)#logging synchronous
group10router(config-line)#login local
```

Figure 5.2.16.1: SSH Configuration on Router

```
group10router#
*Jan  1 02:07:58.359: %SYS-5-CONFIG_I: Configured from console by console
group10router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
group10router(config)#line con 0
group10router(config-line)#logging synchronous
group10router(config-line)#login local
group10router(config-line)#exit
group10router(config)#ip ssh version 2
group10router(config)#exit
group10router#
*Jan  1 02:09:12.007: %SYS-5-CONFIG_I: Configured from console by console
group10router#exit
```

Figure 5.2.16.2: SSH Configuration on Router

B) After finish typing all the command, remember to save the configuration to avoid the configuration loss after the router restart by using the following Command.

```
Router # copy run start
```

C) Check the SSH whether the SSH is on or off by using following command.

```
Router # show ssh
```

D) A list of ssh connection will be displayed if there are any connection using ssh.

```
Router # show ip ssh
```

```
group10#show ssh
Connection Version Mode Encryption Hmac      State          Username
0           2.0   IN    aca256 cbc  hmac sha1  Session started group10
0           2.0   OUT   aes256-cbc hmac-sha1  Session started group10
<No SSHv1 server connections running.
group10#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
```

*Figure 5.2.16.3: Check the SSH whether the SSH is on or off*

## Step 2: Configure SSH in Switch

SSH had been configured through the router by using commands below.

```
Switch>ena
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Group10
Group10(config)#ip domain-name group10.com
Group10(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: Group10.group10.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Group10(config)#
Group10(config)#
*Mar  1 01:08:19.512: %SSH-5-ENABLED: SSH 1.99 has been enabled
Group10(config)#line vty 0 4
Group10(config-line)#password AAssddl23
Group10(config-line)#transport input ssh
Group10(config-line)#login local
Group10(config-line)#username group10 privilege 15 secret AAssddl23
Group10(config)#exit
Group10#
*Mar  1 01:11:14.591: %SYS-5-CONFIG_I: Configured from console by console
```

Figure 5.2.16.4: SSH Configuration on Switch

```
*Mar  1 01:08:19.512: %SSH-5-ENABLED: SSH 1.99 has been enabled
Group10(config)#line vty 0 4
Group10(config-line)#password AAssddl23
Group10(config-line)#transport input ssh
Group10(config-line)#login local
Group10(config-line)#username group10 privilege 15 secret AAssddl23
Group10(config)#exit
Group10#
*Mar  1 01:11:14.591: %SYS-5-CONFIG_I: Configured from console by console
Group10#config t
Enter configuration commands, one per line. End with CNTL/Z.
Group10(config)#line con 0
Group10(config-line)#logging synchronous
Group10(config-line)#login local
Group10(config-line)#exit
Group10(config)#ip ssh version2
^
% Invalid input detected at '^' marker.

Group10(config)#ip ssh version 2
Group10(config)#exit
Group10#
*Mar  1 01:12:38.804: %SYS-5-CONFIG_I: Configured from console by console
Group10#
```

Figure 5.2.16.5: SSH Configuration on switch

“ip domain-name” used to configure DNS domain name of the router and switch. “crypto key generate rsa” used to generate Rivest, Shamir and Adelman (RSA) key pairs. “general-keys” used to generate a general-purpose key pair. “modulus 1024” used to specifies the IP size of the key modulus which is 1024 bits. “line vty 0 4” used to insert configuration of logical connection point to the router and switch that needed for SSH to remote access. “login local” used to tell the router and switch to used the local username and password for user authentication. “transport input ssh” used to prevent non-SSH connection.

### Step 3 : Configure SSH in Ubuntu Server

Download and install the openssh-client and openssh-server.

```
group10@group10:~$ sudo apt install -y openssh-server
[sudo] password for group10:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  ssh-askpass rssh molly-guard monkeysphere
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 13 not upgraded.
Need to get 633 kB of archives.
After this operation, 5,136 kB of additional disk space will be used.
Get:1 http://my.archive.ubuntu.com/ubuntu xenial/main amd64 ncurses-term all 6.0
+20160213-1ubuntu1 [249 kB]
Get:2 http://my.archive.ubuntu.com/ubuntu xenial-updates/main amd64 openssh-sftp
```

*Figure 5.2.16.6: Configuration on ubuntu server*

```

Processing triggers for man-db (2.7.5-1) ...
Processing triggers for systemd (229-4ubuntu21.4) ...
Processing triggers for ureadahead (0.100.0-19) ...
ureadahead will be reprofiled on next reboot
Processing triggers for ufw (0.35-0ubuntu2) ...
Setting up ncurses-term (6.0+20160213-1ubuntu1) ...
Setting up openssh-sftp-server (1:7.2p2-4ubuntu2.5) ...
Setting up openssh-server (1:7.2p2-4ubuntu2.5) ...
Creating SSH2 RSA key; this may take some time ...
2048 SHA256:20v6/8P7a2dqsCRku6H8cFmkQoev2DDU97zeDEW7C6M root@group10.com (RSA)
Creating SSH2 DSA key; this may take some time ...
1024 SHA256:P+8Y+PYvQNHLQVB/74io0+LEATfx6FnXnc4ycjLVTU root@group10.com (DSA)
Creating SSH2 ECDSA key; this may take some time ...
256 SHA256:ZjrHf+triDEuelkSFsikhM0qk/q7Up3WT65eyea+VcLM root@group10.com (ECDSA)
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:VRGksCONs8MG8vN9n/n/z5A/2UfqvlIuK9okdC21Zm8 root@group10.com (ED25519)
)
Setting up ssh-import-id (5.5-0ubuntu1) ...
Processing triggers for systemd (229-4ubuntu21.4) ...
Processing triggers for ureadahead (0.100.0-19) ...
Processing triggers for ufw (0.35-0ubuntu2) ...
group10@group10:~$ █

```

*Figure 5.2.16.7: SSH Configuration on ubuntu server*

#### Step 4: Configure SSH in Fedora Server

##### A) Download and install the openssh-server and openssh-client

```

[root@Nuqman ~]# yum install openssh-server openssh-clients
Fedora 28 - x86_64 - Updates                               4.4 MB/s | 26 MB   00:05
Last metadata expiration check: 0:00:09 ago on Mon 22 Oct 2018 02:35:44 PM +08.
Dependencies resolved.
=====
 Package           Arch      Version       Repository     Size
=====
Installing:
 openssh-clients  x86_64    7.8p1-3.fc28   updates        653 k
 openssh-server   x86_64    7.8p1-3.fc28   updates        472 k
Installing dependencies:
 fipscheck        x86_64    1.5.0-4.fc28   fedora        26 k
 fipscheck-lib    x86_64    1.5.0-4.fc28   fedora        14 k
 openssh          x86_64    7.8p1-3.fc28   updates        502 k
Transaction Summary
=====
Install 5 Packages

Total download size: 1.6 M
Installed size: 5.3 M
Is this ok [y/N]: █

```

*Figure 5.2.16.8: SSH Configuration on Fedora server*

```

root@Nuqman:~ 
File Edit View Search Terminal Help
Preparing : 1/1
Installing : fipscheck-1.5.0-4.fc28.x86_64 1/5
Installing : fipscheck-lib-1.5.0-4.fc28.x86_64 2/5
Running scriptlet: fipscheck-lib-1.5.0-4.fc28.x86_64 2/5
Running scriptlet: openssh-7.8pl-3.fc28.x86_64 3/5
Installing : openssh-7.8pl-3.fc28.x86_64 3/5
Running scriptlet: openssh-server-7.8pl-3.fc28.x86_64 4/5
Installing : openssh-server-7.8pl-3.fc28.x86_64 4/5
Running scriptlet: openssh-server-7.8pl-3.fc28.x86_64 4/5
Installing : openssh-clients-7.8pl-3.fc28.x86_64 5/5
Running scriptlet: openssh-clients-7.8pl-3.fc28.x86_64 5/5
Verifying : openssh-server-7.8pl-3.fc28.x86_64 1/5
Verifying : openssh-7.8pl-3.fc28.x86_64 2/5
Verifying : fipscheck-lib-1.5.0-4.fc28.x86_64 3/5
Verifying : fipscheck-1.5.0-4.fc28.x86_64 4/5
Verifying : openssh-clients-7.8pl-3.fc28.x86_64 5/5

Installed:
  openssh-clients.x86_64 7.8pl-3.fc28           openssh-server.x86_64 7.8pl-3.fc28
  fipscheck.x86_64 1.5.0-4.fc28                 fipscheck-lib.x86_64 1.5.0-4.fc28
  openssh.x86_64 7.8pl-3.fc28

Complete!
[root@Nuqman ~]#

```

*Figure 5.2.16.9: SSH Configuration on Fedora server*

B) To start the sshd daemon (openssh-server) in the current session type “Systemctl start sshd” and “netstat -ant | grep 22 to enable the service

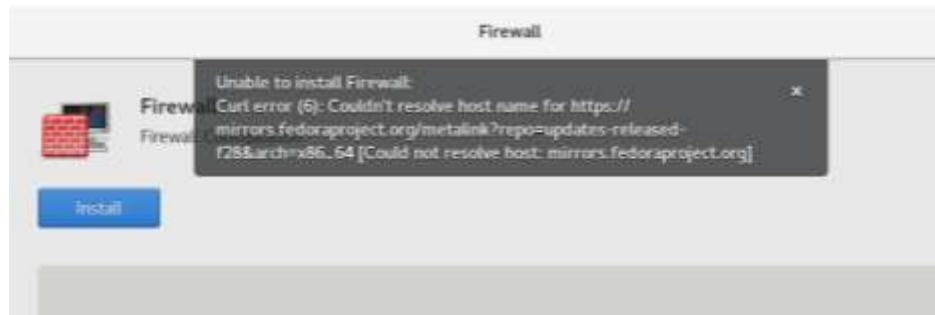
```

[root@Nuqman ~]# systemctl start sshd
[root@Nuqman ~]# netstat -ant | grep 22
tcp        0      0 192.168.1.22.1:53          0.0.0.0:*          LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*          LISTEN
tcp        0      0 10.73.33.72:53584       13.228.211.31:443    TIME_WAIT
tcp        0      0 10.73.33.72:37822       52.71.116.75:443    ESTABLISHED
tcp        0      0 10.73.33.72:48060       54.165.222.237:443   TIME_WAIT
tcp        0      0 10.73.33.72:59210       104.18.21.226:80     ESTABLISHED
tcp        0      0 10.73.33.72:40104       52.72.225.121:443   TIME_WAIT
tcp        0      0 10.73.33.72:34166       52.221.118.237:443  TIME_WAIT
tcp        0      0 10.73.33.72:53042       23.220.203.9:80      ESTABLISHED
tcp        0      0 10.73.33.72:46176       52.0.214.228:443    ESTABLISHED
tcp        0      0 10.73.33.72:57726       54.64.220.62:443    TIME_WAIT
tcp        0      0 10.73.33.72:48238       8.41.222.241:443    ESTABLISHED
tcp        0      0 10.73.33.72:48328       8.41.222.241:443    ESTABLISHED
tcp        0      0 10.73.33.72:50022       13.35.23.41:443    ESTABLISHED
tcp        0      0 10.73.33.72:50150       103.229.205.253:443 ESTABLISHED
tcp        0      0 10.73.33.72:39644       35.165.254.225:443  TIME_WAIT
tcp        0      0 10.73.33.72:39032       103.243.221.109:443 TIME_WAIT
tcp        0      0 10.73.33.72:48328       52.220.145.158:443  TIME_WAIT
tcp        0      0 10.73.33.72:41424       104.20.223.2:443    TIME_WAIT
tcp        0      0 10.73.33.72:53944       23.74.221.202:443    ESTABLISHED
tcp        0      0 10.73.33.72:49270       23.74.228.201:443    ESTABLISHED
tcp        0      0 10.73.33.72:52046       23.220.203.9:80      ESTABLISHED

```

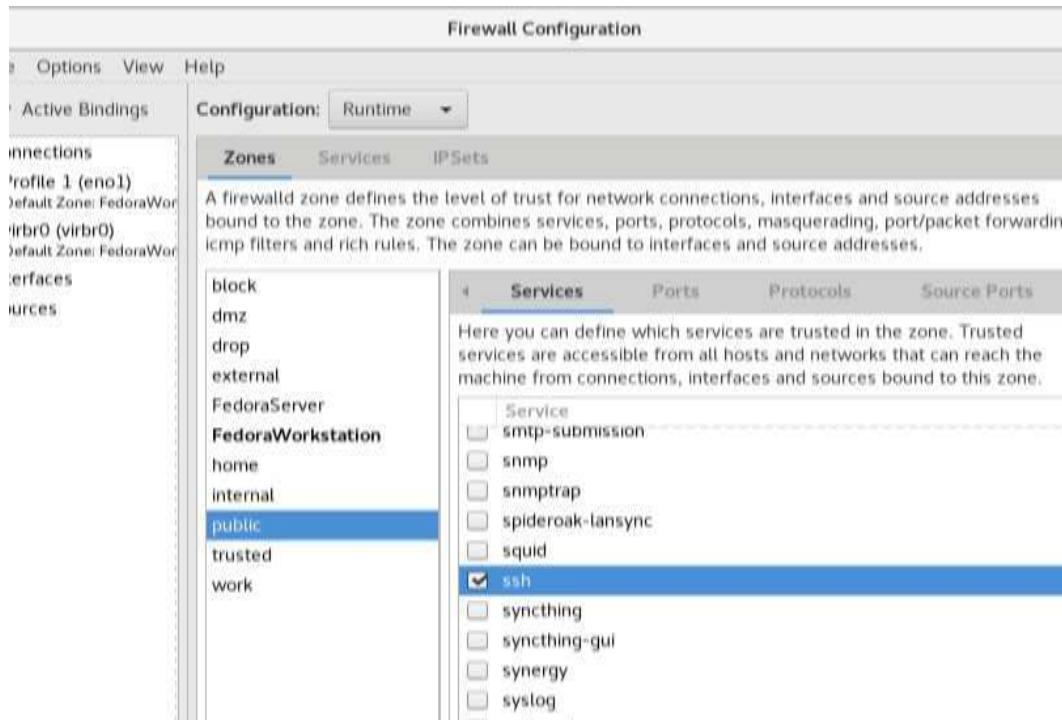
*Figure 5.2.16.10: SSH Configuration on Fedora server*

C) Install firewall to protect your system you will need to allow SSH connections before you be able to connect from a remote system.



*Figure 5.2.16.11: SSH Configuration on Fedora server*

D) Then, go to firewall configuration tool and tick the box ssh in service to allow SSH connections .



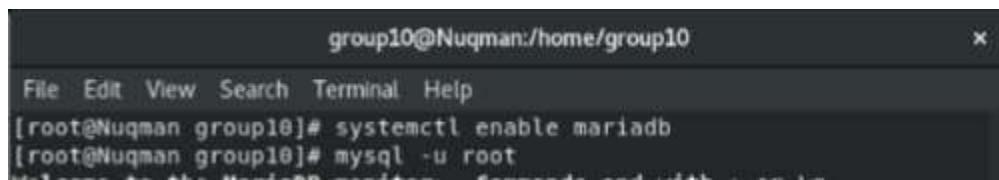
*Figure 5.2.16.12: SSH Configuration on Fedora server*

## 5.2.17 Network Management System

### Network Management System (NMS)

Network Management System is an application or set of applications that lets network administrators manage a network's independent component inside a bigger network management framework.

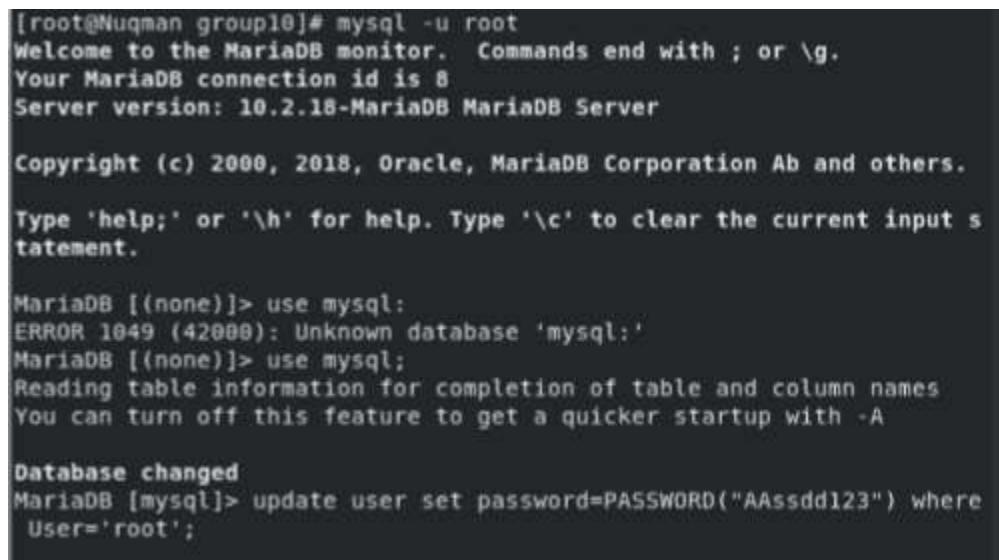
1. Install the Mariadb Server, enable and start the service



```
group10@Nuqman:/home/group10
File Edit View Search Terminal Help
[root@Nuqman group10]# systemctl enable mariadb
[root@Nuqman group10]# mysql -u root
```

Figure show Installing the Mariadb Server

2. Configure the settings in Mariadb for root user



```
[root@Nuqman group10]# mysql -u root
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 8
Server version: 10.2.18-MariaDB MariaDB Server

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

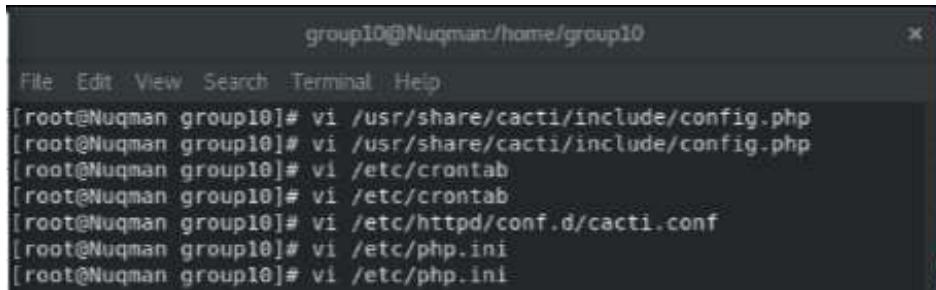
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> use mysql;
ERROR 1049 (42000): Unknown database 'mysql';
MariaDB [(none)]> use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [mysql]> update user set password=PASSWORD("AAssdd123") where
User='root';
```

Figure show the Configuration of Settings in Mariadb for Root User

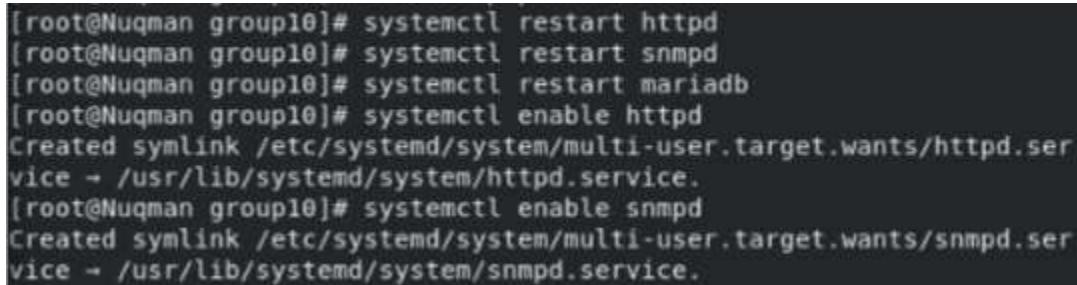
### 3. Configure the repository for installing



```
group10@Nuqman:/home/group10
File Edit View Search Terminal Help
[root@Nuqman group10]# vi /usr/share/cacti/include/config.php
[root@Nuqman group10]# vi /usr/share/cacti/include/config.php
[root@Nuqman group10]# vi /etc/crontab
[root@Nuqman group10]# vi /etc/crontab
[root@Nuqman group10]# vi /etc/httpd/conf.d/cacti.conf
[root@Nuqman group10]# vi /etc/php.ini
[root@Nuqman group10]# vi /etc/php.ini
```

Figure show the Configuration of Repository for Installing

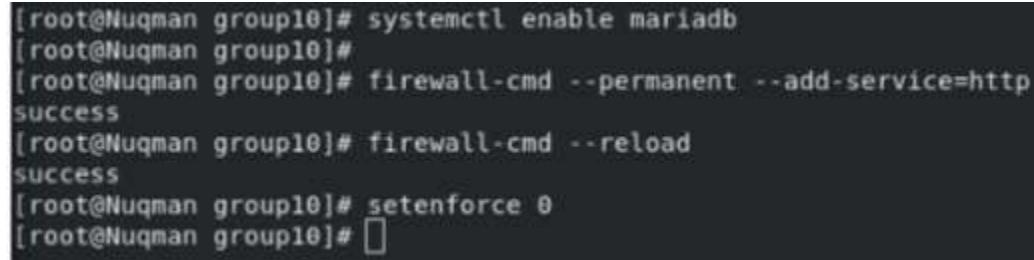
### 4. Enable the HTTPD and SNMPD Server



```
[root@Nuqman group10]# systemctl restart httpd
[root@Nuqman group10]# systemctl restart snmpd
[root@Nuqman group10]# systemctl restart mariadb
[root@Nuqman group10]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[root@Nuqman group10]# systemctl enable snmpd
Created symlink /etc/systemd/system/multi-user.target.wants/snmpd.service → /usr/lib/systemd/system/snmpd.service.
```

Figure show the Configuration of Enable the HTTPD and SNMPD Server

### 5. Firewall Configuration



```
[root@Nuqman group10]# systemctl enable mariadb
[root@Nuqman group10]#
[root@Nuqman group10]# firewall-cmd --permanent --add-service=http
success
[root@Nuqman group10]# firewall-cmd --reload
success
[root@Nuqman group10]# setenforce 0
[root@Nuqman group10]# 
```

Figure show the Configuration of the Firewall

## 6. Cacti Installation Wizard

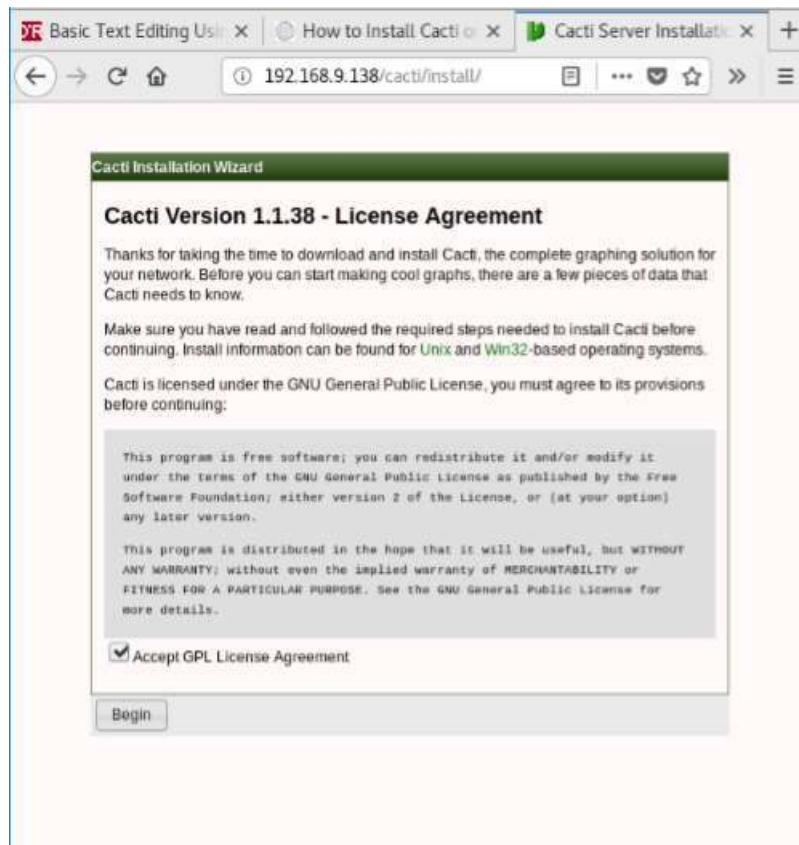


Figure show the Cacti Version 1.1.38 Installation Wizard

### 5.2.18 Port Security

**Step 1:** Configure port security for windows server with interface FastEthernet 0/1 and FastEthernet 0/2.

```
interface FastEthernet0/1
switchport access vlan 10
switchport mode access
switchport port-security maximum 5
switchport port-security
switchport port-security mac-address sticky
!
interface FastEthernet0/2
switchport access vlan 10
switchport mode access
switchport port-security maximum 10
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0015.5d09.8200
switchport port-security mac-address sticky 00ae.75b9.8293
switchport port-security mac-address sticky 6400.6a59.0afd
switchport port-security mac-address sticky 90b1.lc81.7172
switchport port-security mac-address sticky da50.7abc.40d5
switchport port-security mac-address sticky da89.b2d5.6d50
```

*Figure 5.2.18.1: Configure Port for Windows Server*

**Step 2:**Configure port security for Fedora server with interface FastEthernet 0/3 and FastEthernet 0/4.

```
interface FastEthernet0/3
switchport access vlan 20
switchport mode access
switchport port-security
switchport port-security violation protect
switchport port-security mac-address sticky
switchport port-security mac-address sticky 90b1.lc81.7068
!
interface FastEthernet0/4
switchport access vlan 20
switchport mode access
switchport port-security
switchport port-security violation protect
switchport port-security mac-address sticky
```

*Figure 5.2.18.2: Configure Port for Fedora Server*

**Step 3:** Configure port security for Ubuntu server with interface FastEthernet 0/5 and FastEthernet 0/6.

```
interface FastEthernet0/5
switchport access vlan 30
switchport mode access
switchport port-security maximum 2
switchport port-security
switchport port-security violation protect
switchport port-security mac-address sticky
switchport port-security mac-address sticky 90b1.lc81.7172
switchport port-security mac-address sticky a08c.fd7f.6df6
!
interface FastEthernet0/6
switchport access vlan 30
switchport mode access
switchport port-security maximum 2
switchport port-security
switchport port-security violation protect
switchport port-security mac-address sticky
```

*Figure 5.2.18.3: Configure Port for Ubuntu Server*

**Step 4:** Configure port security for Client wired server with interface FastEthernet 0/7 until FastEthernet 0/14.

```
interface FastEthernet0/7
switchport access vlan 40
switchport mode access
switchport port-security
switchport port-security violation protect
switchport port-security mac-address sticky
switchport port-security mac-address sticky 6400.6a59.1634
!
interface FastEthernet0/8
switchport access vlan 80
switchport mode access
switchport port-security
switchport port-security violation protect
switchport port-security mac-address sticky
shutdown
!
interface FastEthernet0/9
switchport access vlan 80
switchport mode access
switchport port-security
switchport port-security violation protect
switchport port-security mac-address sticky
switchport port-security mac-address sticky 90b1.lc81.7172
shutdown
!
```

*Figure 5.2.18.4: Configure Port for Client Wired Server*

```

!
interface FastEthernet0/10
switchport access vlan 80
switchport mode access
switchport port-security
switchport port-security violation protect
switchport port-security mac-address sticky
shutdown
!
interface FastEthernet0/11
switchport access vlan 80
switchport mode access
switchport port-security
switchport port-security violation protect
switchport port-security mac-address sticky
shutdown
!
interface FastEthernet0/12
switchport access vlan 80
switchport mode access
switchport port-security
switchport port-security violation protect
switchport port-security mac-address sticky
shutdown
!
interface FastEthernet0/13
switchport access vlan 80
switchport mode access
switchport port-security
switchport port-security violation protect
switchport port-security mac-address sticky
shutdown
!
interface FastEthernet0/14
switchport access vlan 80
switchport mode access
switchport port-security
switchport port-security violation protect
switchport port-security mac-address sticky
shutdown
!
```

*Figure 5.2.18.5: Configure Port for Client Wired Server*

**Step5:** Configure the error disable recovery with interval 300 seconds

```

Group10Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Group10Switch(config)#errdisable recovery cause psecure-violation
Group10Switch(config)#errdisable recovery interval 300
```

*Figure 5.2.18.6: Assign Error Disable to management*

## 5.2.19 Linux Server Hardening

### Ubuntu Server Hardening

#### 1) System Update

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

**Step 1:** Install the system update

Type command *sudo apt get update*

```
group10@group10:~$ sudo su
root@group10:/home/group10# sudo apt-get update
Hit:1 http://my.archive.ubuntu.com/ubuntu xenial InRelease
Get:2 http://security.ubuntu.com/ubuntu xenial-security InRelease [107 kB]
Get:3 http://my.archive.ubuntu.com/ubuntu xenial-updates InRelease [109 kB]
Hit:4 http://archive.canonical.com/ubuntu xenial InRelease
Get:5 http://my.archive.ubuntu.com/ubuntu xenial-backports InRelease [107 kB]
Fetched 323 kB in 2s (148 kB/s)
Reading package lists... Done
```

Figure 5.2.19.1: command to update

**Step 2 :** To Set daily update, go to Software and Updates. Then click *Updates* bar

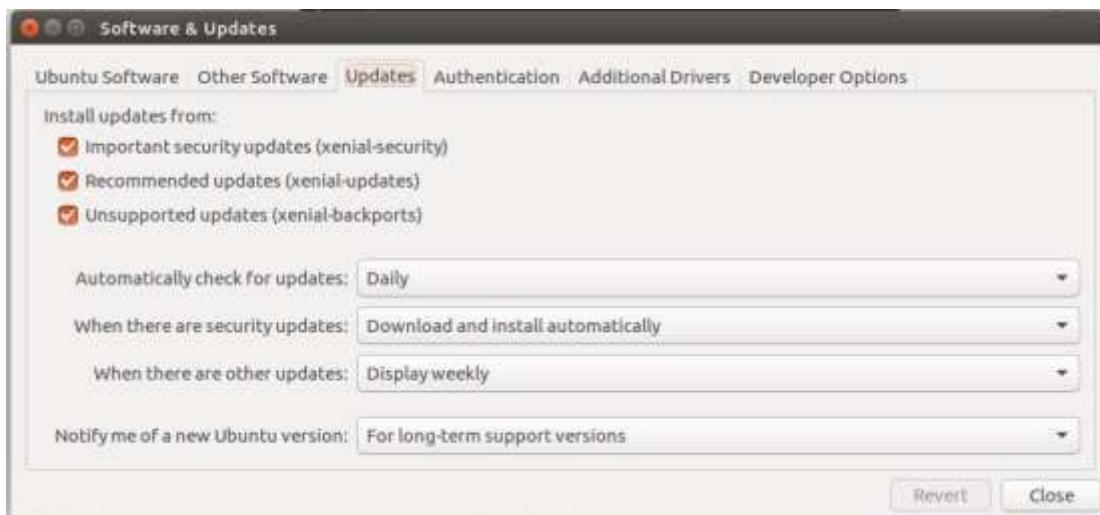


Figure 5.2.19.2: softwares and updates interface

**Step 3 :** Download Ubuntu Software Center if it not available. Ubuntu Software Center can used to monitor or check the software updates



Figure 5.2.19.3: interface of ubuntu software center

## 2) Password Expiration

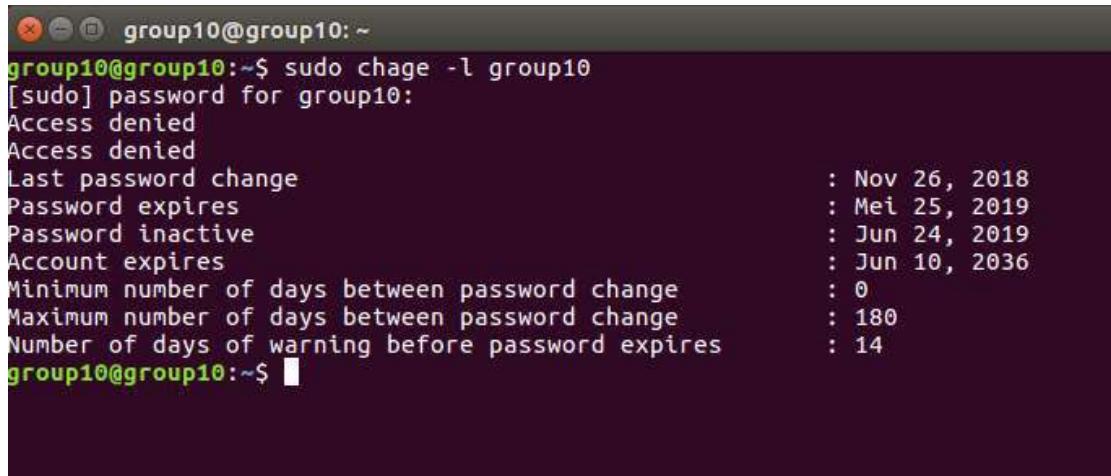
**Step1 :** When creating user accounts, we make the policy where it have minimum and maximum password age to force the user to change password.

```
root@group10:/home/group10# sudo chage -M 180 -I 30 -W 14 group10
```

Figure 5.2.19.4: Command to set the password

The following command is an example of how you manually change the password :

- > Maximum password age (-M) of 180 days,
- > Inactivity period (-I) of 30 days after password expiration
- > Warning time period (-W) of 14 days before password expiration.

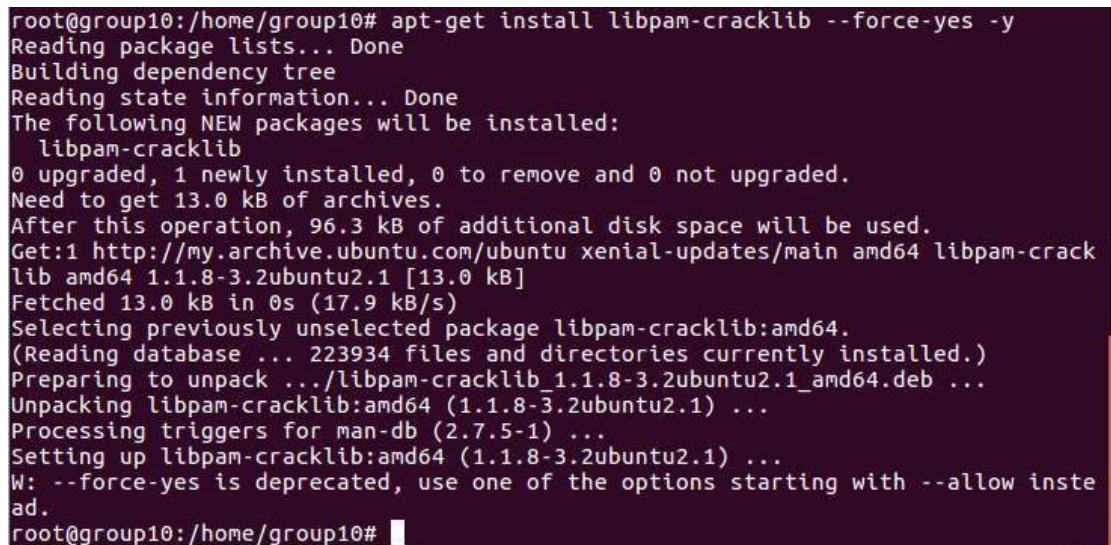


```
group10@group10:~$ sudo chage -l group10
[sudo] password for group10:
Access denied
Access denied
Last password change : Nov 26, 2018
Password expires      : Mei 25, 2019
Password inactive     : Jun 24, 2019
Account expires        : Jun 10, 2036
Minimum number of days between password change : 0
Maximum number of days between password change : 180
Number of days of warning before password expires : 14
group10@group10:~$
```

Figure 5.2.19.5: Show the password information

### 3) Set the minimum number of password

**Step 1 :** We set the minimum number of password to avoid the password easy to be crack



```
root@group10:/home/group10# apt-get install libpam-cracklib --force-yes -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  libpam-cracklib
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 13.0 kB of archives.
After this operation, 96.3 kB of additional disk space will be used.
Get:1 http://my.archive.ubuntu.com/ubuntu xenial-updates/main amd64 libpam-cracklib amd64 1.1.8-3.2ubuntu2.1 [13.0 kB]
Fetched 13.0 kB in 0s (17.9 kB/s)
Selecting previously unselected package libpam-cracklib:amd64.
(Reading database ... 223934 files and directories currently installed.)
Preparing to unpack .../libpam-cracklib_1.1.8-3.2ubuntu2.1_amd64.deb ...
Unpacking libpam-cracklib:amd64 (1.1.8-3.2ubuntu2.1) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up libpam-cracklib:amd64 (1.1.8-3.2ubuntu2.1) ...
W: --force-yes is deprecated, use one of the options starting with --allow instead.
root@group10:/home/group10#
```

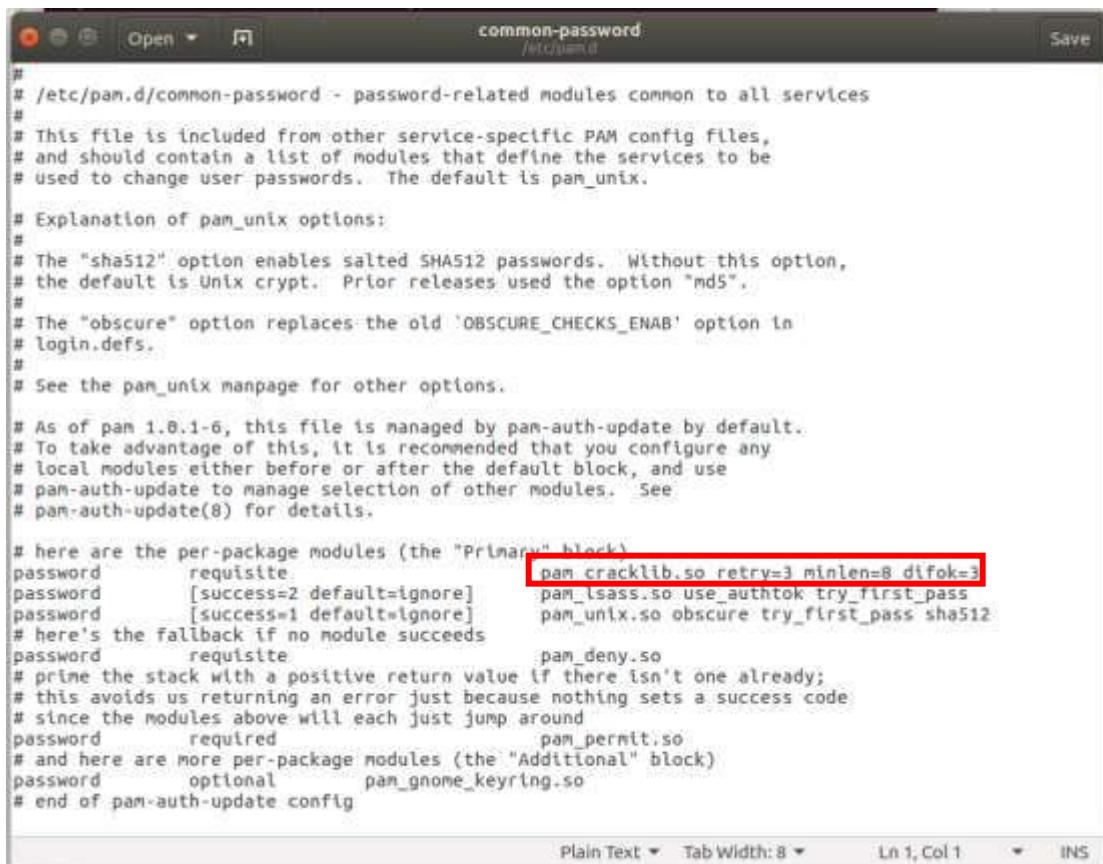
Figure 5.2.19.6: Command to install library for minimum password

**Step 2 :** Edit the configuration file of password



```
root@group10:/home/group10# gedit /etc/pam.d/common-password
```

Figure 5.2.19.7: Edit the configuration file



```
# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords. The default is pam_unix.
#
# Explanation of pam_unix options:
#
# The "sha512" option enables salted SHA512 passwords. Without this option,
# the default is Unix crypt. Prior releases used the option "md5".
#
# The "obscure" option replaces the old 'OBSCURE_CHECKS_ENAB' option in
# login.defs.
#
# See the pam_unix manpage for other options.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.
#
# here are the per-package modules (the "Primary" block)
password requisite pam_cracklib.so retry=3 minlen=8 difok=3
password [success=2 default=ignore] pam_lsass.so use_authtok try_first_pass
password [success=1 default=ignore] pam_unix.so obscure try_first_pass sha512
# here's the fallback if no module succeeds
password requisite pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password required pam_permit.so
# and here are more per-package modules (the "Additional" block)
password optional pam_gnome_keyring.so
# end of pam-auth-update config
```

Figure 5.2.19.8: Configuration file for minimum password

#### 4) Port Scanning

To find out which services are currently running, we need to install Nmap which is software for scanning port that has been used and running. Install Nmap software by using command below.

##### Step 1 :Installing Nmap

```
root@group10:/home/group10# apt-get install nmap
Reading package lists... Done
Building dependency tree
Reading state information... Done
nmap is already the newest version (7.01-2ubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Figure 5.2.19.9: install nmap

**Step 2 :** By using the command to identify open port:

```
root@group10:/home/group10# sudo nmap -v -sS localhost
Starting Nmap 7.01 ( https://nmap.org ) at 2018-11-27 09:34 +08
Failed to resolve "-v".
Failed to resolve "-sS".
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000080s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
143/tcp   open  imap
587/tcp   open  submission
631/tcp   open  ipp
993/tcp   open  imaps
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds
root@group10:/home/group10#
```

Figure 5.2.19.10: list of service in ubuntu server

Explanation of each port:

**Port 22:** used for ssh service

**Port 25:** used for smtp service

**Port 80:** port that the server "listens to" or expects to receive from a Web client.

**Port 143:** The Internet Message Access Protocol (IMAP) is a mail protocol used for accessing email on a remote web server from a local client.

**Port 587 :**This is the default mail submission port. When a mail client or server is submitting an email to be routed by a proper mail server, it should always use this port.

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

**Port 993 :** Use a defined protocol to communicate depending on the application. A protocol is a set of formalized rules that explains how data is communicated over a network.

**Port 3306 :** MySql Database

## 5) Disable CUPS and close port IPP

CUPS is a Common Unix Printing System is a modular printing system for Unix-like computer operating system which allow a computer to acts as a printing server. Our server does no need these services and we disabled it.

**Step 1:** Hardening system by disabling or removing unnecessary services to enhance security and improve overall system performance.

```
group10@group10:~$ sudo -i  
root@group10:~# echo "manual">> /etc/init/cups.override  
root@group10:~# sudo service cups stop
```

*Figure 5.2.19.11: Command to stop the services*

**Step 2 :**List of port using this command

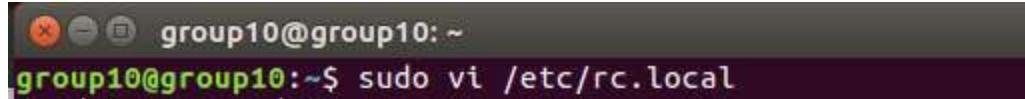
```
root@group10:~# sudo nmap -v -sT localhost  
  
Starting Nmap 7.01 ( https://nmap.org ) at 2018-11-28 03:15 +08  
Initiating Connect Scan at 03:15  
Scanning localhost (127.0.0.1) [1000 ports]  
Discovered open port 3306/tcp on 127.0.0.1  
Discovered open port 22/tcp on 127.0.0.1  
Discovered open port 25/tcp on 127.0.0.1  
Discovered open port 143/tcp on 127.0.0.1  
Discovered open port 80/tcp on 127.0.0.1  
Discovered open port 587/tcp on 127.0.0.1  
Discovered open port 993/tcp on 127.0.0.1  
Completed Connect Scan at 03:15, 0.01s elapsed (1000 total ports)  
Nmap scan report for localhost (127.0.0.1)  
Host is up (0.000074s latency).  
Not shown: 993 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
25/tcp    open  smtp  
80/tcp    open  http  
143/tcp   open  imap  
587/tcp   open  submission  
993/tcp   open  imaps  
3306/tcp  open  mysql  
  
Read data files from: /usr/bin/../share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds  
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
```

*Figure 5.2.19.12: show port and services*

## 6) Disable Bluetooth

Bluetooth is a standard for the short-range wireless interconnection of cellular phones, computers, and other electronic devices. As we do not use Bluetooth service so we can disabled Bluetooth service for security.

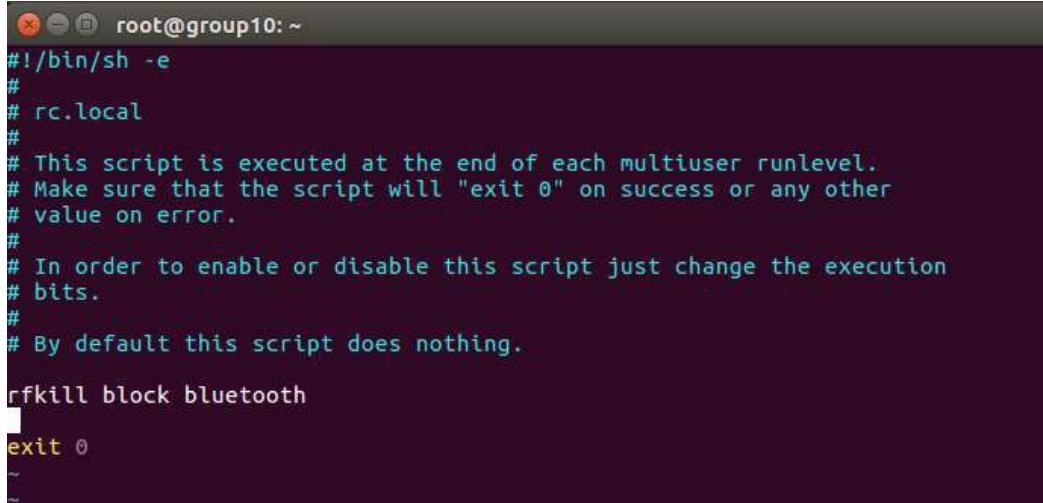
**Step 1 :** Open the local Configuration file of bluetooth



```
group10@group10:~$ sudo vi /etc/rc.local
```

Figure 5.2.19.13: command to open local configuration

**Step 2 :** Add this line “rfkill block bluetooth” before exit 0



```
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.

rfkill block bluetooth

exit 0
```

Figure 5.2.19.14: Edit local configuration

**Step 3 :** Save and Exit

**Step 4 :** Open the main configuration file of bluetooth



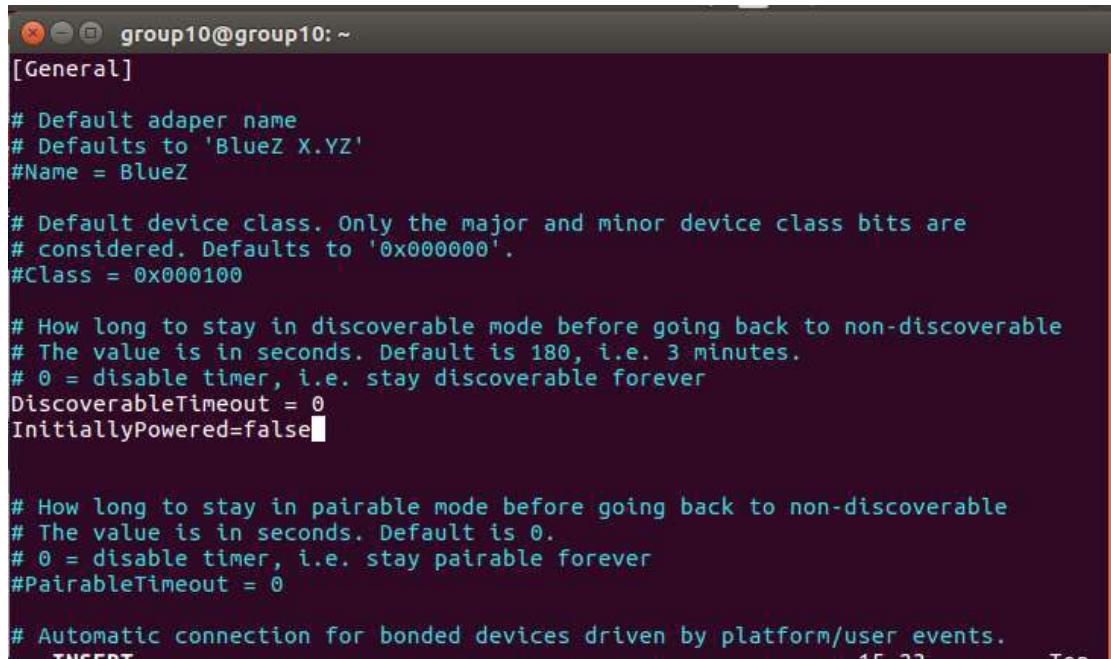
```
group10@group10:~$ sudo vi /etc/bluetooth/main.conf
```

Figure 5.2.19.15: command to open main configuration

**Step 5 :** Add this command

*DiscoverableTimeout=0*

*InitiallyPowered=false*



```
group10@group10:~ [General]
# Default adapter name
# Defaults to 'BlueZ X.YZ'
#Name = BlueZ

# Default device class. Only the major and minor device class bits are
# considered. Defaults to '0x000000'.
#Class = 0x000100

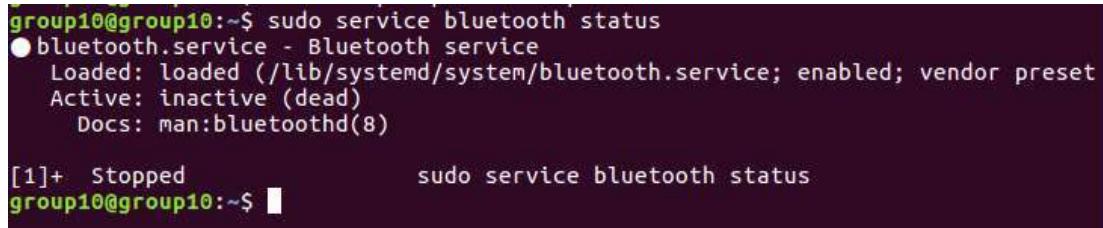
# How long to stay in discoverable mode before going back to non-discoverable
# The value is in seconds. Default is 180, i.e. 3 minutes.
# 0 = disable timer, i.e. stay discoverable forever
DiscoverableTimeout = 0
InitiallyPowered=false

# How long to stay in pairable mode before going back to non-discoverable
# The value is in seconds. Default is 0.
# 0 = disable timer, i.e. stay pairable forever
#PairableTimeout = 0

# Automatic connection for bonded devices driven by platform/user events.
#INSERT
```

Figure 5.2.19.16: Edit the main configuration

**Step 6 :** Save and exit

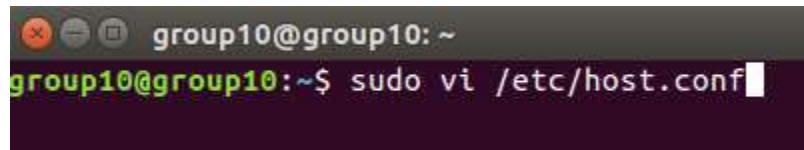


```
group10@group10:~$ sudo service bluetooth status
● bluetooth.service - Bluetooth service
  Loaded: loaded (/lib/systemd/system/bluetooth.service; enabled; vendor preset: enabled)
  Active: inactive (dead)
    Docs: man:bluetoothd(8)

[1]+  Stopped                  sudo service bluetooth status
group10@group10:~$
```

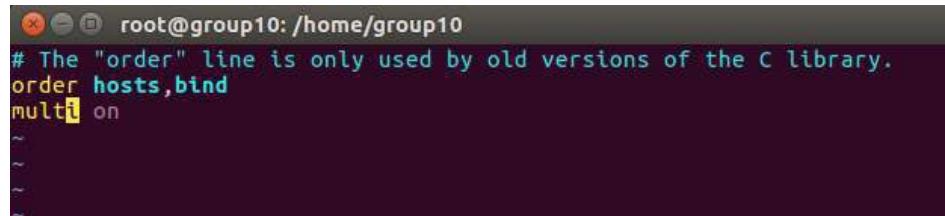
Figure 5.2.19.17: command to check status bluetooth

## 7) Prevent IP spoofing



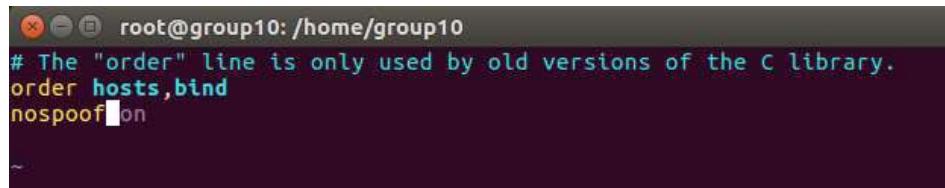
```
group10@group10:~$ sudo vi /etc/host.conf
```

Figure 5.2.19.18: command to open host configuration



```
root@group10: /home/group10
# The "order" line is only used by old versions of the C library.
order hosts,bind
multi on
~
```

Figure 5.2.19.19: Before edit the configuration



```
root@group10: /home/group10
# The "order" line is only used by old versions of the C library.
order hosts,bind
nospoof on
~
```

Figure 5.2.19.20: After edit the configuration

## Fedora Server Hardening

### 1) System Update

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

**Step 1:** Install the system update

Type command # *dnf get update*

```
[group10@Nuqman ~]$ sudo -i
[sudo] password for group10:
[root@Nuqman ~]# dnf update
Last metadata expiration check: 0:41:51 ago on Thu 29 Nov 2018 10:33:04 AM +08.
Dependencies resolved.
=====
Package           Arch   Version      Repository  Size
=====
Installing:
  kernel          x86_64 4.19.3-200.fc28    updates     100 k
  kernel-core      x86_64 4.19.3-200.fc28    updates     24 M
  kernel-modules   x86_64 4.19.3-200.fc28    updates     28 M
  kernel-modules-extra x86_64 4.19.3-200.fc28    updates     2.2 M
Upgrading:
  authselect       x86_64 1.0.2-1.fc28     updates     70 k
  authselect-compat x86_64 1.0.2-1.fc28     updates     34 k
  authselect-libs   x86_64 1.0.2-1.fc28     updates     151 k
  babl             x86_64 0.1.60-1.fc28    updates     330 k
  compat-ffmpeg28  x86_64 2.8.15-1.fc28   rpmfusion-free-updates
                                         5.6 M
  cups-filters      x86_64 1.20.0-12.fc28   updates     774 k
  cups-filters-libs x86_64 1.20.0-12.fc28   updates     133 k
  curl              x86_64 7.59.0-9.fc28    updates     330 k
  distribution-gpg-keys noarch 1.26-1.fc28    updates     187 k
  edk2-ovmf        noarch 20180815gitcb5f4f45ce-2.fc28
                                         3.3 M
  elfutils          x86_64 0.174-5.fc28     updates     340 k
  elfutils-default-libs noarch 0.174-5.fc28   updates     45 k
```

Figure 5.2.19.21: update fedora server system

```
root@Nuqman:~  
File Edit View Search Terminal Help  
xorg-x11-drv-ati           x86_64 18.1.0-1.fc28      updates   171 k  
zchunk-libs                 x86_64 0.9.15-1.fc28    updates   44 k  
Installing weak dependencies:  
  p11-kit-server             x86_64 0.23.14-1.fc28    updates   234 k  
Removing:  
  kernel                     x86_64 4.18.14-200.fc28 @updates   0  
  kernel-core                x86_64 4.18.14-200.fc28 @updates   60 M  
  kernel-modules              x86_64 4.18.14-200.fc28 @updates   27 M  
  kernel-modules-extra        x86_64 4.18.14-200.fc28 @updates   2.1 M  
  
Transaction Summary  
=====  
Install  5 Packages  
Upgrade  94 Packages  
Remove   4 Packages  
  
Total download size: 285 M  
Is this ok [y/N]: y  
Downloading Packages:  
(1/99): kernel-4.19.3-200.fc28.x86_64.rpm      82 kB/s | 100 kB  00:01  
(2/99): kernel-modules-extra-4.19.3-200.fc28.x8 1.1 MB/s | 2.2 MB  00:02  
(3/99): p11-kit-server-0.23.14-1.fc28.x86_64.rp 646 kB/s | 234 kB  00:00  
(4/99): authselect-1.0.2-1.fc28.x86_64.rpm     197 kB/s | 70 kB   00:00  
(5/99): authselect-libs-1.0.2-1.fc28.x86_64.rpm 295 kB/s | 151 kB  00:00  
(6/99): authselect-compat-1.0.2-1.fc28.x86_64.r 136 kB/s | 34 kB   00:00  
(7/99): babl-0.1.60-1.fc28.x86_64.rpm       798 kB/s | 330 kB  00:00  
(8/99): kernel-core-4.19.3-200.fc28.x86_64.rpm 3.5 MB/s | 24 MB   00:06  
(9/99): cups-filters-1.20.0-12.fc28.x86_64.rpm 2.6 MB/s | 774 kB  00:00  
(10/99): cups-filters-libs-1.20.0-12.fc28.x86_6 336 kB/s | 133 kB  00:00  
(11/99): curl-7.59.0-9.fc28.x86_64.rpm       919 kB/s | 330 kB  00:00
```

Figure 5.2.19.22: update process 1

```

root@Nuqman:~ x
File Edit View Search Terminal Help
(97/99): zchunk-libs-0.9.15-1.fc28.x86_64.rpm 230 kB/s | 44 kB 00:00
(98/99): webkit2gtk3-plugin-process-gtk2-2.22.4 2.5 MB/s | 11 MB 00:04
(99/99): flash-player-npapi-31.0.0.153-release. 71 kB/s | 8.6 MB 02:04
-----
Total 2.0 MB/s | 285 MB 02:23

Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Running scriptlet: firefox-63.0.3-2.fc28.x86_64 1/1
  Preparing : 1/1
  Running scriptlet: ghc-base-4.10.1.0-70.fc28.x86_64 1/1
  Upgrading : ghc-base-4.10.1.0-70.fc28.x86_64 1/198
  Upgrading : ghc-array-0.5.2.0-70.fc28.x86_64 2/198
  Upgrading : ghc-deepseq-1.4.3.0-70.fc28.x86_64 3/198
  Upgrading : libxcrypt-4.4.0-2.fc28.x86_64 4/198
  Upgrading : ghc-bytestring-0.10.8.2-70.fc28.x86_64 5/198
  Upgrading : ghc-time-1.8.0.2-70.fc28.x86_64 6/198
  Upgrading : libarchive-3.3.3-1.fc28.x86_64 7/198
  Upgrading : ibus-libs-1.5.19-8.fc28.x86_64 8/198
  Installing : kernel-core-4.19.3-200.fc28.x86_64 9/198
  Running scriptlet: kernel-core-4.19.3-200.fc28.x86_64 9/198
  Installing : kernel-modules-4.19.3-200.fc28.x86_64 10/198
  Running scriptlet: kernel-modules-4.19.3-200.fc28.x86_64 10/198
  Upgrading : ghc-unix-2.7.2.2-70.fc28.x86_64 11/198
  Upgrading : ghcfilepath-1.4.1.2-70.fc28.x86_64 12/198
  Upgrading : webkit2gtk3-jsc-2.22.4-1.fc28.x86_64 13/198
  Upgrading : mariadb-config-3:10.2.19-1.fc28.x86_64 14/198
  Upgrading : mariadb-common-3:10.2.19-1.fc28.x86_64 15/198

```

*Figure 5.2.19.23: update process 2*

```
root@Nuqman:~  
File Edit View Search Terminal Help  
Cleanup : libconfuse-3.2.1-2.fc28.x86_64 190/198  
Running scriptlet: libconfuse-3.2.1-2.fc28.x86_64 190/198  
Cleanup : gtksourceview3-3.24.8-1.fc28.x86_64 191/198  
Cleanup : gnome-abrt-1.2.6-5.fc28.x86_64 192/198  
Cleanup : glx-utils-8.3.0-9.fc28.x86_64 193/198  
Cleanup : glibmm24-2.56.0-1.fc28.x86_64 194/198  
Cleanup : gjs-1.52.3-1.fc28.x86_64 195/198  
Running scriptlet: flash-plugin-31.0.0.148-release.x86_64 196/198  
Cleanup : flash-plugin-31.0.0.148-release.x86_64 196/198  
Running scriptlet: flash-plugin-31.0.0.148-release.x86_64 196/198  
Cleanup : eog-3.28.3-1.fc28.x86_64 197/198  
Cleanup : babl-0.1.56-2.fc28.x86_64 198/198  
Running scriptlet: kernel-core-4.19.3-200.fc28.x86_64 198/198  
Running scriptlet: ibus-1.5.19-8.fc28.x86_64 198/198  
Running scriptlet: authselect-libs-1.0.2-1.fc28.x86_64 198/198  
Running scriptlet: authselect-compat-1.0.2-1.fc28.x86_64 198/198  
Running scriptlet: firefox-63.0.3-2.fc28.x86_64 198/198  
Running scriptlet: babl-0.1.56-2.fc28.x86_64 198/198  
Verifying : kernel-core-4.19.3-200.fc28.x86_64 1/198  
Verifying : kernel-4.19.3-200.fc28.x86_64 2/198  
Verifying : kernel-modules-4.19.3-200.fc28.x86_64 3/198  
Verifying : kernel-modules-extra-4.19.3-200.fc28.x86_64 4/198  
Verifying : p11-kit-server-0.23.14-1.fc28.x86_64 5/198  
Verifying : authselect-1.0.2-1.fc28.x86_64 6/198  
Verifying : authselect-libs-1.0.2-1.fc28.x86_64 7/198  
Verifying : authselect-compat-1.0.2-1.fc28.x86_64 8/198  
Verifying : babl-0.1.60-1.fc28.x86_64 9/198  
Verifying : compat-ffmpeg28-2.8.15-1.fc28.x86_64 10/198  
Verifying : cups-filters-1.20.0-12.fc28.x86_64 11/198  
Verifying : cups-filters-libs-1.20.0-12.fc28.x86_64 12/198
```

Figure 5.2.19.24: update process 3

```
root@Nuqman:~  
File Edit View Search Terminal Help  
verifying... python3-dbus-1.22-3.fc28.noarch  
190/190  
  
Removed:  
kernel.x86_64 4.18.14-200.fc28  
kernel-core.x86_64 4.18.14-200.fc28  
kernel-modules.x86_64 4.18.14-200.fc28  
kernel-modules-extra.x86_64 4.18.14-200.fc28  
  
Installed:  
kernel.x86_64 4.19.3-200.fc28  
kernel-core.x86_64 4.19.3-200.fc28  
kernel-modules.x86_64 4.19.3-200.fc28  
kernel-modules-extra.x86_64 4.19.3-200.fc28  
p11-kit-server.x86_64 0.23.14-1.fc28  
  
Upgraded:  
authselect.x86_64 1.0.2-1.fc28  
authselect-compat.x86_64 1.0.2-1.fc28  
authselect-libs.x86_64 1.0.2-1.fc28  
babl.x86_64 0.1.60-1.fc28  
compat-ffmpeg28.x86_64 2.8.15-1.fc28  
cups-filters.x86_64 1.20.0-12.fc28  
cups-filters-libs.x86_64 1.20.0-12.fc28  
curl.x86_64 7.59.0-9.fc28  
distribution-gpg-keys.noarch 1.26-1.fc28  
edk2-ovmf.noarch 20180815gitcb5f4f45ce-2.fc28  
elfutils.x86_64 0.174-5.fc28  
elfutils-default-yama-scope.noarch 0.174-5.fc28  
elfutils-libelf.x86_64 0.174-5.fc28  
elfutils-libs.x86_64 0.174-5.fc28
```

Figure 5.2.19.25: update process 4

The screenshot shows a terminal window titled 'root@Nuqman:~'. The window contains the following text:

```
File Edit View Search Terminal Help
mariadb.x86_64 3:10.2.19-1.fc28
mariadb-backup.x86_64 3:10.2.19-1.fc28
mariadb-common.x86_64 3:10.2.19-1.fc28
mariadb-config.x86_64 3:10.2.19-1.fc28
mariadb-cracklib-password-check.x86_64 3:10.2.19-1.fc28
mariadberrmsg.x86_64 3:10.2.19-1.fc28
mariadb-gssapi-server.x86_64 3:10.2.19-1.fc28
mariadb-rocksdb-engine.x86_64 3:10.2.19-1.fc28
mariadb-server.x86_64 3:10.2.19-1.fc28
mariadb-server-utils.x86_64 3:10.2.19-1.fc28
mariadb-tokudb-engine.x86_64 3:10.2.19-1.fc28
nfs-utils.x86_64 1:2.3.3-1.rc1.fc28
poppler.x86_64 0.62.0-10.fc28
poppler-glib.x86_64 0.62.0-10.fc28
poppler-utils.x86_64 0.62.0-10.fc28
python3-hawkey.x86_64 0.11.1-6.fc28.1
python3-urllib3.noarch 1.24.1-2.fc28
soundtouch.x86_64 2.1.1-1.fc28
tzdata.noarch 2018g-1.fc28
tzdata-java.noarch 2018g-1.fc28
vim-minimal.x86_64 2:8.1.513-2.fc28
virtualbox-guest-additions.x86_64 5.2.22-1.fc28
webkit2gtk3.x86_64 2.22.4-1.fc28
webkit2gtk3-jsc.x86_64 2.22.4-1.fc28
webkit2gtk3-plugin-process-gtk2.x86_64 2.22.4-1.fc28
xorg-x11-drv-ati.x86_64 18.1.0-1.fc28
zchunk-libs.x86_64 0.9.15-1.fc28

Complete!
[root@Nuqman ~]#
```

Figure 5.2.19.26: update complete

## 2) Password Expiration

**Step 1 :** Show the current password information

The screenshot shows a terminal window titled '[root@Nuqman ~]#'. The window contains the following text:

```
chage -l group10
Last password change : Mar 05, 2018
Password expires      : never
Password inactive     : never
Account expires        : never
Minimum number of days between password change : 0
Maximum number of days between password change   : 99999
Number of days of warning before password expires  : 7
```

Figure 5.2.19.27: Password info before edit

**Step 2:** When creating user accounts, we make the policy where it have minimum and maximum password age to force the user to change password.

The following command is an example of how you manually change the password :

```
[root@Nuqman ~]# chage -I 30 group10
[root@Nuqman ~]# chage -m 1 group10
[root@Nuqman ~]# chage -M 30 group10
[root@Nuqman ~]# chage -W 25 group10
[root@Nuqman ~]# chage -m 5 group10
```

*Figure 5.2.19.28:command to edit*

```
[root@Nuqman ~]# chage -l group10
Last password change : Dec 30, 2018
Password expires       : Jan 29, 2019
Password inactive      : Feb 28, 2019
Account expires        : Apr 04, 2019
Minimum number of days between password change : 5
Maximum number of days between password change : 30
Number of days of warning before password expires : 25
```

*Figure 5.2.19.29: after edit*

```
[root@Nuqman ~]# chage group10
Changing the aging information for group10
Enter the new value, or press ENTER for the default

    Minimum Password Age [5]:
    Maximum Password Age [30]:
    Last Password Change (YYYY-MM-DD) [2018-12-30]:
    Password Expiration Warning [25]:
    Password Inactive [30]:
    Account Expiration Date (YYYY-MM-DD) [2019-04-04]:
[root@Nuqman ~]#
```

*Figure 5.2.19.30: command to edit password*

### 3) Port Scanning

To find out which services are currently running, we need to install Nmap which is software for scanning port that has been used and running. Install Nmap software by using command below.

#### Step 1 :Installing Nmap

```
[root@Nuqman ~]# yum install nmap
Last metadata expiration check: 2:10:46 ago on Thu 29 Nov 2018 10:33:04 AM +08.
Dependencies resolved.
=====
 Package      Arch      Version       Repository      Size
 =====
 Installing:
 nmap        x86_64    2:7.60-12.fc28      fedora      5.7 M

 Transaction Summary
 =====
 Install 1 Package

 Total download size: 5.7 M
 Installed size: 22 M
 Is this ok [y/N]: y
 Downloading Packages:
 nmap-7.60-12.fc28.x86_64.rpm          1.7 MB/s | 5.7 MB   00:03
 -----
 Total                                         1.1 MB/s | 5.7 MB   00:05

 Running transaction check
 Transaction check succeeded.
 Running transaction test
 Transaction test succeeded.
 Running transaction
   Preparing           : 1/1
   Installing         : nmap-2:7.60-12.fc28.x86_64 1/1
   Running scriptlet: nmap-2:7.60-12.fc28.x86_64 1/1
   Verifying           : nmap-2:7.60-12.fc28.x86_64 1/1

 Installed:
   nmap.x86_64 2:7.60-12.fc28

 Complete!
 [root@Nuqman ~]# █
```

Figure 5.2.19.32: Finish Installing

**Step 2 :** By using the command to identify open port:

```
[root@Nuqman ~]# nmap -v -sT localhost
Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-29 12:47 +08
Initiating Connect Scan at 12:47
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 22/tcp on 127.0.0.1
Discovered open port 3306/tcp on 127.0.0.1
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 199/tcp on 127.0.0.1
Discovered open port 631/tcp on 127.0.0.1
Completed Connect Scan at 12:47, 0.04s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00027s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
199/tcp   open  smux
631/tcp   open  ipp
3306/tcp  open  mysql

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
[root@Nuqman ~]#
```

*Figure 5.2.19.33: View open port*

Explanation of each port:

**Port 22:** used for ssh service

**Port 80:** port that the server "listens to" or expects to receive from a Web client.

**Port 199:** Support for the SMUX (RFC 1227) protocol is unique to Advanced Routing Suite due to its intended installation as a daemon running on a multi-user timeshare operating system. While this paradigm continues to evolve, an original intent of the SMUX protocol implement was to allow Advanced Routing Suite to inter-operate with another daemon handling the SNMP protocol and communicate with management stations

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

**Port 3306 :** MySql Database

#### 4) Disable Services

**Step 1** :List of port using this command

```
[root@Nuqman ~]# nmap -v -sT localhost

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-29 12:47 +08
Initiating Connect Scan at 12:47
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 22/tcp on 127.0.0.1
Discovered open port 3306/tcp on 127.0.0.1
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 199/tcp on 127.0.0.1
Discovered open port 631/tcp on 127.0.0.1
Completed Connect Scan at 12:47, 0.04s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00027s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
199/tcp   open  smux
631/tcp   open  ipp
3306/tcp  open  mysql

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
[root@Nuqman ~]#
```

*Figure 5.2.19.34: Port open*

**Step 2:** Hardening system by disabling or removing unnecessary services to enhance security and improve overall system performance.

```
[root@Nuqman ~]# service cups stop
Redirecting to /bin/systemctl stop cups.service
```

*Figure 5.2.19.35: Disable service*

```
[root@Nuqman ~]# nmap -v -sT localhost
Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-29 12:49 +08
Initiating Connect Scan at 12:49
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 199/tcp on 127.0.0.1
Discovered open port 22/tcp on 127.0.0.1
Discovered open port 3306/tcp on 127.0.0.1
Completed Connect Scan at 12:49, 0.03s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00019s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
199/tcp   open  smux
3306/tcp  open  mysql

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
[root@Nuqman ~]#
```

*Figure 5.2.19.36: Result*

## 5) Disable Bluetooth

Bluetooth is a standard for the short-range wireless interconnection of cellular phones, computers, and other electronic devices. As we do not use Bluetooth service so we can disabled Bluetooth service for security.

### Step 1 : Check the bluetooth status

```
[group10@Nuqman ~]$ bluetooth status
bash: bluetooth: command not found...
Install package 'tlp' to provide command 'bluetooth'? [N/y] y

* Waiting in queue...
* Loading list of packages...
The following packages have to be installed:
esmtp-1.2-10.fc28.x86_64      User configurable send-only Mail Transfer Agent
hdparm-9.56-1.fc28.x86_64      A utility for displaying and/or setting hard disk parameters
kernel-tools-4.19.3-200.fc28.x86_64 Assortment of tools for the Linux kernel
kernel-tools-libs-4.19.3-200.fc28.x86_64 Libraries for the kernels-tools
```

*Figure 5.2.19.37: Bluetooth Status*

```
redhat-lsb-core-4.1-44.fc28.x86_64      LSB Core module support
redhat-lsb-submod-security-4.1-44.fc28.x86_64  LSB Security submodule support
spax-1.5.3-14.fc28.x86_64      Portable archive exchange
tlp-1.1-1.fc28.noarch  Advanced power management tool for Linux
Proceed with changes? [N/y] y

* Waiting in queue...
* Waiting for authentication...
* Waiting in queue...
* Downloading packages...
* Requesting data...
* Testing changes...
* Installing packages...
bluetooth = none (no device)
```

*Figure 5.2.19.38: Processing*

**Step 2 :**Type the command to of the bluetooth service

```
[root@Nuqman ~]# chkconfig bluetooth off
Note: Forwarding request to 'systemctl disable bluetooth.service'.
Removed /etc/systemd/system/dbus-org.bluez.service.
Removed /etc/systemd/system/bluetooth.target.wants/bluetooth.service.
[root@Nuqman ~]# bluetooth status
bash: bluetooth: command not found...
Install package 'tlp' to provide command 'bluetooth'? [N/y]
```

*Figure 5.2.19.39:Command to close*

### 5.2.20 Intrusion Detection System (IDS) & Port Mirror

#### Step 1 : Intrusion Detection System

A) Install Snort prerequisites:

```
group10@group10:~$ sudo apt-get install update
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package update
group10@group10:~$ █
```

Figure 5.2.19.1: install update

```
group10@group10:~$ sudo apt-get install -y build-essential
Reading package lists... Done
Building dependency tree
Reading state information... Done
build-essential is already the newest version (12.1ubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 9 not upgraded.
group10@group10:~$ █
```

Figure 5.2.19.2: install build-essential

```
group10@group10:~$ sudo apt-get install -y libpcap-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libpcap0.8-dev
The following NEW packages will be installed:
  libpcap-dev libpcap0.8-dev
0 upgraded, 2 newly installed, 0 to remove and 9 not upgraded.
Need to get 216 kB of archives.
After this operation, 734 kB of additional disk space will be used.
Get:1 http://my.archive.ubuntu.com/ubuntu xenial/main amd64 libpcap0.8-dev amd64
  1.7.4-2 [212 kB]
Get:2 http://my.archive.ubuntu.com/ubuntu xenial/main amd64 libpcap-dev all 1.7.
4-2 [3,394 B]
Fetched 216 kB in 1s (140 kB/s)
Selecting previously unselected package libpcap0.8-dev.
(Reading database ... 219536 files and directories currently installed.)
Preparing to unpack .../libpcap0.8-dev_1.7.4-2_amd64.deb ...
Unpacking libpcap0.8-dev (1.7.4-2) ...
Selecting previously unselected package libpcap-dev.
```

Figure 5.2.19.3: install libpcap-dev

```
group10@group10:~$ sudo apt-get install libpcre3-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libpcre32-3 libpcrecpp0v5
The following NEW packages will be installed:
  libpcre3-dev libpcre32-3 libpcrecpp0v5
0 upgraded, 3 newly installed, 0 to remove and 9 not upgraded.
Need to get 676 kB of archives.
After this operation, 2,979 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://my.archive.ubuntu.com/ubuntu xenial/main amd64 libpcrecpp0v5 amd64
2:8.38-3.1 [15.2 kB]
Get:2 http://my.archive.ubuntu.com/ubuntu xenial/main amd64 libpcre32-3 amd64 2:
8.38-3.1 [136 kB]
Get:3 http://my.archive.ubuntu.com/ubuntu xenial/main amd64 libpcre3-dev amd64 2
:8.38-3.1 [525 kB]
Fetched 676 kB in 1s (352 kB/s)
Selecting previously unselected package libpcrecpp0v5:amd64.
(Reading database ... 219633 files and directories currently installed.)
Preparing to unpack .../libpcrecpp0v5_2%3a8.38-3.1_amd64.deb ...
Unpacking libpcrecpp0v5:amd64 (2:8.38-3.1) ...
Selecting previously unselected package libpcre32-3:amd64.
```

Figure 5.2.19.4: install libpcre3-dev

```
group10@group10:~$ sudo apt-get install libdumbnet-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libdumbnet1
The following NEW packages will be installed:
  libdumbnet-dev libdumbnet1
0 upgraded, 2 newly installed, 0 to remove and 9 not upgraded.
Need to get 81.7 kB of archives.
After this operation, 321 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://my.archive.ubuntu.com/ubuntu xenial/main amd64 libdumbnet1 amd64 1.
12-7 [25.7 kB]
Get:2 http://my.archive.ubuntu.com/ubuntu xenial/main amd64 libdumbnet-dev amd64
1.12-7 [55.9 kB]
Fetched 81.7 kB in 1s (61.9 kB/s)
Selecting previously unselected package libdumbnet1:amd64.
(Reading database ... 219773 files and directories currently installed.)
Preparing to unpack .../libdumbnet1_1.12-7_amd64.deb ...
Unpacking libdumbnet1:amd64 (1.12-7) ...
Selecting previously unselected package libdumbnet-dev.
Preparing to unpack .../libdumbnet-dev_1.12-7_amd64.deb ...
Unpacking libdumbnet-dev (1.12-7) ...
```

Figure 5.2.19.5: install libdumbnet-dev

```
group10@group10:~$ sudo apt-get install zlib1g-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  zlib1g-dev
0 upgraded, 1 newly installed, 0 to remove and 9 not upgraded.
Need to get 168 kB of archives.
After this operation, 425 kB of additional disk space will be used.
Get:1 http://my.archive.ubuntu.com/ubuntu xenial-updates/main amd64 zlib1g-dev a
md64 1:1.2.8.dfsg-2ubuntu4.1 [168 kB]
Fetched 168 kB in 1s (133 kB/s)
Selecting previously unselected package zlib1g-dev:amd64.
(Reading database ... 219812 files and directories currently installed.)
Preparing to unpack .../zlib1g-dev_1%3a1.2.8.dfsg-2ubuntu4.1_amd64.deb ...
Unpacking zlib1g-dev:amd64 (1:1.2.8.dfsg-2ubuntu4.1) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up zlib1g-dev:amd64 (1:1.2.8.dfsg-2ubuntu4.1) ...
group10@group10:~$
```

Figure 5.2.19.6: install zlib1g-dev

## B) Installing DAQ Pre-Requisites

```
group10@group10:~$ sudo apt-get install bison flex
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libbison-dev libfl-dev libsigsegv2 m4
Suggested packages:
  bison-doc
The following NEW packages will be installed:
  bison flex libbison-dev libfl-dev libsigsegv2 m4
0 upgraded, 6 newly installed, 0 to remove and 9 not upgraded.
Need to get 1,108 kB of archives.
After this operation, 3,101 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://my.archive.ubuntu.com/ubuntu xenial/main amd64 libsigsegv2 amd64 2.
10-4 [14.1 kB]
Get:2 http://my.archive.ubuntu.com/ubuntu xenial/main amd64 m4 amd64 1.4.17-5 [1
95 kB]
Get:3 http://my.archive.ubuntu.com/ubuntu xenial/main amd64 libfl-dev amd64 2.6.
0-11 [12.5 kB]
Get:4 http://my.archive.ubuntu.com/ubuntu xenial/main amd64 flex amd64 2.6.0-11
[290 kB]
```

Figure 5.2.19.7: install bison flex

```

group10@group10:~$ sudo apt-get install openssh-server ethtool build-essential libpcap-dev libpcre3-dev libdumbnet-dev bison flex zlib1g-dev liblzma-dev openssl libssl-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
bison is already the newest version (2:3.0.4.dfsg-1).
build-essential is already the newest version (12.1ubuntu2).
ethtool is already the newest version (1:4.5-1).
flex is already the newest version (2.6.0-11).
libdumbnet-dev is already the newest version (1.12-7).
liblzma-dev is already the newest version (5.1.1alpha+20120614-2ubuntu2).
libpcap-dev is already the newest version (1.7.4-2).
libpcre3-dev is already the newest version (2:8.38-3.1).
libssl-dev is already the newest version (1.0.2g-1ubuntu4.13).
openssh-server is already the newest version (1:7.2p2-4ubuntu2.5).
openssl is already the newest version (1.0.2g-1ubuntu4.13).
zlib1g-dev is already the newest version (1:1.2.8.dfsg-2ubuntu4.1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
group10@group10:~$ █

```

*Figure 5.2.19.8: install all dependencies*

C) Download, build and Install the latest DAQ (Data Acquisition Library) which is 2.0.6.

```

group10@group10:~$ sudo wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
--2018-10-26 03:56:20-- https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
Resolving www.snort.org (www.snort.org)... 2400:cb00:2048:1::6810:3f4b, 2400:cb00:2048:1::6810:404b, 2400:cb00:2048:1::6810:3e4b, ...
Connecting to www.snort.org (www.snort.org)|2400:cb00:2048:1::6810:3f4b|:443...
failed: Network is unreachable.
Connecting to www.snort.org (www.snort.org)|2400:cb00:2048:1::6810:404b|:443...
failed: Network is unreachable.
Connecting to www.snort.org (www.snort.org)|2400:cb00:2048:1::6810:3e4b|:443...
failed: Network is unreachable.
Connecting to www.snort.org (www.snort.org)|2400:cb00:2048:1::6810:414b|:443...
failed: Network is unreachable.
Connecting to www.snort.org (www.snort.org)|2400:cb00:2048:1::6810:424b|:443...
failed: Network is unreachable.
Connecting to www.snort.org (www.snort.org)|104.16.66.75|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/008/756/original/daq-2.0.6.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20181026%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20181026T061840Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=122d6990c0be1c3f696c3679679fc00824e5d729359fdf75d5b1d148c8e4c289 [following]
--2018-10-26 03:56:21-- https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/008/756/original/daq-2.0.6.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20181026%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20181026T061840Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=122d6990c0be1c3f696c3679679fc00824e5d729359fdf75d5b1d148c8e4c289
Resolving snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)... 5

```

*Figure 5.2.19.9: install daq-2.0.6*

E) After DAQ completely install, extract the source code and change into the new directory with the following commands.

```
group10@group10:~  
group10@group10:/home$ cd group10  
group10@group10:~/group10$ tar -zxvf daq-2.0.6.tar.gz  
daq-2.0.6/  
daq-2.0.6/ChangeLog  
daq-2.0.6/missing  
daq-2.0.6/daq.dsp  
daq-2.0.6/configure  
daq-2.0.6/sfbpf/  
daq-2.0.6/sfbpf/sf_bpf_printer.c  
daq-2.0.6/sfbpf/IP6_misc.h  
daq-2.0.6/sfbpf/sf_gencode.c  
daq-2.0.6/sfbpf/llc.h  
daq-2.0.6/sfbpf/ppp.h  
daq-2.0.6/sfbpf/grammar.y  
daq-2.0.6/sfbpf/sf_nametoaddr.c  
daq-2.0.6/sfbpf/sf_bpf_filter.c  
daq-2.0.6/sfbpf/sfbpf_dlt.h  
daq-2.0.6/sfbpf/etherstype.h  
daq-2.0.6/sfbpf/arcnet.h  
daq-2.0.6/sfbpf/ieee80211.h  
daq-2.0.6/sfbpf/sfbpf-int.h  
daq-2.0.6/sfbpf/namedb.h  
daq-2.0.6/sfbpf/Makefile.am  
daq-2.0.6/sfbpf/runlex.sh  
daq-2.0.6/sfbpf/atmuni31.h  
daq-2.0.6/sfbpf/sf-redefines.h  
daq-2.0.6/sfbpf/win32-stdinc.h  
daq-2.0.6/sfbpf/sunatmpos.h  
daq-2.0.6/sfbpf/sf_optimize.c  
daq-2.0.6/sfbpf/sfbpf-int.c  
daq-2.0.6/sfbpf/sfbpf.h  
daq-2.0.6/sfbpf/gencode.h  
daq-2.0.6/sfbpf/scanner.l  
daq-2.0.6/sfbpf/bittypes.h  
daq-2.0.6/sfbpf/sll.h  
daq-2.0.6/sfbpf/nlpid.h  
daq-2.0.6/sfbpf/Makefile.in  
daq-2.0.6/sfbpf/ipnet.h  
daq-2.0.6/compile  
daq-2.0.6/install-sh  
daq-2.0.6/Makefile.am  
daq-2.0.6/config.sub  
daq-2.0.6/os-daq-modules/  
daq-2.0.6/os-daq-modules/daq_ipfw.c  
daq-2.0.6/os-daq-modules/daq_ipq.c  
daq-2.0.6/os-daq-modules/daq_static_modules.c  
daq-2.0.6/os-daq-modules/daq_pcap.c  
daq-2.0.6/os-daq-modules/daq_nfq.c  
daq-2.0.6/os-daq-modules/daq_afpacket.c  
daq-2.0.6/os-daq-modules/daq-modules-config.in  
daq-2.0.6/os-daq-modules/Makefile.am
```

Figure 5.2.19.10: extract daq-2.0.6

F) Then unpack the files, configure, make, and then install. Run the configuration script with defaults, then use make to compile the program and then finally install DAQ.

```
group10@group10:~$ cd daq-2.0.6
group10@group10:~/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... no
checking for mawk... mawk
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
```

Figure 5.2.19.11: configure make and install in daq-2.0.6

## Step 2 : Snort installation

A) Download, build and Install the latest version of Snort which is 2.9.12.

```
 wget https://www.snort.org/downloads/snort/snort-2.9.12.tar.gz
```

B) Once the download is complete, extract the source and change into the new directory with these commands.

```
group10@group10:~$ cd /home/group10
group10@group10:~$ tar -zxvf snort-2.9.12.tar.gz
snort-2.9.12/
snort-2.9.12/depcomp
snort-2.9.12/tools/
snort-2.9.12/tools/u2streamer/
snort-2.9.12/tools/u2streamer/sf_error.h
snort-2.9.12/tools/u2streamer/sf_error.c
snort-2.9.12/tools/u2streamer/UnifiedLog.h
snort-2.9.12/tools/u2streamer/UnifiedLog.c
snort-2.9.12/tools/u2streamer/TimestampedFile.h
snort-2.9.12/tools/u2streamer/TimestampedFile.c
snort-2.9.12/tools/u2streamer/Unified2File.h
snort-2.9.12/tools/u2streamer/Unified2File.c
snort-2.9.12/tools/u2streamer/Unified2.h
snort-2.9.12/tools/u2streamer/Unified2.c
snort-2.9.12/tools/u2streamer/SpoolFileIterator.h
snort-2.9.12/tools/u2streamer/SpoolFileIterator.c
snort-2.9.12/tools/u2streamer/u2streamer.c
snort-2.9.12/tools/u2streamer/Makefile.in
snort-2.9.12/tools/u2streamer/Makefile.am
```

Figure 5.2.19.12: Extract snort-2.9.12

C) Then configure the installation with sourcefire mode enabled, run make and make install

```
group10@group10:~/snort-2.9.12
group10@group10:~$ cd snort-2.9.12
group10@group10:~/snort-2.9.12$ ./configure --enable-sourcefire && 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... no
checking for mawk... mawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking for style of include used by make... GNU
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
checking dependency style of gcc... gcc3
checking for gcc option to accept ISO C99... none needed
checking for gcc option to accept ISO Standard C... (cached) none needed
```

Figure 5.2.19.13: enable sourefire and make install in Snort-2.9.12

### Step 3 : Snort Configuration

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

```
group10@group10:~$ sudo ldconfig
```

*Figure 5.2.19.14: Command to update shared library*

- C) Create a symlink to the Snort library

```
group10@group10:~$ sudo ln -s /usr/local/bin/snort /usr/sbin/snort
```

*Figure 5.2.19.15: Command to craete symlink*

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

```
group10@group10:~$ sudo groupadd snort  
group10@group10:~$ sudo useradd snort -r -s /sbin/nologin -c SNORT_IDS -g snort
```

*Figure 5.2.19.16: Command to reate user*

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

```

group10@group10:~$ sudo mkdir -p /etc/snort/rules
group10@group10:~$ sudo mkdir /var/log/snort
group10@group10:~$ sudo mkdir /usr/local/lib/snort_dynamicrules
group10@group10:~$ 
group10@group10:~$ sudo chmod -R 5775 /etc/snort
group10@group10:~$ sudo chmod -R 5775 /var/log/snort
group10@group10:~$ sudo chmod -R 5775 /usr/local/lib/snort_dynamicrules
group10@group10:~$ sudo chown _R snort:snort /etc/snort
chown: invalid user: '_R'
group10@group10:~$ sudo chown -R snort:snort /etc/snort
group10@group10:~$ sudo chown -R snort:snort /var/log/snort
group10@group10:~$ sudo chown -R snort:snort /usr/local/lib/snort_dynamicrules
group10@group10:~$ 

```

*Figure 5.2.19.17: Command to create file and set permissions*

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

```

group10@group10:~$ 
group10@group10:~$ sudo touch /etc/snort/rules/white_list.rules
group10@group10:~$ sudo touch /etc/snort/rules/black_list.rules
group10@group10:~$ sudo touch /etc/snort/rules/local.rules

```

*Figure 5.2.19.18: Command to create file in rules*

G) Copy the configuration files and the dynamic preprocessors:

```

group10@group10:~$ sudo cp /home/group10/snort-2.9.12/etc/*.conf* /etc/snort
group10@group10:~$ sudo cp /home/group10/snort-2.9.12/etc/*.map /etc/snort
group10@group10:~$ 

```

*Figure 5.2.19.19: Command to copy configuration*

```

group10@group10:~$ ls
daq-2.0.6          Pictures
daq-2.0.6.tar.gz   Public
Desktop            snap
Documents           snort
Downloads           snort-2.9.12
examples.desktop    snort-2.9.12.tar.gz
group_10            Templates
mail                sudo apt install dovecot-core dovecot-imapd
Music               Videos
nextcloud-9.0.52.zip

```

*Figure 5.2.19.20: check the download in extraction snort and daq*

#### Step 4 : Install community rules

```
group10@group10:~$ sudo wget https://www.snort.org/rules/community -O /community.tar.gz
--2018-10-26 11:00:06-- https://www.snort.org/rules/community
Resolving www.snort.org (www.snort.org)... 2400:cb00:2048:1::6810:3e4b, 2400:cb00:2048:1::6810:404b, 2400:cb00:2048:1::6810:414b, ...
Connecting to www.snort.org (www.snort.org)|2400:cb00:2048:1::6810:3e4b|:443...
failed: Network is unreachable.
Connecting to www.snort.org (www.snort.org)|2400:cb00:2048:1::6810:404b|:443...
failed: Network is unreachable.
Connecting to www.snort.org (www.snort.org)|2400:cb00:2048:1::6810:414b|:443...
failed: Network is unreachable.
Connecting to www.snort.org (www.snort.org)|2400:cb00:2048:1::6810:3f4b|:443...
failed: Network is unreachable.
Connecting to www.snort.org (www.snort.org)|2400:cb00:2048:1::6810:424b|:443...
failed: Network is unreachable.
Connecting to www.snort.org (www.snort.org)|104.16.64.75|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/008/895/original/community-rules.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20181026%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20181026T132226Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=c09d59f5e98adf19a1c312c75dd8fb5b8681a15a69636caa4569445a735e4084 [following]
--2018-10-26 11:00:07-- https://snort-org-site.s3.amazonaws.com/production/rele
```

Figure 5.2.19.21: Install community rules

```
group10@group10:~$ sudo tar -xvf /community.tar.gz -C /
community-rules/
community-rules/community.rules
community-rules/VRT-License.txt
community-rules/LICENSE
community-rules/AUTHORS
community-rules/snort.conf
community-rules/sid-msg.map
group10@group10:~$ sudo cp /community-rules/* /etc/snort/rules
group10@group10:~$ sudo sed -i 's/include \$RULE\_PATH/#include \$RULE\_PATH/' /etc/snort/snort.conf
group10@group10:~$
```

Figure 5.2.19.22: Extract the download community rules

```
group10@group10:~
2018-10-26 11:33:25 (285 KB/s) - '/registered.tar.gz' saved [102457296/102457296]

group10@group10:~$ sudo tar -xvf /registered.tar.gz -C /etc/snort
rules/
rules/VRT-License.txt
rules/app-detect.rules
rules/attack-responses.rules
rules/backdoor.rules
rules/bad-traffic.rules
rules/blacklist.rules
rules/botnet-cnc.rules
rules/browser-chrome.rules
rules/browser-firefox.rules
rules/browser-ie.rules
rules/browser-other.rules
rules/browser-plugins.rules
rules/browser-webkit.rules
rules/chat.rules
rules/content-replace.rules
rules/ddos.rules
rules/deleted.rules
rules/dns.rules
rules/dos.rules
rules/experimental.rules
rules/exploit-kit.rules
rules/exploit.rules
rules/file-executable.rules
rules/file-flash.rules
rules/file-identify.rules
rules/file-image.rules
```

Figure 5.2.19.23: Extract to /etc/snort

```
group10@group10:~
group10@group10:~$ sudo wget https://www.snort.org/rules/snortrules-snapshot-29111.tar.gz?oinkcode=604cb8e7c4753ad57fb387b90d40d5cee3f653f6529f -O /registered.tar.gz
[sudo] password for group10:
--2018-10-26 11:27:38-- https://www.snort.org/rules/snortrules-snapshot-29111.tar.gz?oinkcode=604cb8e7c4753ad57fb387b90d40d5cee3f6529f
Resolving www.snort.org (www.snort.org)... 2400:cb00:2048:1::6810:424b, 2400:cb00:2048:1::6810:414b, 2400:cb00:2048:1::6810:3f4b, ...
Connecting to www.snort.org (www.snort.org)|2400:cb00:2048:1::6810:424b|:443... failed: Network is unreachable.
Connecting to www.snort.org (www.snort.org)|2400:cb00:2048:1::6810:414b|:443... failed: Network is unreachable.
Connecting to www.snort.org (www.snort.org)|2400:cb00:2048:1::6810:3f4b|:443... failed: Network is unreachable.
Connecting to www.snort.org (www.snort.org)|2400:cb00:2048:1::6810:404b|:443... failed: Network is unreachable.
Connecting to www.snort.org (www.snort.org)|2400:cb00:2048:1::6810:3e4b|:443... failed: Network is unreachable.
Connecting to www.snort.org (www.snort.org)|104.16.65.75|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/008/899/original/snortrules-snapshot-29111.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMS7GAK2F20181026%2Fus-east-1%2F%3Faws4 request&X-Amz-Date=20181026T134950Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=bd435e0ae14c500c5d4629c467a138fcc1ff166358d9b3e465c078d8a09b5c08 [following]
--2018-10-26 11:27:32-- https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/008/899/original/snortrules-snapshot-29111.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMS7GAK2F20181026%2Fus-east-1%2F%3Faws4 request&X-Amz-Date=20181026T134950Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=bd435e0ae14c500c5d4629c467a138fcc1ff166358d9b3e465c078d8a09b5c06.
Resolving snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)... 52.216.105.179
Connecting to snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)|52.216.105.179|:443... connected.
```

Figure 5.2.19.24: download oinkcode of snort

A) With the configuration and rule files in place, edit the *snort.conf* to modify a few parameters.

Open the configuration file to edit with the following

```
group10@group10:~$ sudo nano /etc/snort/snort.conf
group10@group10:~$
```

Figure 5.2.19.25: Command to edit configuration snort

**Figure 5.2.19.26:** Edit configuration snort

*# Setup the network addresses you are protecting*

ipvar HOME\_NET 192.168.9.146/26

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

ipvar EXTERNAL NET !\$HOME NET

*# Path to your rules files (this can be a relative path)*

var RULE PATH rules

var SO RULE PATH so rules

var PREPROC RULE PATH preproc rules

*# Set the absolute path appropriately*

```
var WHITE_LIST_PATH /etc/snort/rules
```

```
var BLACK_LIST_PATH /etc/snort/rules
```

B) Then, scroll down to the bottom of the file to find the list of included rule sets. We need to uncomment the *local.rules* include line to allow Snort to load any custom rules.

*include \$RULE\_PATH/local.rules*

### C) Creating a custom Snort rule to test Snort

Sudo nano /etc/Snort/rules/local.rule

D) We can add any rules using this format:

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

```
GNU nano 2.5.3                               File: /etc/snort/rules/local.rules

alert icmp 192.168.9.130 any <> 192.168.9.146 any (msg: "Windows Server pinging Ubuntu Server"; sid:10000001; rev:001; )
alert icmp 192.168.9.138 any <> 192.168.9.146 any (msg: "Fedora Server Pinging ubuntu Server";sid:10000002; rev:001; )
alert icmp 192.168.9.66 any <> 192.168.9.146 any (msg: "Window Client pinging Ubuntu Server";sid:10000003; rev:001; )

alert icmp 192.168.9.146 any <> 192.168.9.130 any (msg:"Ubuntu Server pinging Windows Server";sid:10000011; rev:001)
alert icmp 192.168.9.146 any <> 192.168.9.138 any (msg:"Ubuntu Server pinging Fedora Server";sid:10000012; rev:001)
alert icmp 192.168.9.146 any <> 192.168.9.66 any (msg:"Ubuntu Server pinging Windows Client Server";sid:10000013; rev:001)

alert icmp 192.168.9.154 any <> 192.168.9.146 any (msg: "Switch Pinging Ubuntu Server";sid:10000004; rev:001; )
alert icmp 192.168.9.153 any <> 192.168.9.146 any (msg: "Router Pinging Ubuntu Server";sid:10000005; rev:001; )
alert icmp 192.168.9.146 any <> 192.168.9.154 any (msg:"Ubuntu Server pinging Switch";sid:10000014; rev:001)
alert icmp 192.168.9.146 any <> 192.168.9.153 any (msg:"Ubuntu Server pinging Router";sid:10000015; rev:001)

#alert tcp any any -> any 21 (msg: "FTP Packet found"; sid:10000006; )
#alert tcp any any -> any 22 (msg: "SSH Packet found"; sid:10000007; )
#alert tcp any any -> any 80 (msg: "HTTP Packet found"; sid:10000008; )

#####port Mirror#####

alert icmp 192.168.9.130 any <> 192.168.9.138 any (msg: "Windows Server pinging Fedora Server"; sid:10000009; rev:001; )
alert icmp 192.168.9.138 any <> 192.168.9.130 any (msg: "Fedora Server pinging Windows Server"; sid:10000010; rev:001; )
```

*Figure 5.2.19.27: Configure the local.rules*

The rules consist of the following parts:

1. Action for traffic matching the rule, alert in this case.
2. Traffic protocol like TCP, UDP or ICMP like here
3. Source address and port, simply marked as any to include all addresses and ports
4. Destination address and port, \$HOME\_NET as declared in the configuration and any for port
5. Some additional bits
  - log message
  - unique rule identifier (sid) which for local rules needs to be 1000001 or higher
  - rule version number.

E) Save all the rule files and exit the editor.

## **Port Mirroring**

**Step 1:** Setup int fa0/20 as destination port

**Step 2 :** Setup int fa0/23 as source port

**Step 3 :**Check the source and destination port at monitor session 1

```
Group10Switch#sh monitor session 1
Session 1
-----
Type          : Local Session
Source Ports  :
    Both      : Fa0/23
Destination Ports  :
    Fa0/20
Encapsulation  : Native
Ingress       : Disabled
```

*Figure 5.2.19.28: show port mirror setup*

**Step 4 :**Check port fa0/20 which is up or not

```
Group10Switch#sh int fa0/20
FastEthernet0/20 is up, line protocol is down (monitoring)
    Hardware is Fast Ethernet, address is f4ac.c190.8414 (bia f4ac.c190.8414)
    MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
        reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA, loopback not set
    Keepalive set (10 sec)
    Full-duplex, 100Mb/s, media type is 10/100BaseTX
    input flow-control is off, output flow-control is unsupported
    ARP type: ARPA, ARP Timeout 04:00:00
    Last input never, output 01:06:08, output hang never
    Last clearing of "show interface" counters never
    Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
    Queueing strategy: fifo
    Output queue: 0/40 (size/max)
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 106000 bits/sec, 21 packets/sec
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts (0 multicasts)
        0 runts, 0 giants, 0 throttles
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
        0 watchdog, 0 multicast, 0 pause input
        0 input packets with dribble condition detected
        436156 packets output, 380361065 bytes, 0 underruns
        0 output errors, 0 collisions, 2 interface resets
        0 babbles, 0 late collision, 0 deferred
        0 lost carrier, 0 no carrier, 0 PAUSE output
        0 output buffer failures, 0 output buffers swapped out
Group10Switch#
```

*Figure 5.2.19.29: show the int fa0/20*

### 5.2.21 Security Policy

No installation required.

### 5.2.22 Router Hardening

**Step 1:** Encrypt password on the device

```
?  
username group10 privilege 15 secret 5 $1$w8Fx$apefYr51H2Oq6x34Nre4d0  
!
```

*Figure 5.2.22.1: Encrypt password on the device*

**Step 2:** Setup Password minimal length

```
security passwords min-length 8
```

*Figure 5.2.22.2: Setup Password minimal length*

**Step 3:** Setup Login Failure limited to 3 times only

```
security authentication failure rate 3 log
```

*Figure 5.2.22.3: Setup Login Failure*

**Step 4:** Implement password at line console

```
?  
line con 0  
exec-timeout 3 0  
password 7 01322717480F025E731F1A5C  
logging synchronous
```

*Figure 5.2.22.4: Password Implementation At Line Console*

**Step 5:** Setup exec-timeout to 3 minutes

```
exec-timeout 3 0
```

*Figure 5.2.22.5: Setup Exec-Timeout*

## 5.2.23 Window Server Hardening

### I. Configure security policy

The purpose of hardening is eliminating as many security risks as possible. Techniques to harden systems are protecting accounts with passwords, disabling unnecessary accounts, disabling unnecessary services and protecting management interfaces and application. Hardening the Microsoft Windows Server 2012 R2 operating system reduces the attack surface by disabling functionality that is not required while maintaining the minimum functionality that is required.

#### 1. Security Policy Configuration

Install Security Configuration Wizard through add and remove windows components which detect ports and services, and configure registry and audit setting according to the server's role.

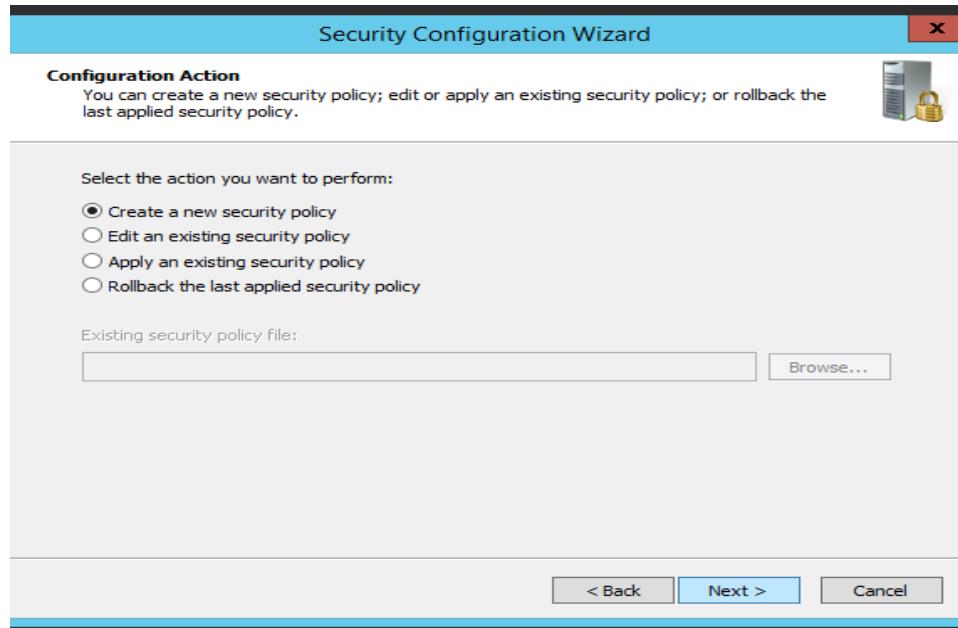
- Disable unnecessary services based on the server role.
- Remove unused firewall rules and limit existing firewall rules.
- Define restricted audit policies.

**Step 1:** For configuring the Security Policy Wizard go to Start > Programs > Administrative Tools > Security Policy Wizard > Click next to start the configuration.



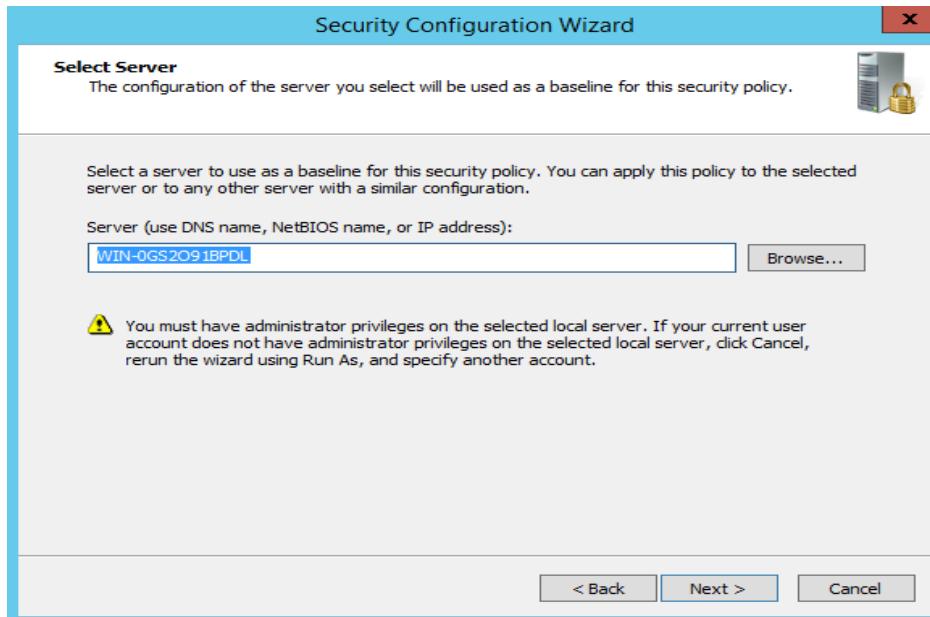
Figure 5.2.23.1: Security Policy Wizard

**Step 2:** Click “Create a new security policy” on the list. Then click next.



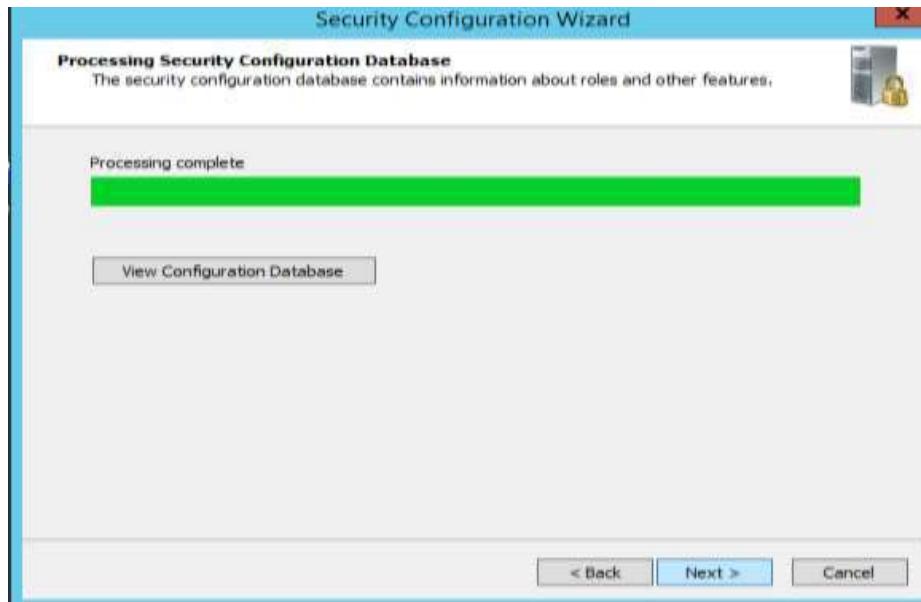
*Figure 5.2.23.2: Create new security policy*

**Step 3:** Enter the DNS's name and click next to continue the configuration. A pop-up with processing bar will appear. After Security Configure Database is completely processed, click next to proceed.



*Figure 5.2.23.3: Enter the DNS's name*

**Step 4:** Wait until process for configuration database complete. Then click next.



*Figure 5.2.23.4: Processing Securing Configuration Database*

**Step 5:** Role-based service configuration is to configure the service based on selected server's roles and other features. Then click next.



*Figure 5.2.23.5: Role-Based service configuration*

**Step 6:** Continue the configuration with Role-Based Service Configuration. Select the features, roles and options that had been installed. Then click next.



Figure 5.2.23.6: Select Server Roles

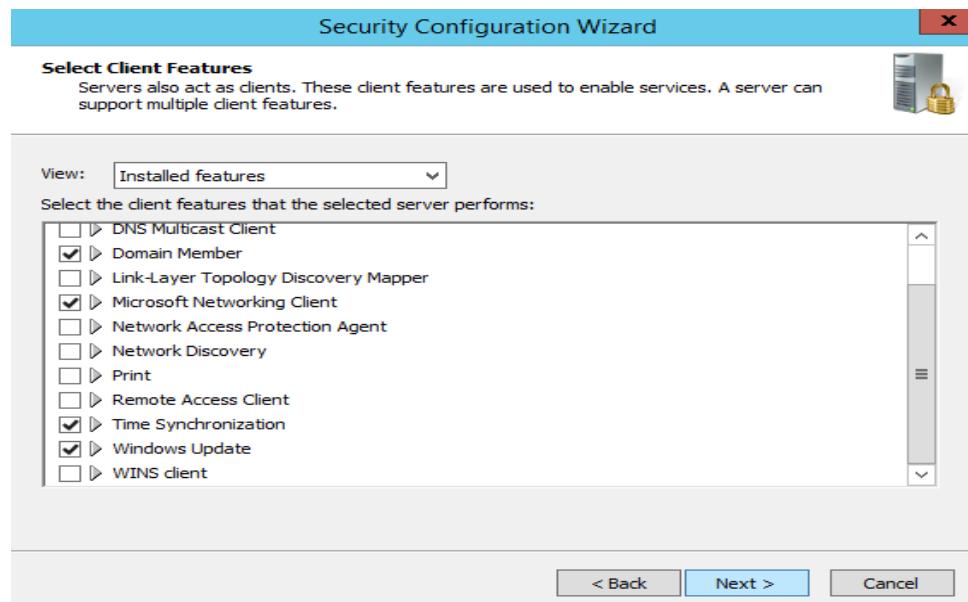


Figure 5.2.23.7: Select Client Features

**Step 7:** Select the administration and the other options used to enable services and open ports. Then click next.



*Figure 5.2.23.8: Select Administration and Other Options*

**Step 8:** Select the additional services that have been installed in the server. Then click next to continue.



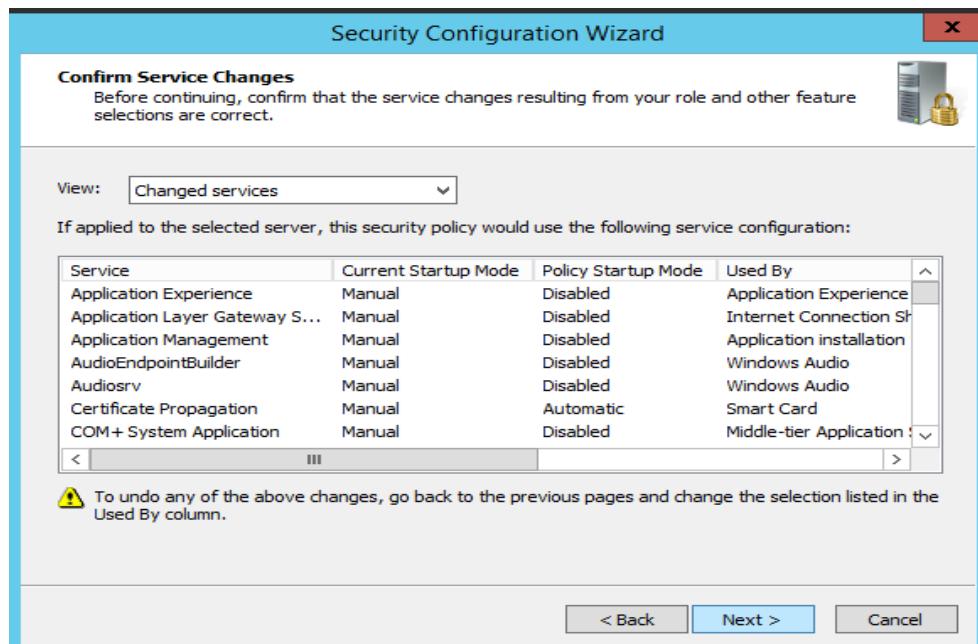
*Figure 5.2.23.9: Selected Additional Services*

**Step 9:** For Handling Unspecified Service, select “Do not change the startup mode of the service” to avoid the system from disabling the services. Then click next.



*Figure 5.2.23.10: Handling Unspecified Services*

**Step 10:** View the services to confirm the changes. If there is nothing to change, then click next.



*Figure 5.2.23.11: Confirm Service Changes*

**Step 11:** Proceed with network security. Network security roles list all the Windows Firewall rules that are needed for the roles.



*Figure 5.2.23.12: Network Security*

**Step 12:** Selecting Network Security Rules. Then click next.



*Figure 5.2.23.13: Network Security Rules*

**Step 13:** Continue with registry settings. Then click next.



*Figure 5.2.23.14: Registry Settings*

**Step 14:** Select the options that require Server Message Block (SMB) Signatures. Then click next.

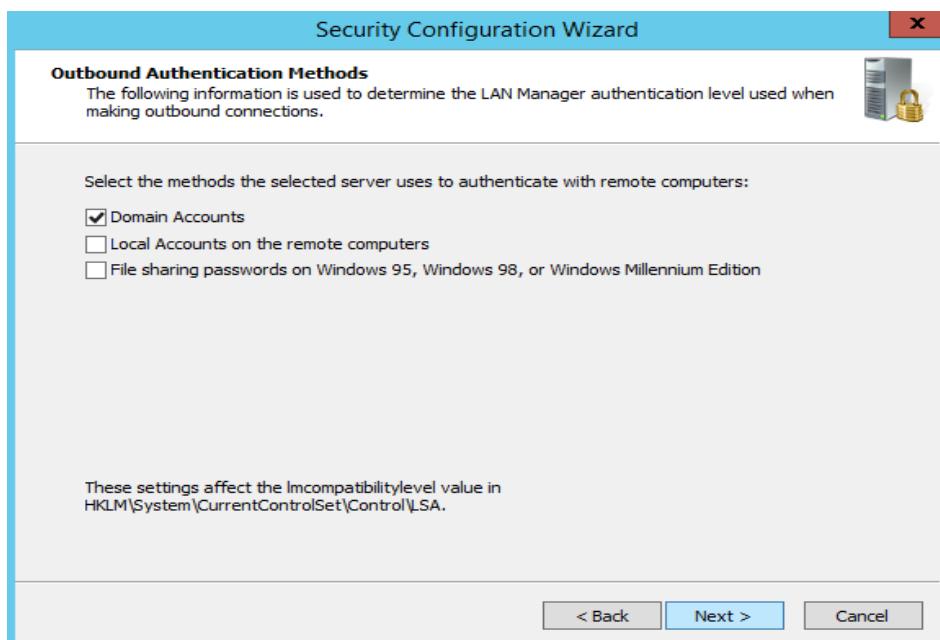


*Figure 5.2.23.15: Security Signatures*



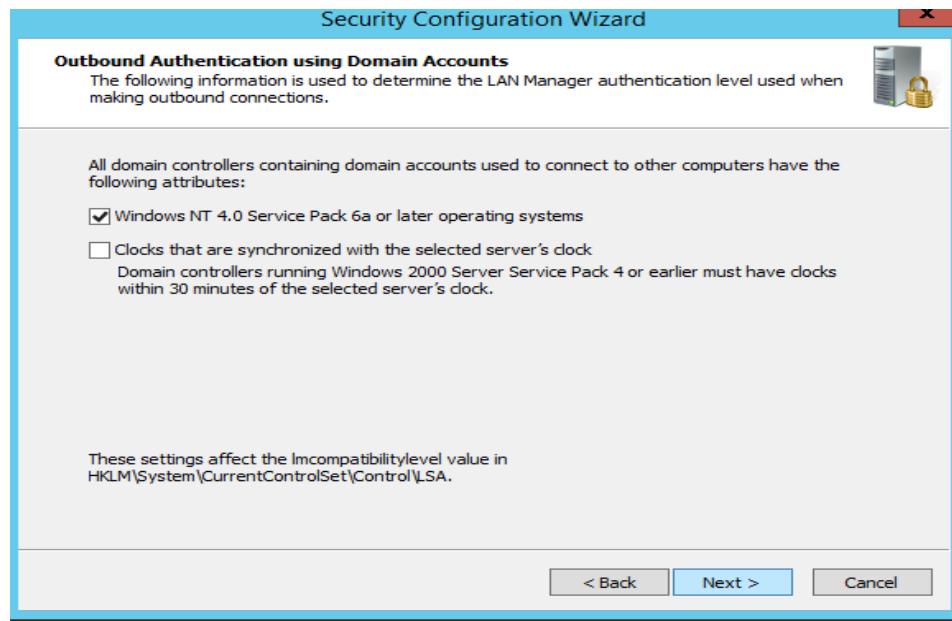
*Figure 5.2.23.16: Require LDAP Signing*

**Step 15:** Select the methods that the selected server uses to authenticate with remote computers and click next.



*Figure 5.2.23.17: Set Authentication Methods*

**Step 16:** Select the option that used in domain accounts for outbound authentication and click next.



*Figure 5.2.23.19: Authentication using Domain Accounts*

**Step 17:** The window displays the registry settings summary. View the settings and confirm that the registry settings are correct.



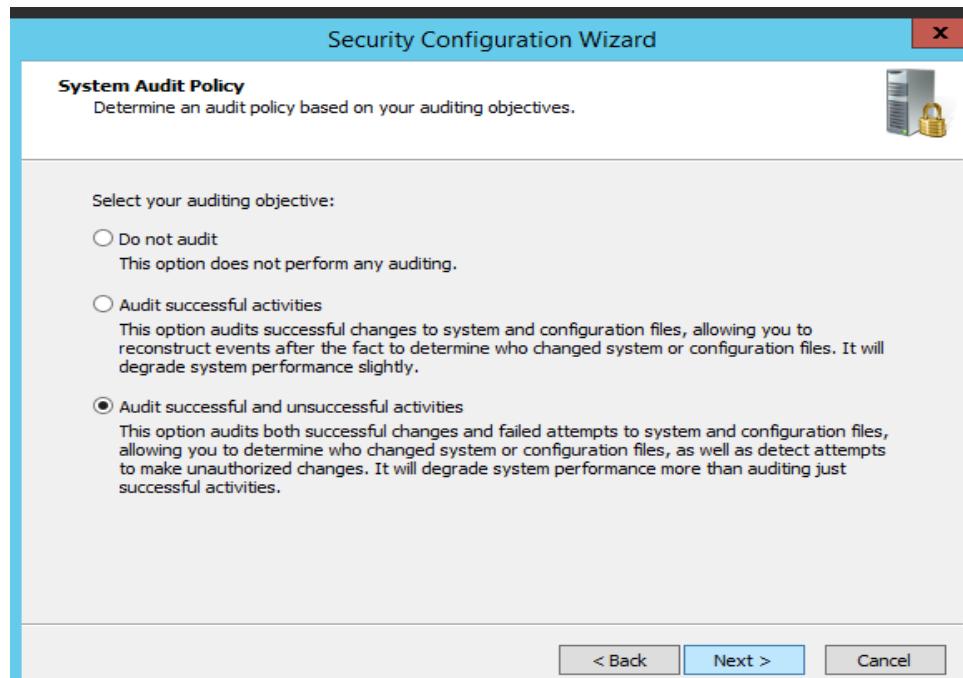
*Figure 5.2.23.20: Registry Setting Summary*

**Step 18:** Continue with system audit policy. Select the options of auditing objectives and click next.



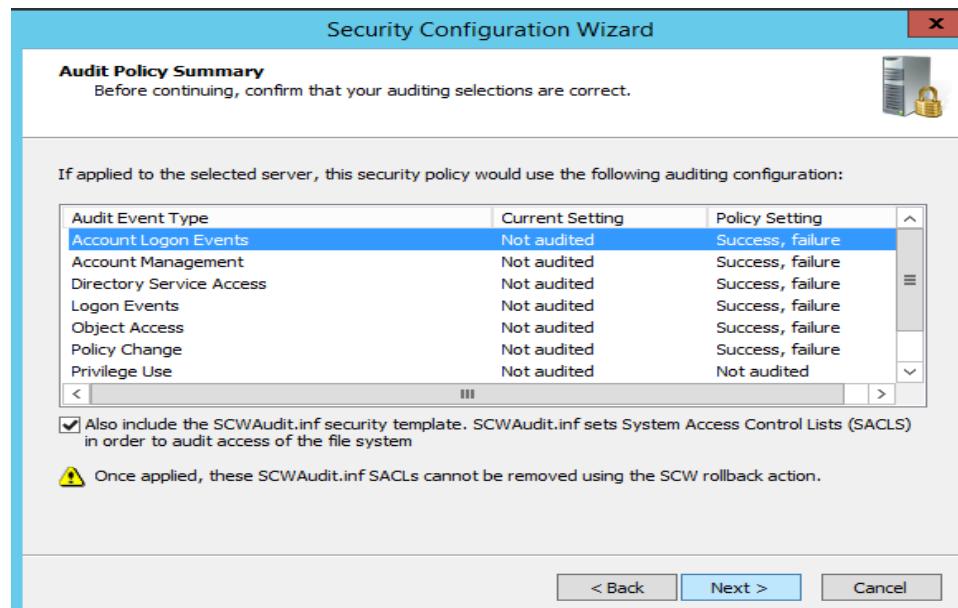
*Figure 5.2.23.21: Audit Policy*

**Step 19:** Set the system audit policy to determine an audit policy based on our auditing objectives. Then click next.



*Figure 5.2.23.22: System Audit Policy*

**Step 20:** Audit Policy summary is to confirm that the auditing selections are correct. Then click next.



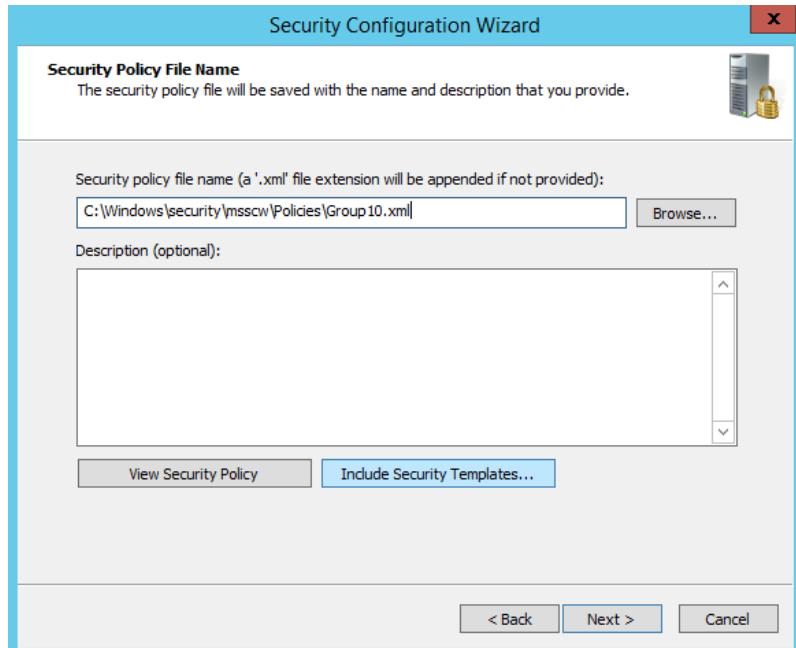
*Figure 5.2.23.23: Audit Policy Summary*

**Step 21:** Save the policy created. Then click next.



**Figure 5.2.23.24: Saved Security Policy**

**Step 22:** Save the security policy with the file named “Group10.xml”. Then click next.

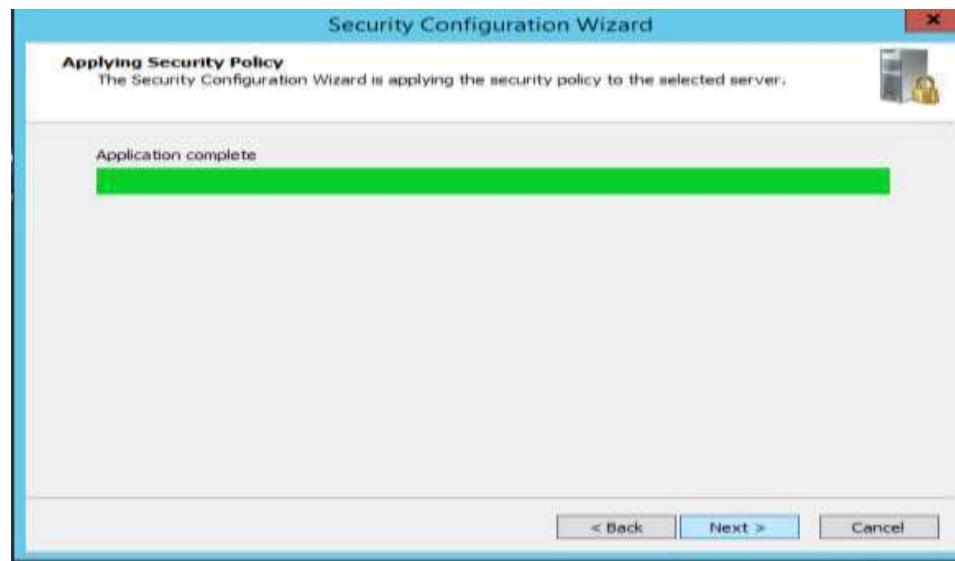


**Figure 5.2.23.25: Security Policy File Name**

**Step 23:** Select “Apply Now” as we need to apply this security policy at a later time. Then click next.



*Figure 5.2.23.26: Apply Security Policy*



*Figure 5.2.23.27: Processing Security Policy*

**Step 24:** After the entire step above, the securepolicies.xml created the configuration of security policy successfully complete.

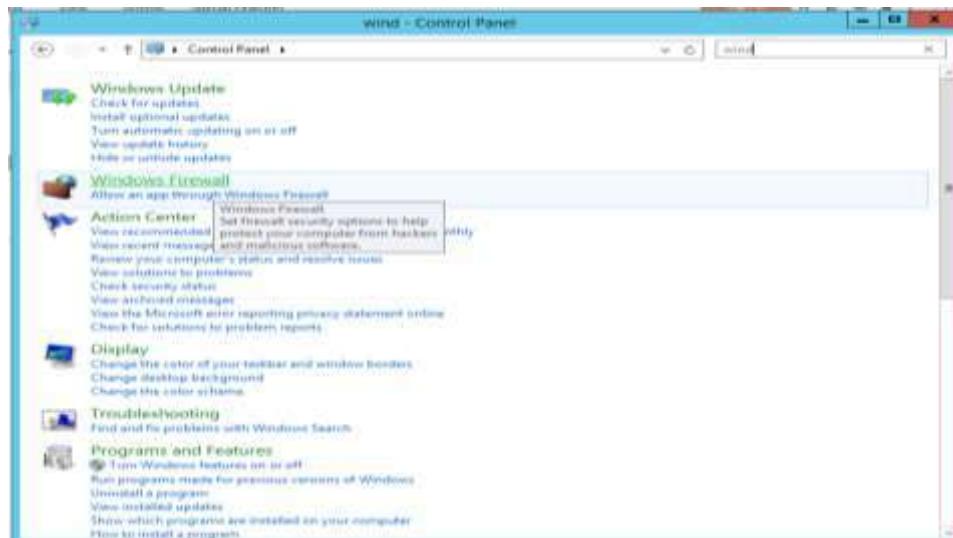


*Figure 5.2.23.28: Completing the security Configuration Wizard*

## II. Configure windows Firewall

Windows 2012 server comes with a built in firewall called the Windows Firewall with Advance Security. As a security best practices, all server should have its own host based firewall. Bidirectional firewall which filters the outbound traffic as well as inbound traffic.

**Step 1:** Open the control panel to configure window firewall.



*Figure 5.2.23.29: Configure Windows Firewall*

**Step 2:** Check whether the firewall on or off.



*Figure 5.2.23.30: Firewall Status*

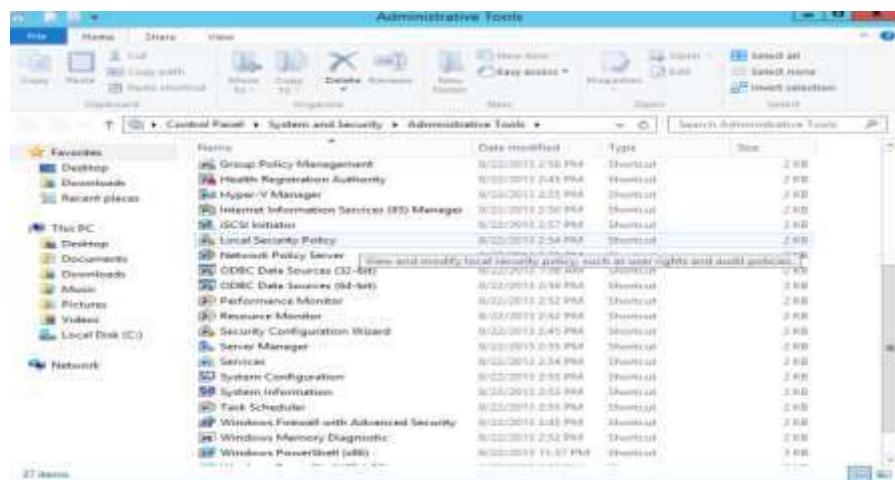


*Figure 5.2.23.31: Customize Settings*

### III. Configure Auditing

The following events should be logged and audited. One of the most significant changes on Windows Server 2012 auditing is that now you can not only audit who and what attribute was changed but also what the new and old value was. This is significant because you can now tell why it was changed and if something doesn't look right you're able to easily find what it should be restored to. Another significant change is that in the past server versions you were only able to turn auditing policy on or off for the entire Active Directory structure.

#### Step1: Open Local Security Policy



*Figure 5.2.23.32: Open Local Security Policy*

**Step 2:** Double click the policies one by one to change the security setting.



Figure 5.2.23.33: Configure the auditing

**Step 3:** check both Success and Failure, click Apply then OK.

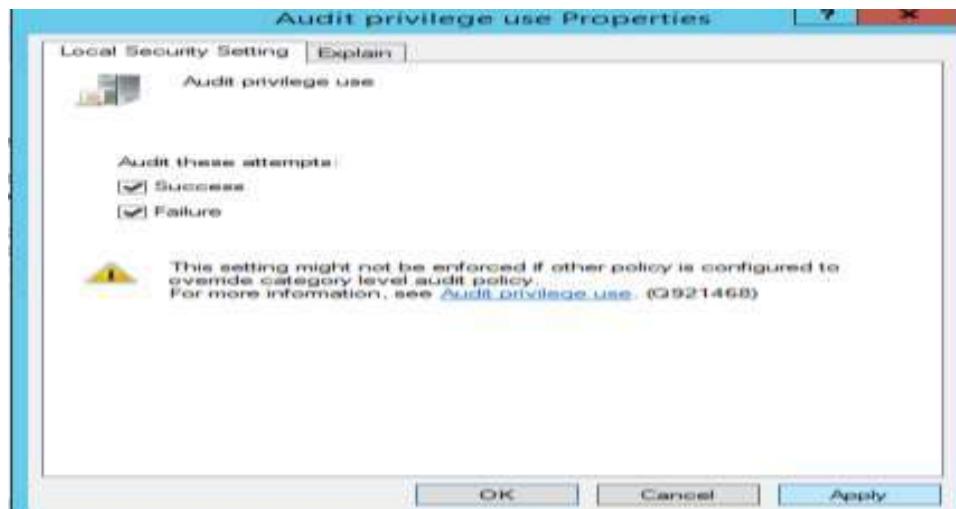


Figure 5.2.23.34: Audit account logon events

**Step 4:** All security setting have been configured



*Figure 5.2.23.35: Configuration Done*

**Step 5:** After change the security setting

Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
<b>Audit privilege use</b>	<b>Success, Failure</b>
Audit process tracking	Success, Failure
Audit system events	Success, Failure

*Figure 5.2.23.36: After auditing*

#### IV. Configure Encryption

The servers require host sensitive information to make use of the encryption system. Windows Server 2012 provides a built in whole disk encryption feature called Bit Locker Drive Encryption (BitLocker) which protects the operating systems and data stored on the disk.

**Step 1:** Open the command prompt for administrator. Type “Net –share” command to display list of shares on the server as the unnecessary share will create a threat to critical server.



Administrator: Command Prompt  
Microsoft Windows [Version 6.3.9600]  
(c) 2013 Microsoft Corporation. All rights reserved.  
C:\Users\Administrator>Net share  
Share name    Resource                              Remark  
-----  
C\$            C:\                                  Default share  
IPC\$          C:\Windows                          Remote IPC  
ADMIN\$        C:\Windows                          Remote Admin  
NETLOGON      C:\Windows\SYSVOL\sysvol\Group12.com\SCRIPTS  
SYSVOL        C:\Windows\SYSVOL\sysvol        Logon server share  
Users          C:\Users                              Logon server share  
The command completed successfully.

Figure 5.2.23.37: Display list of shares on the server

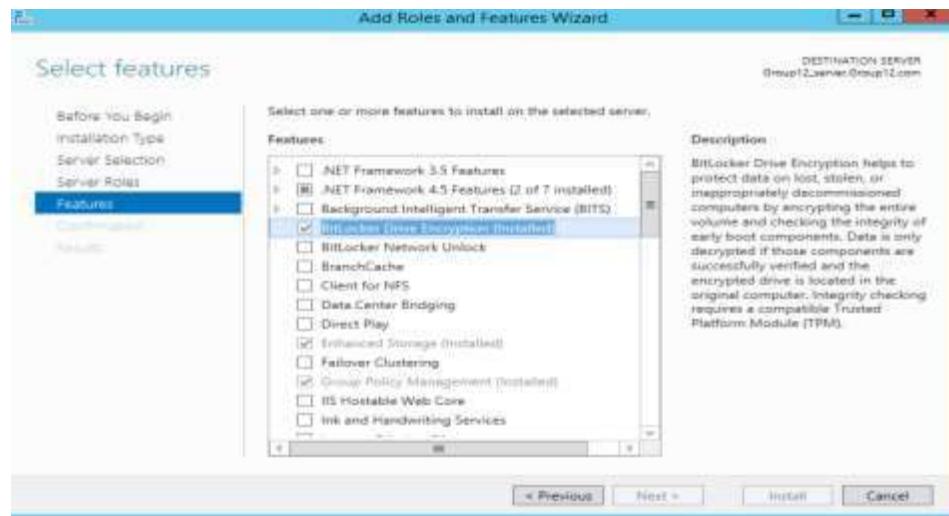
**Step 2:** Then type “-install BitLocker –restart” command for installation of bit locker.



```
C:\Users\Administrator>cd..  
C:\Users>cd..  
C:\>ServerManagerCmd -install BitLocker -restart
```

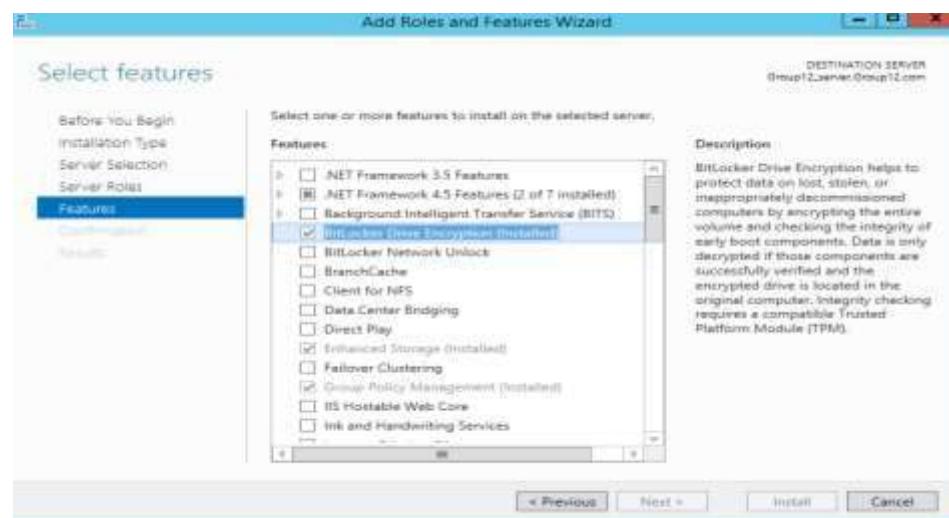
Figure 5.2.23.38: Installation of bit locker

**Step 3:** Check either BitLocker had been installed or not in the system.



*Figure 5.2.23.39: BitLocker installation*

**Step 4:** The BitLocker not installed. Click feature and tick BitLocker Drive Encryption. Then click NEXT.



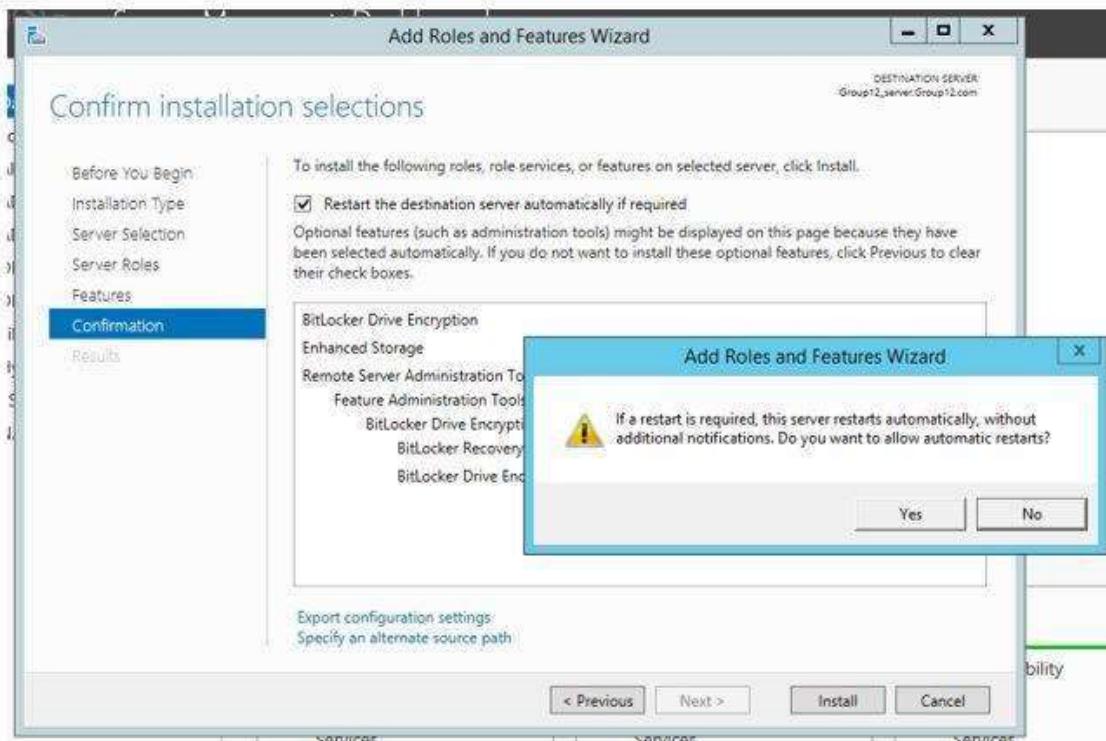
*Figure 5.2.23.40: BitLocker installation*

**Step 5:** Tick the include management tools if applicable and click Add Feature



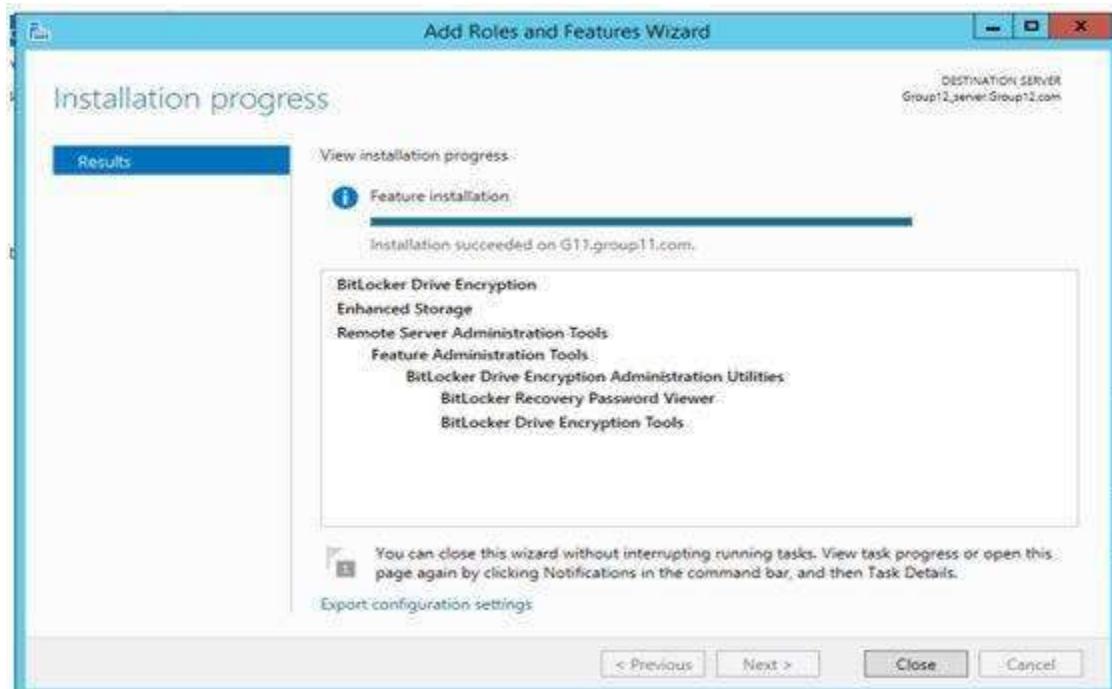
*Figure 5.2.23.41: Add Roles and features*

**Step 6:** Tick yes for restart the server and install BitLocker Drive Encryption.



*Figure 5.2.23.42: Configure installation*

**Step 7:** BitLocker Drive Encryption has been installed.



*Figure 5.2.23.43: Installation progress*

## V. Least Privilege

Most of the security threats are often caused by high privileges bared by accounts. Server services should not be configured using enterprise wide administrator accounts.

**Step 1:** Open Windows Firewall with Advanced Security.



Figure 5.2.23.44: Open windows firewall with Advanced Security

**Step 2:** At Windows Firewall with Advanced Security, choose properties. It's to make sure the firewall status is on.



Figure 5.2.23.45: Firewall status

**Step 3:** Check the inbound and outbound connection.

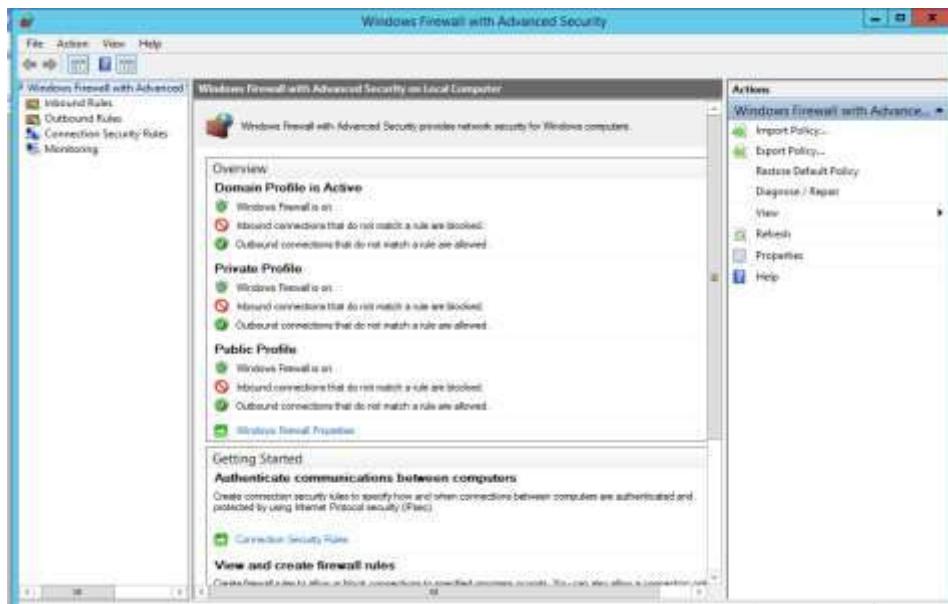


Figure 5.2.23.46: Firewall Setting

## VI. Disable automatic Services

**Step 1:** Run services.msc

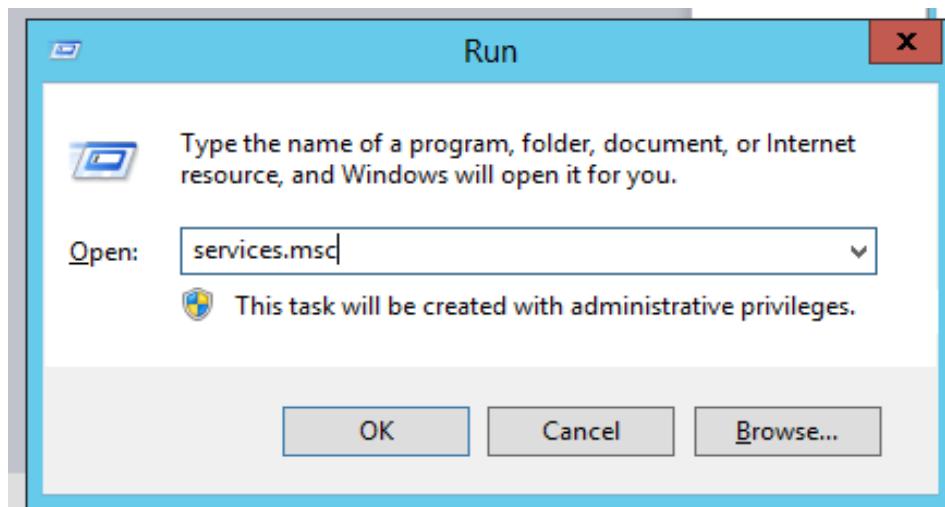


Figure 5.2.23.47: Run services msc

**Step 2:** Double click print spooler service and change start up type from automatic to disable. This service is disabled because the server is not used to print.

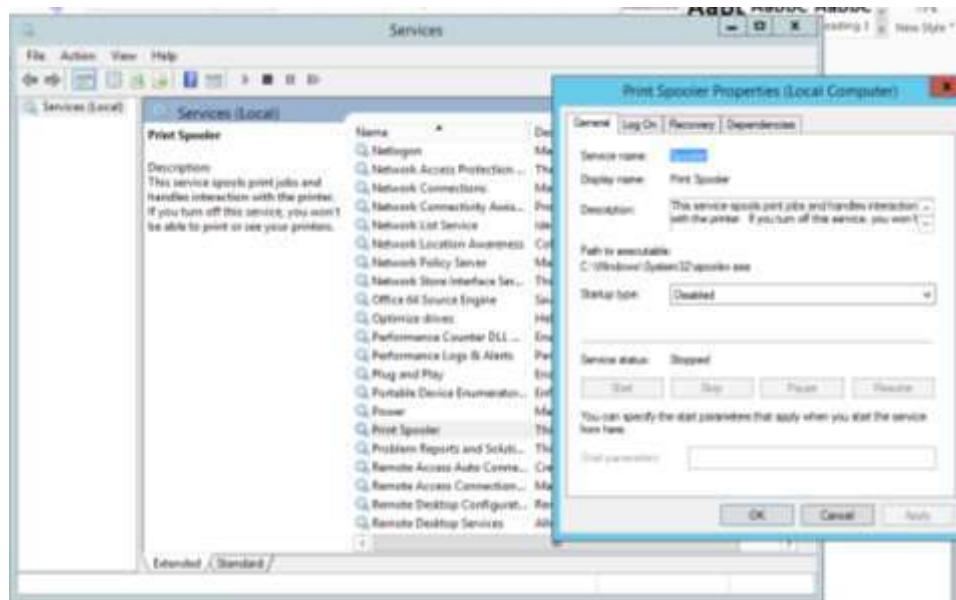


Figure 5.2.23.48: Print Spooler

**Step 3:** Double click Distributed Transaction Coordinator service. Change start up type from automatic to disable. The Distributed transaction Coordinator service is responsible for coordinating transaction that span multiple resource managers, such as databases, message queues and file systems. It is disabled because it is used for SQL server and Windows Server is not used as SQL server.

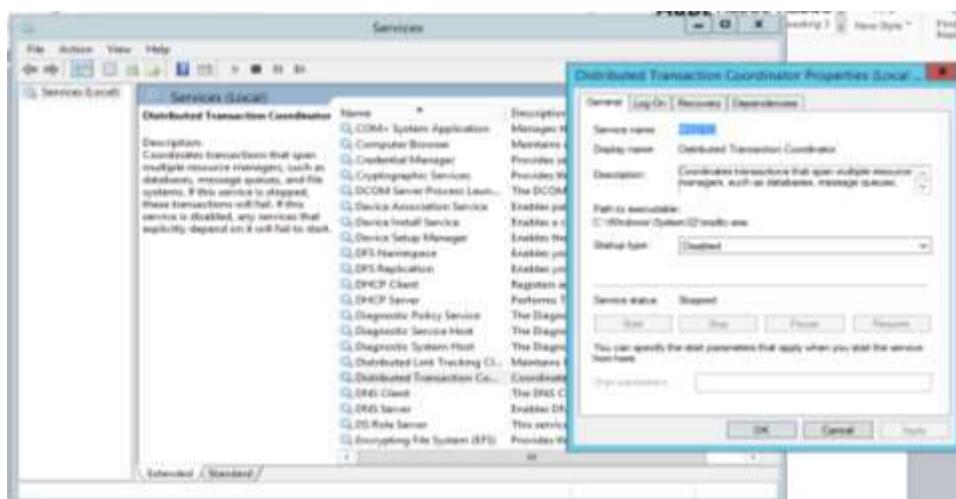
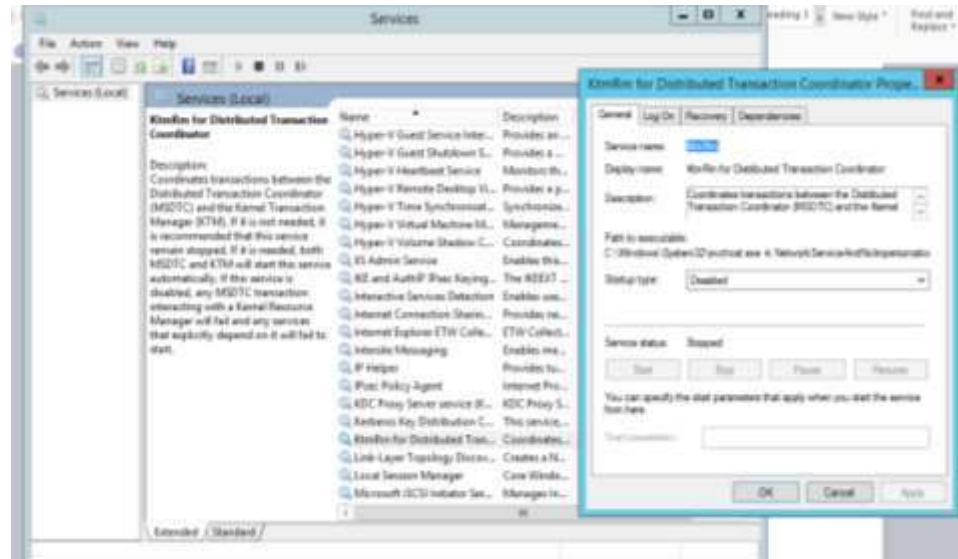


Figure 5.2.23.49: Distributed Transaction Coordinator

**Step 4:** Double click Distributed Transaction Coordinator service. Change start up type from automatic to disable. This is used to coordinate transaction between the Distributed Transaction Coordinator (DTC) and the Kernel Transaction Manager (KTM). Since DTC is disabled, this service is not needed.

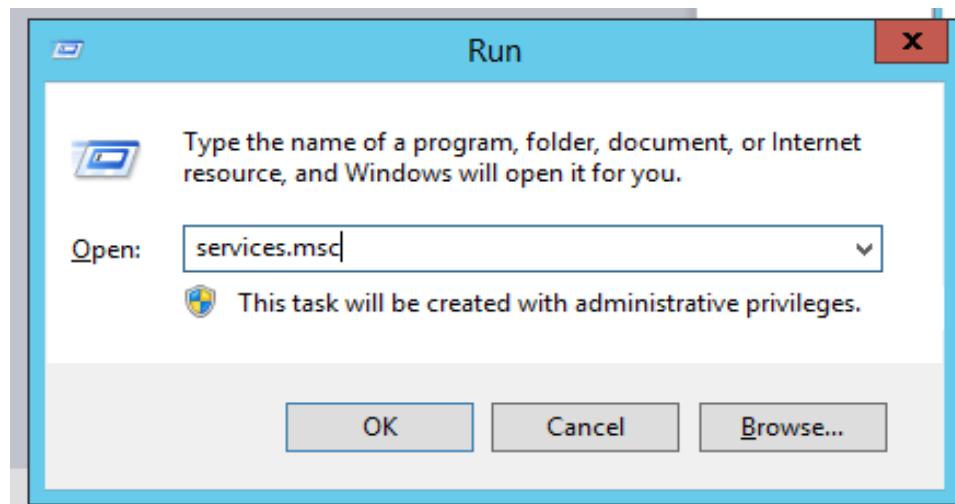


**Figure 5.2.23.50: KtmRm for Distributed Transaction**

## VII. Windows Error Reporting Service

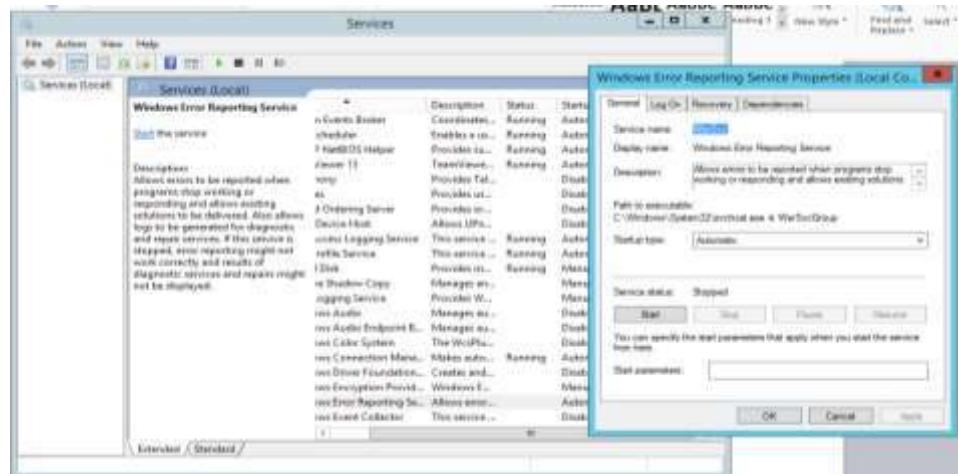
Windows Error Reporting (WER) is a set Windows technologies that capture software crash data and support end-user reporting of crash information. Though Winqual services, software and hardware vendors can access reports in order to analyse and respond to these problems.

**Step 1:** Run services.msc



*Figure 5.2.23.51: Run services msc*

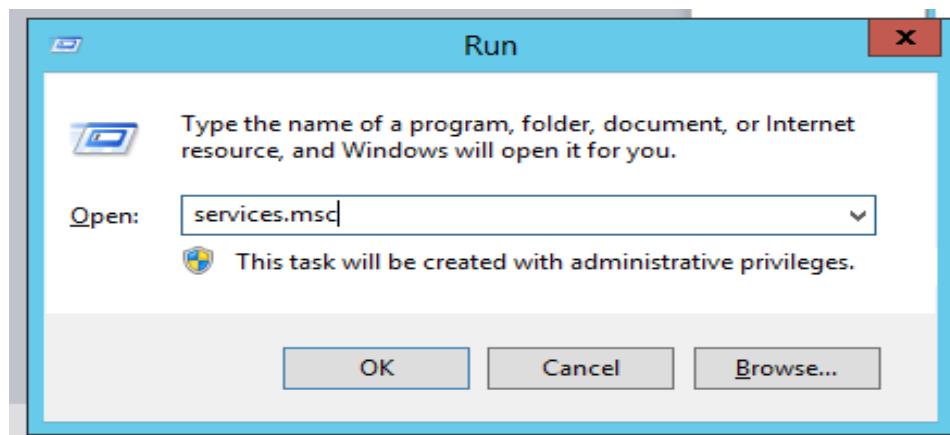
**Step 2:** Ensure the Windows Error Reporting Service startup type is Automatic and it has to be enabled so that it will capture software crash data and support end-user reporting of crash information.



*Figure 5.2.23.52: Windows Error Reporting Service*

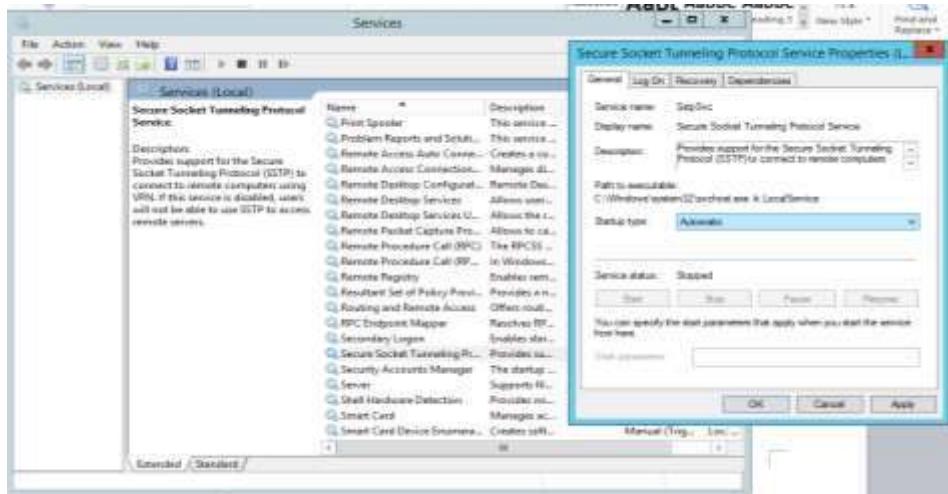
## VIII. Secure Socket Tunnelling Protocol (SSTP) service

**Step 1:** Run services.msc



*Figure 5.2.23.53: Run services msc*

**Step 2:** Double click Secure Socket Tunnelling Protocol and change startup type from disable to automatic.

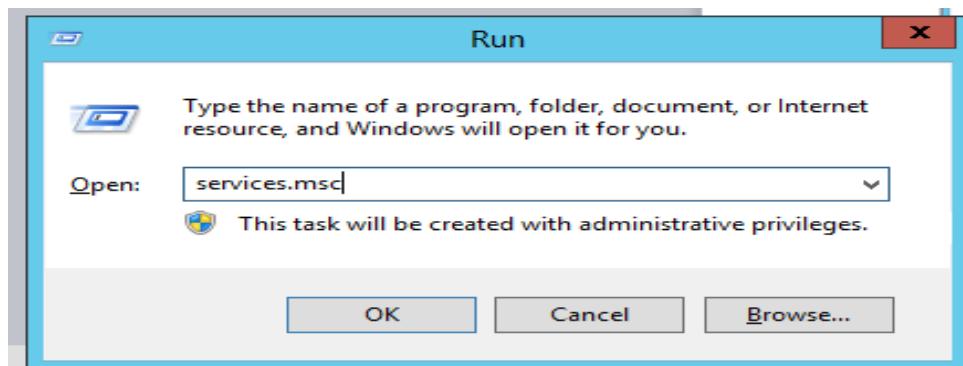


**Figure 5.2.23.54: Secure Socket Tunnelling Protocol**

**Step 3:** The start up type have been changed to Automatic. Secure Socket Tunneling Protocol (SSTP) is a form of VPN tunnel that provides a mechanism to transport PPP or L2TP traffic through an SSL 3.0 channel. SSL provides transport-level security with key-negotiation, encryption and traffic integrity checking. Hence, it should start automatically to provide protection all the time.

## IX. Enable NetLogon

**Step 1:** Run services.msc



**Figure 5.2.23.55: Run services msc**

**Step 2:** Ensure NetLogon start up type is Automatic and Started. This maintains a channel between computer and domain controller. The NetLogon sub-key stores information for the NetLogon service. The NetLogon service verifies log-on requests and it registers, authenticates and locates domain controllers.

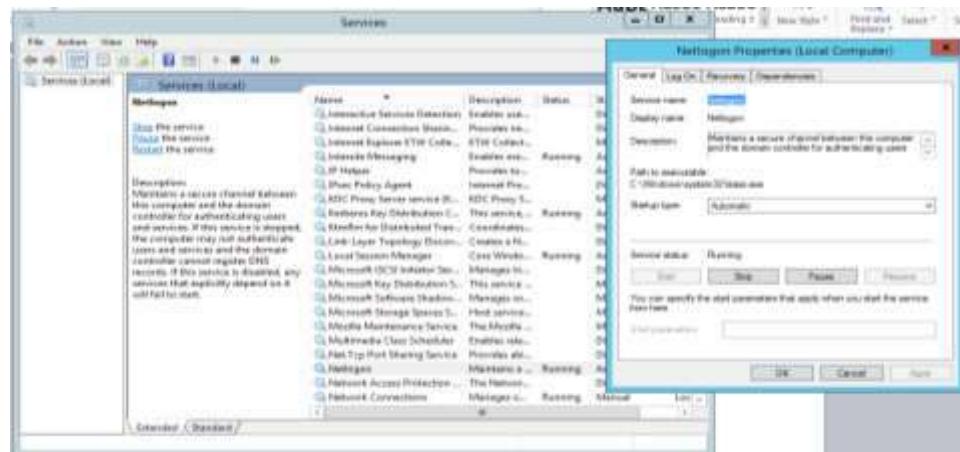


Figure 5.2.23.56: NetLogon service

## X. Disable unnecessary service

**Step 1:** Enter the target IP address which is 192.168.9.130, select “Intense scan” and click scan.

**Step 2:** Result generated that shows the open ports.

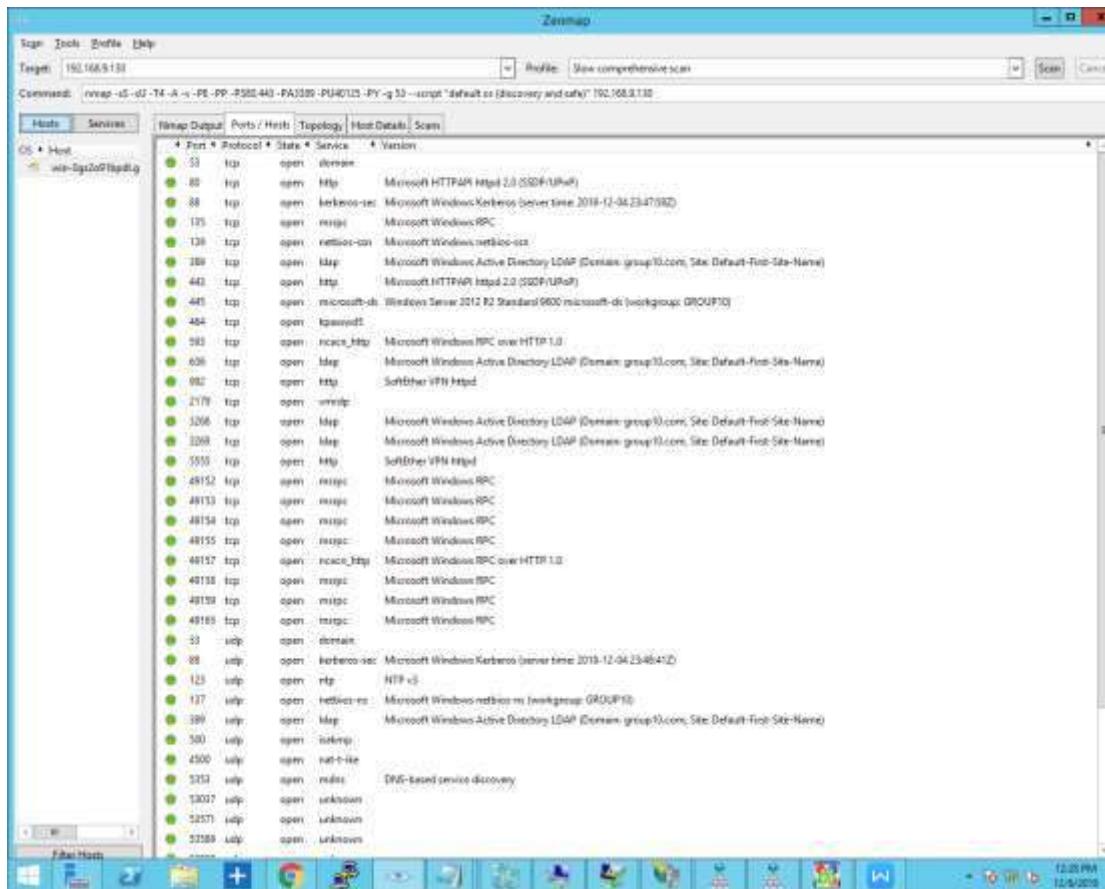


Figure 5.2.23.57: Show open port

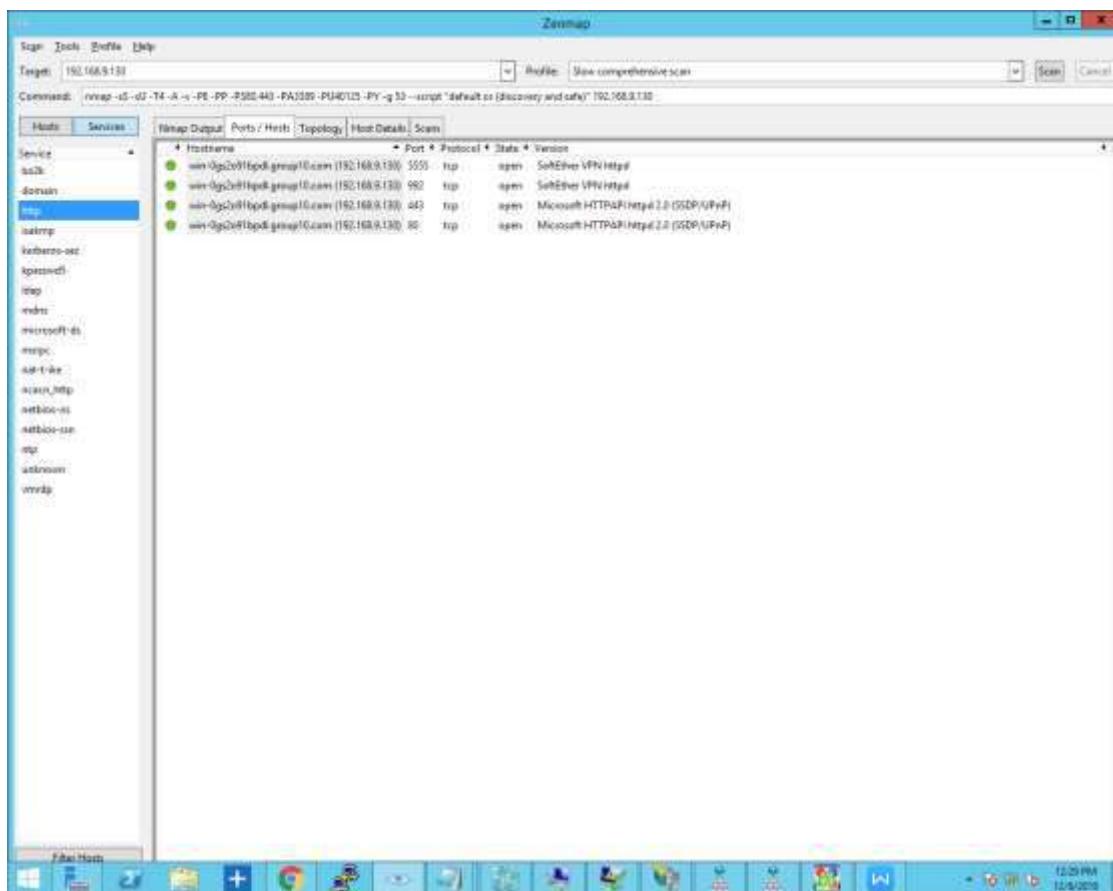
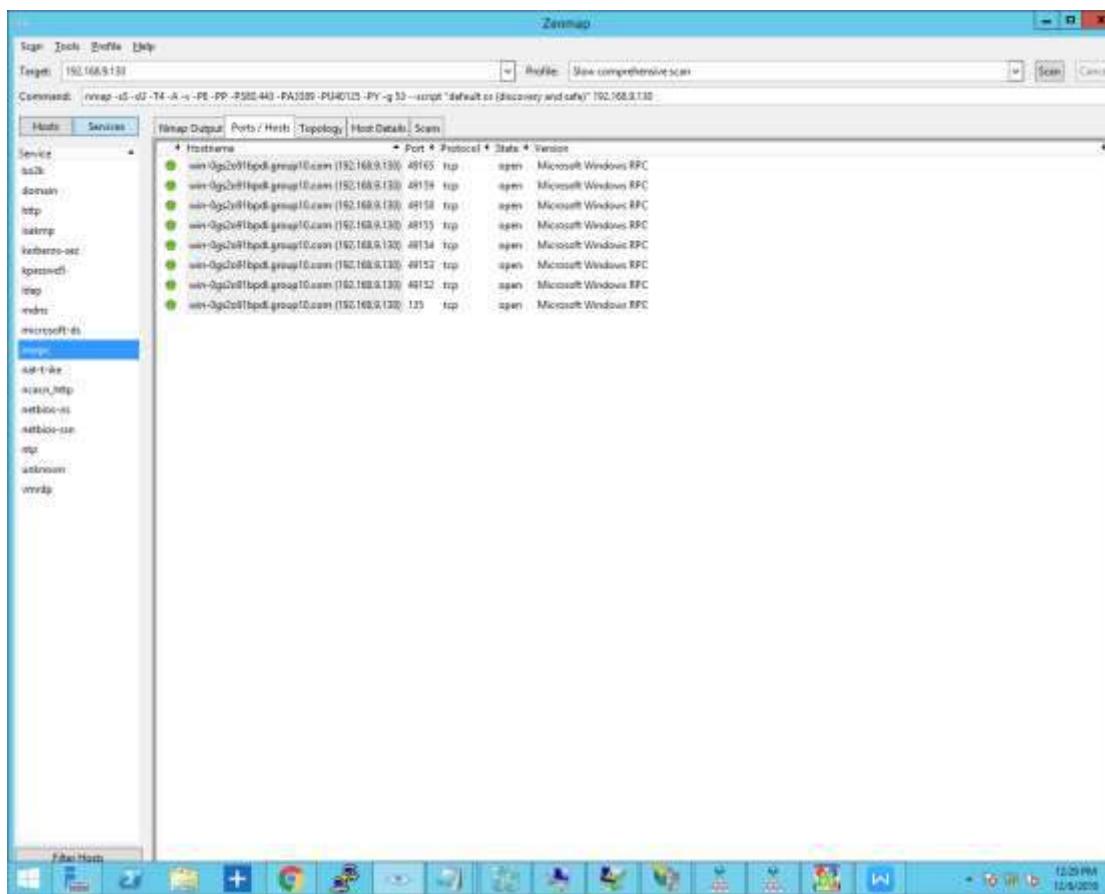


Figure 5.2.23.58: Show open port in HTTP



**Figure 5.2.23.59: Show open port in MSRPC**

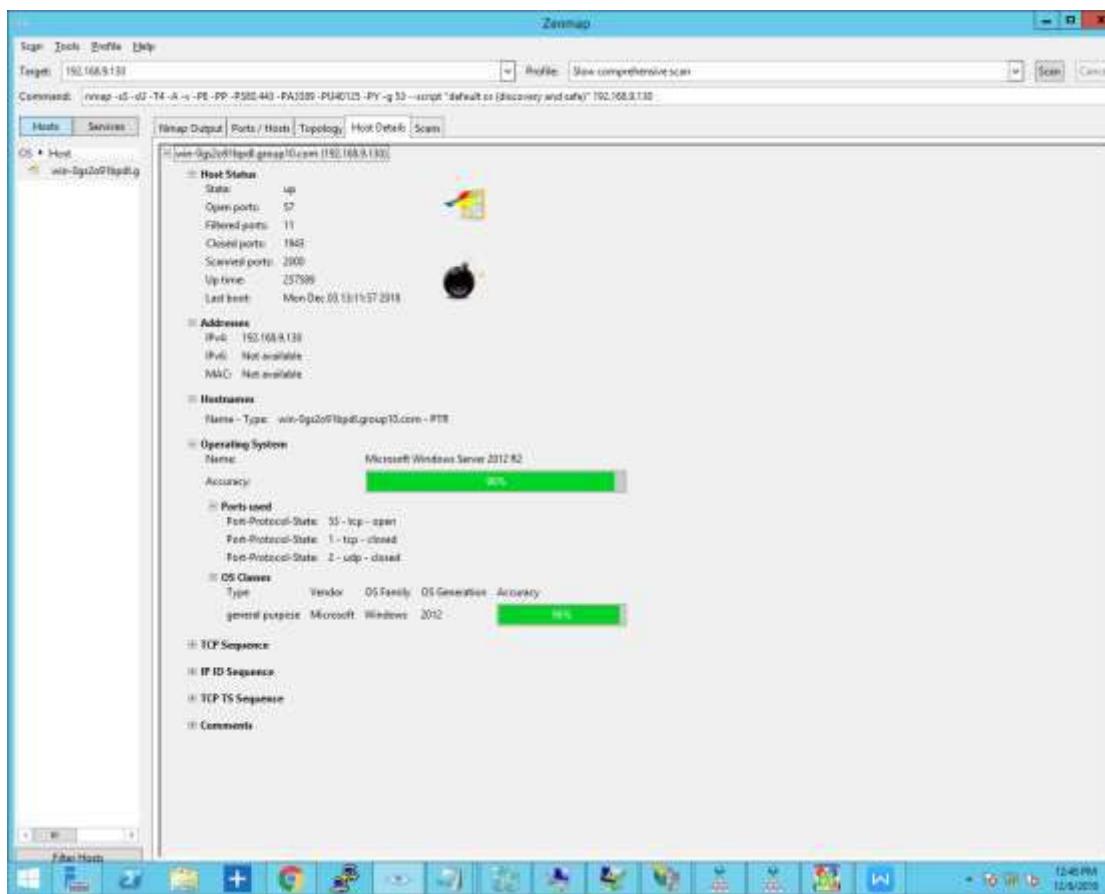


Figure 5.2.23.60: Port scanning status

As shown in the result in Figure , 1000 ports were scanned, 21 ports were opened, 0 ports were closed and 976 ports were filtered before hardening process. The ports are opened means that an application is actively accepting TCP connection. Besides, it shows services available for use on the network. A closed port means it is accessible but there is no application listening on it. Filtered ports that Nmap cannot determine whether the port is opened or closed because packet filtering prevents its probes from reaching the port.

The open ports are explained as the following:

- Port 53

Used by TCP/ UDP protocol for DNS is used for domain name resolution.

- Port 80,443,992,5555

Used by TCP/ UDP protocol for Hypertext Transfer Protocol (HTTP)

- Port 443

Used by TCP for HTTP services for IIS

- Port 88

Used by TCP/ UDP protocol for Kerberos authentication system.

- Port 135, 49153, 49154, 49155, 49158

Used by TCP/ UDP protocol for Microsoft EPMAP (End Point Mapper), also known as DCE/RPC Locator Service, used to remotely manage services including DHCP server, DNS server and WINS. Also used by DCOM.

- Port 139

Used by TCP/ UDP protocol for NetBIOS session Service.

- Port 389, 636, 3268, 3269

Used by TCP for Lightweight Directory Access Protocol services (LDAP). LDAP is an Internet protocol used by MS Active Directory, as well as some email programs to look up contact information from a server.

- Port 445

Used by TCP for Microsoft-DS services. It is used for direct TCP/IP MS Networking access without the need for a NetBIOS layer.

- Port 464

Used by TCP/ UDP protocol for Kerberos password

- Port 593, 49157

Used for ncacn\_http that identifies the Microsoft Internet Information Server (IIS) as the protocol family for the endpoint.

### **Problem:**

In a time when nearly every computing resource is online and susceptible to attack, server hardening is a near absolute must to perform on your servers. The internet has vastly altered the complexion of the server hardening industry over the last decade. Much of the applications and system that is now developed is intended for use on the internet, and for connection to the internet. Many servers online today are attacked thousands of times per hour, tens and sometimes hundreds of thousands of times each and every day. The best defenses against such attacks is to ensure that server hardening is well-established practice within your organization or to outsource this task to an experienced and established server hardening agency.

**Solution:**

Windows operating system can be hardened, system, hardening is more often done on Windows machines, since they are more likely to have their security compromised. Process of securing a system by reducing its surface of vulnerability, which is larger when a system performs more functions; in principle a single-function system is more secure than multi-purpose one. Reducing available ways of attack typically includes the removal of unnecessary software, unnecessary usernames or logins and the disabling or removal of unnecessary services.

## 5.2.24 Authentication user by Integrating AD with Linux

### Integrating Active Directory with Linux (Ubuntu & Fedora)

Integrating active directory will allow user to login to their account which already register and created on Window Server. This will ensure that all the personnel that login into the Linux pc is n authorized person. Besides, it also will be more efficient because all the authorized person no need to keep registering their account on different pc. On this case, both our Linux operating system will be integrated with active directory.

#### Configuration of Integrating Active Directory with Ubuntu

1. Download and install Power Broker Integration Service (PBIS) from GitHub.

```
group10@group10:~$ wget https://github.com/BeyondTrust/pbis-open/releases/download/8.7.1/pbis-open-8.7.1.494.linux.x86_64.deb.sh
--2018-10-28 05:59:30-- https://github.com/BeyondTrust/pbis-open/releases/download/8.7.1/pbis-open-8.7.1.494.linux.x86_64.deb.sh
Resolving github.com (github.com)... 192.30.253.112, 192.30.253.113
Connecting to github.com (github.com)|192.30.253.112|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://github-production-release-asset-2e65be.s3.amazonaws.com/66377182/8562bd00-d6b7-11e8-88f6-7cc766fbfe1e?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53AK2F20181027%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20181027T095949Z&X-Amz-Expires=3008X-Amz-Signature=d7ab0365211c62c253a5e38d182bab45ef652d8ce8104c0b70fde64f5ce1d278X-Amz-SignedHeaders=host&actor_id=0&response-content-disposition=attachment%3B%20filename%3Dpbis-open-8.7.1.494.linux.x86_64.deb.sh&response-content-type=application%2Foctet-stream [following]
--2018-10-28 05:59:32-- https://github-production-release-asset-2e65be.s3.amazonaws.com/66377182/8562bd00-d6b7-11e8-88f6-7cc766fbfe1e?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53AK2F20181027%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20181027T095949Z&X-Amz-Expires=3008X-Amz-Signature=d7ab0365211c62c253a5e38d182bab45ef652d8ce8104c0b70fde64f5ce1d278X-Amz-SignedHeaders=host&actor_id=0&response-content-disposition=attachment%3B%20filename%3Dpbis-open-8.7.1.494.linux.x86_64.deb.sh&response-content-type=application%2Foctet-stream
Resolving github-production-release-asset-2e65be.s3.amazonaws.com (github-production-release-asset-2e65be.s3.amazonaws.com)... 52.216.169.115
Connecting to github-production-release-asset-2e65be.s3.amazonaws.com (github-production-release-asset-2e65be.s3.amazonaws.com)|52.216.169.115|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 8317027 (7.9M) [application/octet-stream]
Saving to: 'pbis-open-8.7.1.494.linux.x86_64.deb.sh'

pbis-open-8.7.1.494.linux.x86_64. 100%[=====] 7.93M 1.33MB/s in 11s

2018-10-28 05:59:44 (746 KB/s) - 'pbis-open-8.7.1.494.linux.x86_64.deb.sh' saved [8317027/8317027]
```

Figure 5.2.24.1: Download PBIS (Ubuntu)

2. Next, make the file downloaded executable.

```
group10@group10:~$ sudo chmod +x pbis-open-8.7.1.494.linux.x86_64.deb.sh
[sudo] password for group10:
group10@group10:~$
```

Figure 5.2.24.2: Configure PBIS (Ubuntu)

3. Execute install file.

```
group10@group10:~$ sudo ./pbis-open-8.7.1.494.linux.x86_64.deb.sh
Creating directory pbis-open-8.7.1.494.linux.x86_64.deb
Verifying archive integrity... All good.
Uncompressing pbis-open-8.7.1.494.linux.x86_64.deb.....
Installing packages and old packages will be removed
Selecting previously unselected package pbis-open-upgrade.
(Reading database ... 221438 files and directories currently installed.)
Preparing to unpack .../pbis-open-upgrade_8.7.1.494_amd64.deb ...
Unpacking pbis-open-upgrade (8.7.1.494) ...
Setting up pbis-open-upgrade (8.7.1.494) ...
Selecting previously unselected package pbis-open.
(Reading database ... 221440 files and directories currently installed.)
Preparing to unpack .../pbis-open_8.7.1.494_amd64.deb ...
Unpacking pbis-open (8.7.1.494) ...
Setting up pbis-open (8.7.1.494) ...
Importing registry...
```

*Figure 5.2.24.3: Execute PBIS (Ubuntu)*

4. Restart avachi service.

```
group10@group10:~$ sudo service avahi-daemon restart
group10@group10:~$ sudo domainjoin-cli join group10.com Administrator
Joining to AD Domain: group10.com
With Computer DNS Name: group10.group10.com

Administrator@GROUP10.COM's password:
Warning: System restart required
Your system has been configured to authenticate to Active Directory for the
first time. It is recommended that you restart your system to ensure that all
applications recognize the new settings.

SUCCESS
```

*Figure 5.2.24.4: Restart avachi (Ubuntu)*

5. Next join the PC to domain and user.

```
group10@group10:~$ sudo domainjoin-cli join group10.com teng
Joining to AD Domain: group10.com
With Computer DNS Name: group10.group10.com

teng@GROUP10.COM's password:
SUCCESS
```

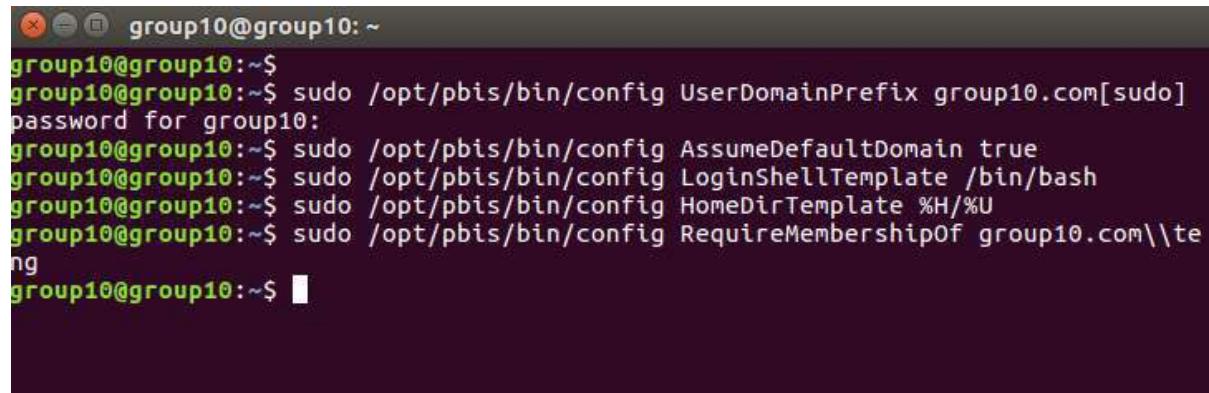
*Figure 5.2.24.5: Join Domain (Ubuntu)*

6. Next, restart SSH service.

```
group10@group10:~$ sudo service ssh restart  
[sudo] password for group10:
```

*Figure 5.2.24.6: Restart SSH (Ubuntu)*

7. Set Active Directory login settings.



The screenshot shows a terminal window with the following command history:

```
group10@group10:~$  
group10@group10:~$ sudo /opt/pbis/bin/config UserDomainPrefix group10.com[sudo]  
password for group10:  
group10@group10:~$ sudo /opt/pbis/bin/config AssumeDefaultDomain true  
group10@group10:~$ sudo /opt/pbis/bin/config LoginShellTemplate /bin/bash  
group10@group10:~$ sudo /opt/pbis/bin/config HomeDirTemplate %H/%U  
group10@group10:~$ sudo /opt/pbis/bin/config RequireMembershipOf group10.com\te  
ng  
group10@group10:~$
```

*Figure 5.2.24.7: Login setting (Ubuntu)*

8. Edit lightdm (login screen settings)

```
group10@group10:~$ sudo nano /usr/share/lightdm/lightdm.conf.d/50-unity-greeter.  
conf
```

*Figure 5.2.24.8: Login setting 2 (Ubuntu)*

Change the configuration like below.

```
[Seat:1]  
greeter-session=unity-greeter  
allow-guest=false  
greeter-show-manual-login=true
```

*Figure 5.2.24.9: Login setting 3 (Ubuntu)*

9. Reboot the PC and sign in to the active directory account that integrated.

## Configuration of Integrating Active Directory with Fedora

1. Install some required packages.

```
[group10@Nuqman ~]$ sudo dnf -y install realmd sssd oddjob oddjob-mkhomedir adcli  
i samba-common-tools  
[sudo] password for group10:  
Last metadata expiration check: 2:38:45 ago on Sat 27 Oct 2018 01:45:19 PM +08.  
Package realmd-0.16.3-12.fc28.x86_64 is already installed, skipping.  
Package sssd-1.16.3-2.fc28.x86_64 is already installed, skipping.  
Package oddjob-0.34.4-4.fc28.x86_64 is already installed, skipping.  
Package oddjob-mkhomedir-0.34.4-4.fc28.x86_64 is already installed, skipping.  
Package adcli-0.8.0-6.fc28.x86_64 is already installed, skipping.  
Package samba-common-tools-2:4.8.6-0.fc28.x86_64 is already installed, skipping.  
Dependencies resolved.  
Nothing to do.  
Complete!
```

*Figure 5.2.24.10: Get Kerberos (Fedora)*

2. Change DNS settings to refer to Active Directory.

```
[group10@Nuqman ~]$ nmcli connection mod eno1 ipv4.dns 192.168.9.130  
[group10@Nuqman ~]$ nmcli connection down eno1; nmcli connection up eno1  
Connection 'eno1' successfully deactivated (D-Bus active path: /org/freedesktop/  
NetworkManager/ActiveConnection/7)  
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkMa  
nager/ActiveConnection/9)  
[group10@Nuqman ~]$ █
```

*Figure 5.2.24.11: DNS settings (Fedora)*

3. Discover Active Directory domain.

```
[group10@Nuqman ~]$ realm discover Group10.com  
group10.com  
  type: kerberos  
  realm-name: GROUP10.COM  
  domain-name: group10.com  
  configured: kerberos-member  
  server-software: active-directory  
  client-software: sssd  
  required-package: oddjob  
  required-package: oddjob-mkhomedir  
  required-package: sssd  
  required-package: adcli  
  required-package: samba-common-tools  
  login-formats: %U@group10.com  
  login-policy: allow-realm-logins
```

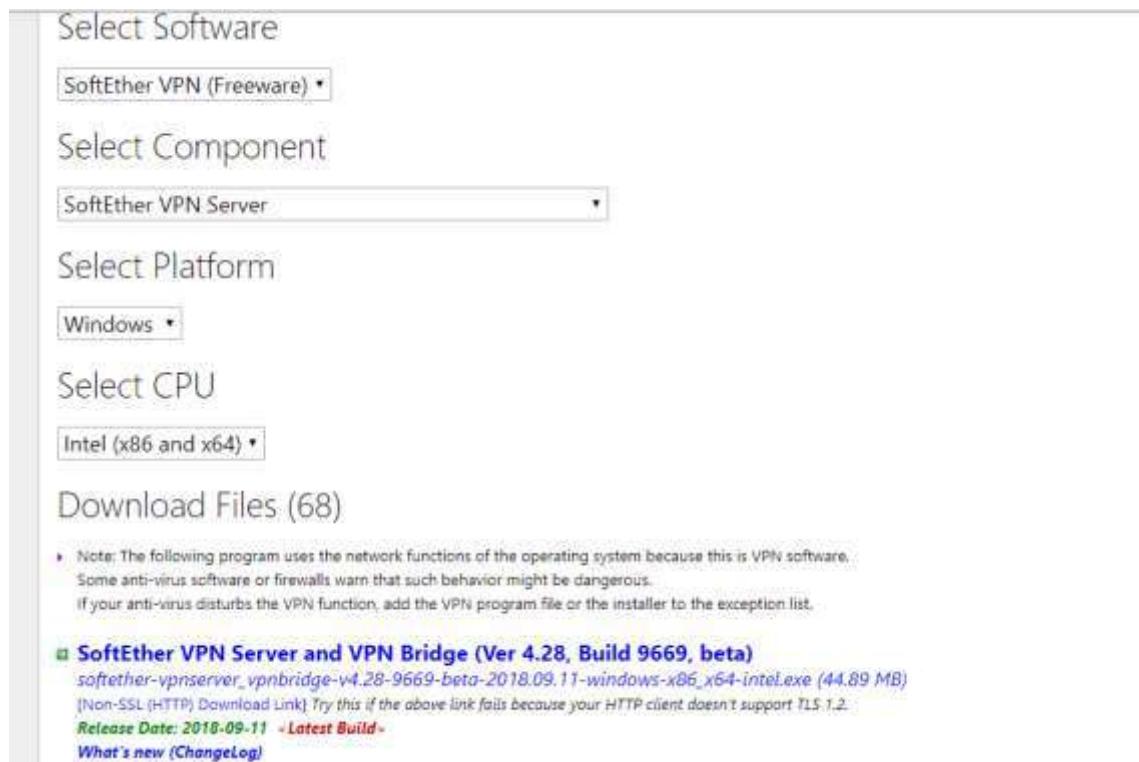
*Figure 5.2.24.12: Discover domain (Fedora)*

### 5.2.25 IPSec VPN for remote employee

If you want to securely extend your network to remote users or knit together branch offices into a single virtual network, IPsec VPN is the tool you need. Working remotely—from home, a remote branch, or even a café—is increasingly popular, but it creates serious risks for network administrators and users. These days, users expect access to everything from their phone or laptop, wherever they are. If they access the Internet directly, they are exposed to Wi-Fi hackers, viruses, and more. IPsec VPN solves all of that by routing them through Untangle, where all the same policies and protections are provided via a secure encrypted tunnel directly between your network and the user. For this IPsec VPN, Softether will be used due to its open source and reliable. In this case, there is 2 environment for connection of VPN, one is having internet connection and other one is without internet connection.

#### Setup and configuration for Softether VPN server manager.

1. Go to Softether website and choose the Softether VPN Server component and select Operating System type. Then click on the below Download Files.



*Figure 5.2.25.1: Installation*

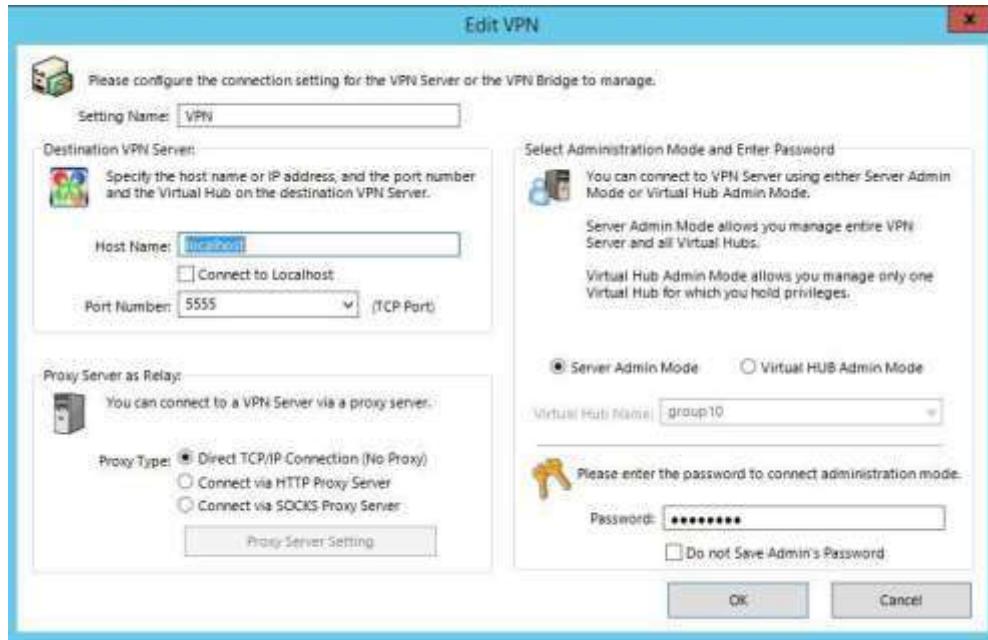
2. After download, install with default setting.

3. Open Softether and below will be shown.



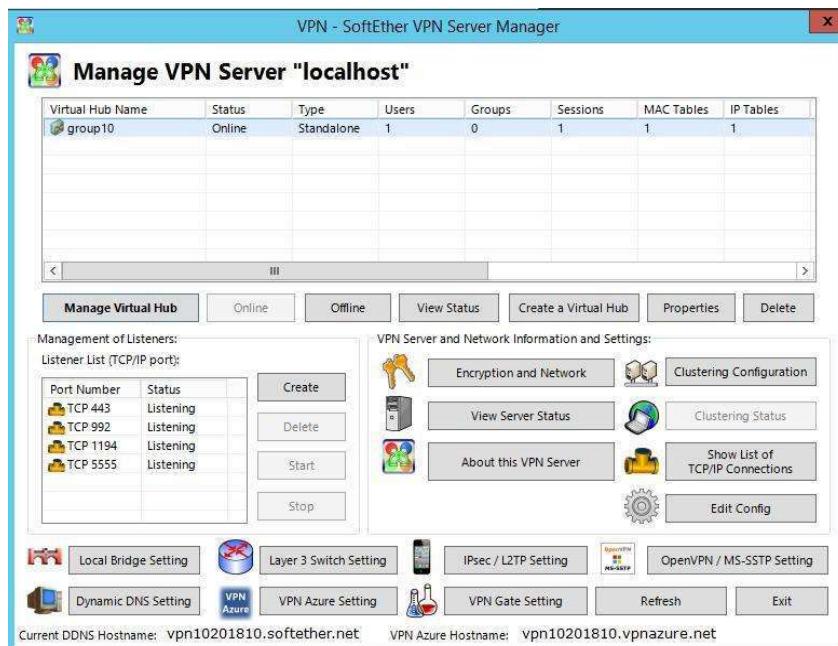
*Figure 5.2.25.2: Interface Softether VPN Server Manager*

4. Configure the VPN server by click new setting. After enter new setting, below window will be shown. Change the host name to localhost so that it define device IP Address automatically of your window and select port 5555 to perform VPN-port.



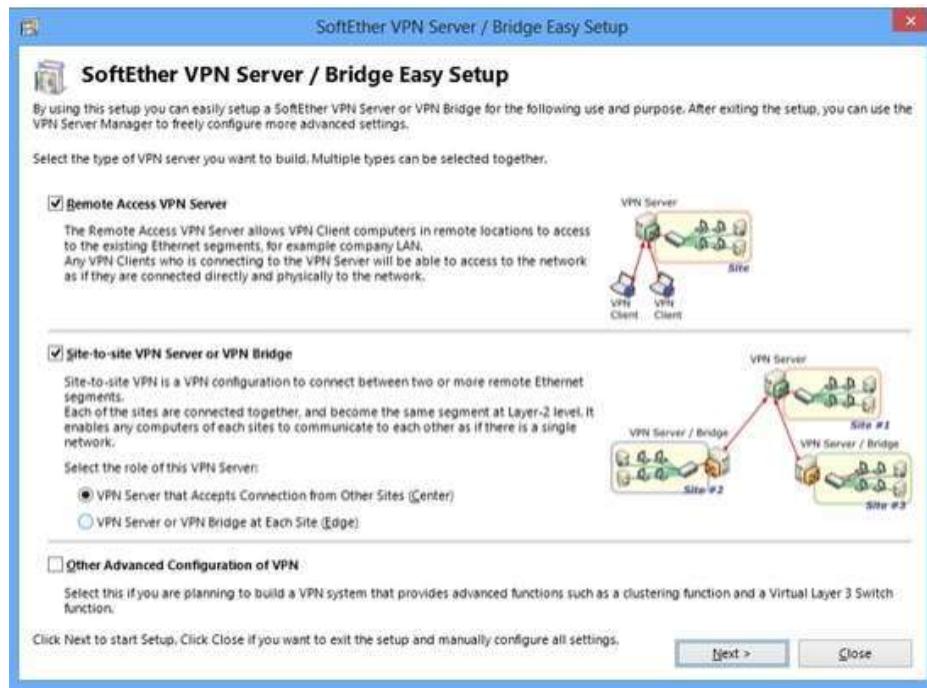
**Figure 5.2.25.3: Configuration VPN Server Manager 1**

6. After that choose to connect and below will be shown with other settings.



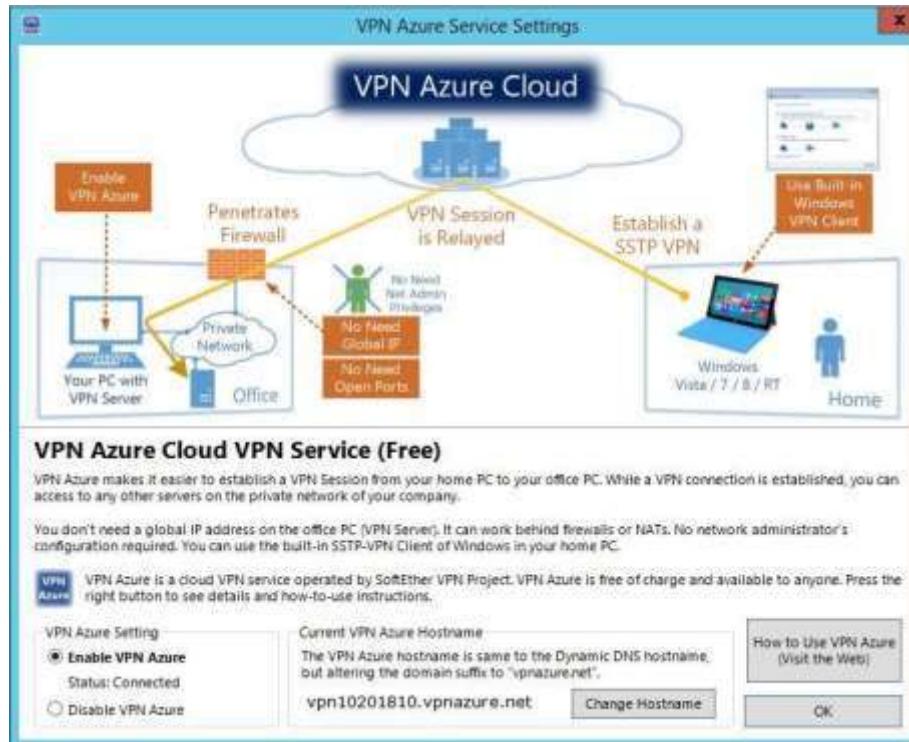
**Figure 5.2.25.4: Configuration VPN Server Manager 2**

To enable bridge on remote access VPN server, tick the box below.



*Figure 5.2.25.5: Configuration VPN Server Manager 3*

Enable VPN Azure then change the host name accordingly. In this case, vpn10201810.vpnazure.net is chosen.



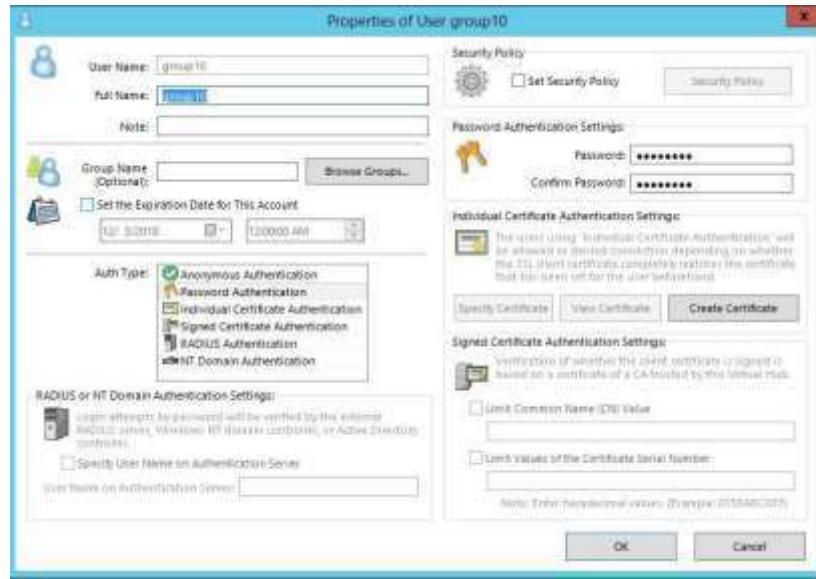
*Figure 5.2.25.6: Configuration VPN Server Manager 4*

Then tick Enable L2TP Server Function (L2TP over IPsec).



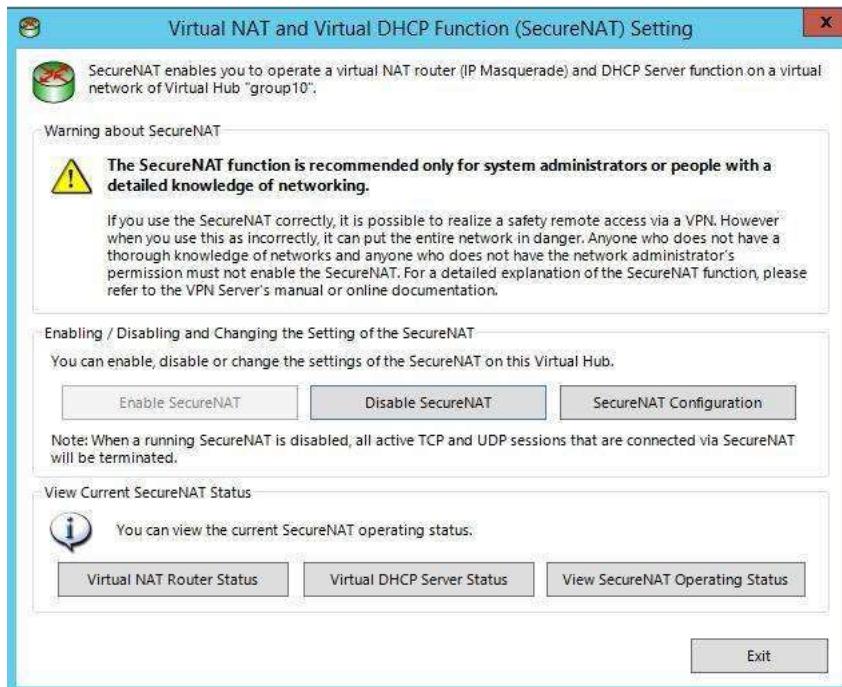
*Figure 5.2.25.7: Configuration VPN Server Manager 5*

7. Create a user for VPN connection. It has some option to choose when log in to the VPN. In this case, we choose Password Authentication to log in to VPN.



**Figure 5.2.25.8: Configuration VPN Server Manager 6**

8. Before exit, enable Enable SecureNAT. This will allow other user to establish the connection to VPN through internet.



**Figure 5.2.25.9: Configuration VPN Server Manager 8**

9. Finally the user is created.

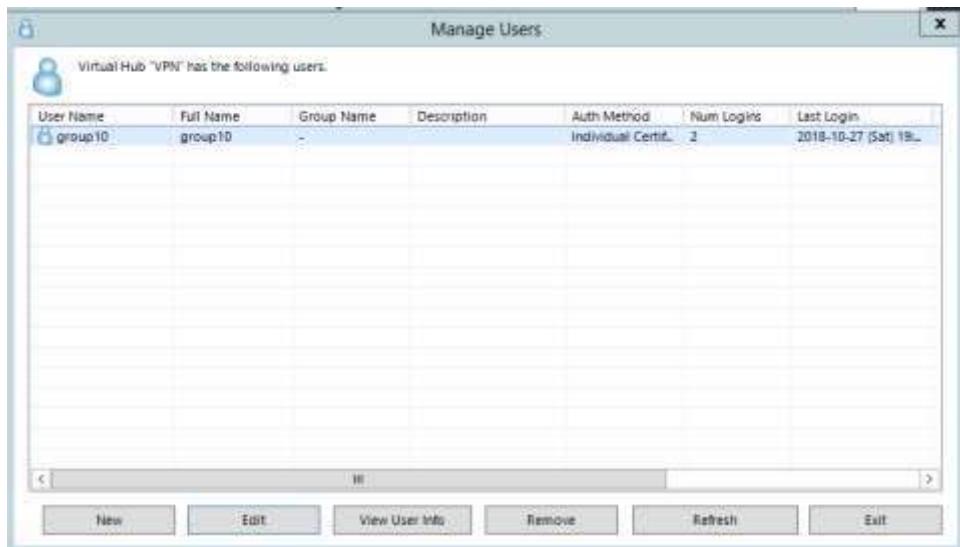


Figure 5.2.25.10: Configuration VPN Server Manager 9

10. At this screenshot, the VPN server is finally online for user to connect.

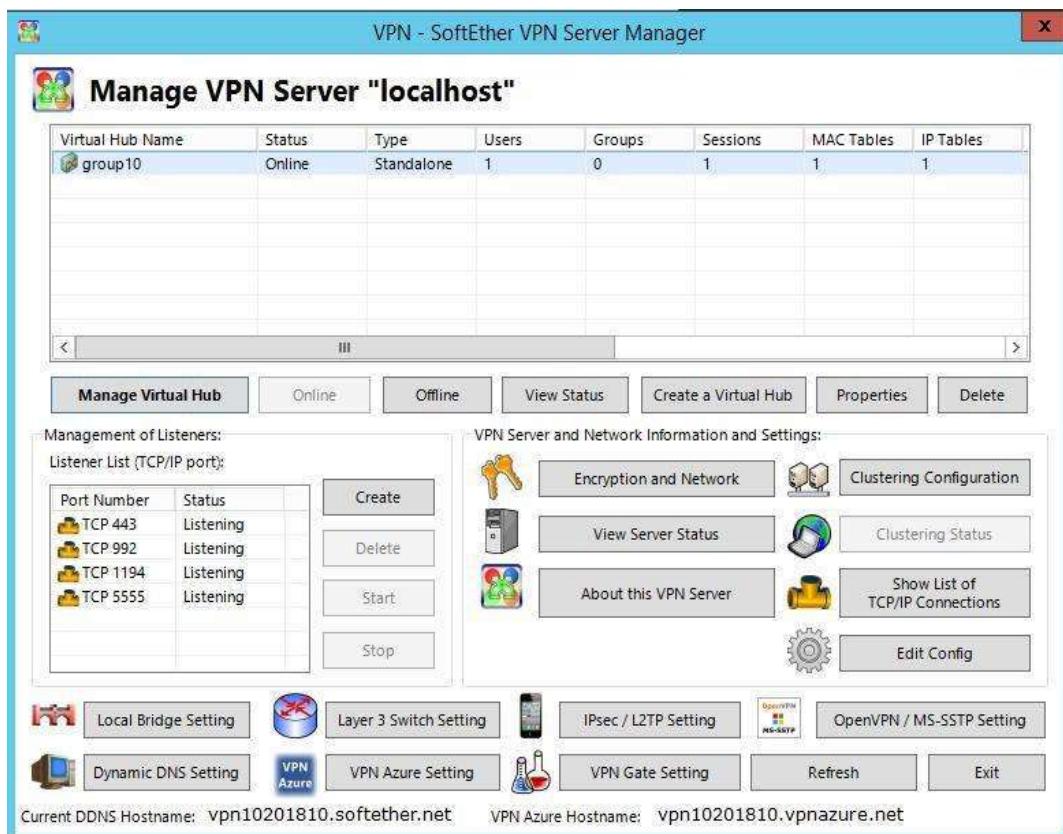


Figure 5.2.25.11: Configuration VPN Server Manager 10

## 5.2.26 Samba Security Services

Samba security is a method to secure our share file with restrict access to unauthorized user.

Below are the smb.conf file of samba to set rules and regulation to the access of Samba.

There are two files are share:

- Share
  - Require membership to log in.
  - A range of IP address can access to this folder.
  - User and group can read and write, while other cannot read, write and execute.
  - User and group can read, write and execute while other doesn't have any permission.
- HighAuthority
  - Only teng can access.
  - Able to read, write and execute.
  - Require membership to login.
  - Only for higher authority personal.
  - Only a PC with a IP address can access to this folder.
  - User and group can read and write, while other cannot read, write and execute.
  - User and group can read, write and execute while other doesn't have any permission.

Configuration of samba.conf.

```
File Edit View Search Terminal Help
GNU nano 2.9.8

[global]
workgroup = WORKGROUP
server string = 192.168.9.138
interfaces = eno1 lo virbr0
bind interfaces only = yes
server role = standalone server
log file = /var/log/samba/smb.log
max log size = 10000
smb ports = 445
disable netbios = yes
idmap config * : backend = tdb

[Share]
path = /home/SharedFolder
browsable = yes
read only = no
force create mode = 0660
force directory mode = 2770
valid users = group10
host allow = 192.168.9. 255.255.255.

[HighAuthority]
path = /home/HigherAuth
browsable = yes
read only = no
force create mode = 0660
force directory mode = 2770
valid users = teng
hosts allow = 192.168.9.66/26
```

*Figure 5.2.26.1: Samba Configuration*

### 5.2.27 Active Directory

Active Directory Domain Services (AD DS) is a server role in Active Directory that allows admins to manage and store information about resources from a network, as well as application data, in a distributed database. AD DS can also help admins manage a network's elements (computers and end users) and reorder them into a custom hierarchy

#### Installing Active Directory (AD)

Step 1: Open **Server Manager** and click **Add roles and features**.

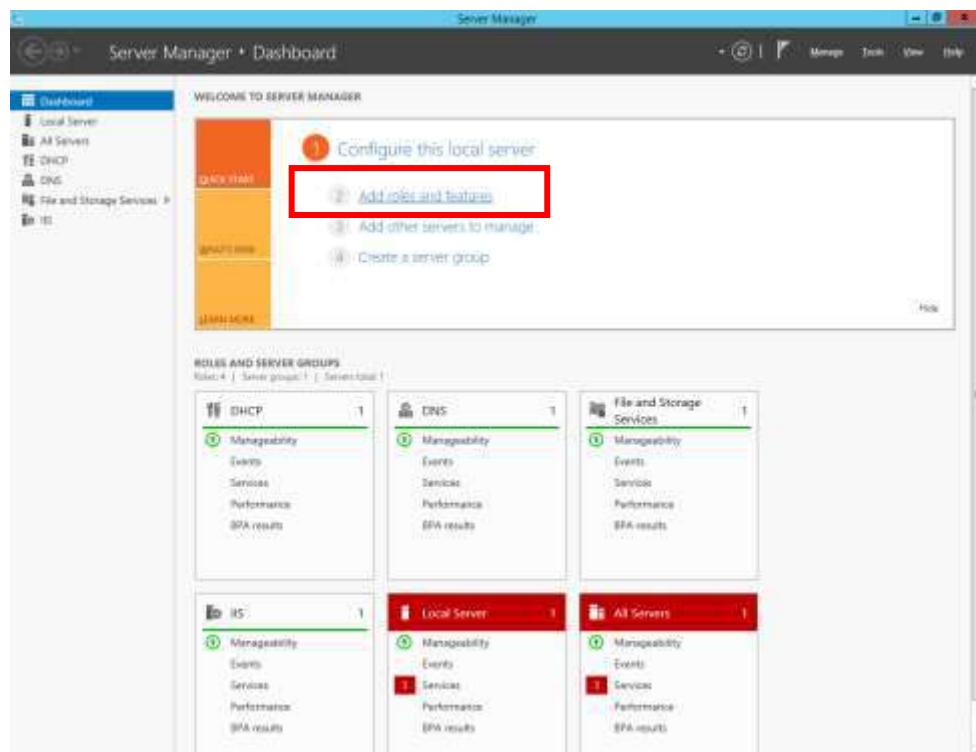
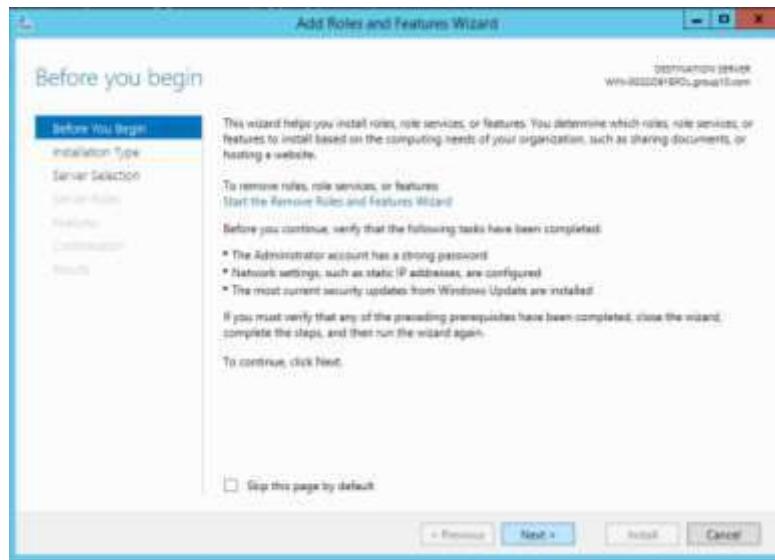


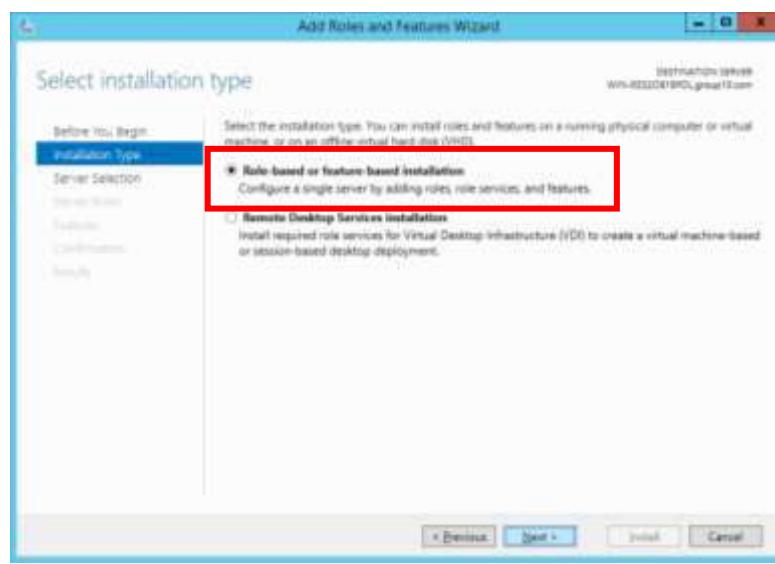
Figure 5.2.27.1: Add Active Directory to Server Manager

Step 2: Click **Next** to proceed with the installation.



*Figure 5.2.27.2: AD Installation*

Step 3: Select **Role-based or feature-based installation** and click **Next** to proceed.



*Figure 5.2.27.3: Role-based AD Installation*

Step 4: Select your server from the server pool and click **Next** to proceed.

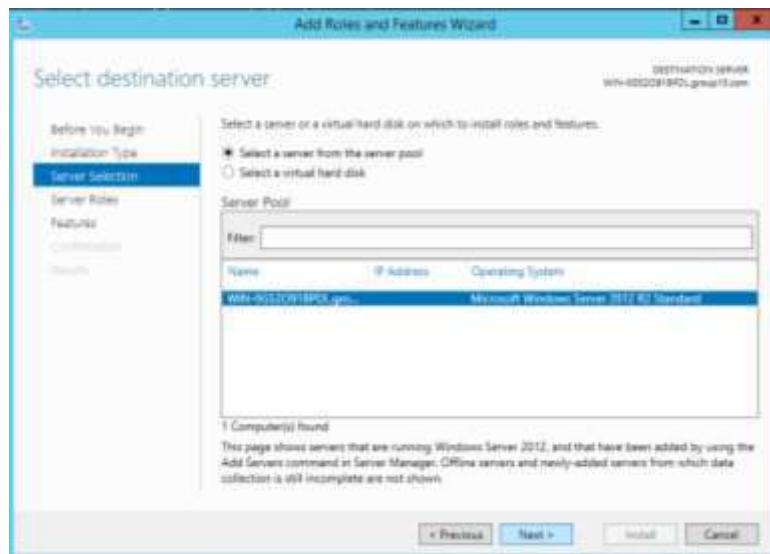


Figure 5.2.27.4: Select server for AD

Step 5: Select **Active Directory Domain Services** from the **Server Roles**.

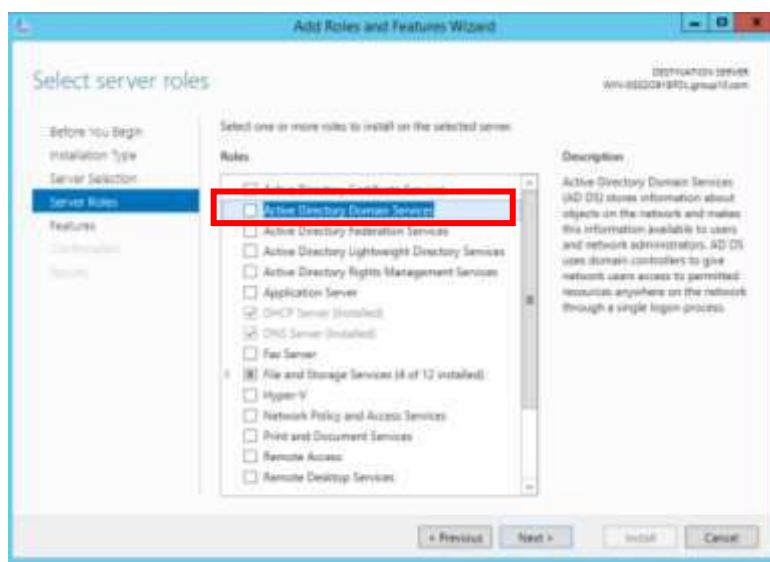


Figure 5.2.27.5: AD Domain Services

Step 6: Click **Add Features** to proceed with the installation.

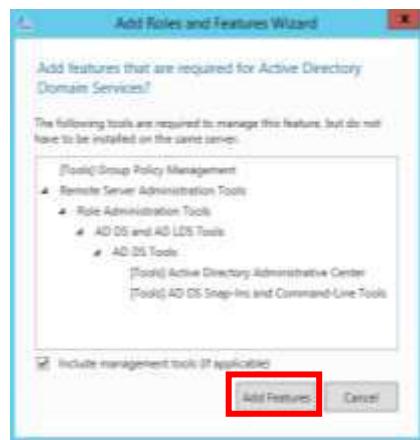


Figure 5.2.27.6: Add AD features required for AD

Step 7: Click **Next** to proceed.

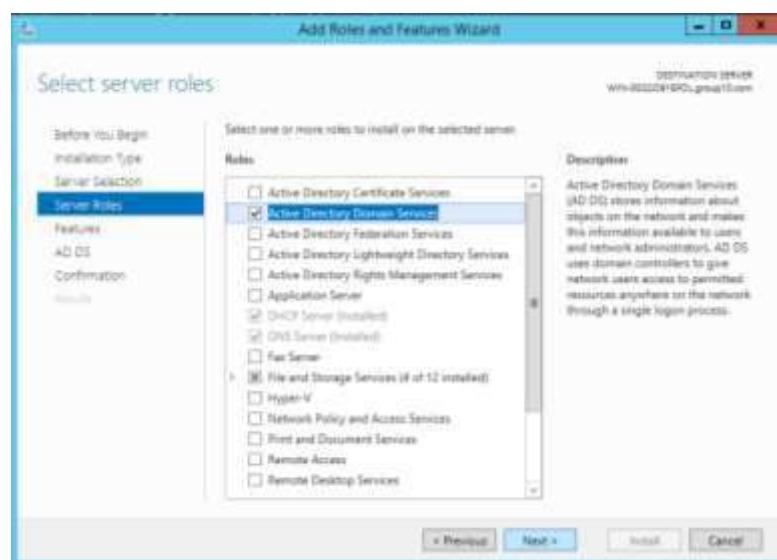


Figure 5.2.27.7: Add additional services for AD

Step 8: Click **Next** to proceed.

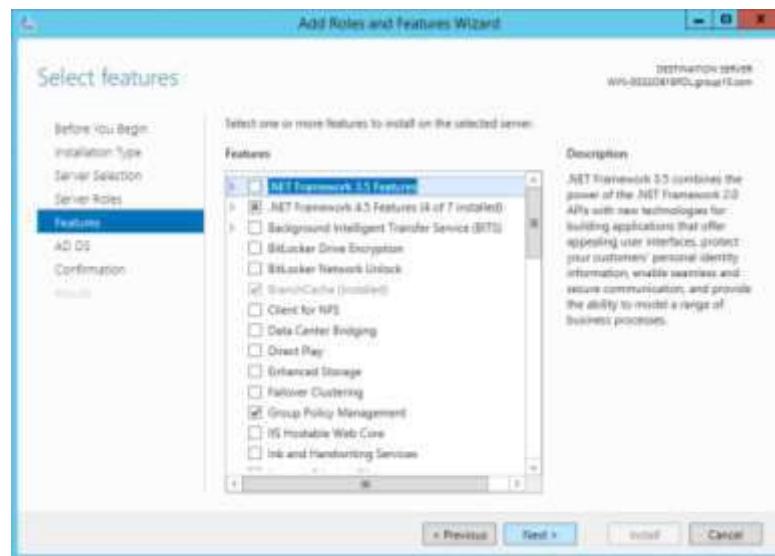


Figure 5.2.27.8: Add additional features for AD

Step 9: Click **Next** to proceed.

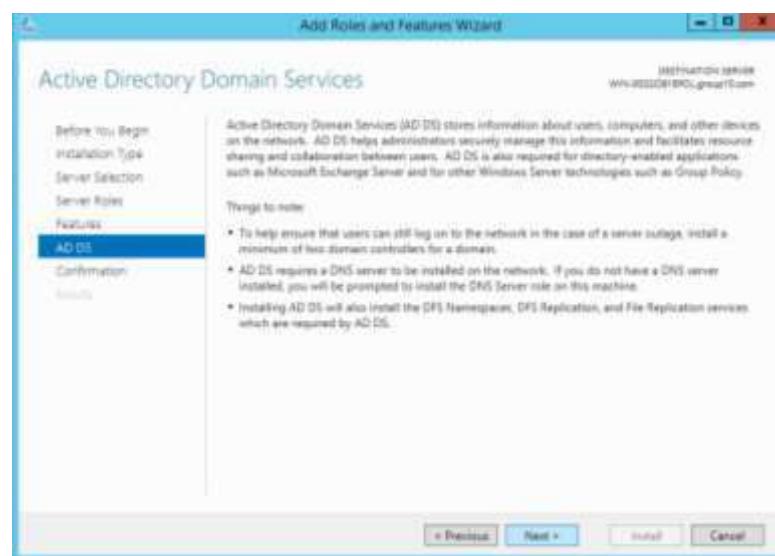


Figure 5.2.27.9: Confirm AD installation

Step 10: Click **Install** to begin with the installation.

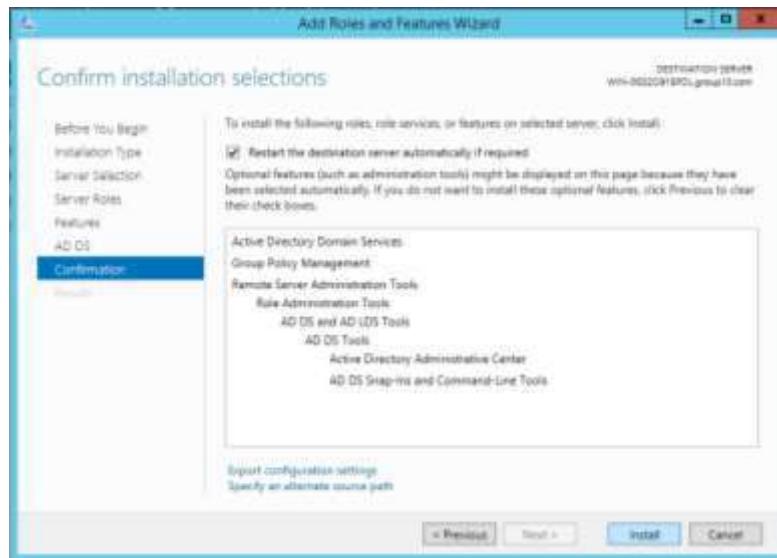


Figure 5.2.27.10: Installing AD to Server Manager

Step 11: Click **Yes** to proceed with the installation.



Figure 5.2.27.11: Confirmation for AD installation

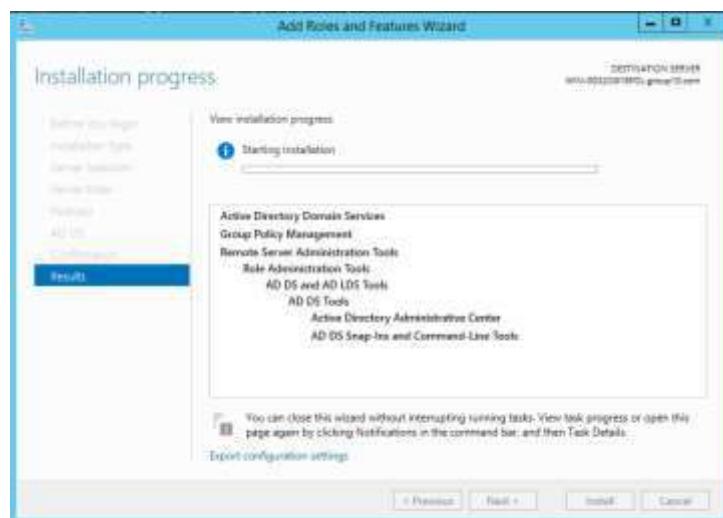


Figure 5.2.27.12: AD Installation progress

Step 12: Click **Close** to finish the installation and your server will restart for the changes to take its effects.

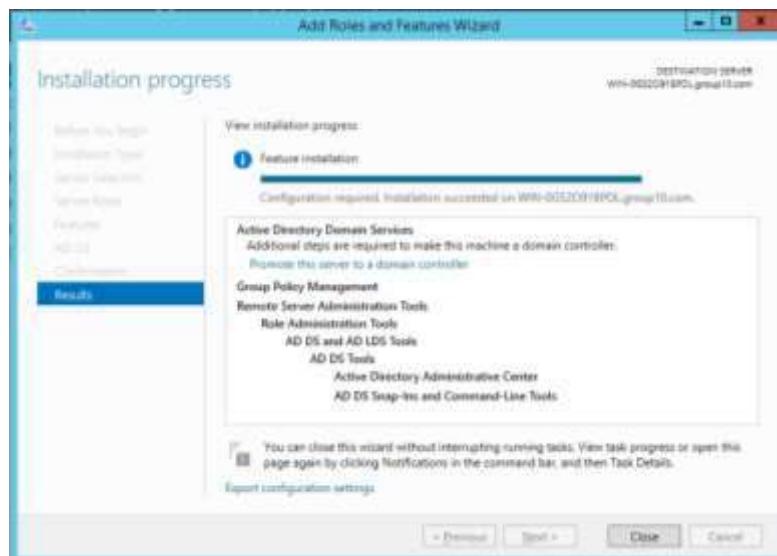
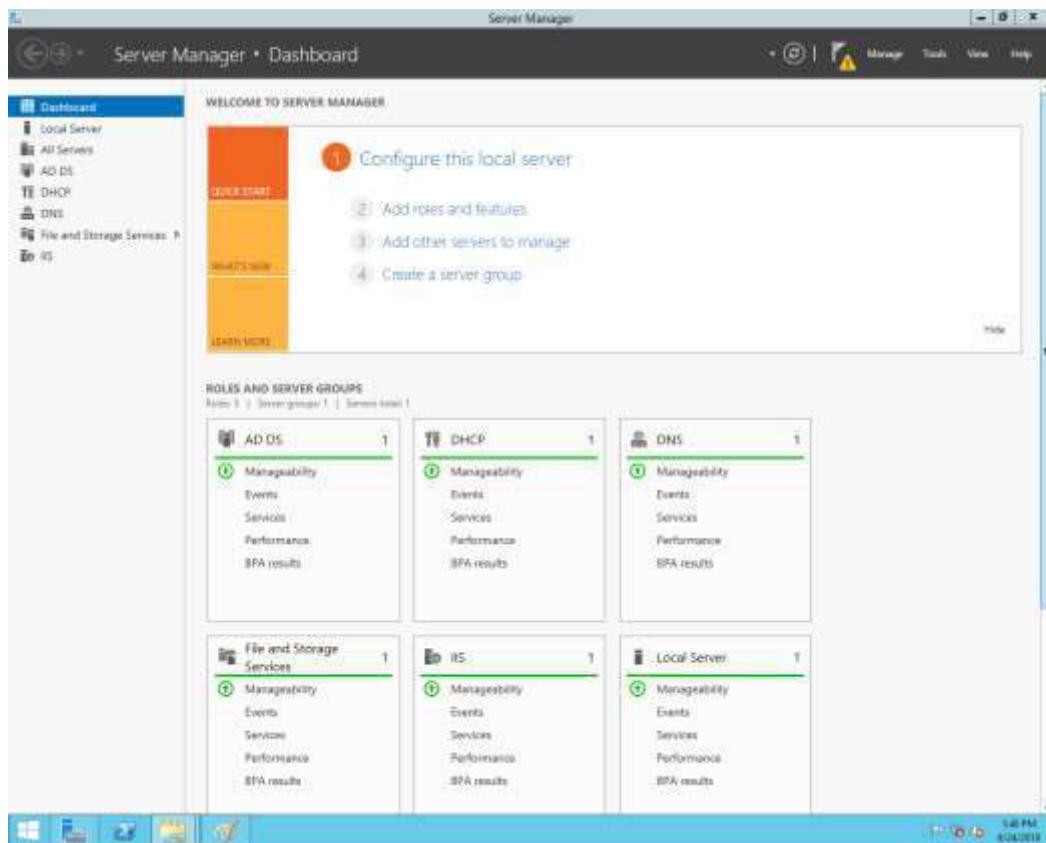


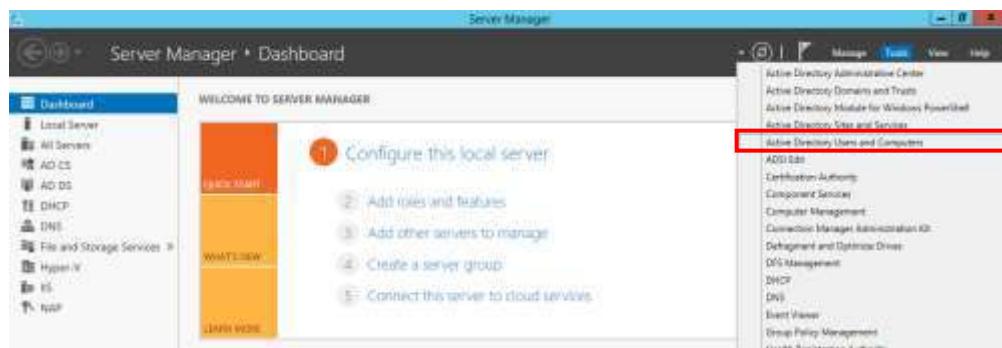
Figure 5.2.27.13: Finishing AD installation



*Figure 5.2.27.14: Finished AD installation*

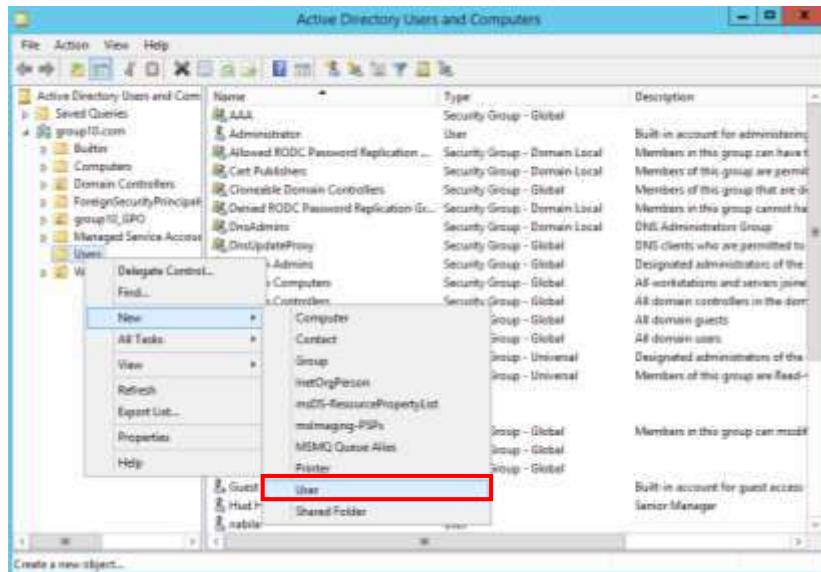
## Create User and Group on Active Directory

Step 1: Open **Server Manager** and click on **Tools** on the top left corner as shown in the figure below, then click on **Active Directory Users and Computers**.



*Figure 5.2.27.15: Server Manager Dashboard*

Step 2: To create a **New User** simply just **right-click** **Users** and navigate to **New** and select **User** from the dropdown list as shown in the figure below.



*Figure 5.2.27.16: Active Directory Users and Computers Window*

Step 3: Enter the user's details and the **User Logon Name** in the form as shown in the figure below and click **Next** to proceed.

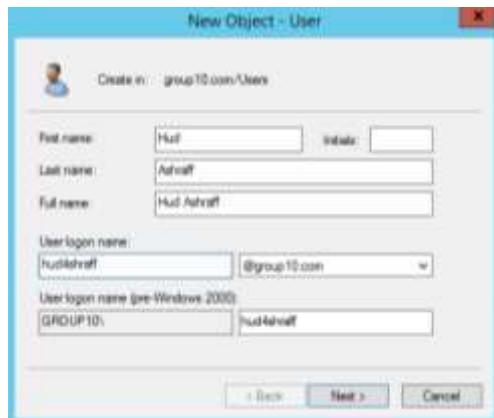


Figure 5.2.27.17: User Information

Step 4: Enter password details and check the box **Password never expires** and click **Next** to proceed.



Figure 5.2.27.18: User Password Information

Step 5: The user name and logon details is shown in the figure below and click the **Next** button to finish add the user into the Active Directory.

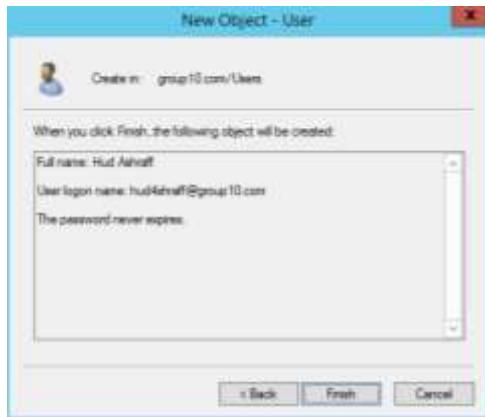


Figure 5.2.27.19: User details confirmation

Step 6: Navigate to **Active Directory Users and Computers**, right-click on **Users** and select **Group** from the dropdown list to create a new Group as shown in the figure below.

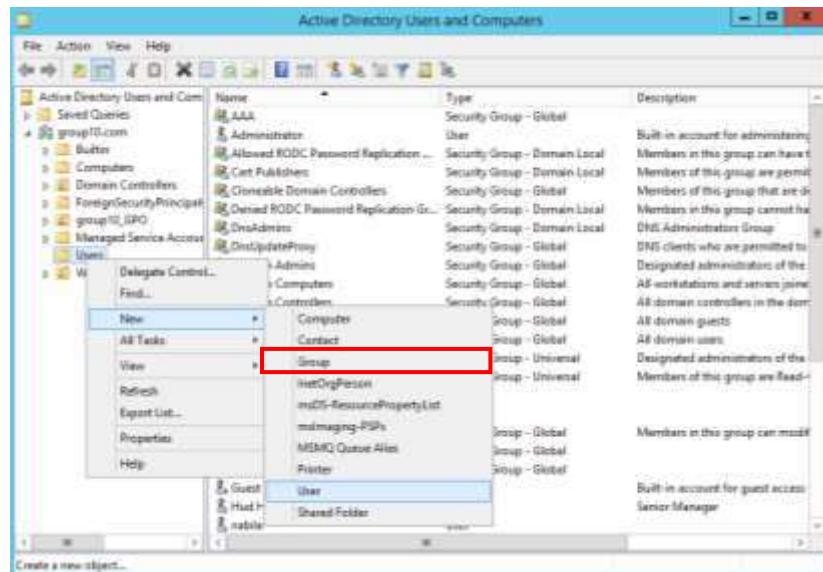


Figure 5.2.27.20: Create new group

Step 7: Enter the Group Name.

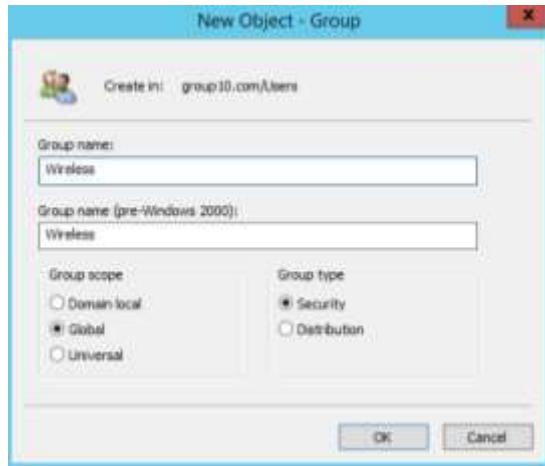


Figure 5.2.27.21: Group Details

Step 8: Navigate to the new group that you have created and right-click and select Properties.

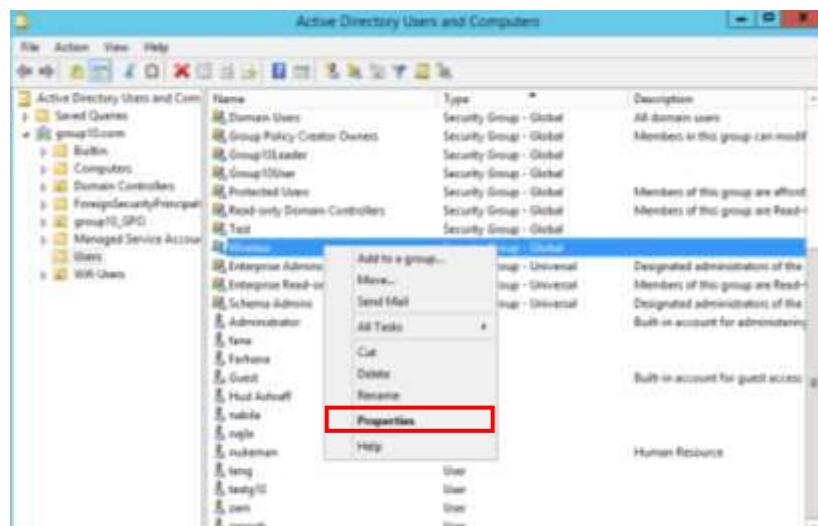


Figure 5.2.27.22: Group Properties

Step 9: Go to the **Members** tab to view all the members that are listed in the group and click on the **Add..** button to proceed.

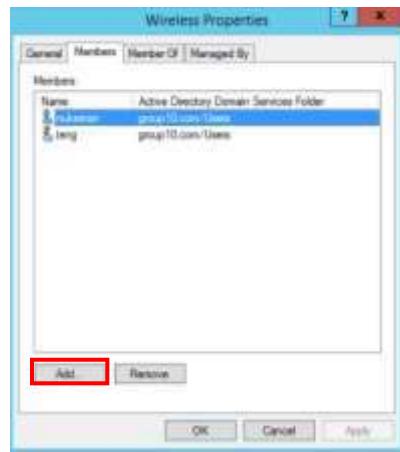


Figure 5.2.27.23: Add members to group

Step 10: Enter the created user name and click Check Names box to verify that the user exist in the AD. Then click OK to proceed.

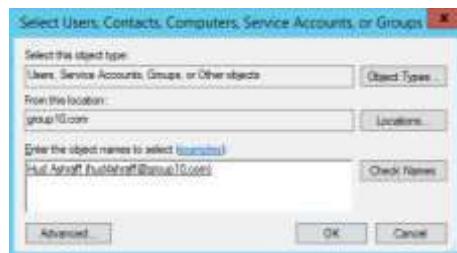
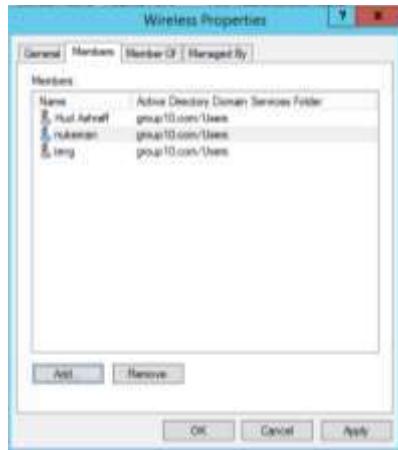


Figure 5.2.27.24: User search

Step 11: Check the user that are Members of the Wireless Group Properties.



**Figure 5.2.27.25: Group user members**

## 5.2.28 VLAN Security

### VLAN Security

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

1. Create a new VLAN and name it.

```
Group10Switch(config)#vlan 5
Group10Switch(config)#name TRUNK
Group10Switch(config)#vlan 10
Group10Switch(config)#name WINSERVER
Group10Switch(config)#vlan 20
Group10Switch(config)#name FEDORA
Group10Switch(config)#vlan 30
Group10Switch(config)#name UBUNTU
Group10Switch(config)#vlan 40
Group10Switch(config)#name CLIENT_WIRED
Group10Switch(config)#vlan 50
Group10Switch(config)#name CLIENT_AP
Group10Switch(config)#vlan 80
Group10Switch(config)#name Unusedport
```

*Figure 5.2.28.1 Create VLAN and name*

2. Move all the port to the corresponding VLAN.

```
Group10Switch(config)#int range fa0/1-2
Group10Switch(config-if-range)#switchport access vlan 10
Group10Switch(config-if-range)#int range fa0/3-4
Group10Switch(config-if-range)#switchport access vlan 20
Group10Switch(config-if-range)#int range fa0/5-6
Group10Switch(config-if-range)#switchport access vlan 30
Group10Switch(config-if)#int fa0/7
Group10Switch(config-if)#switchport access vlan 40
Group10Switch(config-if)#int fa0/15
Group10Switch(config-if)#switchport access vlan 50
```

*Figure 5.2.28.2 Allocate Port*

3. Go to VLAN 80 and state it as suspends.

```
Group10Switch(config)#vlan 80
Group10Switch(config-vlan)#state suspend
```

*Figure 5.2.28.3: Change status*

2. Select all the unused port and switch it to VLAN 80.

```
Group10Switch(config)#int range fa0/8-14
Group10Switch(config-if-range)#switchport access vlan 80
Group10Switch(config-if-range)#int range fa0/16-19
Group10Switch(config-if-range)#switchport access vlan 80
Group10Switch(config-if-range)#int range fa0/21-22
Group10Switch(config-if-range)#switchport access vlan 80
Group10Switch(config-if-range)#exit
Group10Switch(config)#do sh vlan
```

Figure 5.2.28.4: Assign Port to VLAN

### 5.2.29 Cloud Server

The figures show the installation of cloud server inside Ubuntu platform

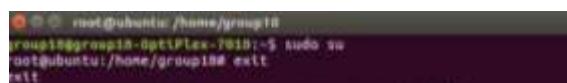


Figure 5.2.29.1: Login in root

```
root@ubuntu:/home/group10# apt-get update
Get:1 http://security.ubuntu.com/ubuntu xenial-security InRelease [107 kB]
Get:2 http://my.archive.ubuntu.com/ubuntu xenial InRelease [309 kB]
Get:3 http://my.archive.ubuntu.com/ubuntu xenial-updates InRelease [107 kB]
Get:4 http://my.archive.ubuntu.com/ubuntu xenial-backports InRelease [107 kB]
Fetched 323 kB in 2s (118 kB/s)
Reading package lists... 95%
```

Figure 5.2.29.2: Update the System

## Installation AMP Server and PHP Extension

```
root@ubuntu:/home/group10# apt-get install lamp-server^
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'libhttp-message-perl' for task 'lamp-server'
Note, selecting 'libencode-locale-perl' for task 'lamp-server'
Note, selecting 'php7.0-clients' for task 'lamp-server'
Note, selecting 'mysql-client-5.7' for task 'lamp-server'
Note, selecting 'libapache2-mod-php' for task 'lamp-server'
Note, selecting 'rename' for task 'lamp-server'
Note, selecting 'mysql-server-5.7' for task 'lamp-server'
Note, selecting 'php-common' for task 'lamp-server'
Note, selecting 'libaprutil1' for task 'lamp-server'
Note, selecting 'mysql-server' for task 'lamp-server'
Note, selecting 'php7.0-opcache' for task 'lamp-server'
Note, selecting 'libcgi-fast-perl' for task 'lamp-server'
Note, selecting 'libwrap0' for task 'lamp-server'
Note, selecting 'libhttp-date-perl' for task 'lamp-server'
Note, selecting 'perl-modules-5.22' for task 'lamp-server'
Note, selecting 'libhttp-mediatypes-perl' for task 'lamp-server'
Note, selecting 'libfcgi-perl' for task 'lamp-server'
Note, selecting 'libcgi-pm-perl' for task 'lamp-server'
Note, selecting 'libaprutil1-dbd-sqlite3' for task 'lamp-server'
Note, selecting 'php7.0-common' for task 'lamp-server'
Note, selecting 'libaiol' for task 'lamp-server'
Note, selecting 'libio-html-perl' for task 'lamp-server'
Note, selecting 'ssl-cert' for task 'lamp-server'
Note, selecting 'apache2-data' for task 'lamp-server'
Note, selecting 'libperl5.22' for task 'lamp-server'
Note, selecting 'libapr1' for task 'lamp-server'
```

Figure 5.2.29.3: Installation Lamp-server I

```

root@ubuntu:/home/group10
creating config file /etc/php/7.0/mods-available/sysvsem.ini with new version
creating config file /etc/php/7.0/mods-available/sysvshm.ini with new version
creating config file /etc/php/7.0/mods-available/tokenizer.ini with new version
setting up php7.0-json (7.0.32-0ubuntu0.16.04.1) ...
creating config file /etc/php/7.0/mods-available/json.ini with new version
setting up php7.0-opcache (7.0.32-0ubuntu0.16.04.1) ...
creating config file /etc/php/7.0/mods-available/opcache.ini with new version
setting up php7.0-readline (7.0.32-0ubuntu0.16.04.1) ...
creating config file /etc/php/7.0/mods-available/readline.ini with new version
setting up php7.0-clit (7.0.32-0ubuntu0.16.04.1) ...
update-alternatives: using /usr/bin/php7.0 to provide /usr/bin/php (php) in auto mode
update-alternatives: using /usr/bin/phar7.0 to provide /usr/bin/phar (phar) in auto mode
update-alternatives: using /usr/bin/phar.phar7.0 to provide /usr/bin/phar.phar (phar.phar) in auto mode
creating config file /etc/php/7.0/cli/php.ini with new version
setting up libapache2-mod-php7.0 (7.0.32-0ubuntu0.16.04.1) ...
creating config file /etc/php/7.0/apache2/php.ini with new version
module rpm_event disabled.
enabling module rpm_prefork.
apache2 switch rpm Switch to prefork
apache2_invoke: enable module php7.0
setting up libapache2-mod-php (1:7.0.33+ubuntu0.1) ...
setting up libhtml-template-perl (2.95-2) ...
setting up mysql-server (5.7.23-0ubuntu0.16.04.1) ...
setting up php7.0-mysql (7.0.32-0ubuntu0.16.04.1) ...
creating config file /etc/php/7.0/mods-available/mysqlind.ini with new version
Creating config file /etc/php/7.0/mods-available/mysqli.ini with new version
creating config file /etc/php/7.0/mods-available/pdo_mysql.ini with new version
setting up php-mysql (1:7.0.33+ubuntu0.1) ...
Processing triggers for libc-bin (2.23-0ubuntu6.1) ...
Processing triggers for systemd (239-4ubuntu21.4) ...
Processing triggers for ureadahead (0.100.0-19) ...
Processing triggers for ufw (0.35-0ubuntu2) ...
Processing triggers for libapache2-mod-php7.0 (7.0.32-0ubuntu0.16.04.1) ...
root@ubuntu:/home/group10# clear

```

*Figure 5.2.29.4: Installation Lamp-server II*

```

root@ubuntu:/home/group10#
root@ubuntu:/home/group10# apt-get install libapache2-mod-php7.0 libphp7.0-mbstring php7.0-curl php7.0-zip php7.0-gd php7.0-mysql php7.0-mcrypt

```

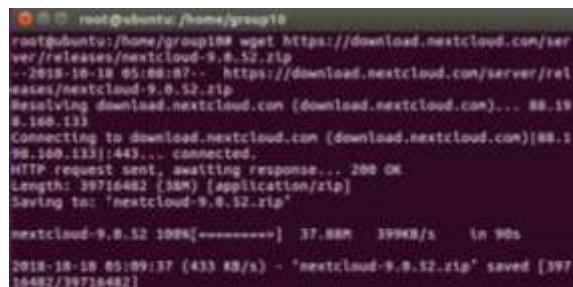
*Figure 5.2.29.5: Installation PHP Extension*

```

root@ubuntu:/home/group10#
root@ubuntu:/home/group10# apt-get install php-xml

```

*Figure 5.2.29.6: Installation another part of PHP Extension*



```
root@ubuntu:/home/group10# wget https://download.nextcloud.com/server/releases/nextcloud-9.0.52.zip
--2018-10-30 05:00:07-- https://download.nextcloud.com/server/releases/nextcloud-9.0.52.zip
Resolving download.nextcloud.com (download.nextcloud.com)... 88.19
8.160.133
Connecting to download.nextcloud.com (download.nextcloud.com):80...
88.190.133:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 39716482 (38M) [application/zip]
Saving to: 'nextcloud-9.0.52.zip'

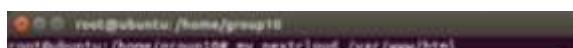
nextcloud-9.0.52 100%[=====] 37.88M 399KB/s   in 9s
2018-10-30 05:00:37 (433 KB/s) - "nextcloud-9.0.52.zip" saved [39716482/39716482]
```

Figure 5.2.29.7: Installation of NextCloud



```
root@ubuntu:/home/group10# ls
Desktop  examples.desktop  Pictures  Videos
Documents  Music  Public
Downloads  nextcloud-9.0.52.zip  Templates
root@ubuntu:/home/group10#
```

Figure 5.2.29.8: Unzip the package



```
root@ubuntu:/home/group10# ls
Desktop  examples.desktop  Pictures  Videos
Documents  Music  Public
Downloads  nextcloud-9.0.52.zip  Templates
root@ubuntu:/home/group10# unzip nextcloud-9.0.52.zip
```

Figure 5.2.29.9: Move the folder to destination folder



```
root@ubuntu:/home/group10# mv nextcloud /var/www/html
```

Figure 5.2.29.10: Edit the permission of the folder

```
root@ubuntu:/home/group10
root@ubuntu:/home/group10# mysql_secure_installation

Securing the MySQL server deployment.

Enter password for user root:

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

Press y|Y for Yes, any other key for No: n
Using existing password for root.
Change the password for root ? ((Press y|Y for Yes, any other key
for No) : n

... skipping.

By default, a MySQL installation has an anonymous user,
allowing anyone to log into MySQL without having to have
a user account created for them. This is intended only for
testing, and to make the installation go a bit smoother.
You should remove them before moving into a production
environment.

Remove anonymous users? (Press y|Y for Yes, any other key for No)
: y
Success.

Normally, root should only be allowed to connect from
'localhost'. This ensures that someone cannot guess at
the root password from the network.

Disallow root login remotely? (Press y|Y for Yes, any other key fo
r No) : y
Success.

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

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

- Removing privileges on test database...
Success.

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

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

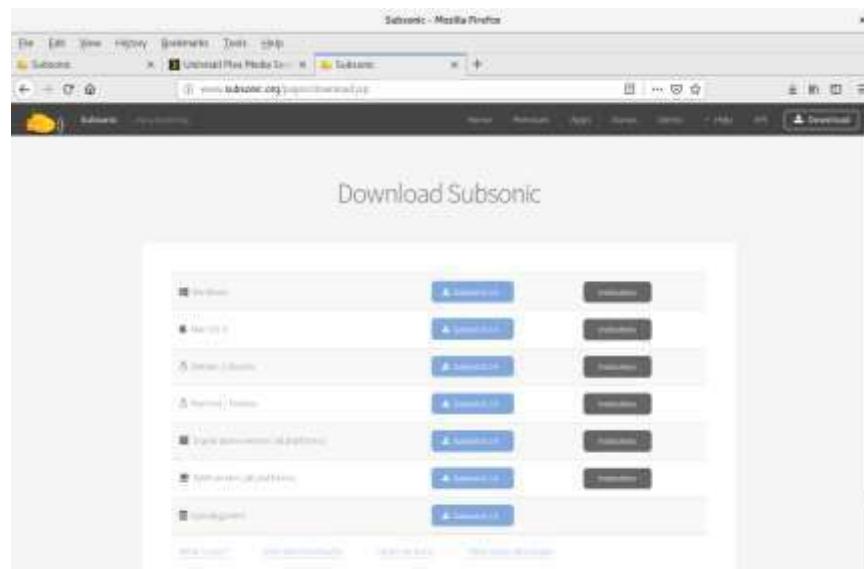
Figure 5.2.29.11: Configuring MariaDB for Nextcloud

### 5.2.30 Media Streaming Server (Subsonic)

Subsonic is a cross platform, free, open source web-based music/video streamer that can provide you with ubiquitous access to your entire music and video collection.

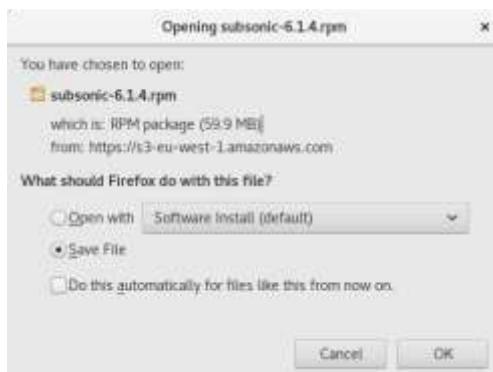
## Installing Subsonic

Step 1: Navigate to **Subsonic Download page** and download the setup installation files for **Fedora**.



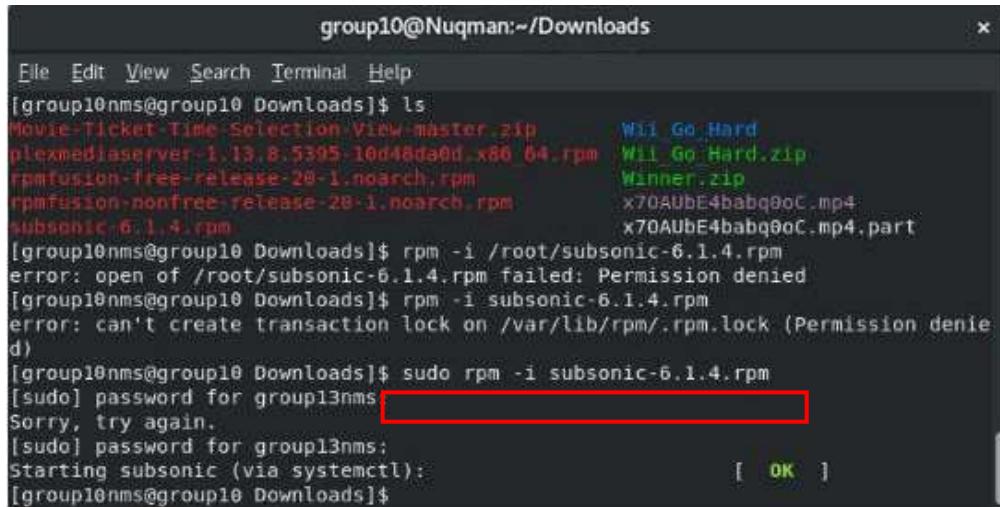
*Figure 5.2.30.1: Subsonic Downloads Page*

Step 2: Check the **Save File** and click **OK** to begin downloading the setup.



*Figure 5.2.30.2: Subsonic Download*

Step 3: Open terminal and type the command as shown in the figure below to start installing Subsonic in Fedora.



```
group10@Nuqman:~/Downloads
File Edit View Search Terminal Help
[group10nms@group10 Downloads]$ ls
Movie-Ticket-Time-Selection-View-master.zip      Will Go Hard
plexmediaserver-1.13.8.5395-10d48da0d.x86_64.rpm  Will Go Hard.zip
rpmfusion-free-release-28-1.noarch.rpm          Winner.zip
rpmfusion-nonfree-release-28-1.noarch.rpm        x70AUbE4babq9oC.mp4
subsonic-6.1.4.rpm                             x70AUbE4babq9oC.mp4.part
[group10nms@group10 Downloads]$ rpm -i /root/subsonic-6.1.4.rpm
error: open of /root/subsonic-6.1.4.rpm failed: Permission denied
[group10nms@group10 Downloads]$ rpm -i subsonic-6.1.4.rpm
error: can't create transaction lock on /var/lib/rpm/.rpm.lock (Permission denied)
[group10nms@group10 Downloads]$ sudo rpm -i subsonic-6.1.4.rpm
[sudo] password for group10nms
Sorry, try again.
[sudo] password for group10nms:
Starting subsonic (via systemctl):
[group10nms@group10 Downloads]$
```

*Figure 5.2.30.3: Subsonic Installation*

Step 4: Open Subsonic- by default Subsonic listens on port **4040**. After the installation, Subsonic should start automatically. Go to the following URL: <http://<your-ip-address>:4040>.

Where your-ip-address is the IP Address or hostname of the machine that it is installed on which result in <http://192.168.9.138:4040> . Login page will appear.



*Figure 5.2.30.4: Subsonic Web Page*

## **Chapter 6**

### **Testing Services**

## 6.1 Introduction

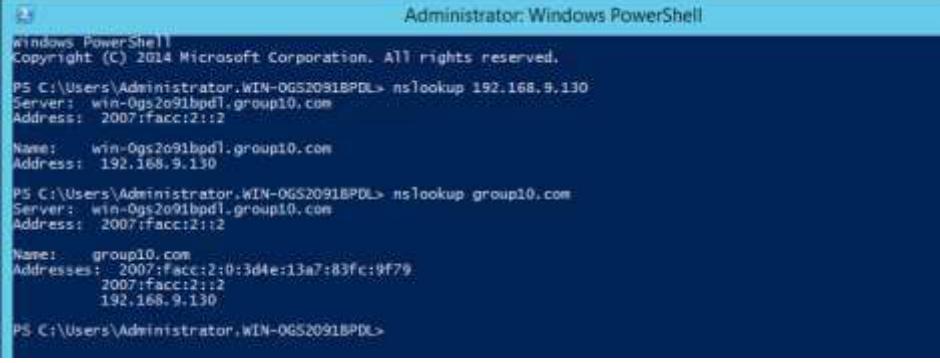
In this chapter will show how to use the service that had been setup and configured. The testing also is to ensure the functioning of the service are successfully up and running. Testing is the practice of making objective judgments regarding the extent to which the system (device) meets, exceeds or fails to meet stated objectives. Moreover, testing is about managing risk.

## 6.2 Service Testing

### 6.2.1 DNS (primary and secondary Servers)

#### 6.2.1.1 Primary DNS

Step 1: Open as administrator in Windows PowerShell, type “nslookup 192.168.9.130” and it will show the Domain name registered under ip address 192.168.9.130.



The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The command "nslookup 192.168.9.130" is run, and the output shows the domain name "group10.com" associated with the IP address "192.168.9.130". A second "nslookup group10.com" command is run, showing the same result. The PowerShell window has a dark blue background and white text.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.WIN-OGS2091BPD\> nslookup 192.168.9.130
Server: win-0gs2o91bpdl.group10.com
Address: 2007:facc:2::2

Name: win-0gs2o91bpdl.group10.com
Address: 192.168.9.130

PS C:\Users\Administrator.WIN-OGS2091BPD\> nslookup group10.com
Server: win-0gs2o91bpdl.group10.com
Address: 2007:facc:2::2

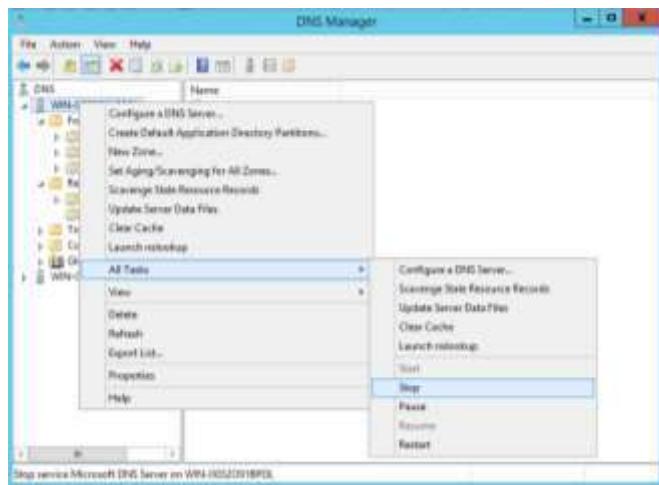
Name: group10.com
Addresses: 2007:facc:2::3d4e:13a7:83fc:9f79
          2007:facc:2::2
          192.168.9.130

PS C:\Users\Administrator.WIN-OGS2091BPD\>
```

Figure 6.2.1 nslookup 192.168.9.130

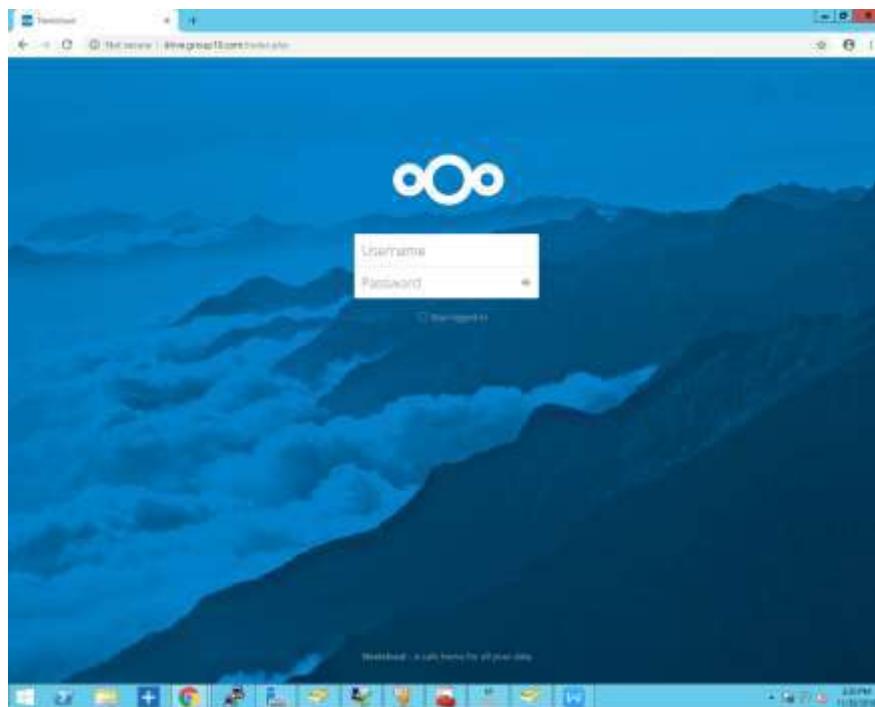
### 6.2.1.2 Secondary DNS

Step 1: Stop the DNS Service in Windows Server



*Figure 6.2.2: Stop DNS Service*

Step 2: Try to access any website registered host under DNS Service. If it's accessible, the Secondary DNS Transfer Zone is working well in Server Ubuntu.



*Figure 6.2.3: drive.group10.com is accessible*

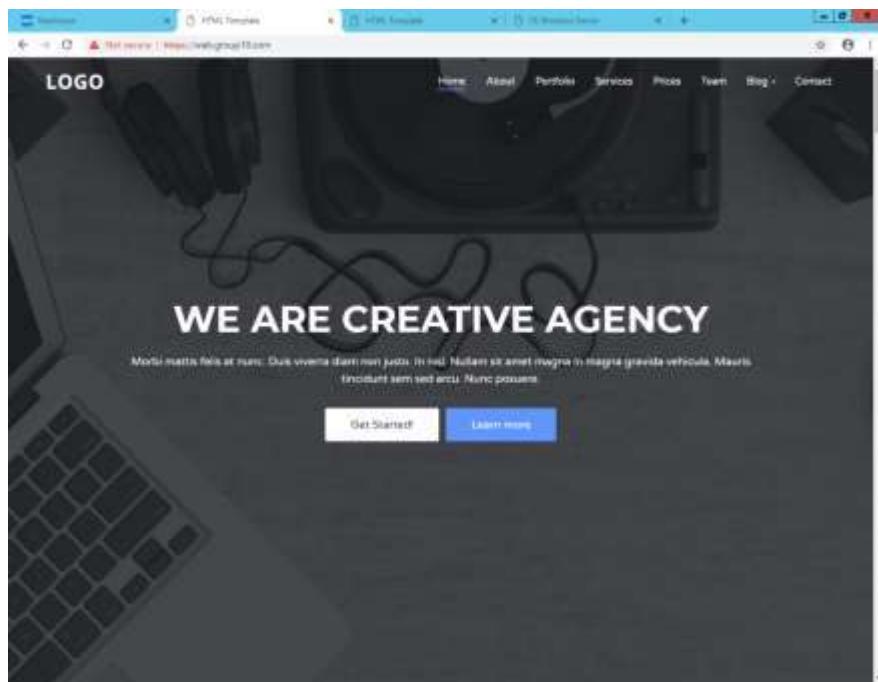


Figure 6.2.4: <https://web.group10.com> is accessible

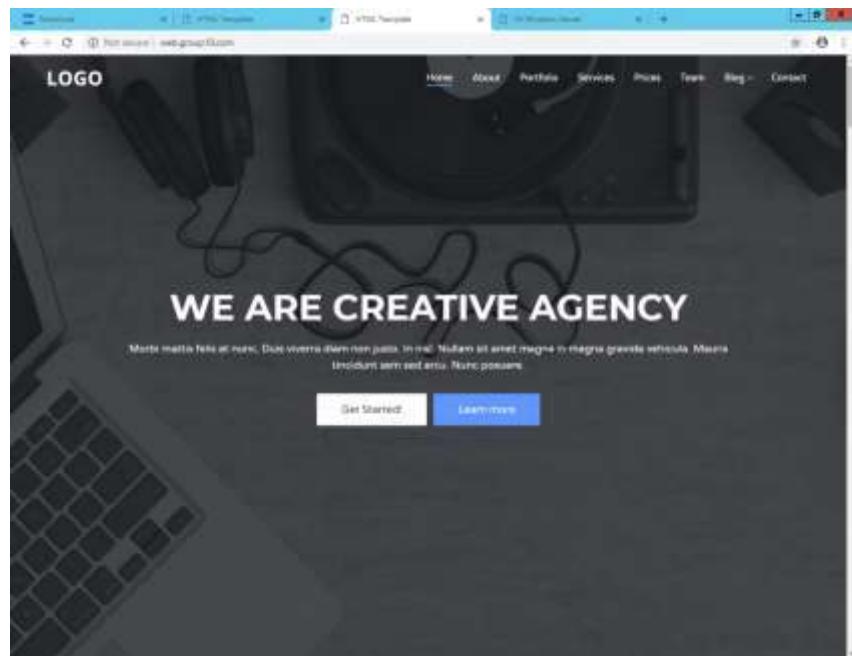


Figure 6.2.5: <http://web.group10.com> is accessible

## 6.2.2 Dynamic Host Configuration Protocol (DHCP) IPv4

1. Open the Command Prompt (CMD) and type ipconfig/all to see DHCP is enable

```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9601]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\administrator.VIN-0632091BPD\>ipconfig/all

Windows IP Configuration

Host Name . . . . . : VIN-0632091BPD
Primary Dns Suffix . . . . . : group0.com
Node Type . . . . . : Hybrid
Is Routing Enabled . . . . . : No
WINS Proxy Enabled . . . . . : No
DNS Suffix Search List . . . . . : group0.com

Ethernet adapter Ethernet 3:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : Check Point Virtual Network Adapter For I
    ndpoint UPN Client
    Physical Address . . . . . : 54-84-87-42-5C-11
    DHCP Enabled . . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes

Ethernet adapter Local Area Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . : TAP-Windows Adapter v9
    Description . . . . . : TAP-Windows Adapter v9
    Physical Address . . . . . : 00-FF-03-81-52-84
    DHCP Enabled . . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes

Ethernet adapter vEthernet (Intel(R) Ethernet Connection I217-LM - Virtual Switch 1):

    Connection-specific DNS Suffix . . . . . : Hyper-V Virtual Ethernet Adapter #2
    Description . . . . . : Hyper-V Virtual Ethernet Adapter #2
    Physical Address . . . . . : 64-80-6A-59-0A-FD
    DHCP Enabled . . . . . : No
    Autoconfiguration Enabled . . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::1d4e:13a7:83fc:9f79%16(PREFERRED)
    IPv4 Address . . . . . : 192.168.9.130(PREFERRED)
    Subnet Mask . . . . . : 255.255.255.248
    Default Gateway . . . . . : 192.168.9.127
```

Figure 6.2.6 show the DHCP is Enable in the CMD

2. Testing can also be done by creating a new wizard scope in the DHCP Manager

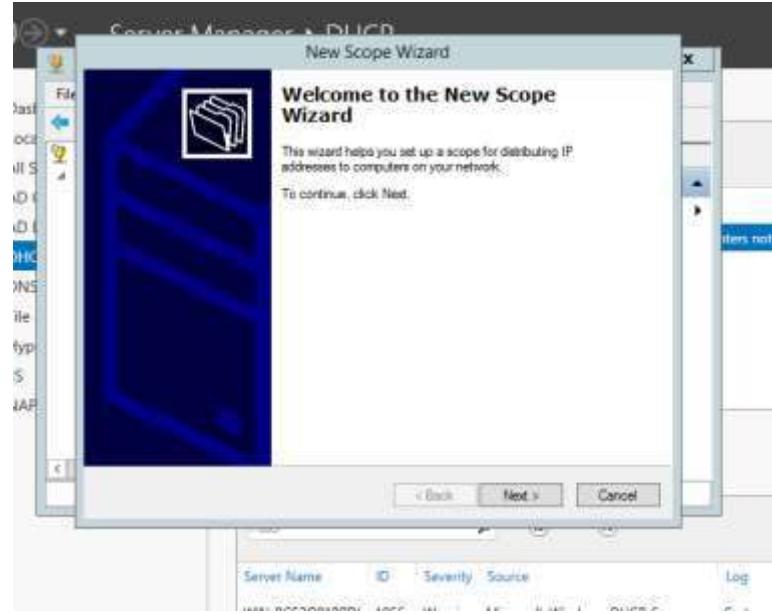


Figure 6.2.7 show create New Wizard Scope in the DHCP Manager

3. Enter the Name and Description for the new scope wizard

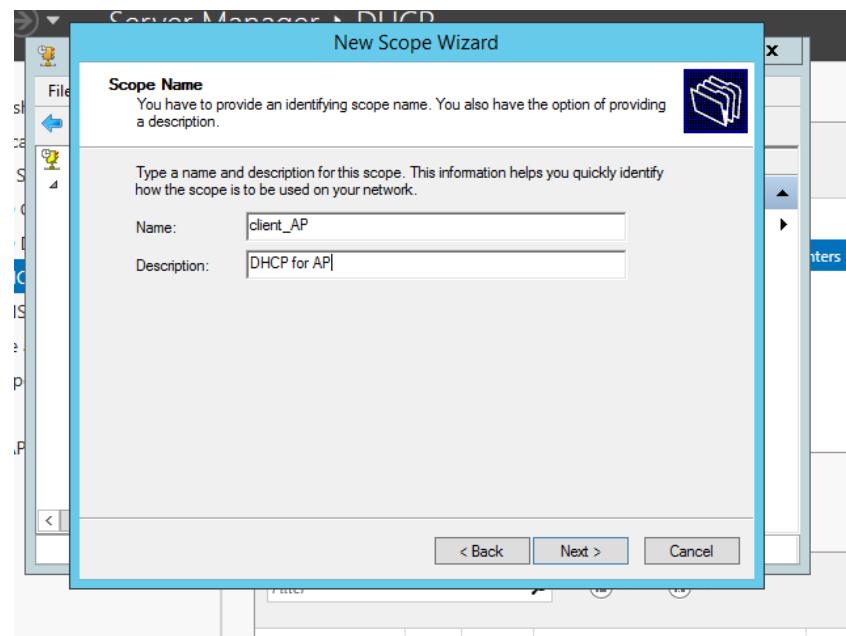


Figure 6.2.8 show Name and Description for the New Scope Wizard

#### 4. Configure the IP Address Range for DHCP Server

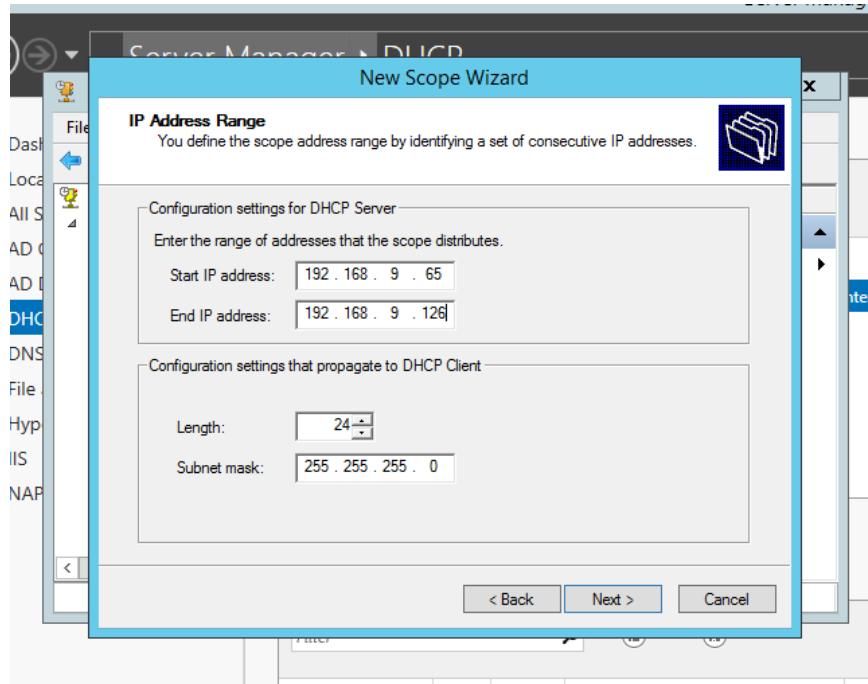


Figure 6.2.9 show the Configuration of IP Address Range

#### 5. Alert Message of the address range conflict with an existing scope showing the DHCP have been done

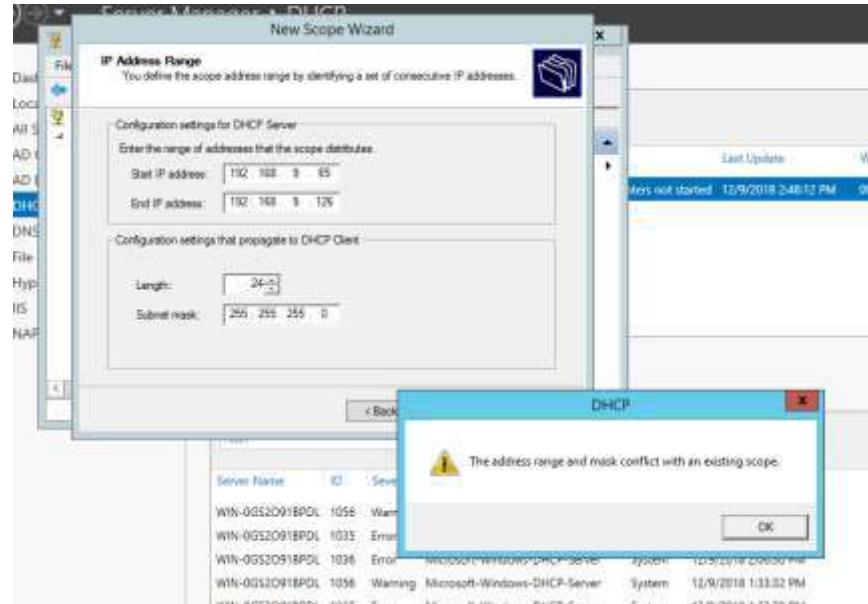


Figure 6.2.10 show the DHCP have been Set

### 6.2.3 Dynamic Host Configuration Protocol (DHCP) IPv6

Step 1: Open Dhcp server , click on address lease to see ipv6 address user for wireless

The screenshot shows the Windows DHCP Management console. The left pane displays a tree view of DHCP configurations for a specific scope. The right pane lists the current IPv6 address leases. There are four entries in the lease table:

Client IPv6 Address	Name	Lease Expiration	IAID	Type	Unique ID	Description
2007:fac:60:182...	SIDDIQ	12/21/2018 3:37:22 PM	49845447	IANA	000100012...	
2007:fac:60:5e7...	asus	12/19/2018 10:31:38 AM	190064414	IANA	000100012...	
2007:fac:60:62b...	LAPTOP-VISLC6TF	12/21/2018 5:12:59 PM	527753151	IANA	000100011...	
2007:fac:60:e71...	SIDDIQ	12/12/2018 7:58:03 PM	53894445	IANA	000100012...	

Figure 6.2.11: Wireless client using Ipv6.

Step 2: Open Dhcp server , click on address lease to see ipv6 address user for wired

The screenshot shows the Windows DHCP Management console. The left pane displays a tree view of DHCP configurations for a specific scope. The right pane lists the current IPv6 address leases. There is one entry in the lease table:

Client IPv6 Address	Name	Lease Expiration	IAID	Type	Unique ID	Description
2007:fac:c5:0:714...	UserHub-group10.c...	12/21/2018 4:20:19 PM	90439786	IANA	000100012...	

Figure 6.2.12: Wired Client using Ipv6.

#### 6.2.4 Ipv6 Web With Ipv6 Tunneling

Once the connection established between neighbour group, access their web IPv6, [www.group9ip6.com](http://www.group9ip6.com) from once of our servers or client.



Figure 6.2.13 Homepage of neighbouring ipv6

## 6.2.5 Secured FTP

**Step 1:** test using cmd at client

```
group10@group10-Virtual-Machine:~$ sftp fana@192.168.9.131
fana@192.168.9.131's password:
Connected to 192.168.9.131.
sftp> ls
fana      group10    nukeman
sftp>
```

Figure 6.2.14 test cmd at client

**Step 2:** test using sftp at client FileZilla

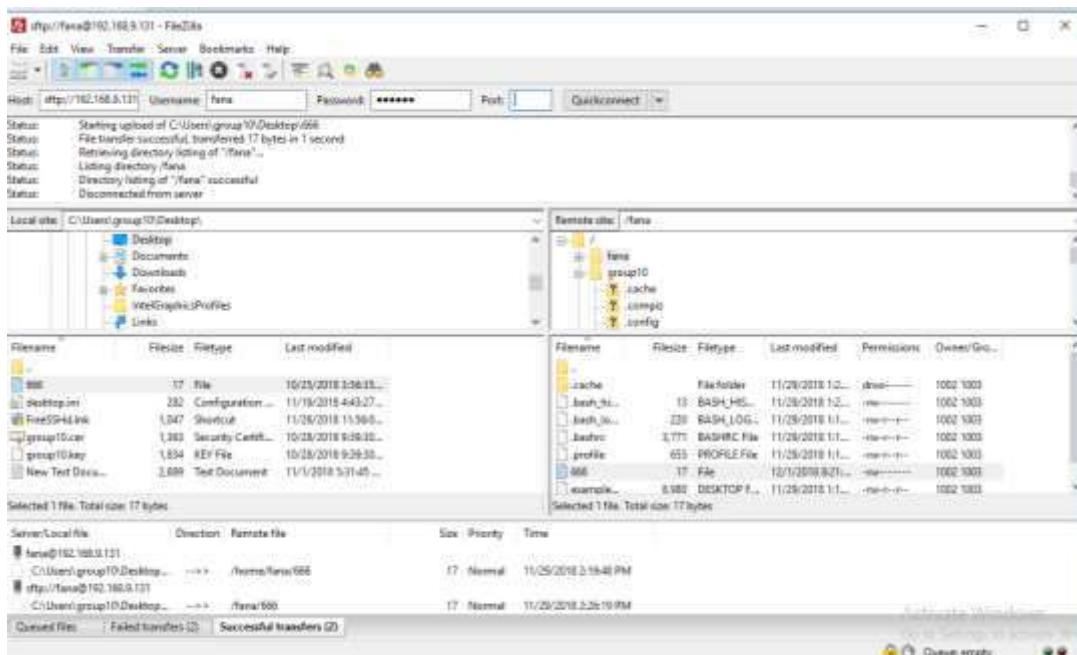
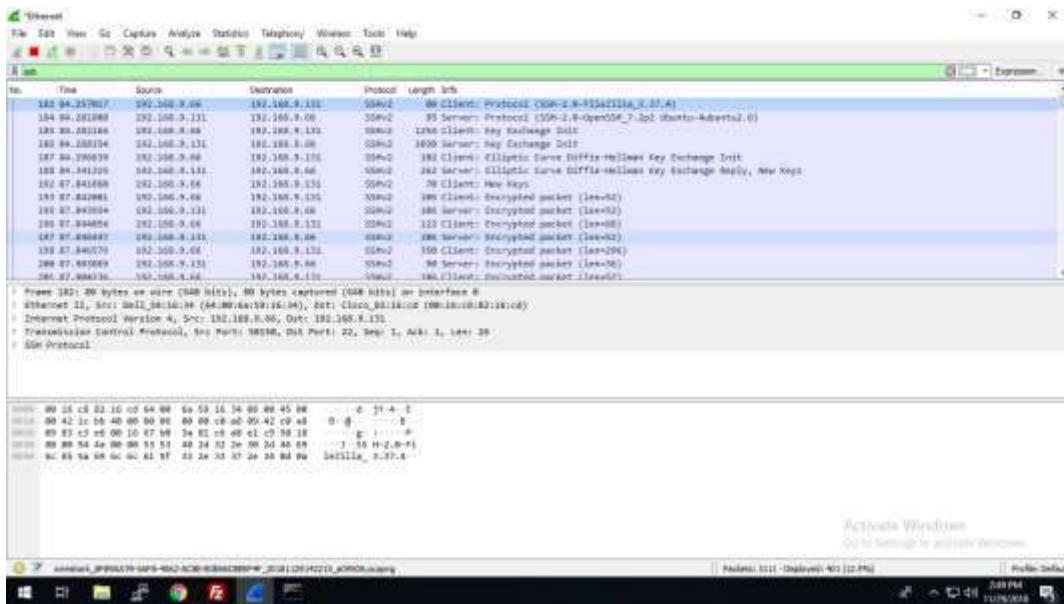


Figure 6.2.15 test using FileZilla

### Step 3: Using wireshark to monitoring.



*Figure 6.2.16 Wireshark monitoring*

## 6.2.6 Routing & Network Address Translation (NAT)

Step 1: Test the connection by ping public ip neighbor using command  
“ping <neighbor ip\_address>”

```
C:\Users\group10>ping 200.200.208.8

Pinging 200.200.208.8 with 32 bytes of data:
Reply from 200.200.208.8: bytes=32 time=2ms TTL=254
Reply from 200.200.208.8: bytes=32 time=1ms TTL=254
Reply from 200.200.208.8: bytes=32 time=1ms TTL=254
Reply from 200.200.208.8: bytes=32 time=1ms TTL=254

Ping statistics for 200.200.208.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\group10>ping 200.200.208.9

Pinging 200.200.208.9 with 32 bytes of data:
Reply from 200.200.208.9: bytes=32 time=1ms TTL=126

Ping statistics for 200.200.208.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Figure 6.2.17 Ping public ip address neighbor from Router.

Step 2 : Show mapping inside global/local and outside global/local by using command “show ip nat translation”.

Pro	Inside global	Inside local	Outside local	Outside global
tcp	200.200.208.4:33970	192.168.9.138:33970	200.200.208.10:80	200.200.208.10:80
tcp	200.200.208.4:35312	192.168.9.138:35312	200.200.208.10:80	200.200.208.10:80
tcp	200.200.208.4:35314	192.168.9.138:35314	200.200.208.10:80	200.200.208.10:80
tcp	200.200.208.4:52722	192.168.9.138:52722	200.200.208.9:80	200.200.208.9:80
tcp	200.200.208.4:52726	192.168.9.138:52726	200.200.208.9:80	200.200.208.9:80
tcp	200.200.208.4:52732	192.168.9.138:52732	200.200.208.9:80	200.200.208.9:80
tcp	200.200.208.4:52734	192.168.9.138:52734	200.200.208.9:80	200.200.208.9:80
tcp	200.200.208.4:52738	192.168.9.138:52738	200.200.208.9:80	200.200.208.9:80
tcp	200.200.208.4:52740	192.168.9.138:52740	200.200.208.9:80	200.200.208.9:80
tcp	200.200.208.4:52742	192.168.9.138:52742	200.200.208.9:80	200.200.208.9:80
tcp	200.200.208.4:52834	192.168.9.138:52834	200.200.208.9:80	200.200.208.9:80
tcp	200.200.208.4:54956	192.168.9.138:54956	200.200.208.10:8980	200.200.208.10:8980

Figure 6.2.18 NAT mapping table.

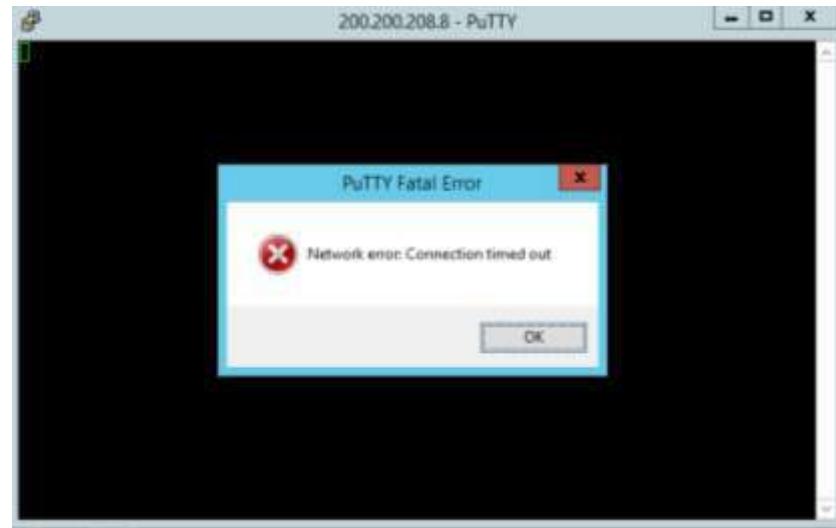
Step 3: Test connection by accessing neighbor services.



*Figure 6.2.19 NAT neighbor services*

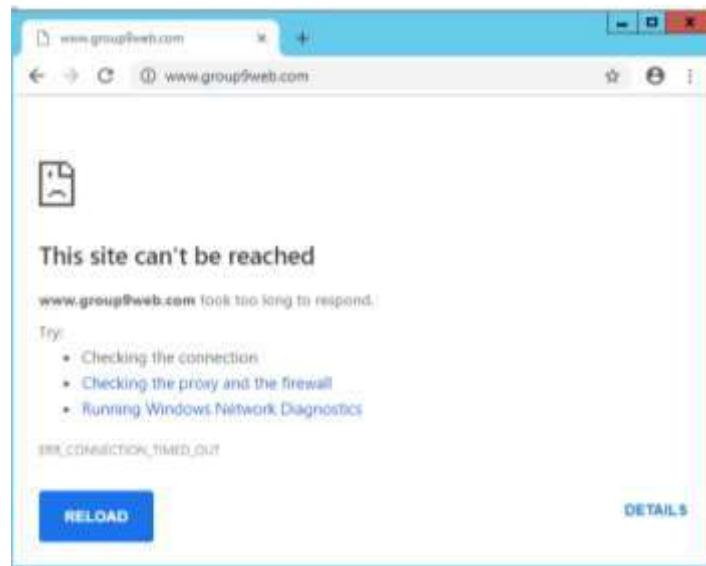
### 6.2.7 Access Control List (ACL)

Step 1: Access to SSH neighbour router is blocked.



*Figure 6.2.20 SSH blocked*

Step 2: Access to neighbour web server is blocked.



*Figure 6.2.21 Web blocked*

## 6.2.8 Samba

### 6.2.8.1 Testing Samba on Fedora

1. Configure `ls /home` on the Fedora Terminal and restart the samba services by configure `/sbin/service smb restart`

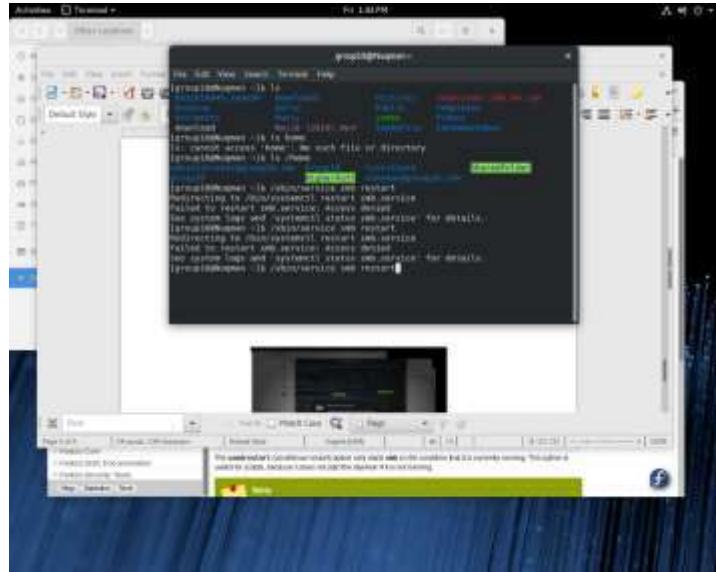


Figure 6.2.22 show directory files for Samba and Restart Samba

2. Authentication Required to start the samba services by entering the password

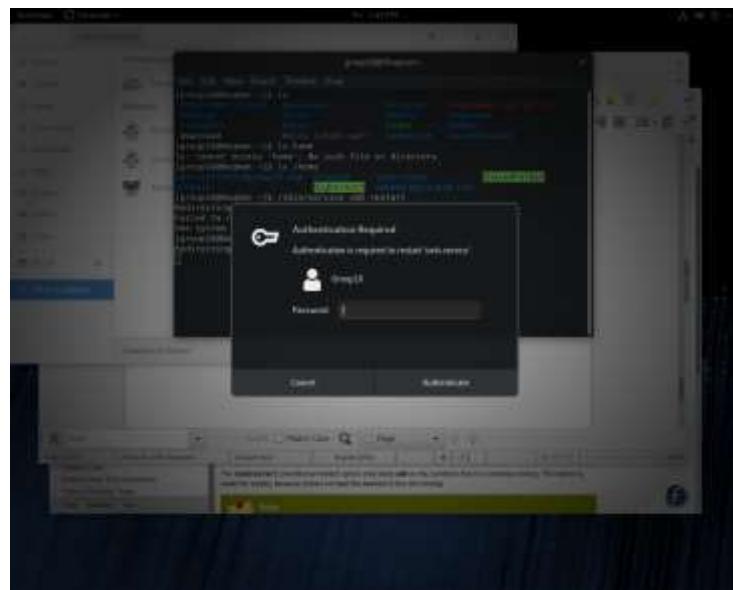
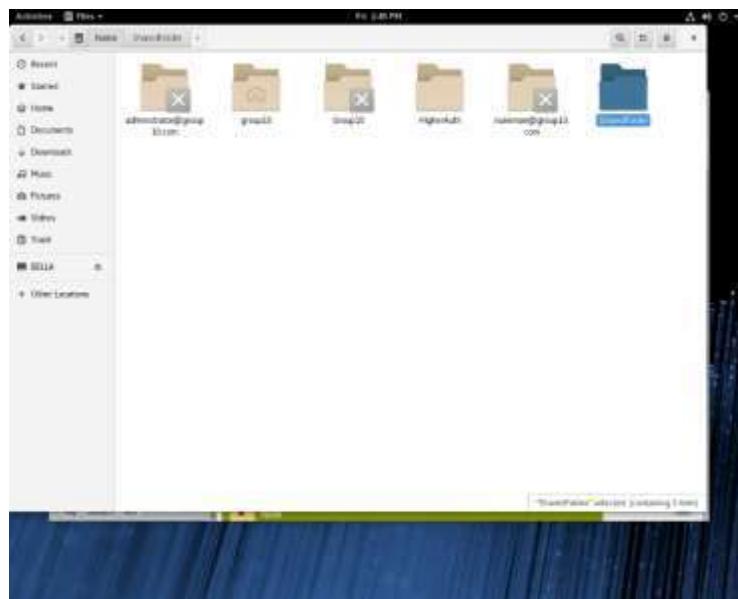


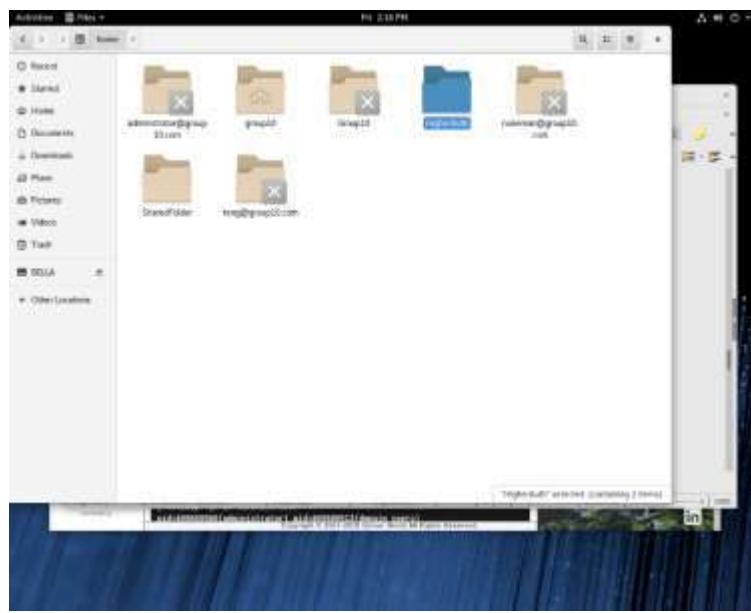
Figure 6.2.23 authentication restarting samba

### 3. Location of the Shared Folders – Other Locations\Computer\Home\SharedFolder



**Figure 6.2.24 show the Locations of the Shared Folders**

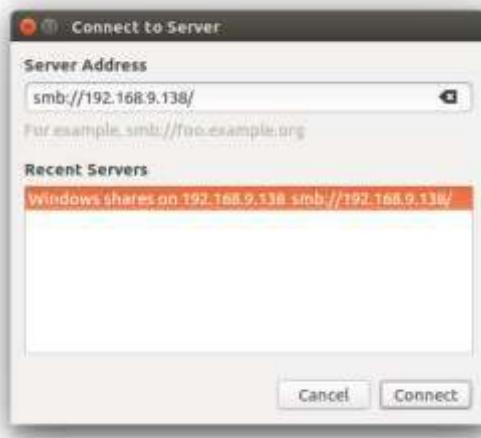
### 4. Location of the HigherAuth – Other Locations\Computer\Home\HigherAuth



**Figure 6.2.25 show the Locations of the HighAuth Folder**

### 6.2.8.2 Testing Samba on Ubuntu

1. Connect to Server in the Ubuntu

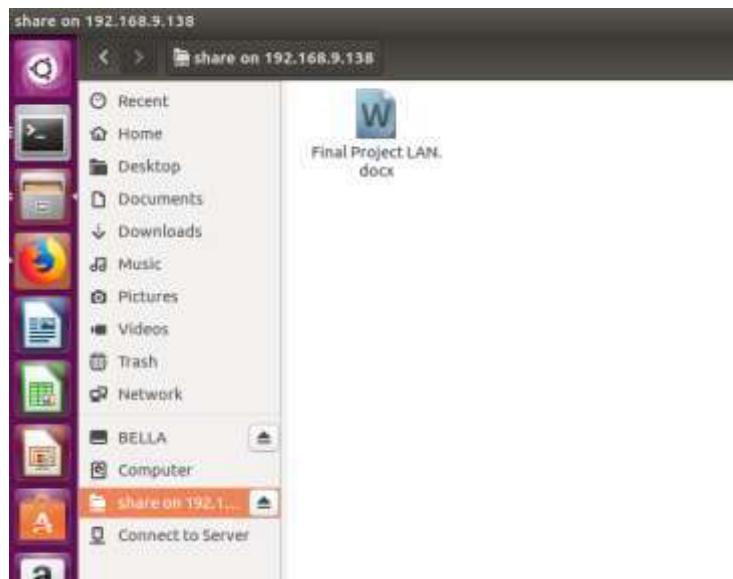


*Figure 6.2.26 show Connection to Server in Ubuntu*

2. Folder and file shared in the Fedora can be seen in the Ubuntu



*Figure 6.2.27 show the Folder in the Ubuntu*

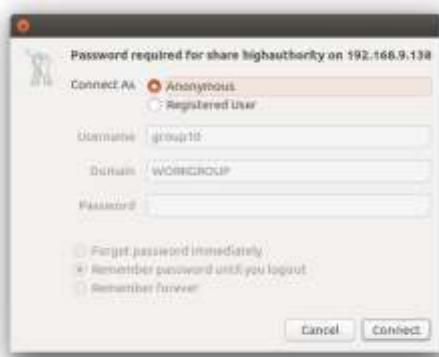


**Figure 6.2.28 show the file in the Shared Folder**

3. The HigherAuth cannot be Open in the Ubuntu as it does not have permission



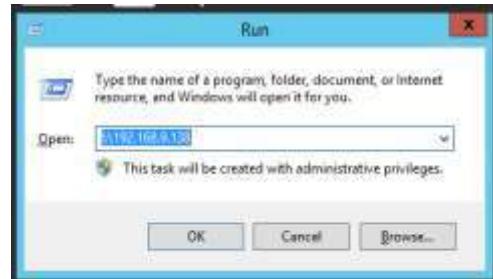
**Figure 6.2.29 show Folder Fail to Open**



**Figure 6.2.30 Password Required to Open Folder**

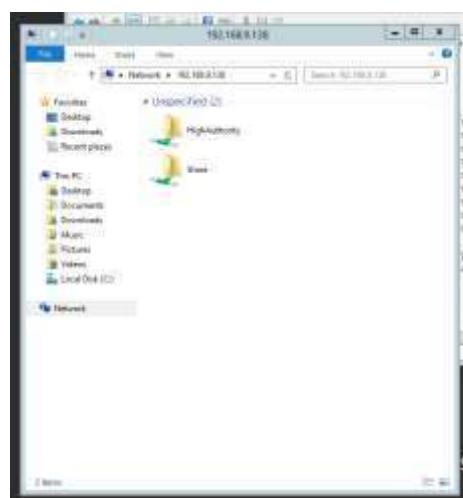
### 6.2.8.3 Testing Samba on Windows Server

1. Type the Fedora IP Address on Windows Server



**Figure 6.2. 31 show the IP Address for Windows to Open**

2. Folder shared by Fedora can be seen in the Windows Server



**Figure 6.2.32 show the Folder in the Windows Server**

3. Both Folder Shared in the Fedora can be access by Windows

## Server

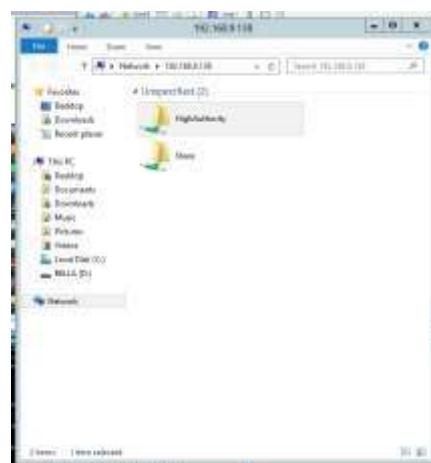


Figure 6.2.33 show Folder of HighAuthority

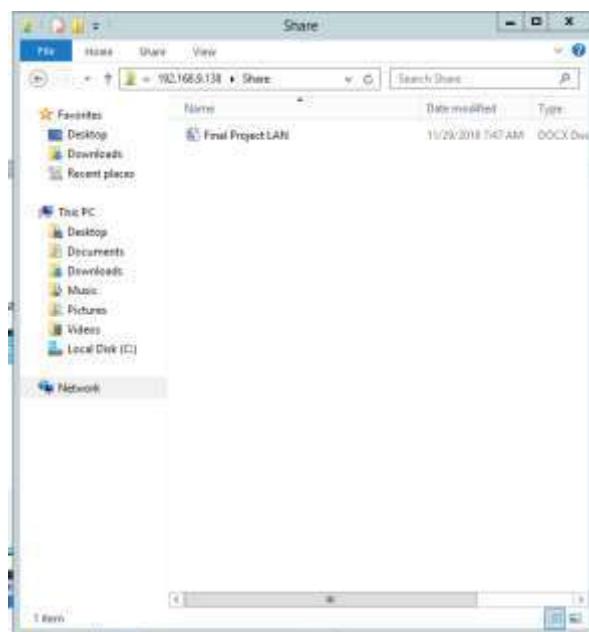
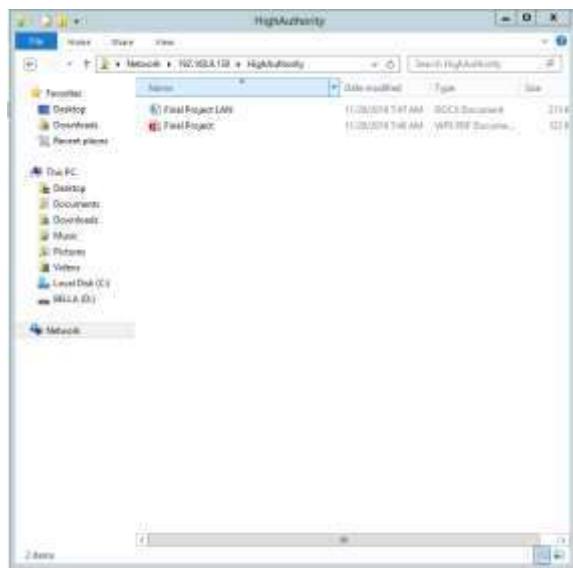


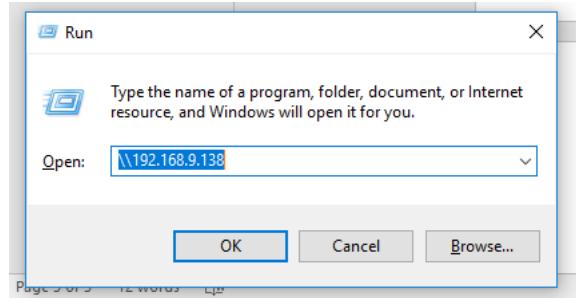
Figure 6.2.34 show File inside the Share Folder



*Figure 6.2.35 show File inside the HighAuthority Folder*

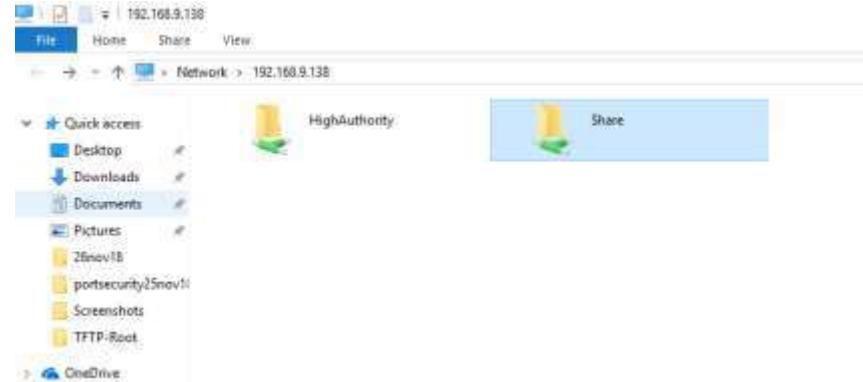
#### 6.2.8.4 Testing Samba on Window Client

1. Type Fedora IP Address on the Windows Client



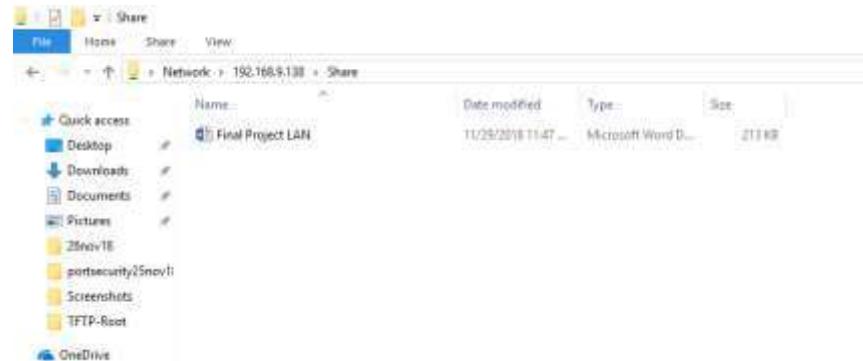
**Figure 6.2.36 show the IP Address for the Windows to Open**

2. Both Folder shared in the Fedora can be seen in the Windows Client



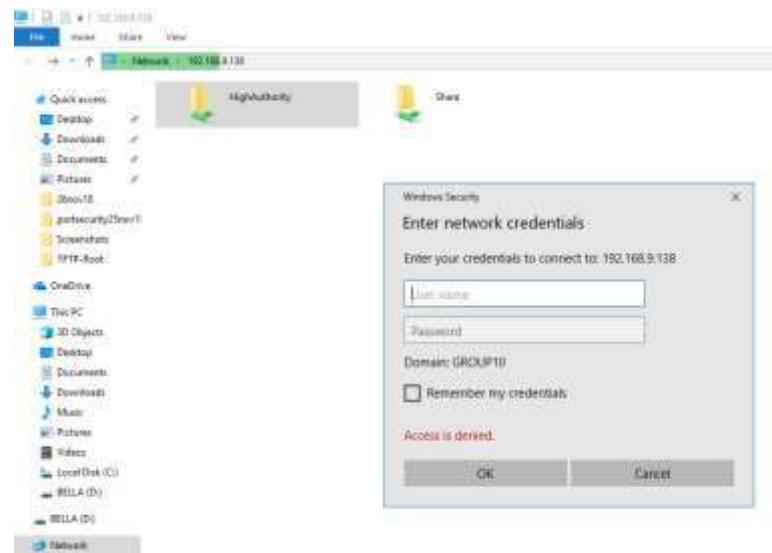
**Figure 6.2.37 show Folder in the Windows Client**

3. File in the Share Folder can be access by Windows Client



**Figure 6.2.38 show the File can be seen in the Share Folder**

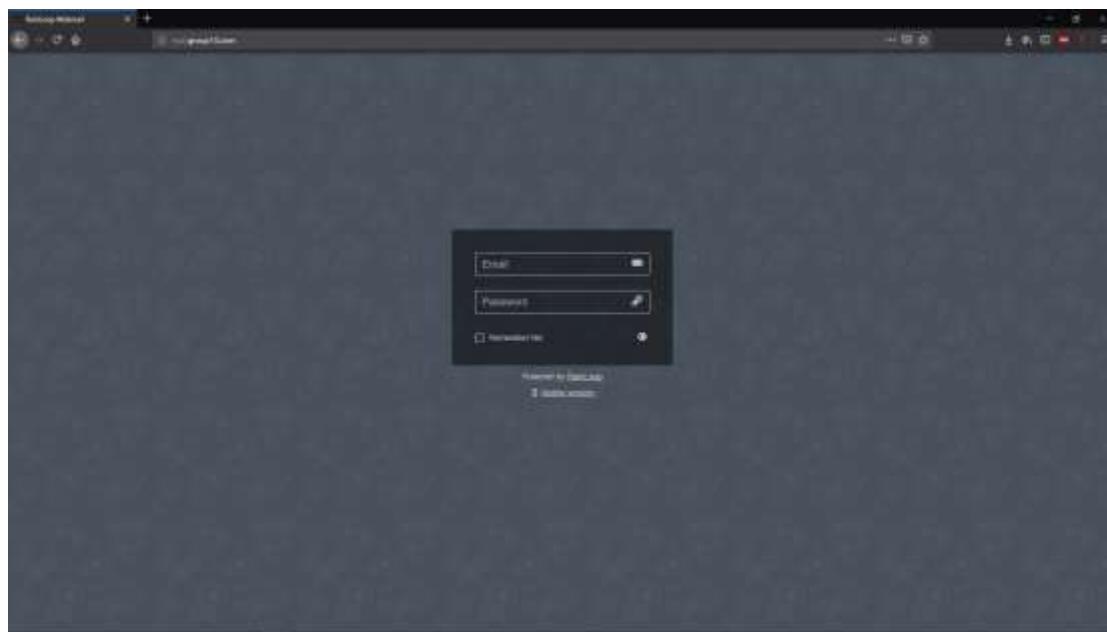
#### 4. Folder HighAuthority cannot be accessed by Windows Client



*Figure 6.2.39 show that Folder HighAuthority cannot be accessed*

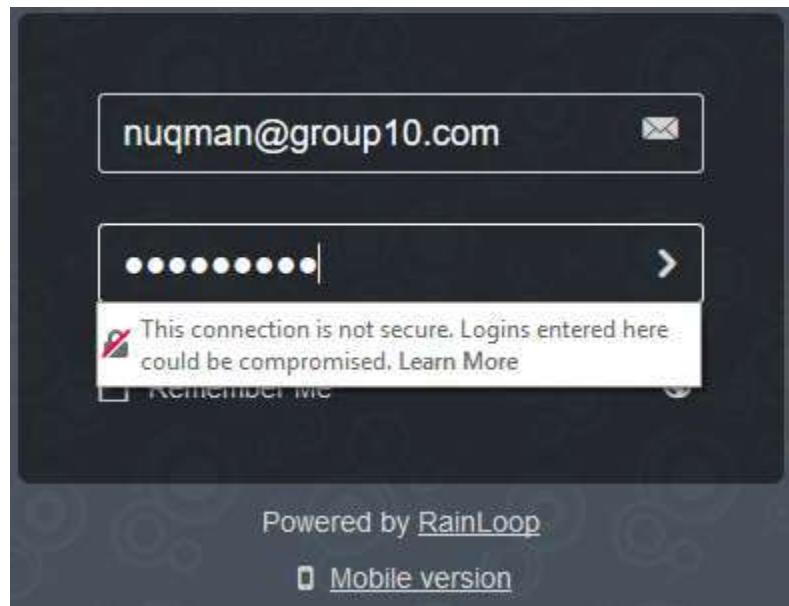
#### 6.2.9 Linux Email Server

Step 1: Open Mail Browser [mail.group10.com](http://mail.group10.com).

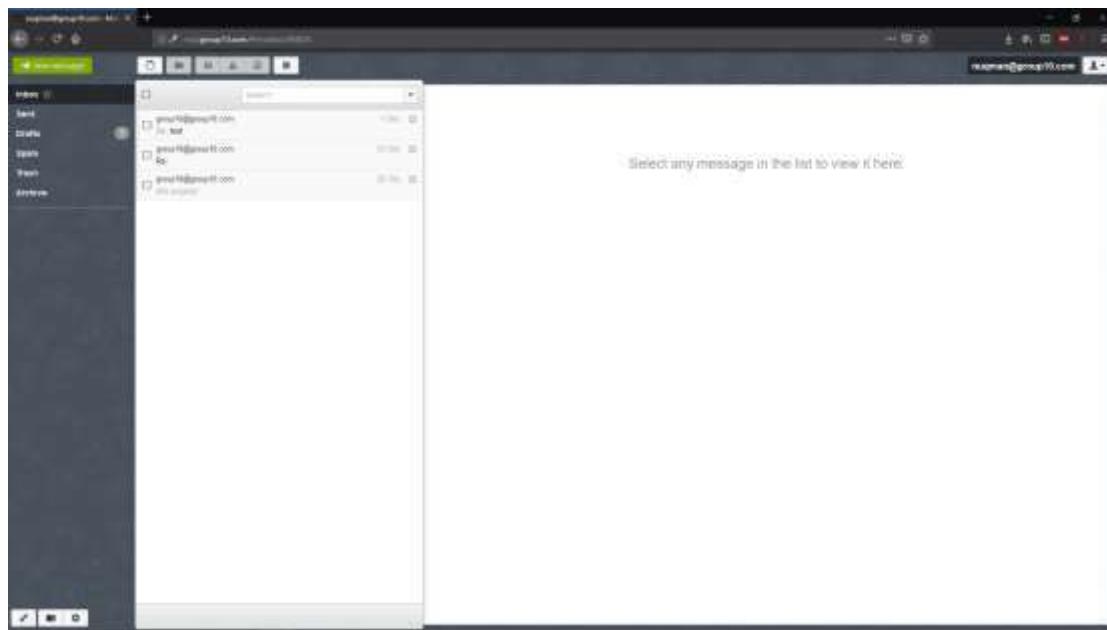


*Figure 6.2.40: Linux Mail interface*

Step 2: Login as user.

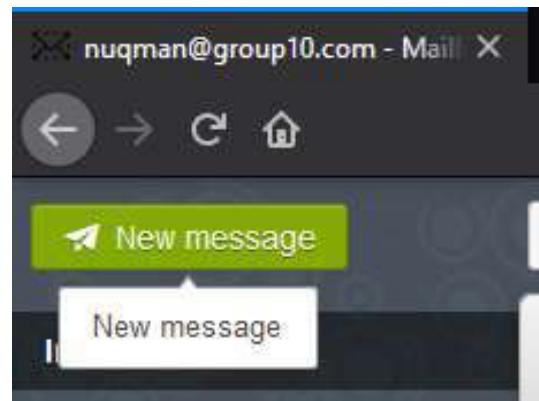


*Figure 6.2.41: Login Interface.*

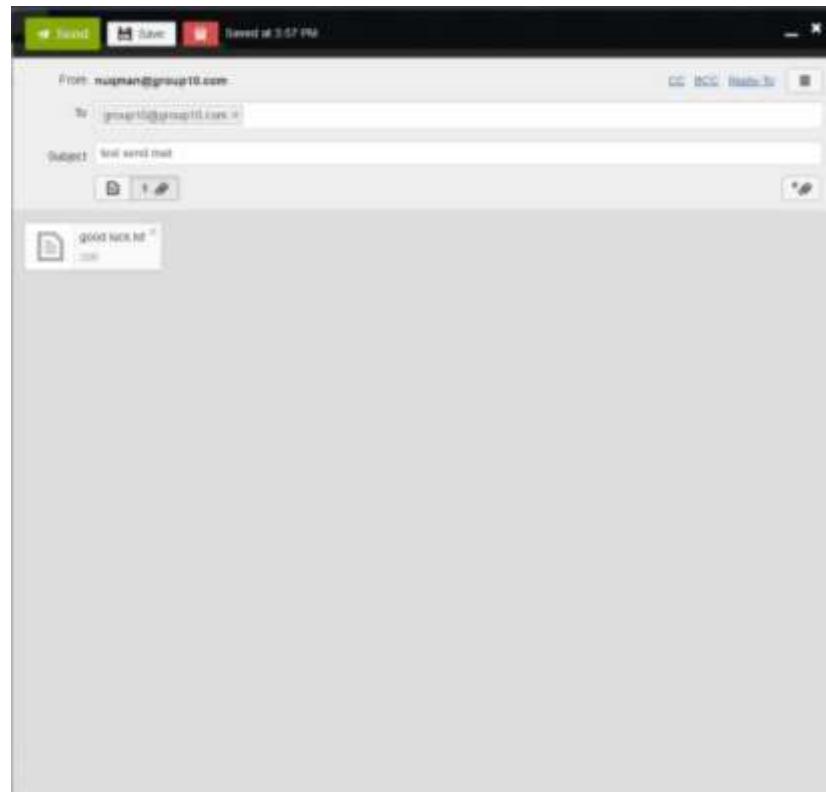


*Figure 6.2.42: User Interface*

Step 3: Test Send an email to another user.



*Figure 6.2.43: Create new message*



*Figure 6.2.44: Compose mail to other user [group10@group10.com](mailto:group10@group10.com) by pressing send button*



Figure 6.2.45: check your sent inbox to make sure message is sent.

Step 4 : Check sent mail from other user.

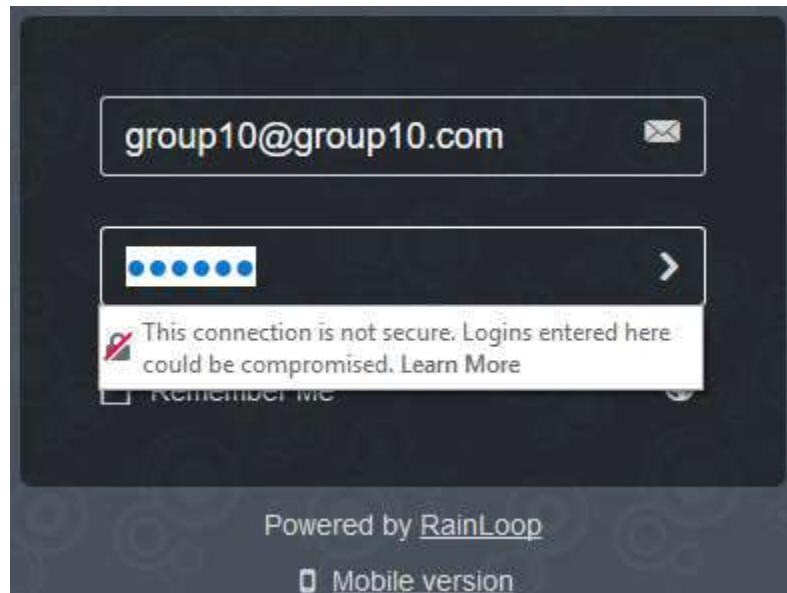


Figure 6.2.46: Login other user



Figure 6.2.47: check inbox

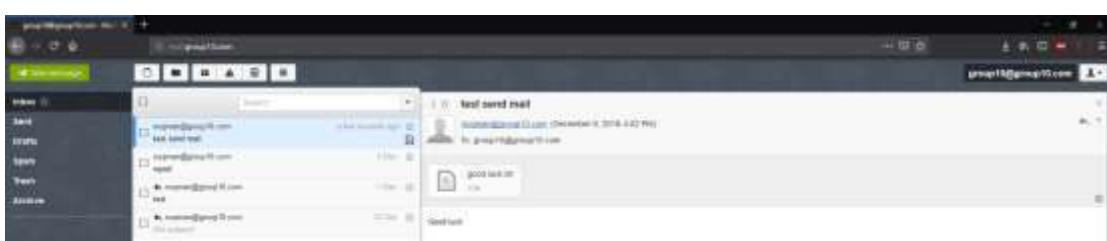


Figure 6.2.48: message/attachment was sent.

### 6.2.10 Proxy Server

Testing Proxy Server on client windows.

Step 1: Open your Internet browser setting on top right corner of screen.

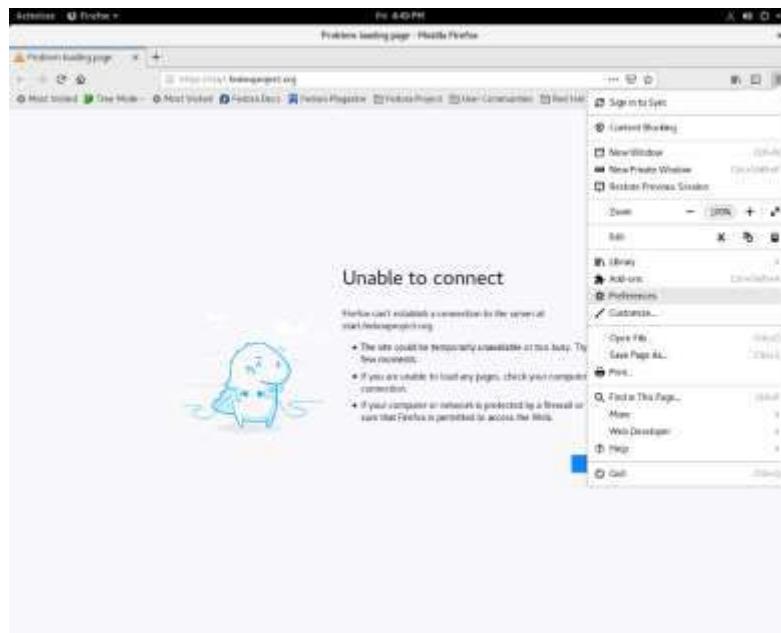
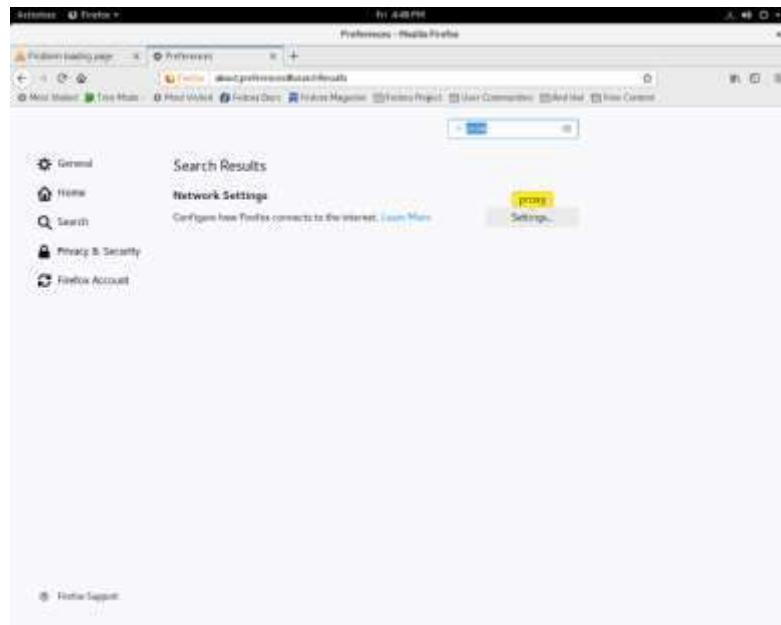


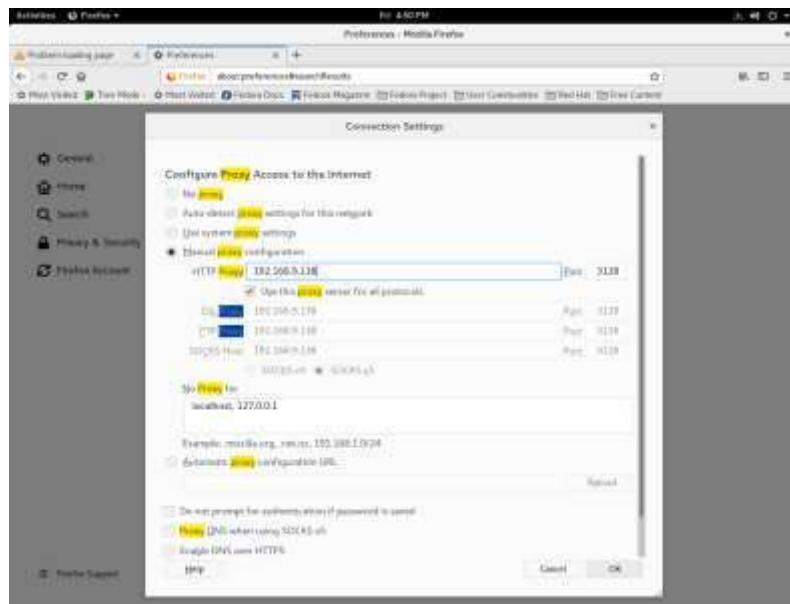
Figure 6.2.49: Internet Browser setting

Step 2: Set up your proxy setting in network setting.

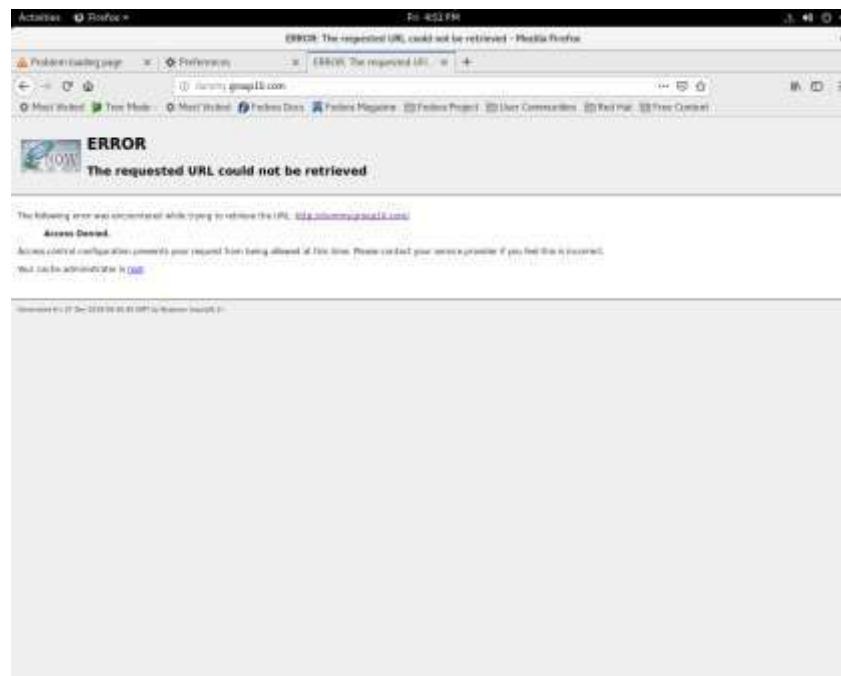


**Figure 6.2.50: Proxy Setting.**

Step 3: Set your proxy into manual, then add the proxy server ip address with same port in “/etc/squid/squid.conf”. Use this proxy server for all protocols.



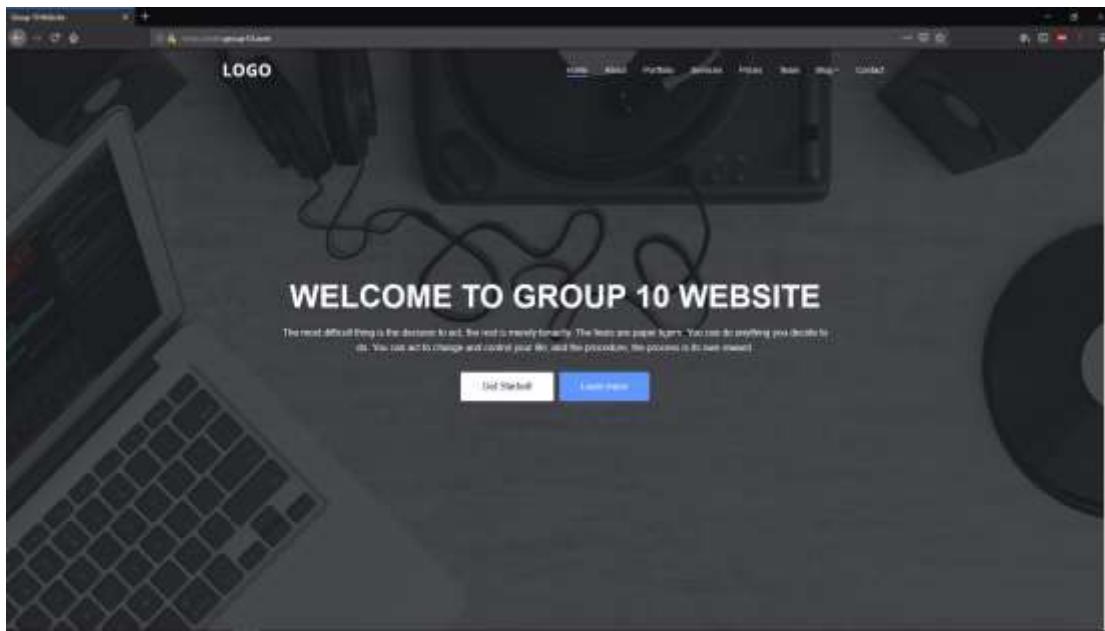
**Figure 6.2.51: Proxy Menu setup.**



**Figure 6.2.52: dummy.group10.com had been blocked by proxy.**

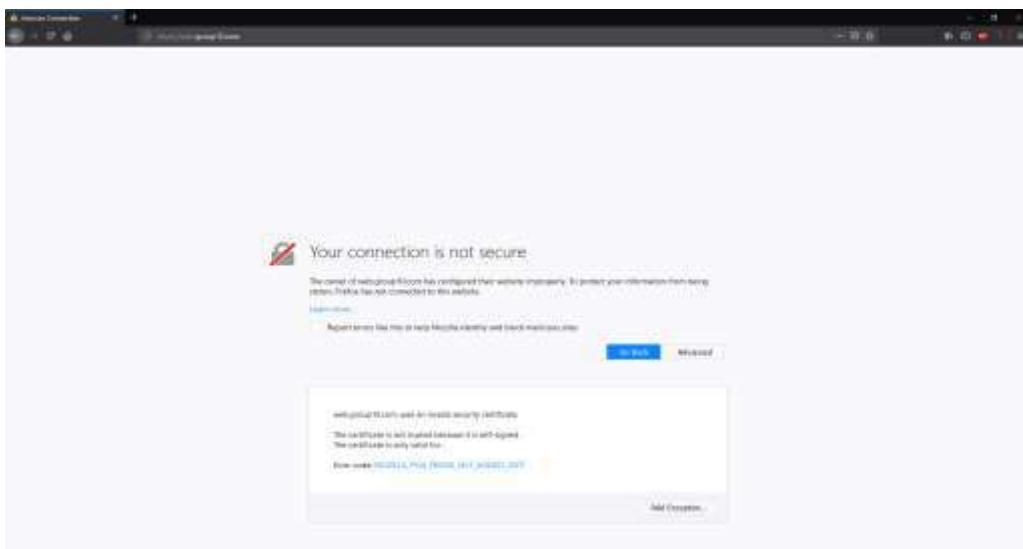
### 6.2.11 Web, SSL & Virtual Hosting

Step 1: For WEB, open up browser and type [web.group10.com](http://web.group10.com)



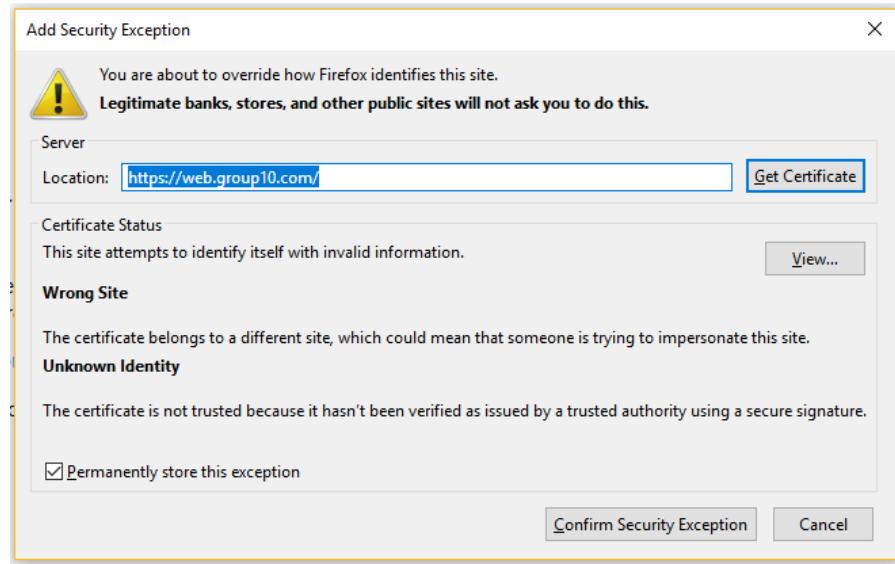
*Figure 6.2.53 It shows the Website has been added successfully*

Step 2: For SSL, go to browser and type <https://web.group10.com> and hit the ENTER. Click on “Advanced”, then click “Add Exception” to enter the website

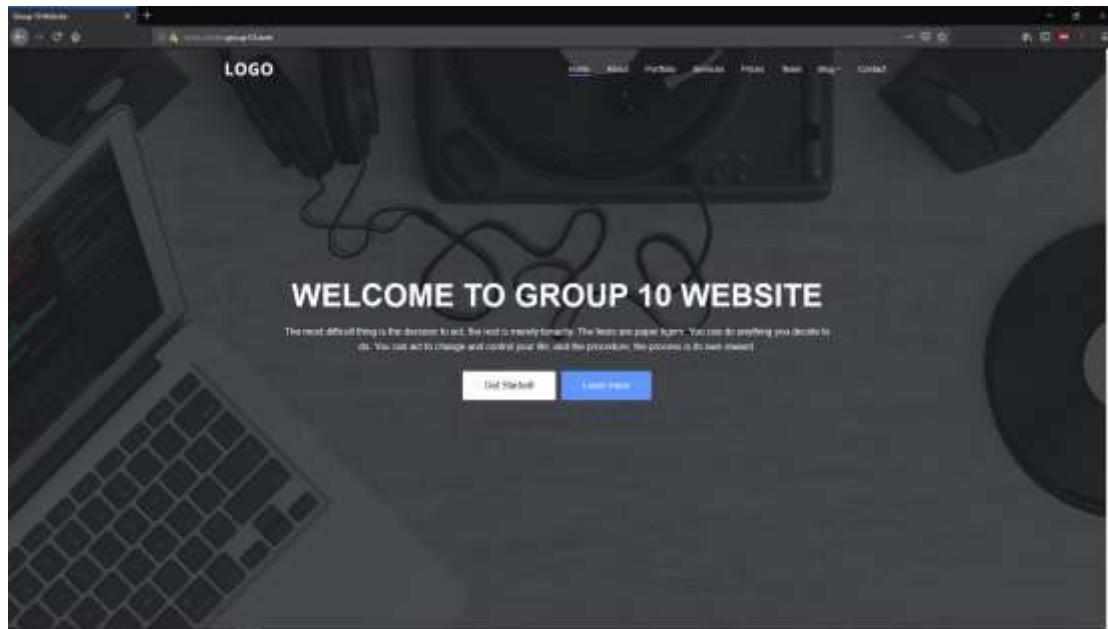


*Figure 6.2.54: Showing the Web is already secured*

### Step 3: Confirm Security Exception



*Figure 6.2.54: Security Exception.*



*Figure 6.2.55: Show the Website.*

Step 4: For Virtual Hosting, open up browser and type [webvirtual.group10.com](http://webvirtual.group10.com).



*Figure 6.2.56: It shows the Website has been added successfully*

### 6.2.12 Server Virtualization

Test open the Ubuntu in your Server Virtualization (Hyper-V).

Step 1: Ubuntu Virtual Machine has been installed

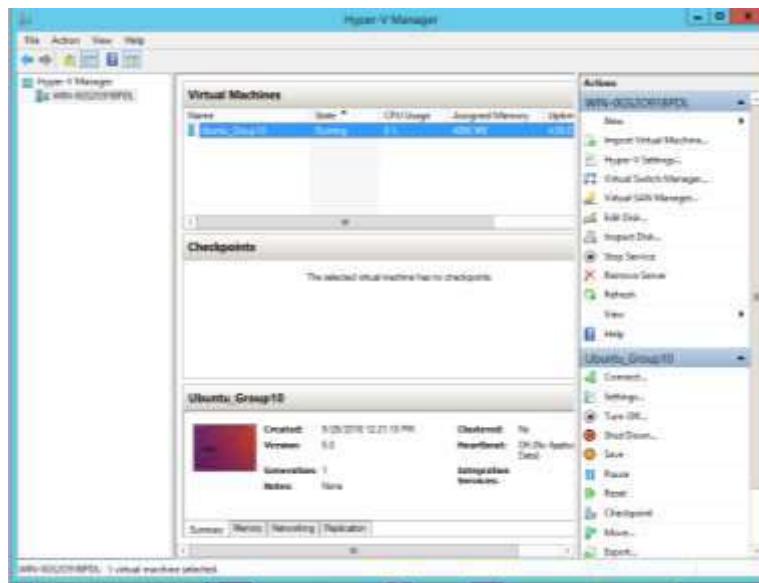


Figure 6.2.57: Hyper-V Manager

Step 2: Ubuntu being installed

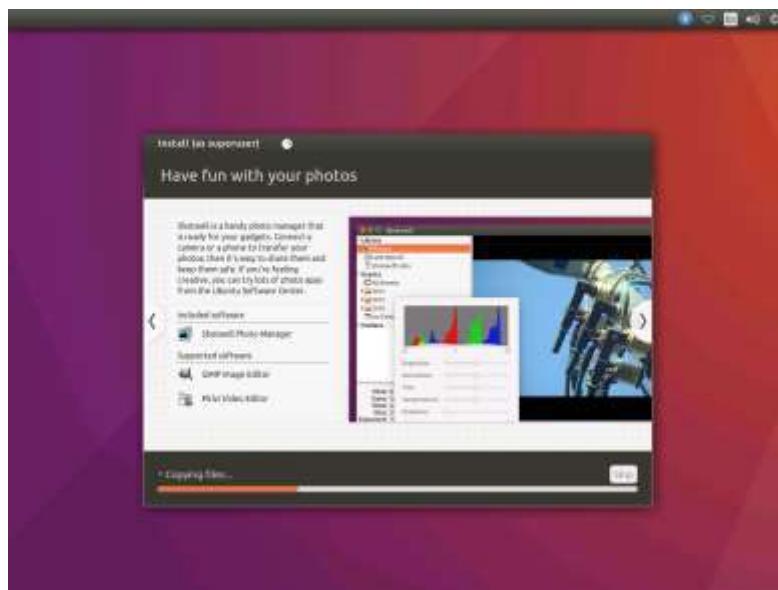
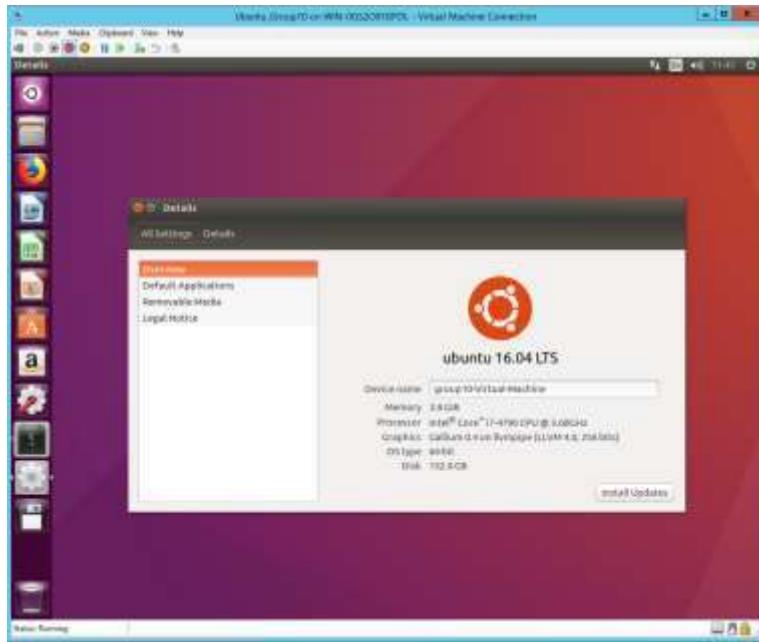


Figure 6.2.58: Installing Ubuntu

Step 3: Ubuntu finished installed



*Figure 6.2.58: Ubuntu is running*

### 6.2.13 Wireless Radius Server

#### WEP

WEP stands for Wired Equivalent Privacy (or Wireless Encryption Protocol). WEP is the most widely used protocol. It's also the default for most routers out there. It started with 64 bit encryption, then went to 128 bit. WEP is common and easy to crack. All you need is some free software.

The original encryption protocol developed for wireless networks. As its name implies, WEP was designed to provide the same level of security as wired networks. However, WEP has many well-known security flaws, is difficult to configure, and is easily broken.

## **WPA**

WPA stands for Wireless Protected Access is what replaced WEP. It was an upgrade to WEP, designed as a firmware upgrade for current devices. Because of this it depended on a lot of old technology. Most current WPA implementations use a pre-shared key (PSK), commonly referred to as WPA Personal, and the Temporal Key Integrity Protocol (TKIP, pronounced tee-kip) for encryption. WPA Enterprise uses an authentication server to generate keys or certificates. All in all, WPA is better than WEP.

## **WPA2**

WPA2 is the second version of the WPA standard. Based on the 802.11i wireless security standard, the most significant enhancement to WPA2 over WPA is the use of the Advanced Encryption Standard (AES) for encryption. The security provided by AES is sufficient (and approved) for use by the U.S. government to encrypt information classified as top secret.

## **PEAP - Protected Extensible Authentication Protocol**

PEAP does not typically use client certificates, nor does it directly use any CA certificates in establishing a TLS connection. However it certainly requires the use of a server certificate (PEAP is a TLS tunneled EAP protocol).

## WIRELESS AUTHENTICATION USING RADIUS

Step 1: Create a new group which is Wireless.

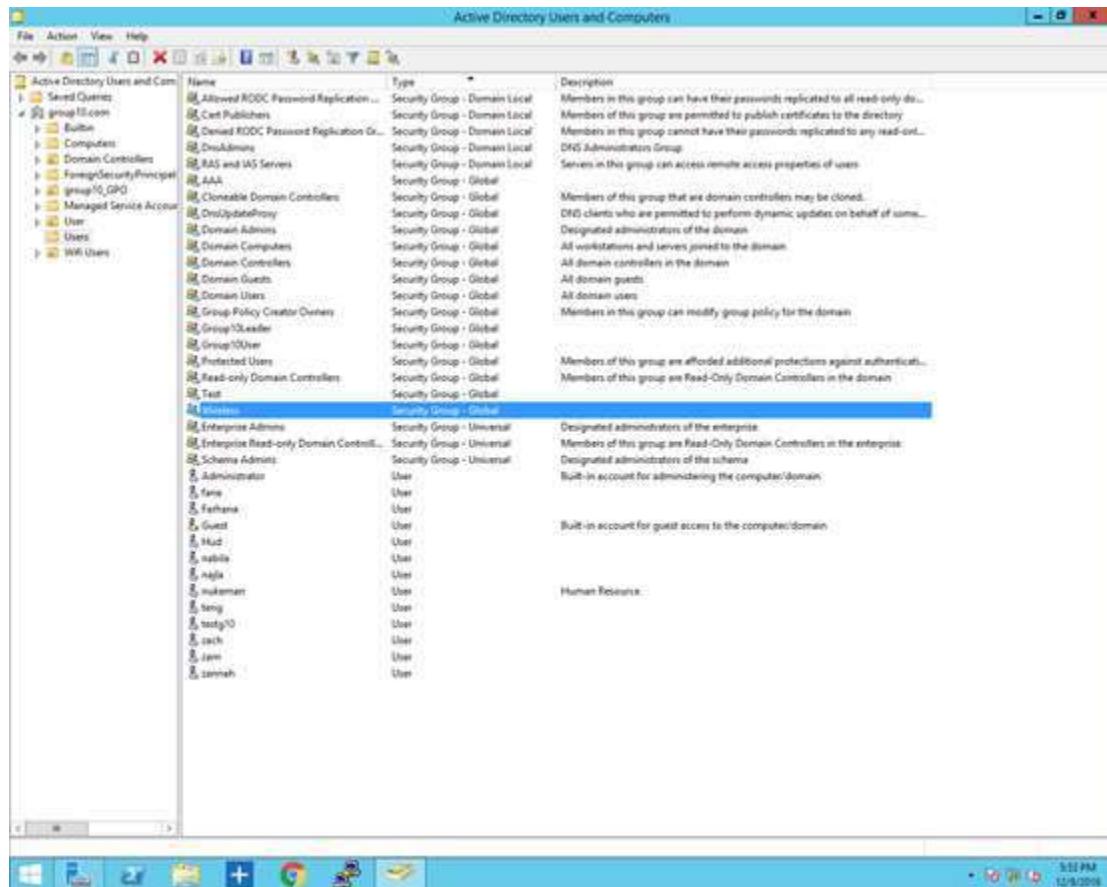
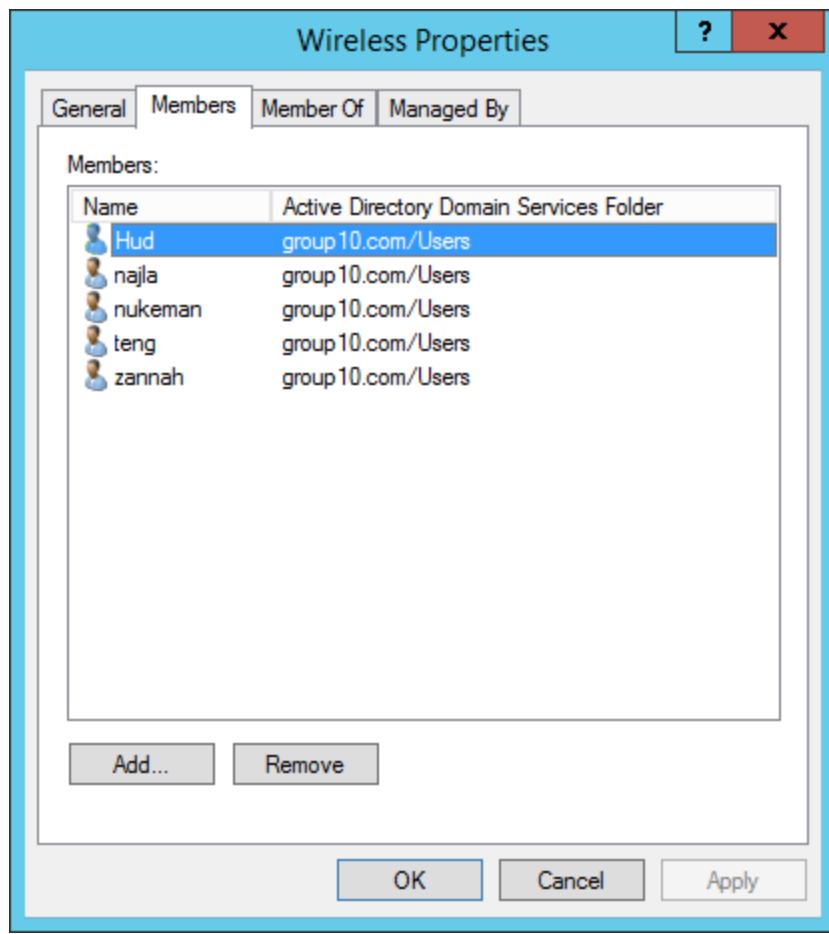


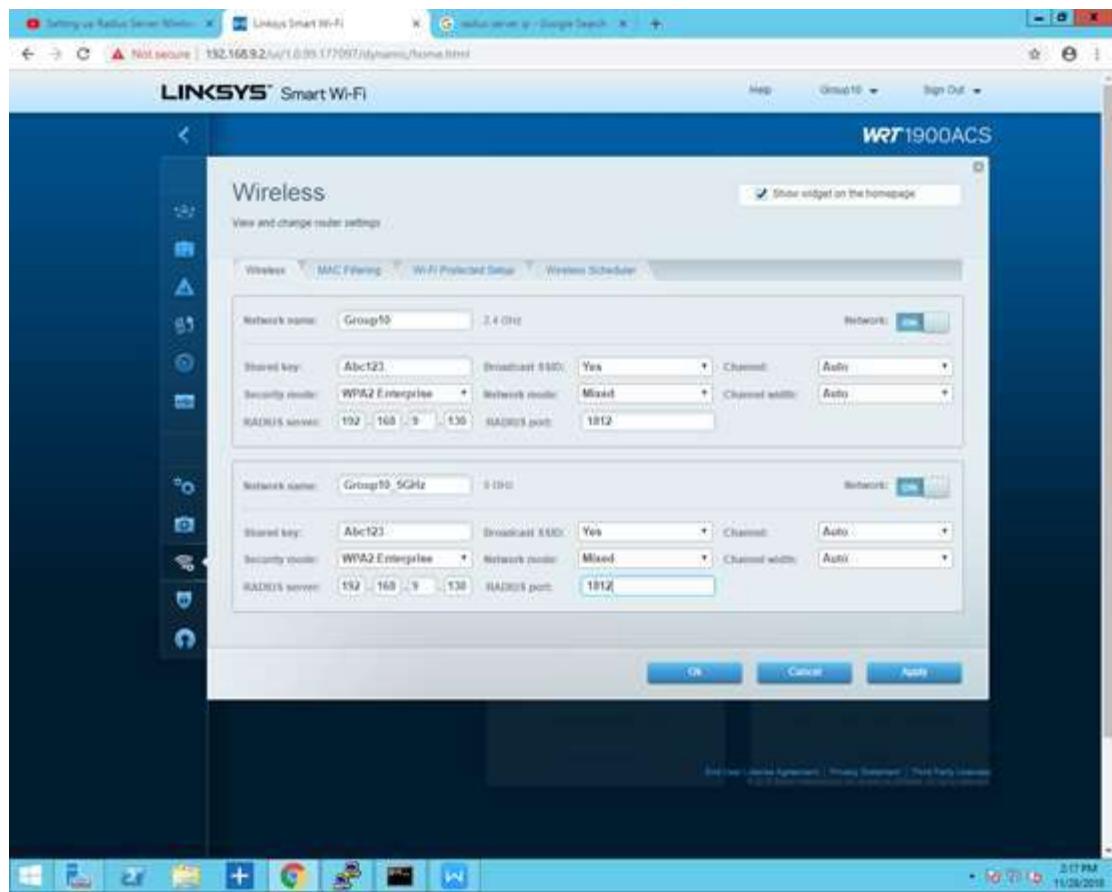
Figure 6.2.59 Active Directory Interfaces

Step 2: Assign members into group Wireless.



*Figure 6.2.60 Wireless Properties*

Step 3: Configure the Access Point (192.168.9.130).



Figure

#### 6.2.61 Configure AP

Step 4: Run and configure mmc.

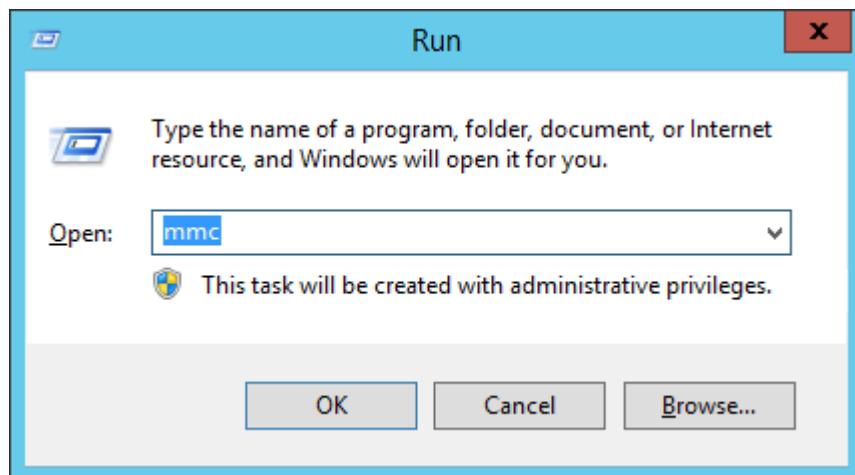
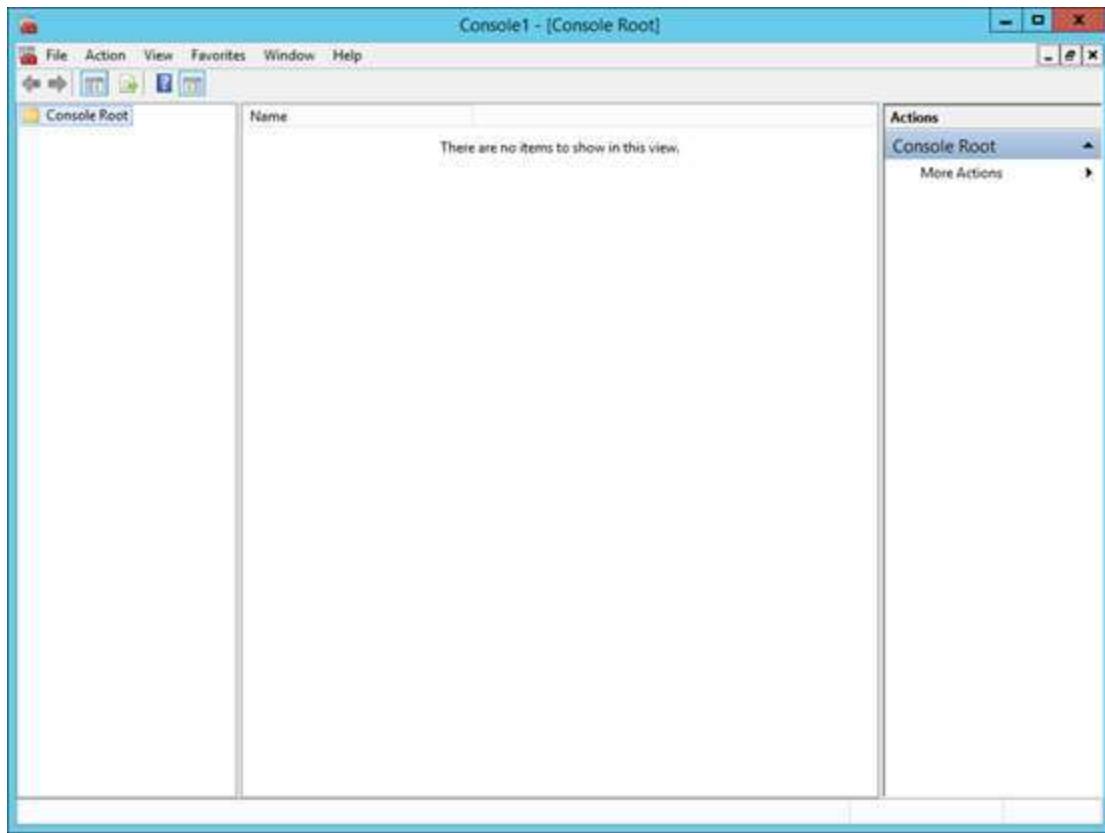


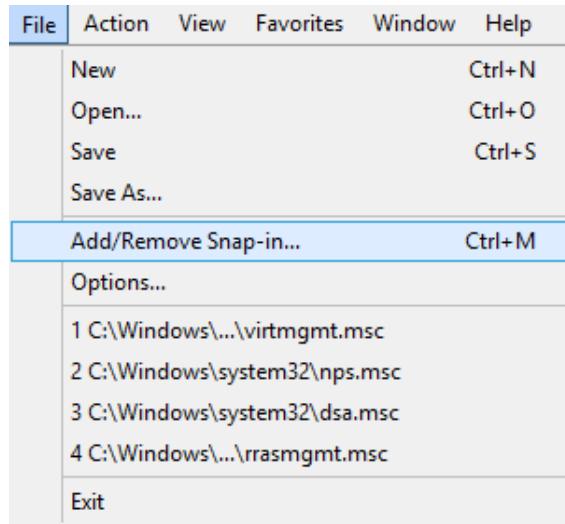
Figure 6.2.62 Run and configure mmc

Step 5: Open new Console1 for console root.



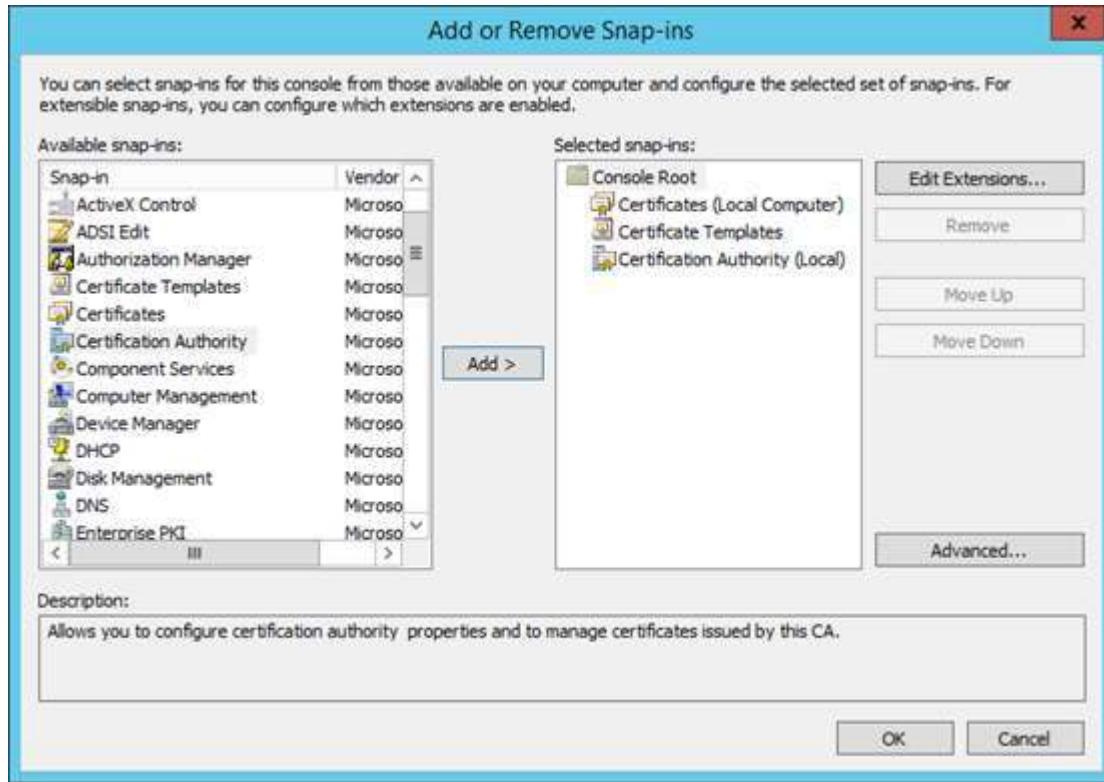
*Figure 6.2.63 New Console*

Step 6: In console Add or remove Snaps-ins, expand Certificates and click on Computer account. Then, click next.



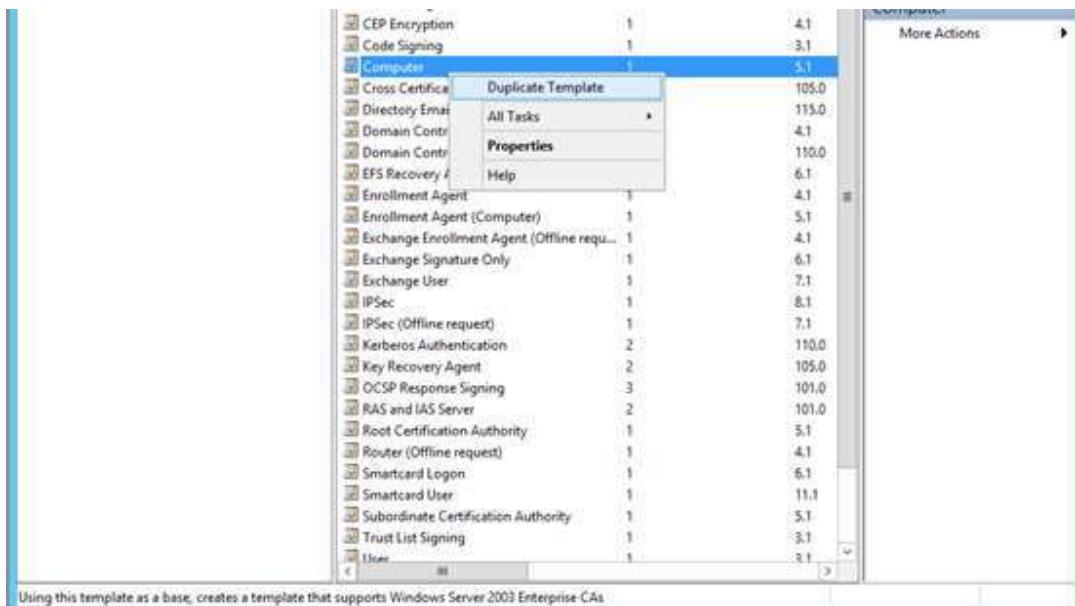
**Figure 6.2.64 Add/Remove Snap-in**

Step 7: In selected snap-ins box, expand Console Root. Then, Add Certificates Templates and Certification Authority (Local).



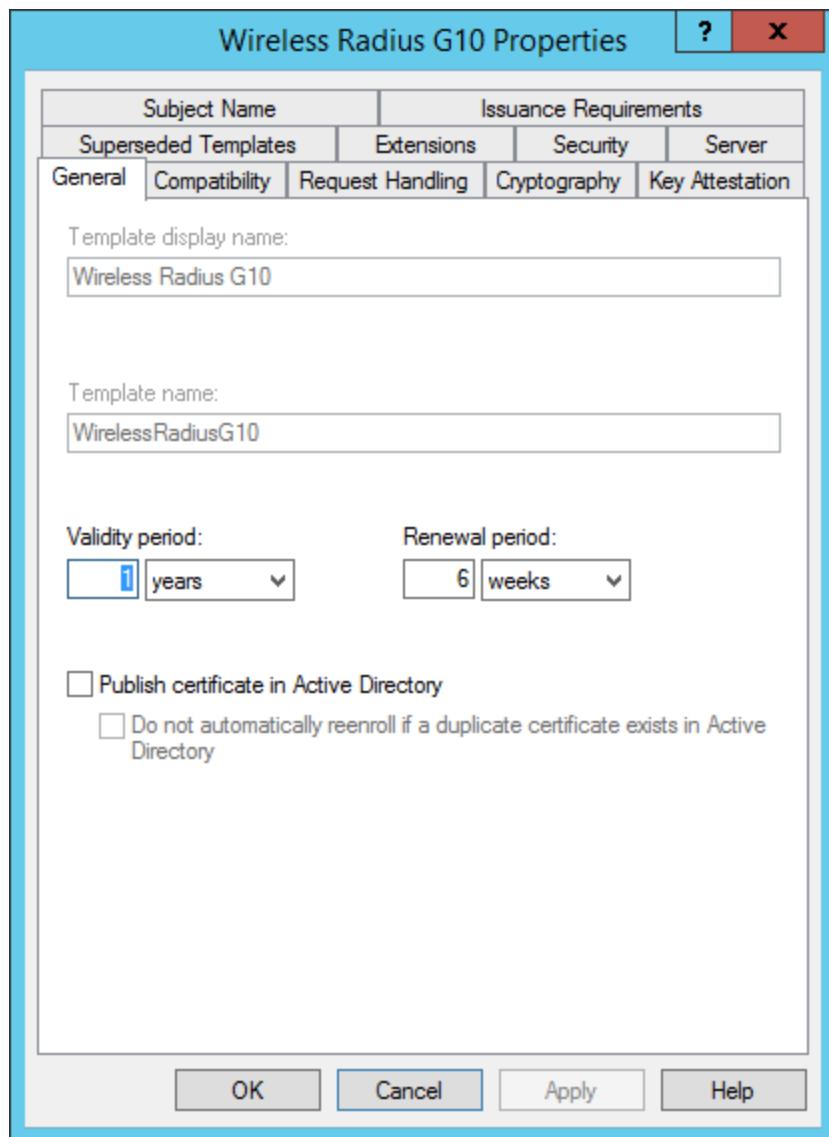
**Figure 6.2.65 Add on console root**

Step 8: In Certification Templates, expand Computer and click on duplicate computer.

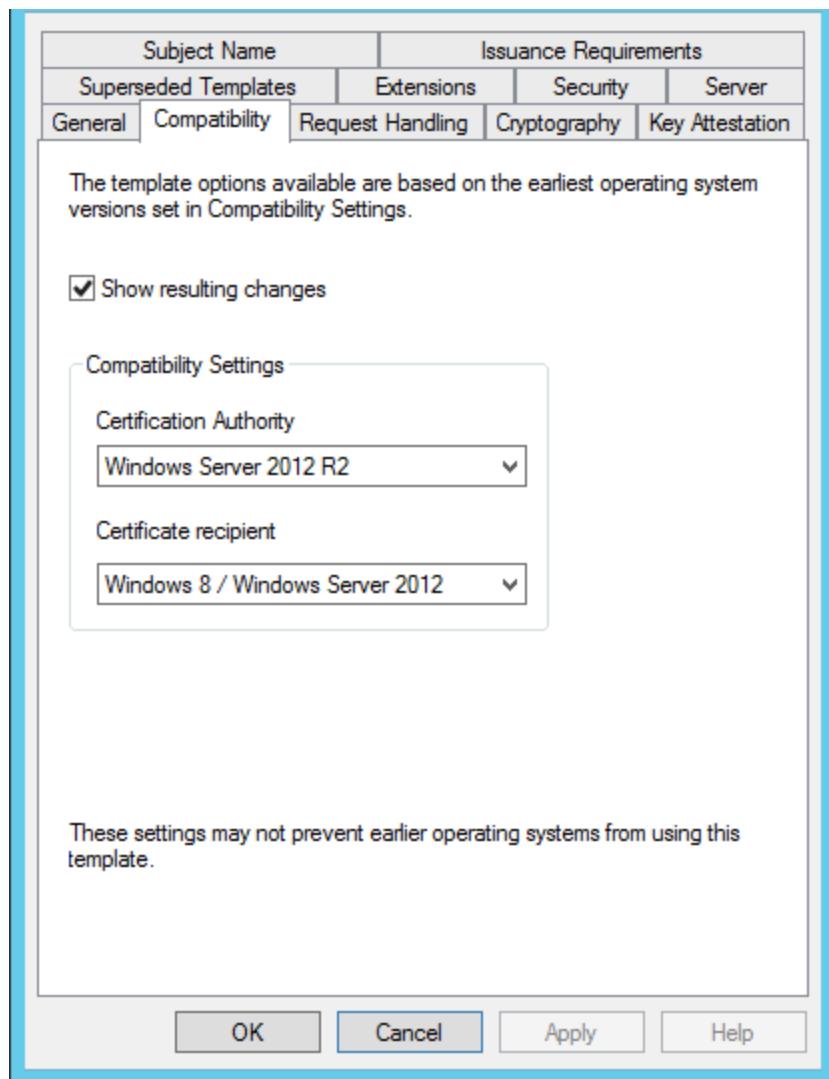


**Figure 6.2.66 Duplicate Template**

Step 9: Setup properties of New Template.



*Figure 6.2.67 Properties of New Template*



*Figure 6.2.13.10 Properties of New Template (continue)*

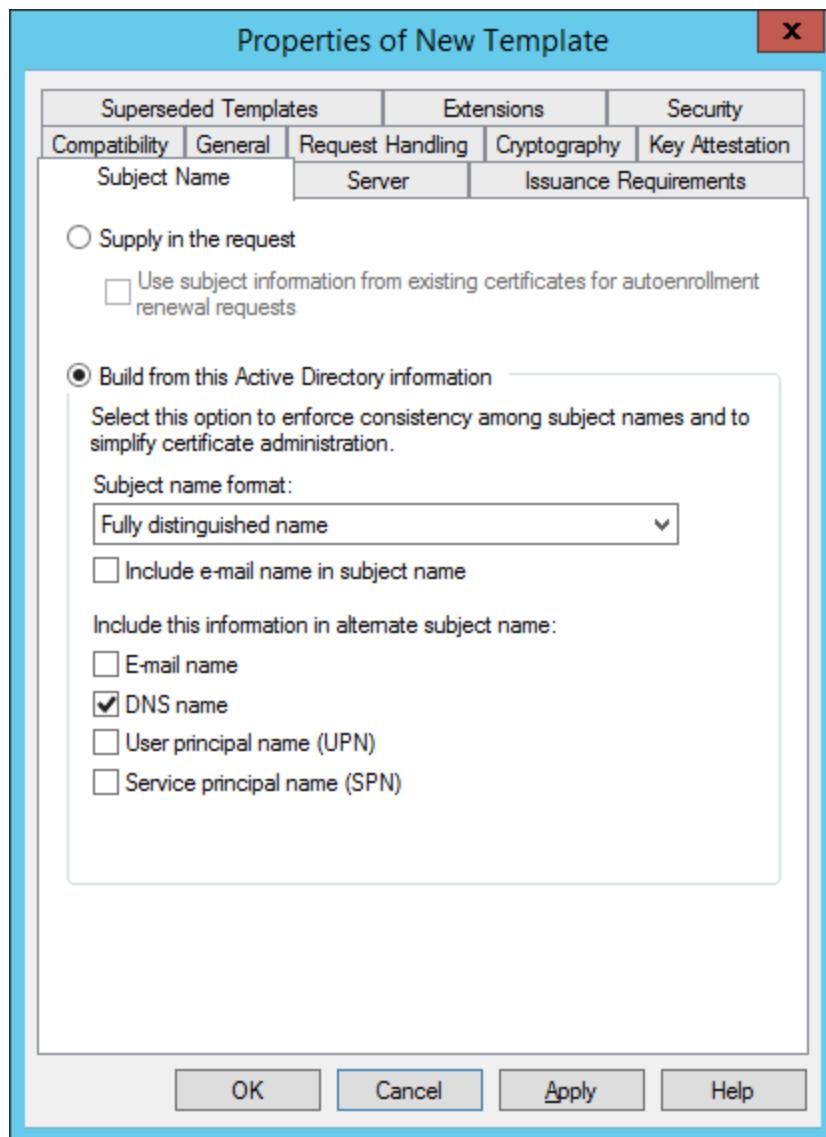
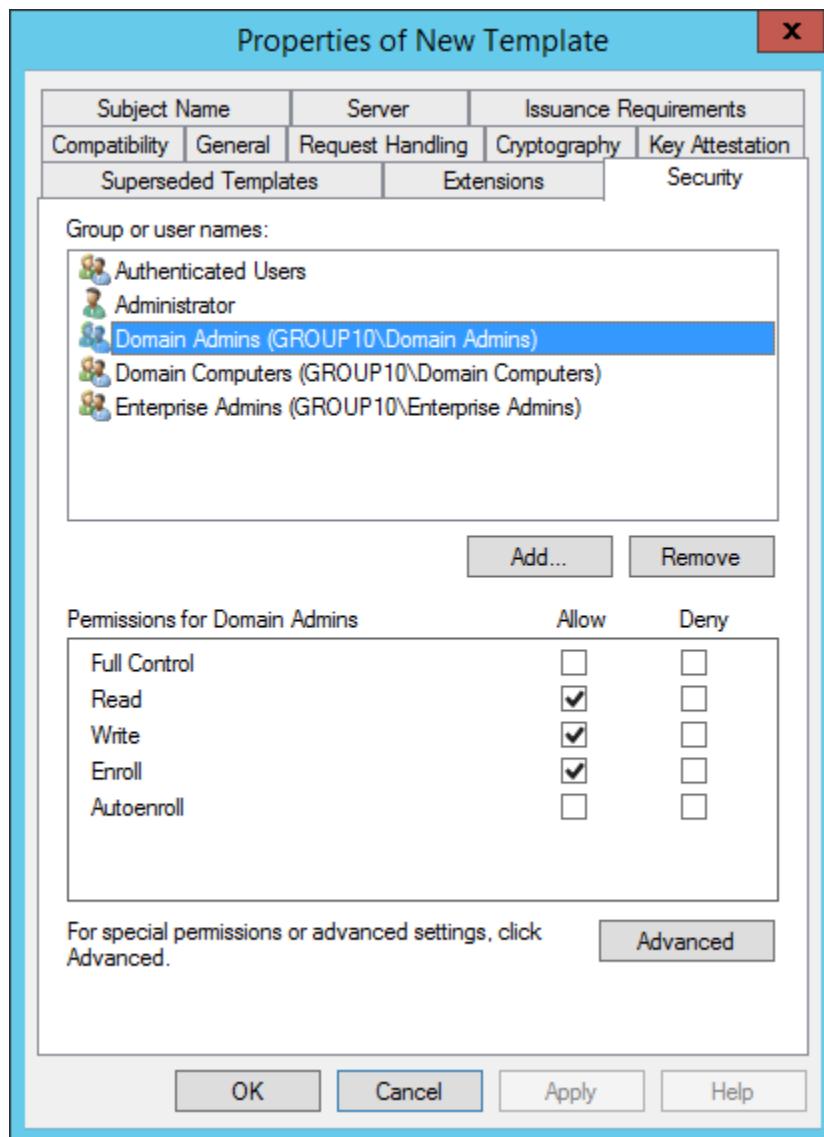


Figure 6.2.68 Properties of New Template (continue)

Step 10: Configure certificate template.



*Figure 6.2.69 Security New Template*

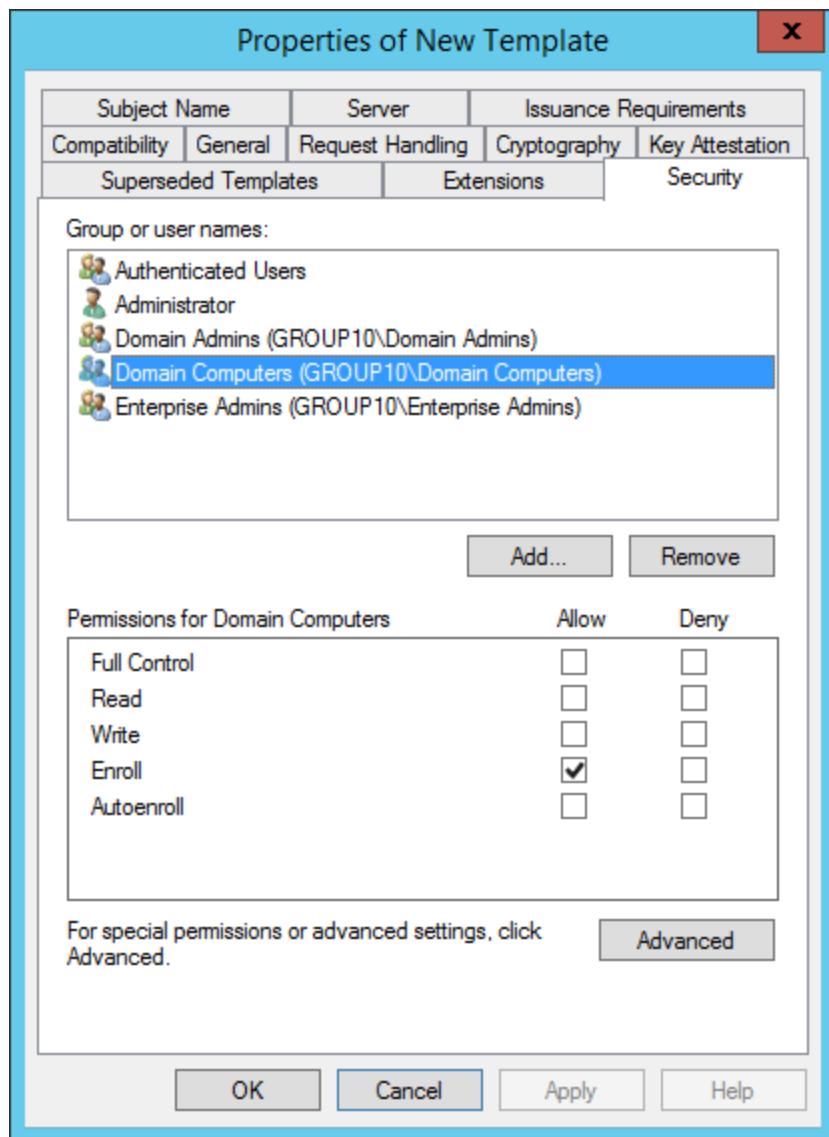
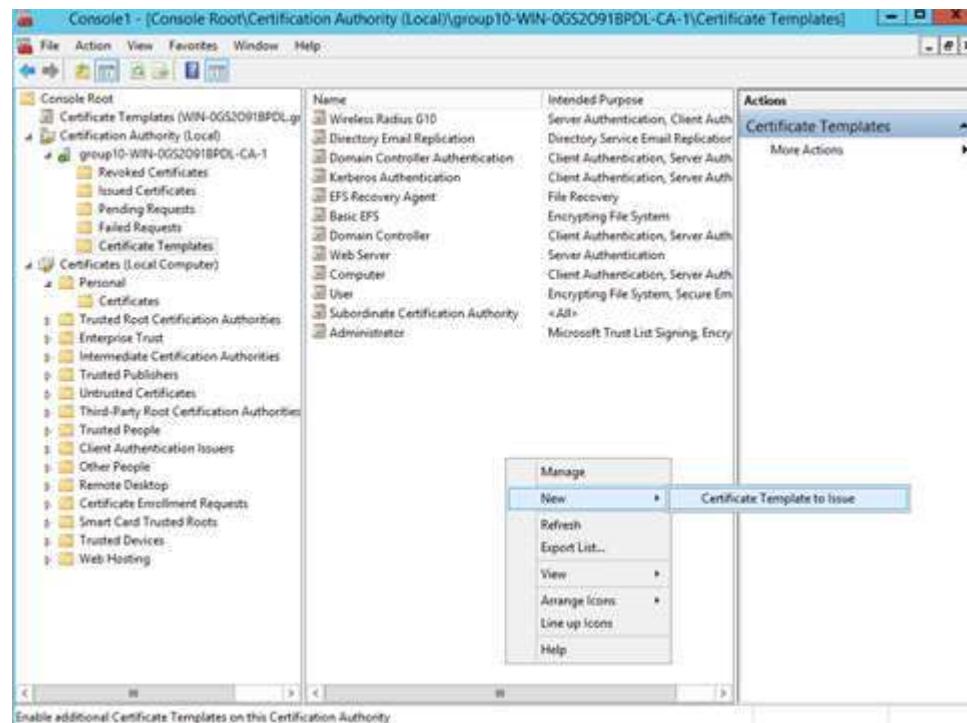


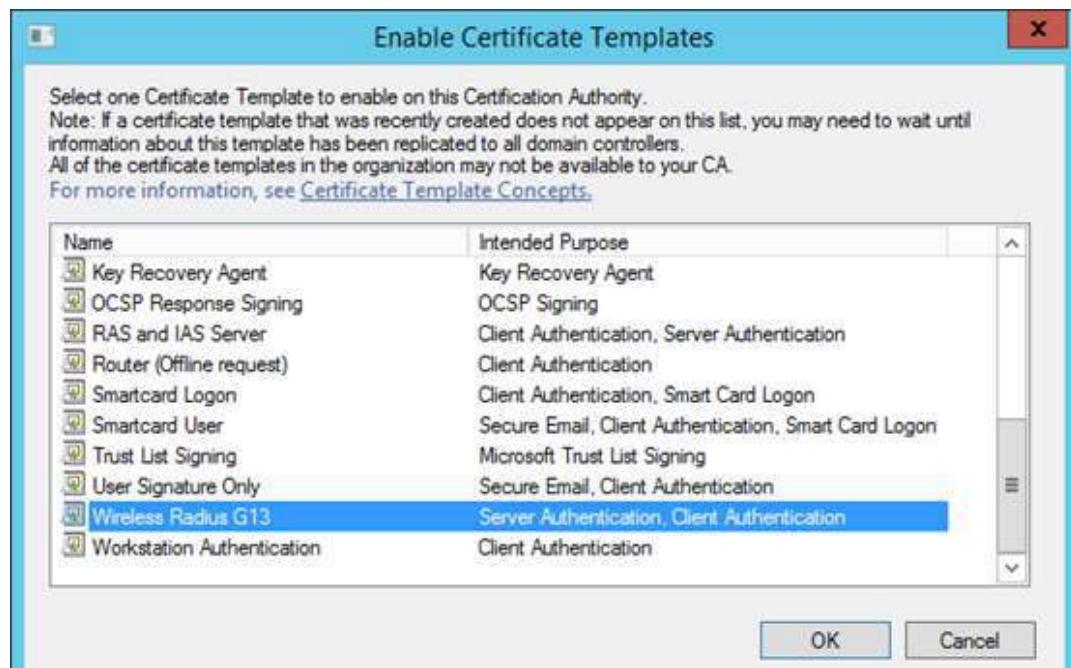
Figure 6.2.70 Security New Template (continue)

Step 11: Go to Certification Authority, expand and select Certificate Templates. Right click and select New> Certificate Template to issue.



*Figure 6.2.71 Certification Authority*

Step 12: Enable Certificate Template box will pop up, tick on Radius Authentication. Then click OK.



Figure

#### 6.2.72 *Enable certification templates*

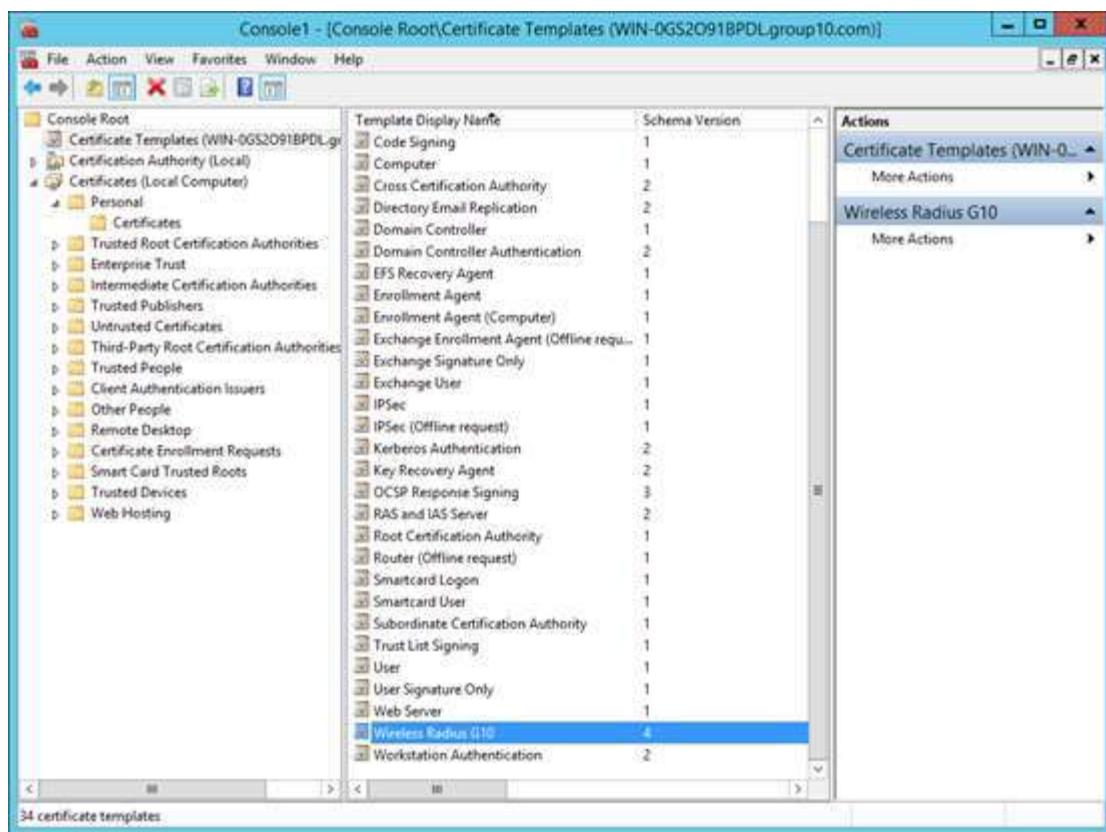


Figure 6.2.73 Success add into Certificate Templates

Step 13: Click on Certificates (Local Computer) > Personal > Certificates, Right-click mouse and select All Tasks > Request New Certificate.

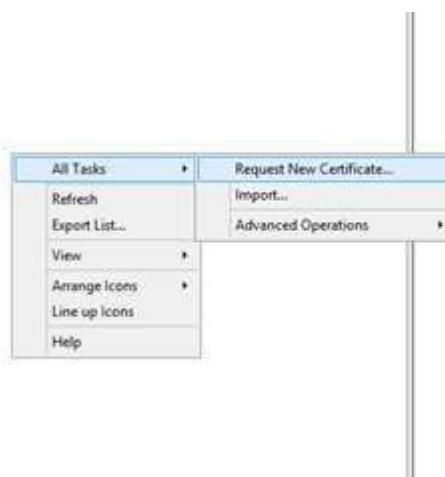
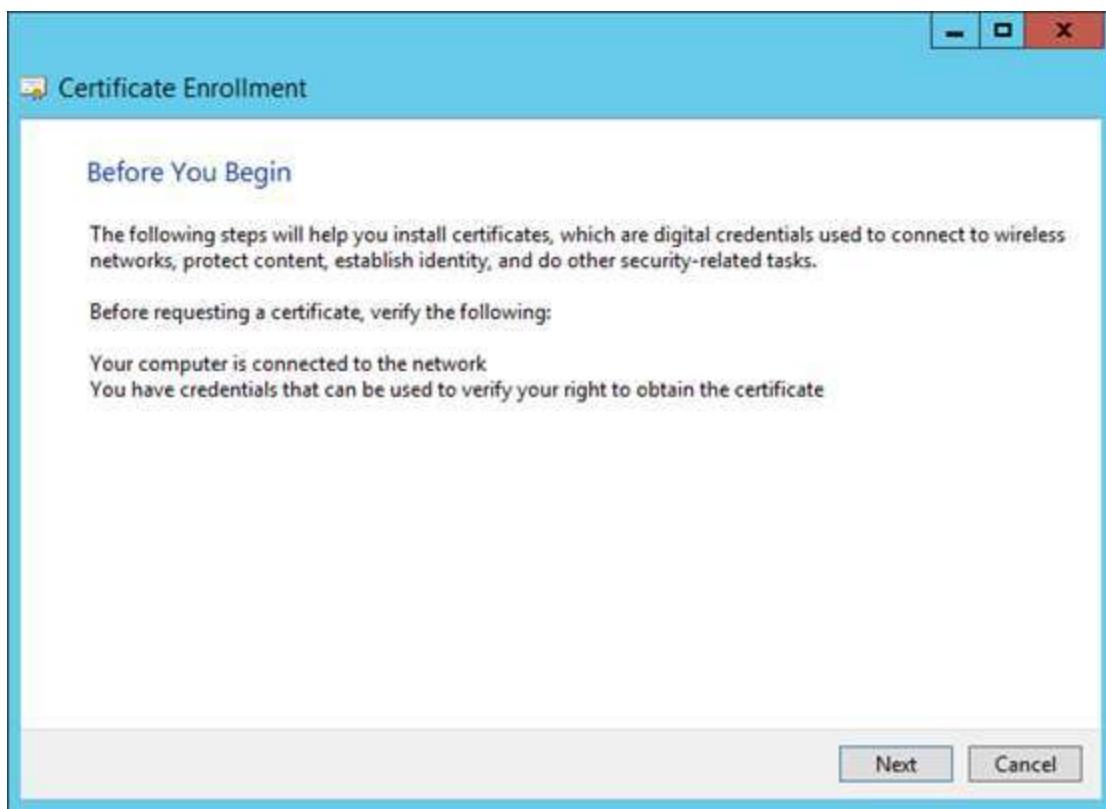
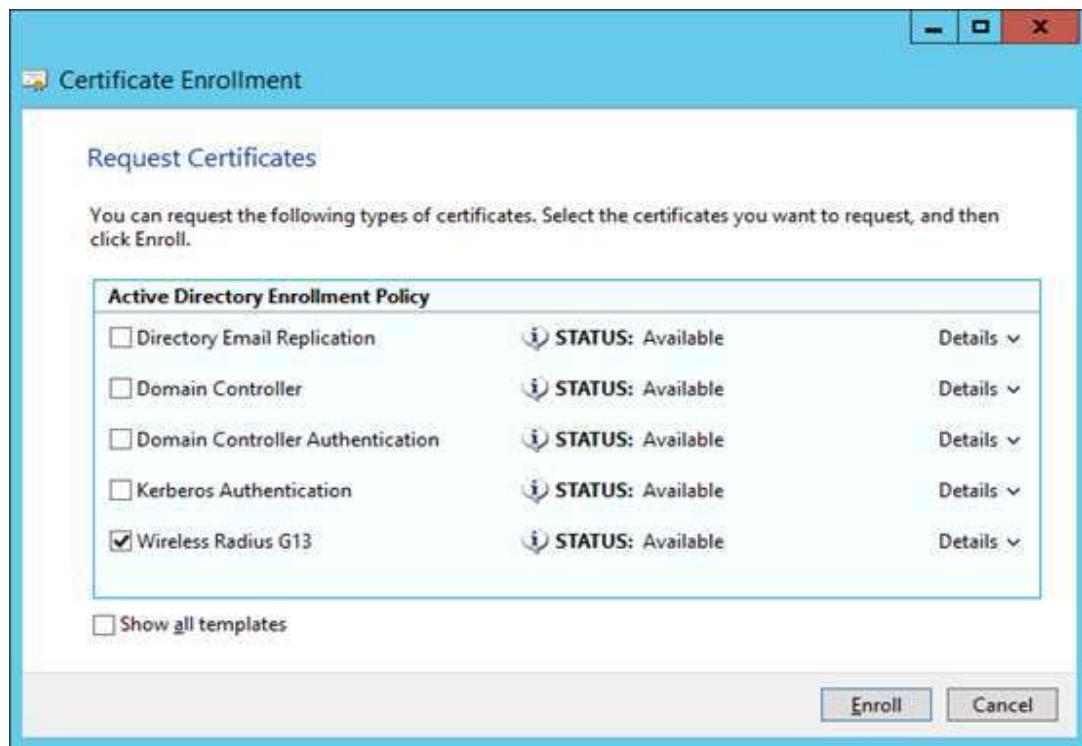


Figure 6.2.74 Request New Certificate

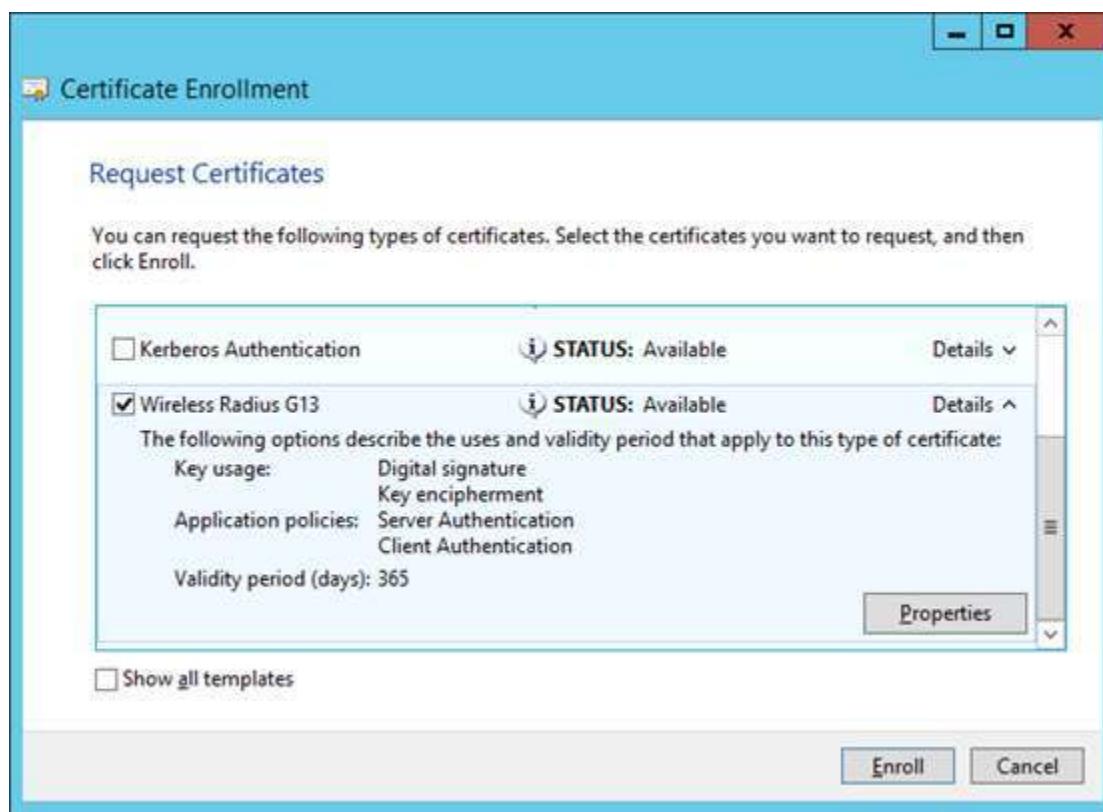


*Figure 6.2.75 Before enroll certificate*

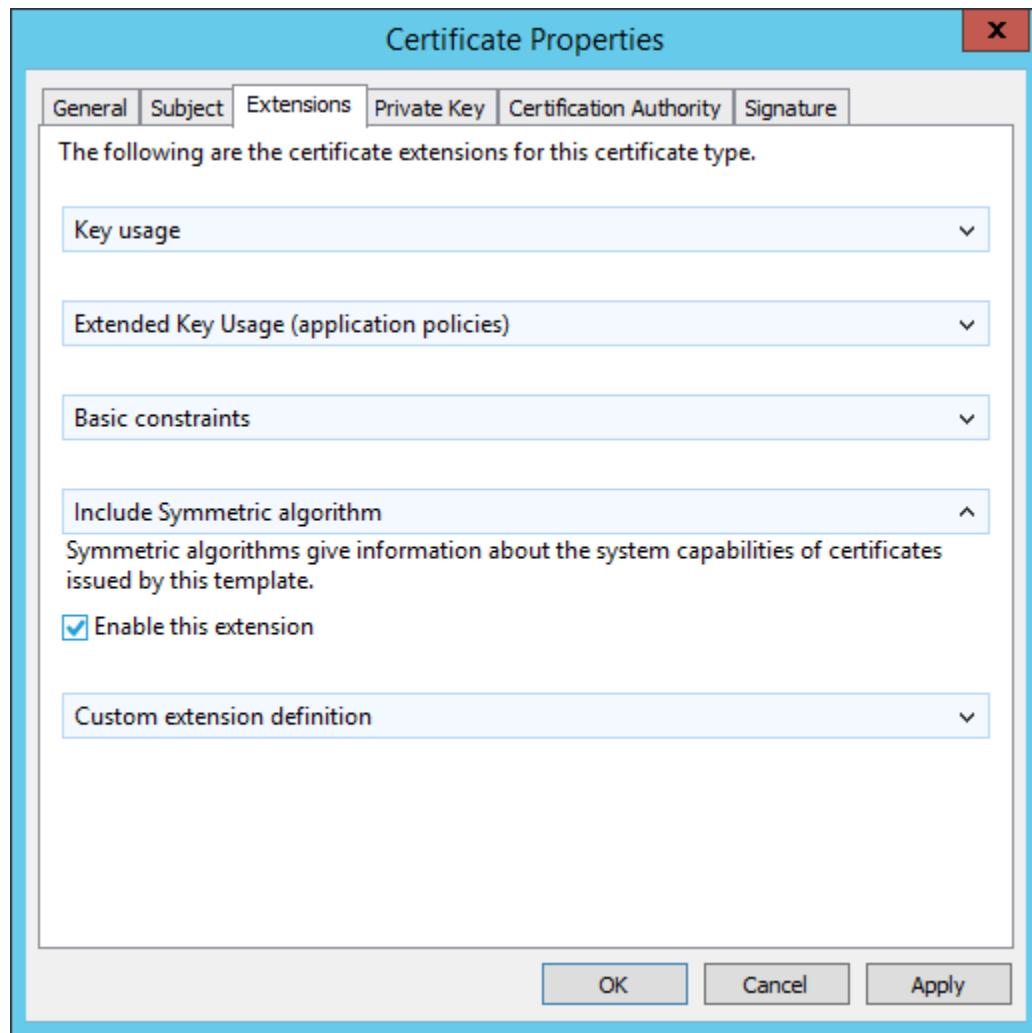


Figure

#### 6.2.76 Show request certificates

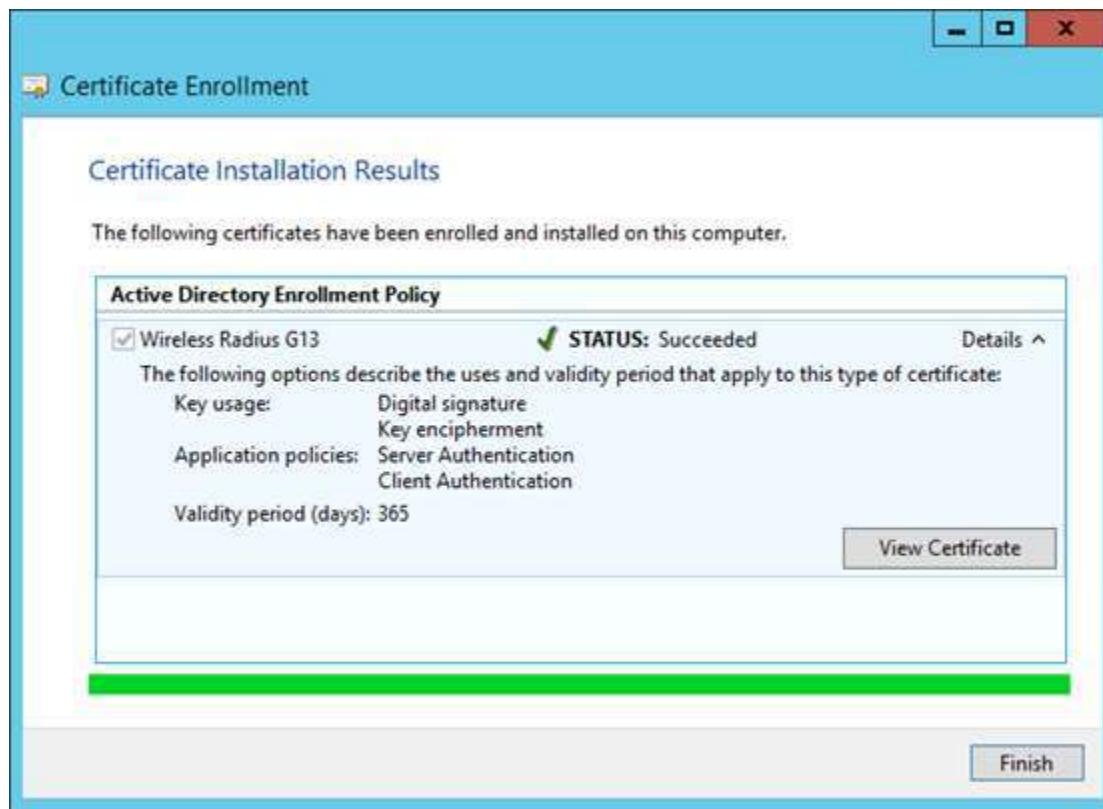


*Figure 6.2.77 Radius Authentication*



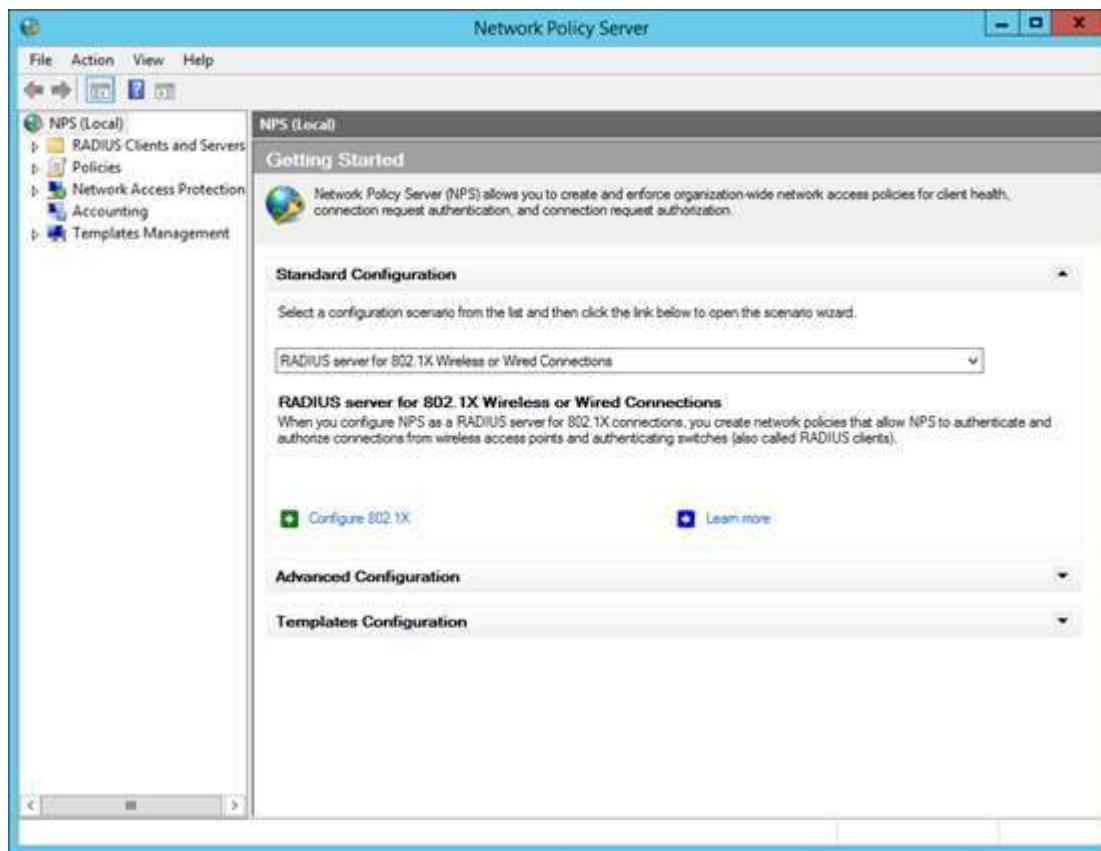
*Figure 6.2.78 Configure certificate properties (continue)*

Step 14: In Certification Installation Results page show Status: succeeded. Then, click Finish.

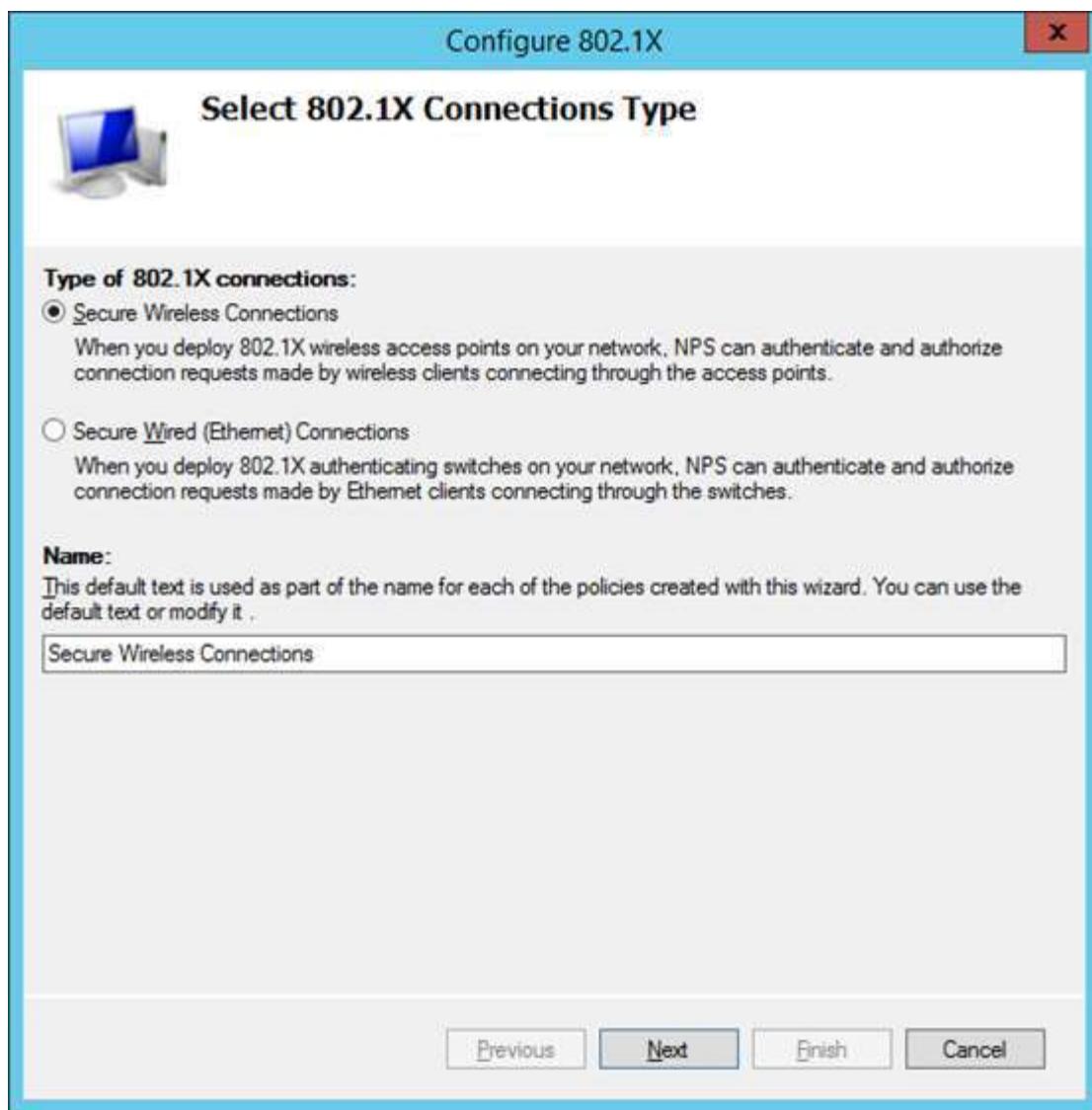


*Figure 6.2.79 Installation Page*

Step 15: Configure Network Policy Server.



*Figure 6.2.80 Network Policy Server*



*Figure 6.2.81 Configure Network Policy Server*

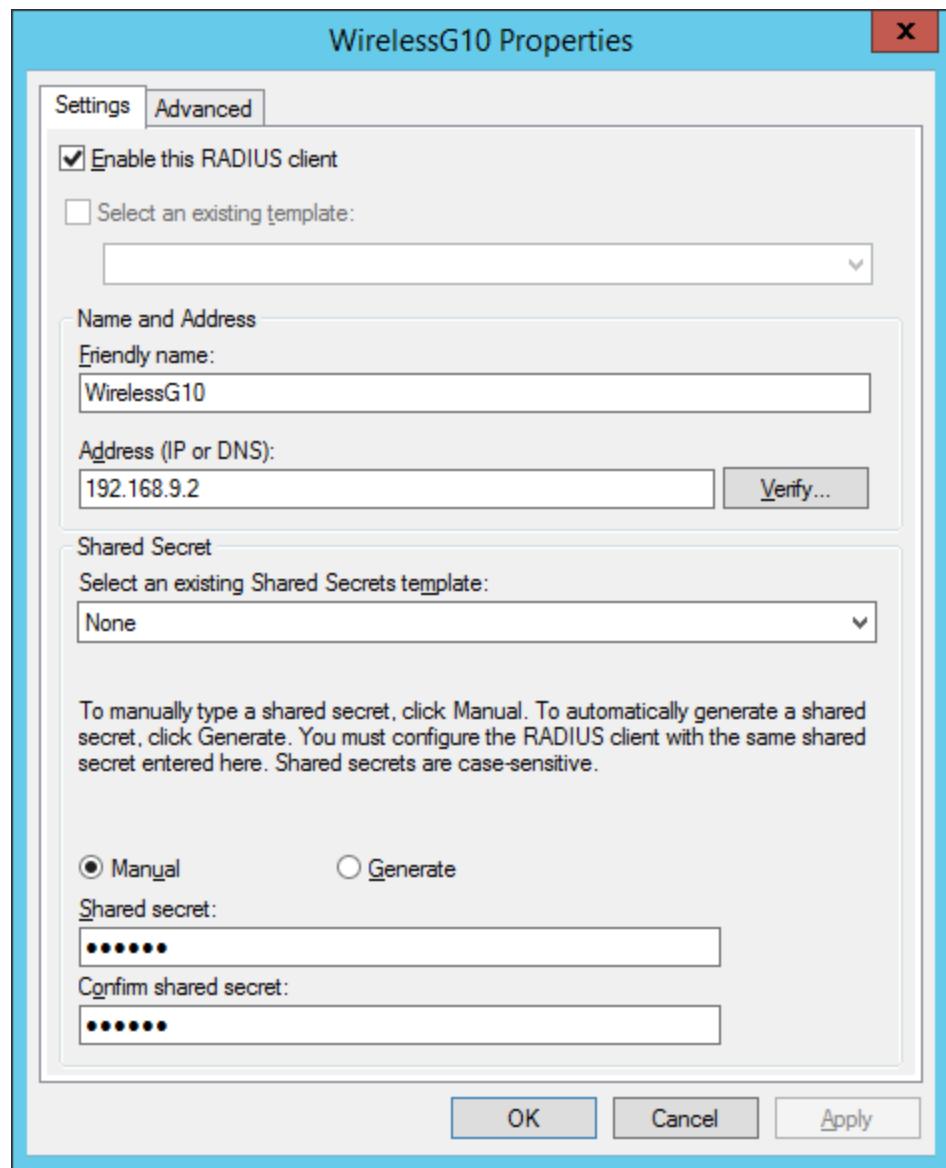
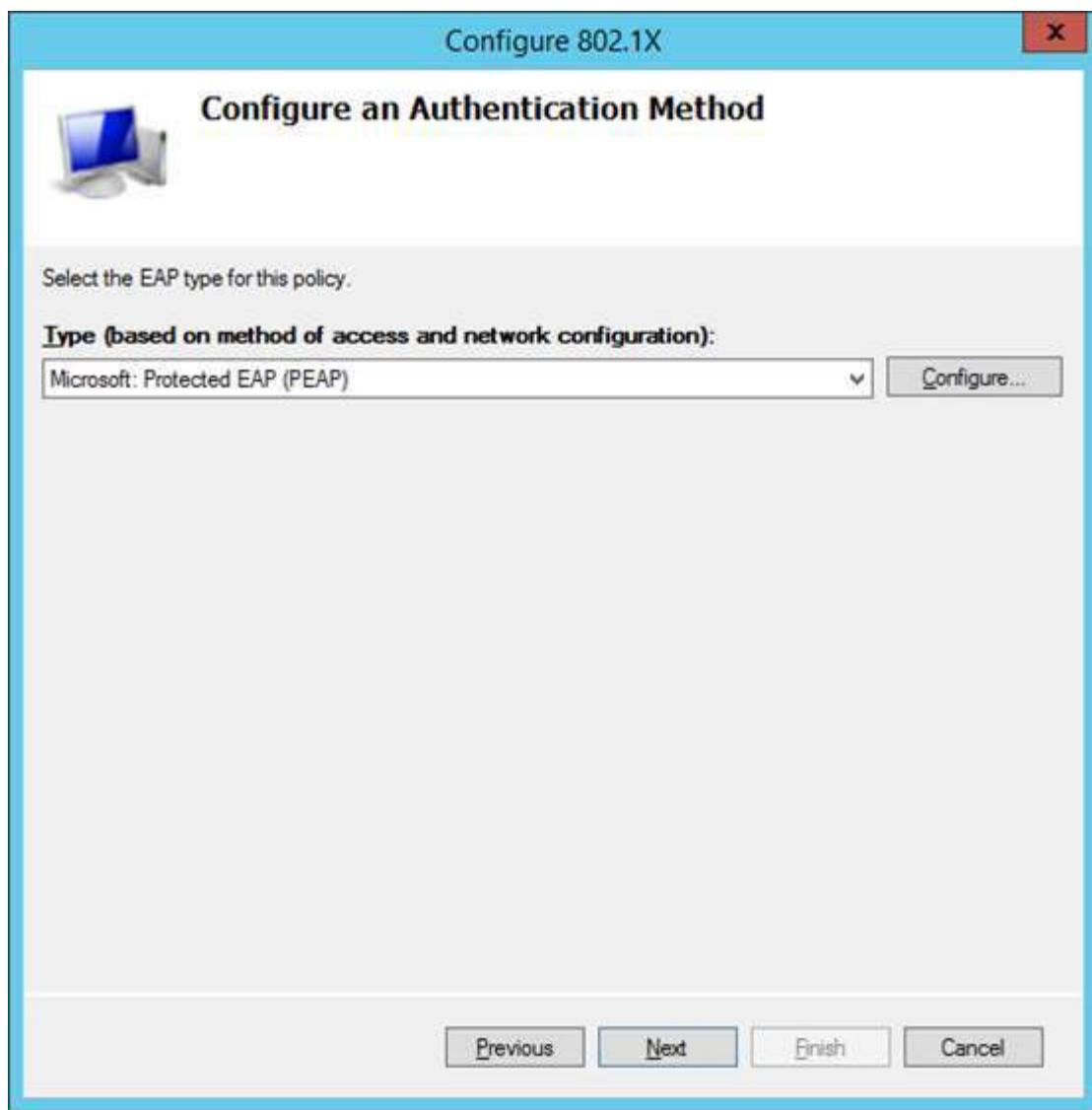
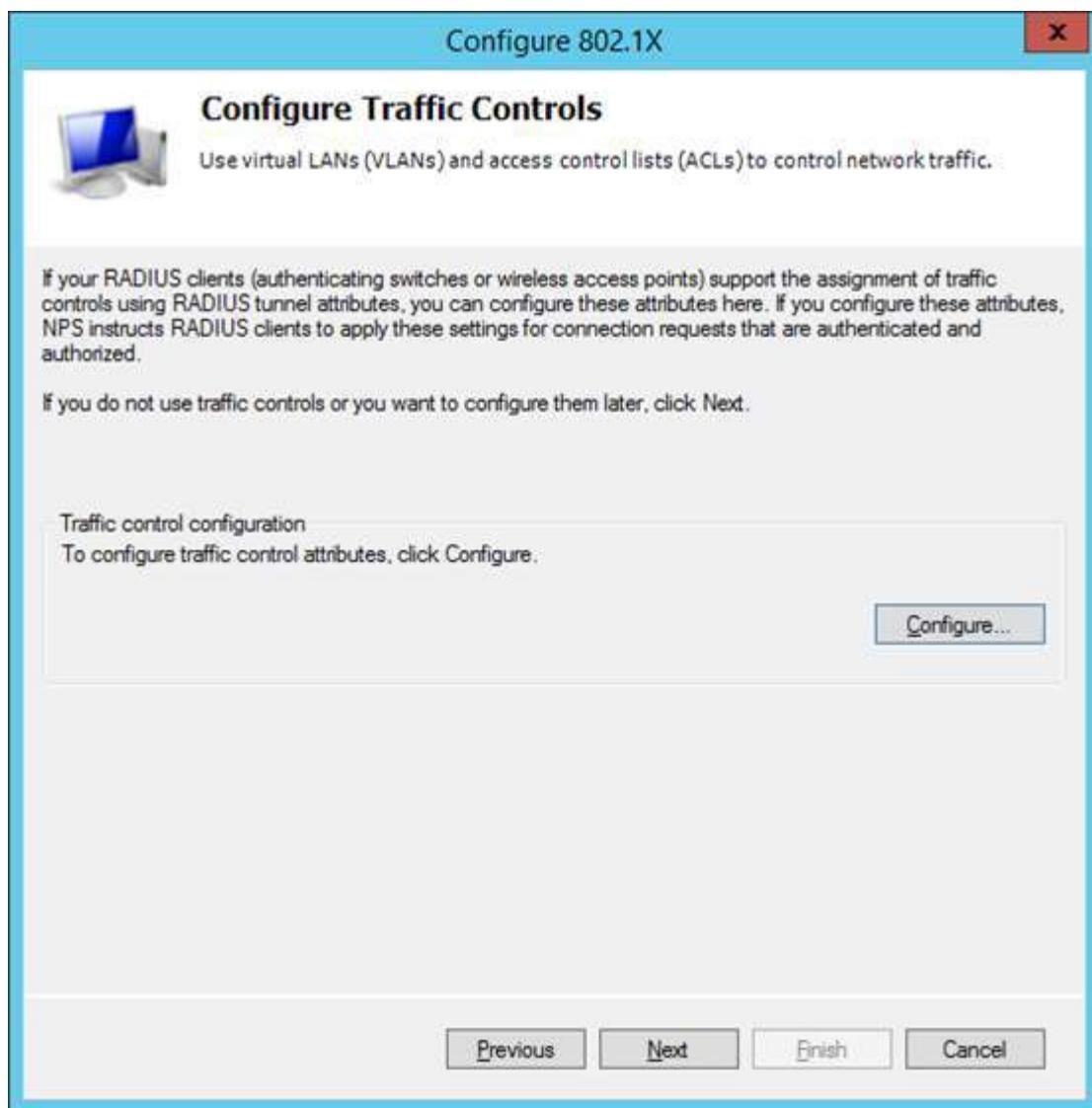


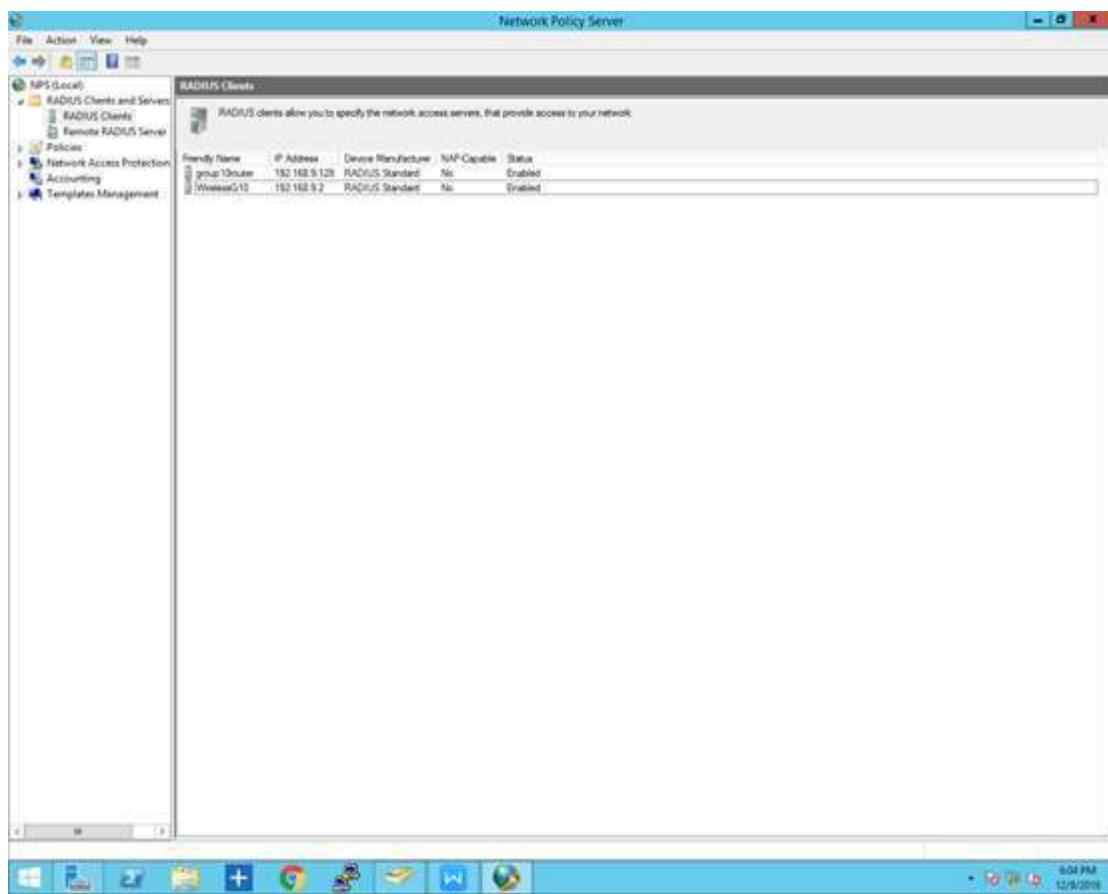
Figure 6.2.82 New RADIUS Client



*Figure 6.2.83 Select EAP type which is PEAP*



*Figure 6.2.84 Configure 802.1X*



*Figure 6.2.85 Friendly Name which is WirelessG10 is Radius Server*

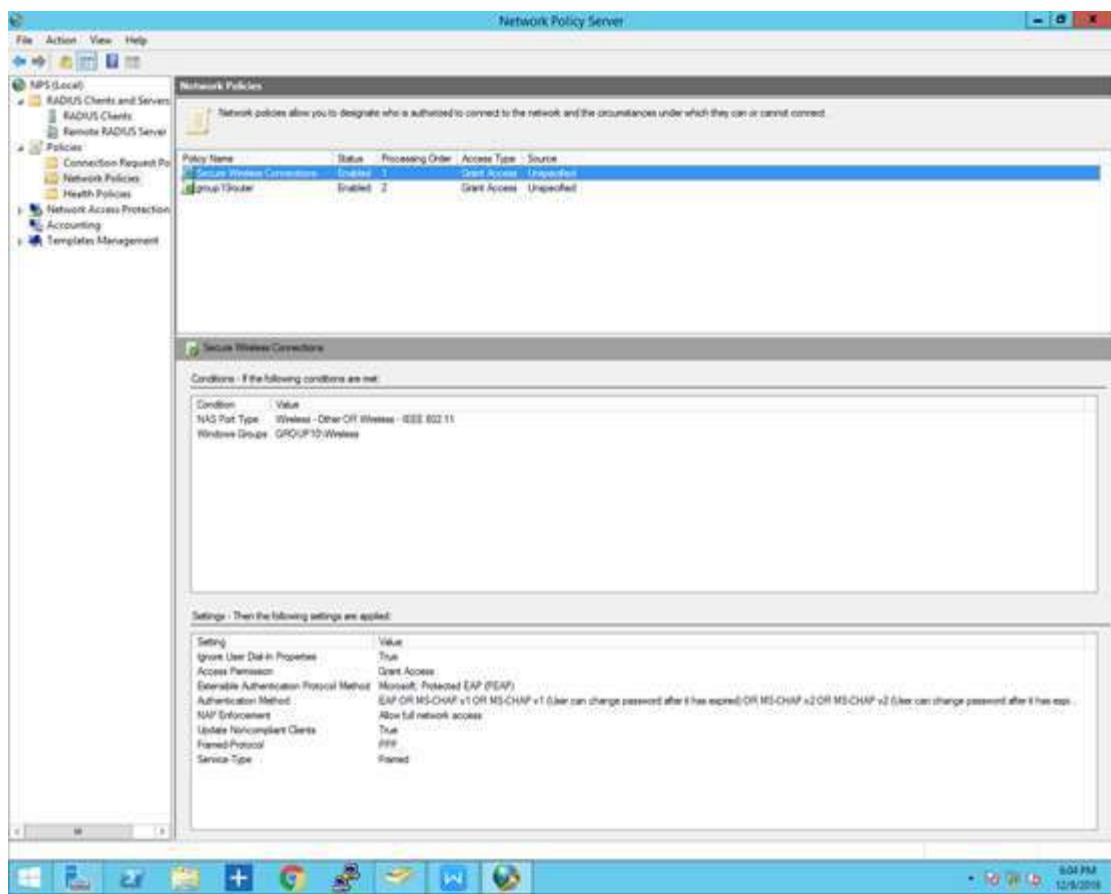
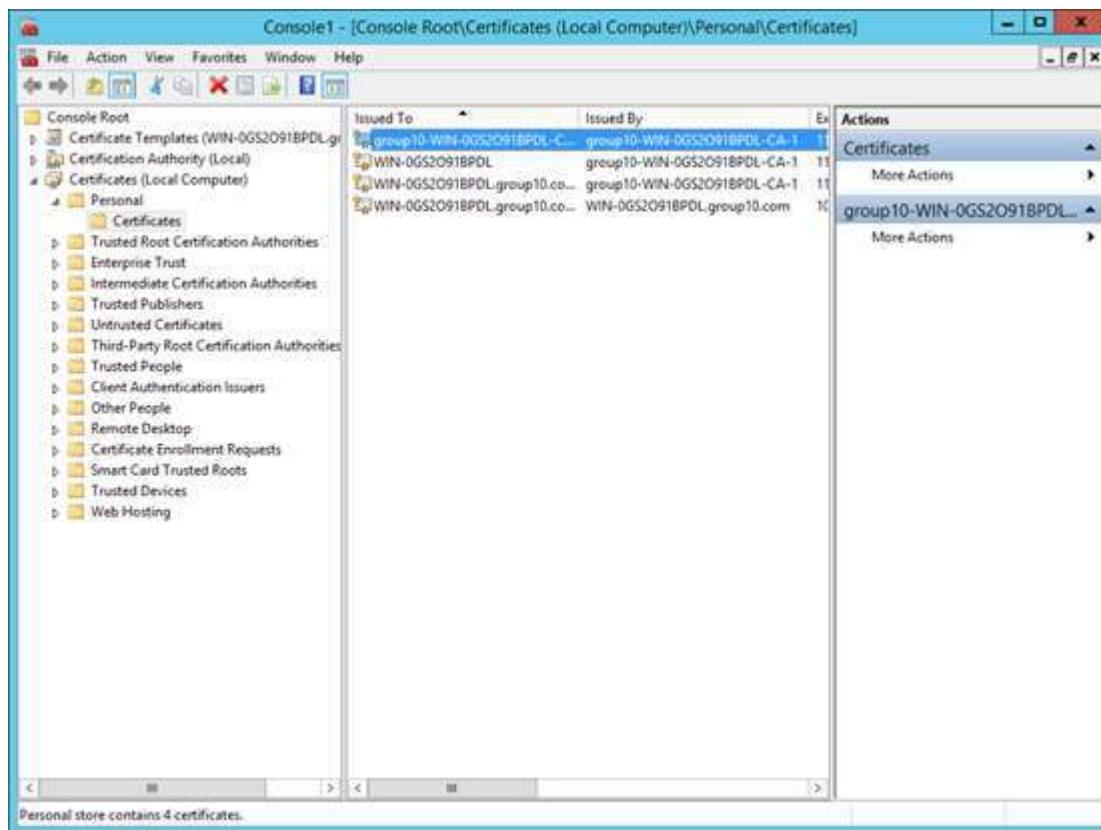
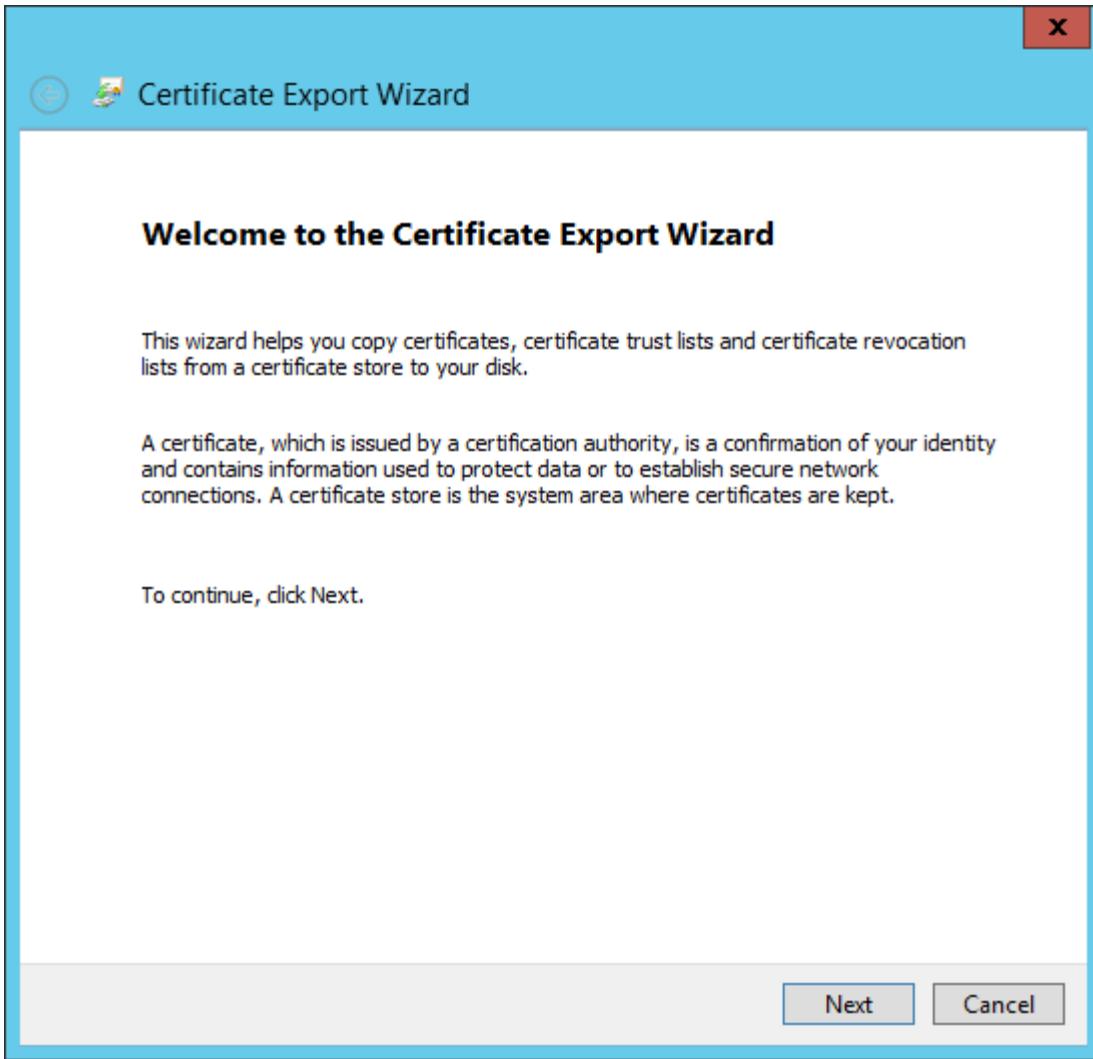


Figure 6.2.86 Secure Wireless Connection

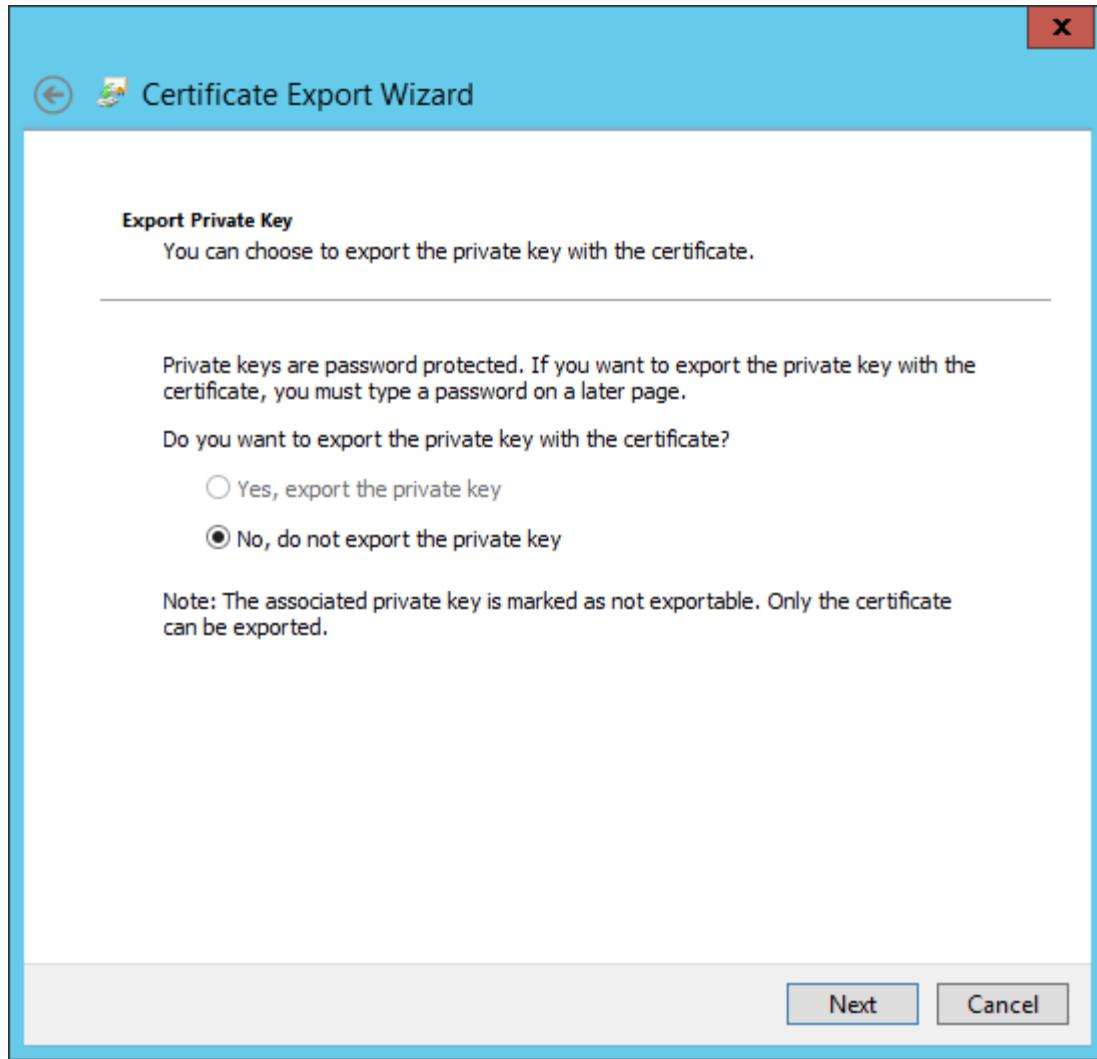
Step 16: Export Wireless Radius Certificate.



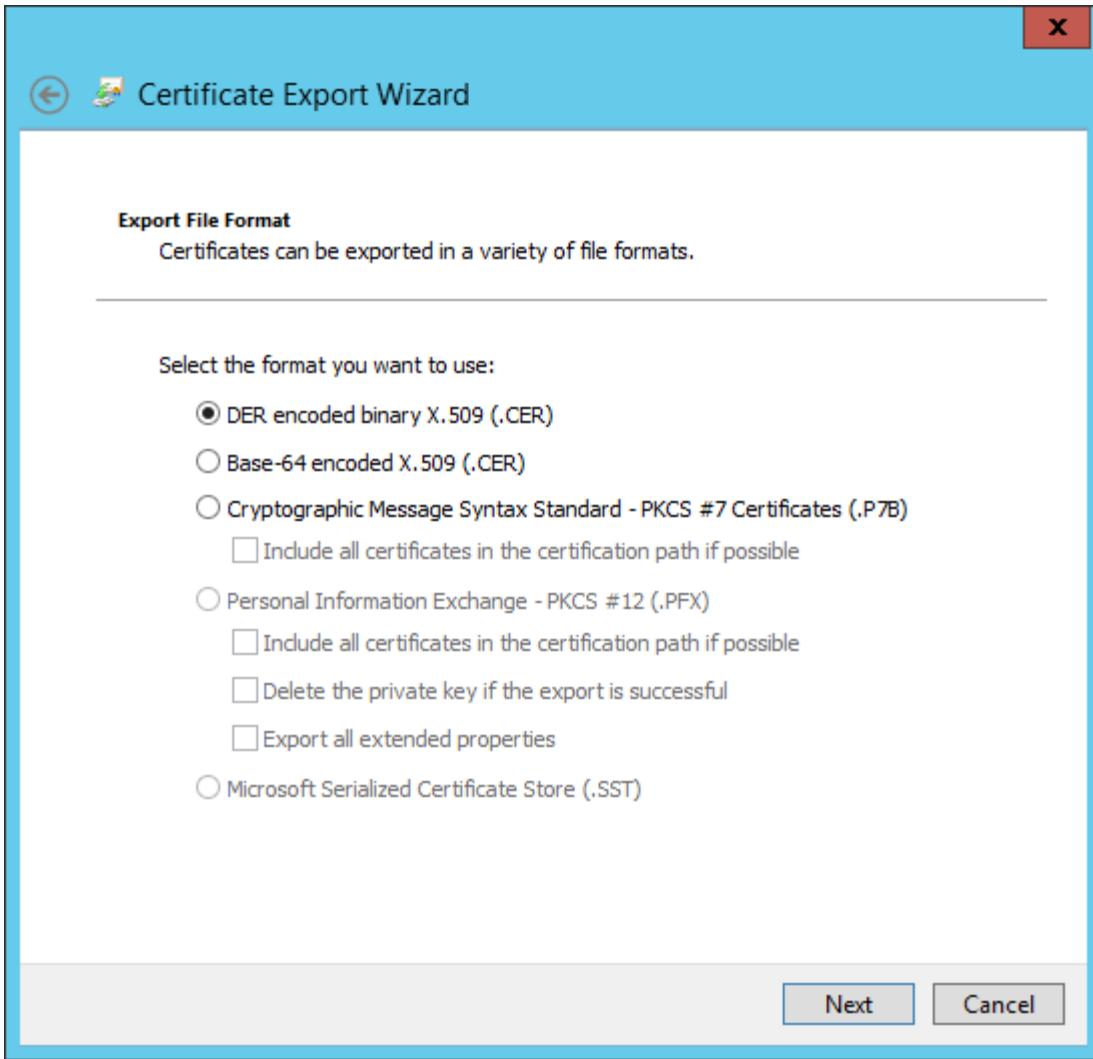
*Figure 6.2.87 Export Wireless Radius Certificate*



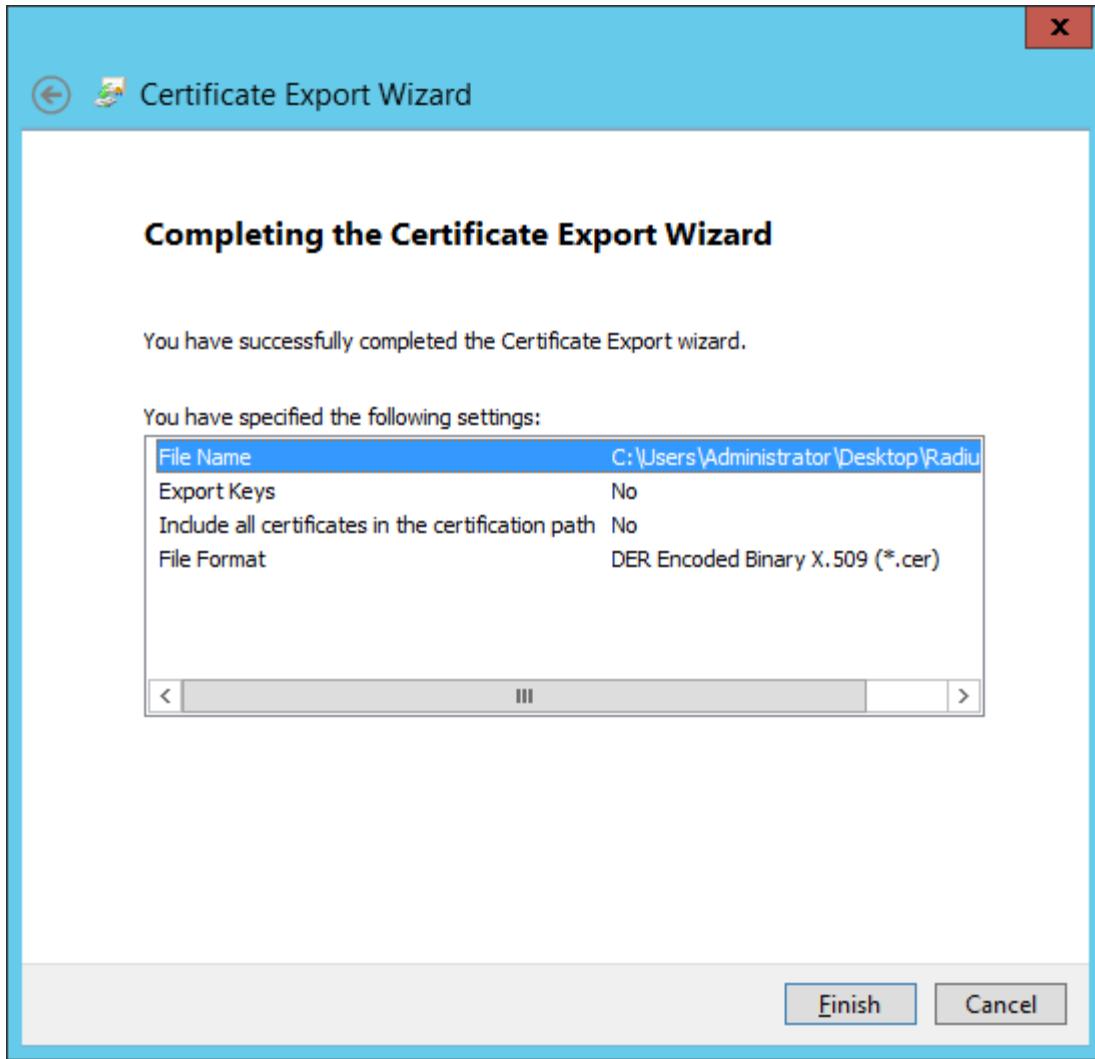
*Figure 6.2.88 Export Wireless Radius Certificate (continue)*



*Figure 6.2.89 Export Wireless Radius Certificate (continue)*



*Figure 6.2.90 Certificate Export Wizard*



*Figure 6.2.91 Completing the Certificate Export Wizard*

**Problem:** Some users want a secure the wireless network access, if the wireless connection is not protected. The network can easily penetrate by unauthorized user.

**Solution:** We install Network Policy Server inside Windows Server 2008 and configure access point as wireless radius client. Each user wants to connect with access point must authenticate using AD before he/she can login into the network. This enhanced more secure network and better network authentication and authorization

### 6.2.14 Remote Login Using SSH

#### Step1 : Router testing using Putty

a)To log in the router interface by using SSH, a software should be installed which is known as, PuTTy. In the PuTTy interfaces, key in the IP address/Host Name of the Router. For my case, is using 192.168.9.153 ,Port 22 and the connection type is SSH. Then “Open”.

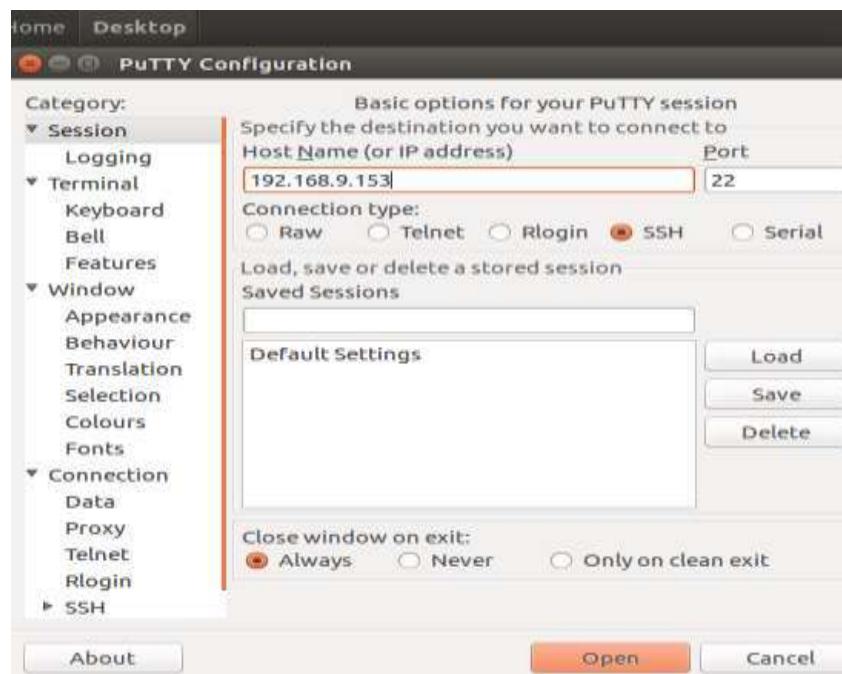
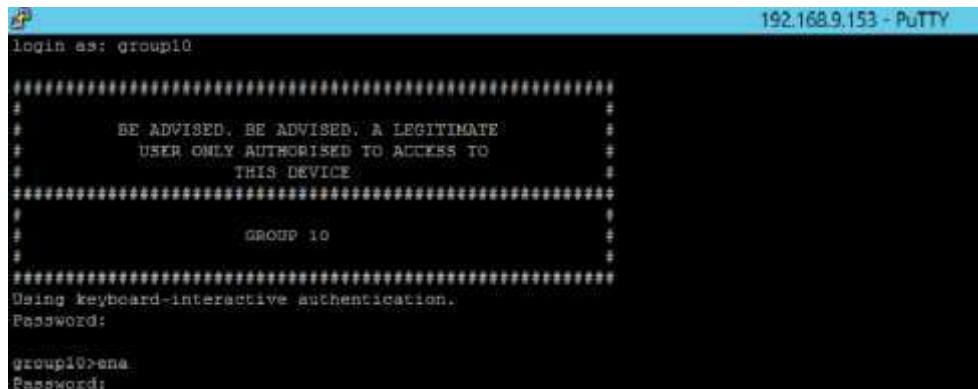


Figure 6.2.92 SSH testing on Router

b)After that, a username and password would be asked before accessing the terminal. Key in the username and password that has been set just now to log in. For example:

Username: group10

Password: AAssdd123



```
192.168.9.153 - Putty
login as: group10
#####
#      BE ADVISED. BE ADVISED. A LEGITIMATE      #
#      USER ONLY AUTHORISED TO ACCESS TO      #
#      THIS DEVICE                            #
#####
#          GROUP 10                           #
#####
Using keyboard-interactive authentication.
Password:
group10>ena
Passwords:
```

Figure 6.2.93 SSH testing on Router

c) If the password is wrong, the access has been denied. If the password is correct, the router interface will displayed. You may configure the router using the interface. This router have been set for retries 3 if more than that it will popup the warning message and the server cannot be access and will automatically close.

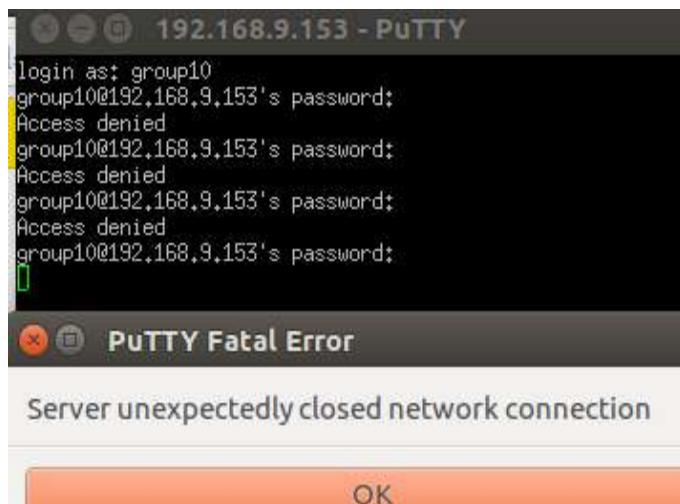
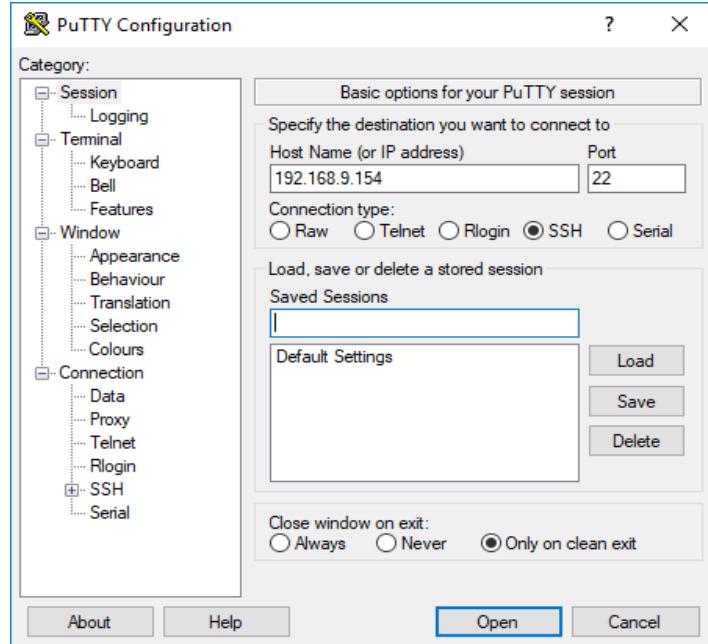


Figure 6.2.94 SSH testing on Router

## Step2: Switch testing Using Putty

a) log in the switch interface by using SSH, a software should be installed which is known as, PuTTy. In the PuTTy interfaces, key in the IP address/Host Name of the Switch. For my case, is using 192.168.9.154 ,Port 22 and the connection type is SSH. Then “Open”.



**Figure 6.2.95 SSH testing on Router**

- b) After that, a username and password would be asked before accessing the terminal. Key in the username and password that has been set just now to log in. For example:
- Username: group10
  - Password: AAssdd123

The screenshot shows a PuTTY terminal window titled '192.168.9.154 - PuTTY'. The session starts with 'login as: group10'. The terminal then displays a multi-line banner message:

```

#####
#           BE ADVISED. BE ADVISED. A LEGITIMATE      #
#           USER ONLY AUTHORISED TO ACCESS TO        #
#           THIS DEVICE                                #
#####
#           GROUP 10                                    #
#####
group10@192.168.9.154's password:
#####
#           WELCOME                                     #
#           #                                         #
#           #                                         #
#####
#           GROUP 10                                    #
#####

```

Finally, the prompt 'Group10Switch#ena' is shown at the bottom, indicating a successful login.

**Figure 6.2.96 SSH testing on Switch**

### **Step 3 : Fedora server testing Using Putty**

- a)Insert ip address fedora at putty “192.168.9.138”
- b)Log in as “group10” and password on fedora server “asd123”

```
group10@Nuqman:~$  
login as: group10  
group10@192.168.9.138's password:  
Last login: Thu Dec  6 12:36:08 2018  
[group10@Nuqman ~]$
```

*Figure 6.2.97 SSH testing on fedora server*

### **Step 4: Ubuntu server testing Using Putty**

- a)Insert ip address ubuntu at putty “192.168.9.146”
- b)Log in as “group10” and password on ubuntu server “asd123”

```
group10@group10: ~$  
login as: group10  
Using keyboard-interactive authentication.  
Password:  
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.15.0-39-generic x86_64)  
  
 * Documentation: https://help.ubuntu.com  
 * Management: https://landscape.canonical.com  
 * Support: https://ubuntu.com/advantage  
  
0 packages can be updated.  
0 updates are security updates.  
  
You have mail.  
Last login: Fri Dec  7 08:37:15 2018 from 192.168.9.138  
group10@group10:~$
```

*Figure 6.2.98 SSH testing on ubuntu*

## Step 5 : Ubuntu Server Testing

- a)Open the terminal and type the command “ sudo systemctl status ssh” Make sure the ssh in active (running) in Ubuntu server

```
group10@group10:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enab
  Active: active (running) since Jun 2016-02-12 01:38:46 +08; 4min 4s ago
    Main PID: 13723 (sshd)
   CGroup: /system.slice/ssh.service
           └─13723 /usr/sbin/sshd -D

Feb 12 01:38:46 group10.com systemd[1]: Starting OpenBSD Secure Shell server...
Feb 12 01:38:46 group10.com sshd[13723]: Server listening on 0.0.0.0 port 22.
Feb 12 01:38:46 group10.com sshd[13723]: Server listening on :: port 22.
Feb 12 01:38:46 group10.com systemd[1]: Started OpenBSD Secure Shell server.

[1]+  Stopped                  sudo systemctl status ssh
group10@group10:~$
```

*Figure 6.2.99 check status on ubuntu server*

- b)Ping the fedora server with ip “192.168.9.138” to test connection between server.

- c)Type “ssh group10@192.168.9.138” to open fedora server

- d)Ubuntu server sucessfully log in into fedora server “[group10@Nuqman~]”

```
group10@group10:~$ ping 192.168.9.138
PING 192.168.9.138 (192.168.9.138) 56(84) bytes of data.
64 bytes from 192.168.9.138: icmp_seq=1 ttl=63 time=1.02 ms
64 bytes from 192.168.9.138: icmp_seq=2 ttl=63 time=1.05 ms
^C
--- 192.168.9.138 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.027/1.042/1.057/0.015 ms
group10@group10:~$ ssh group10@Nuqman
ssh: Could not resolve hostname nuqman: Temporary failure in name resolution
group10@group10:~$ ssh group10@192.168.9.138
group10@192.168.9.138's password:
Last login: Mon Oct 22 16:06:34 2018
```

*Figure 6.2.100 log in fedora server using SSH on ubuntuserver*

- e)At home fedora server, create folder “B031610046\_zannah” and create file “bengkel2.txt”

```
[group10@Nuqman ~]$ mkdir B031610046_zannah
[group10@Nuqman ~]$ cd B031610046_zannah
[group10@Nuqman B031610046_zannah]$ nano bengkel2.txt
[group10@Nuqman B031610046_zannah]$ nano bengkel2.txt
[group10@Nuqman B031610046_zannah]$ █
```

Figure 6.2.101 create folder in fedora server using SSH on ubuntuserver

f)To check whether the created file success or not using ssh, go to PC fedora server and check that folder and file

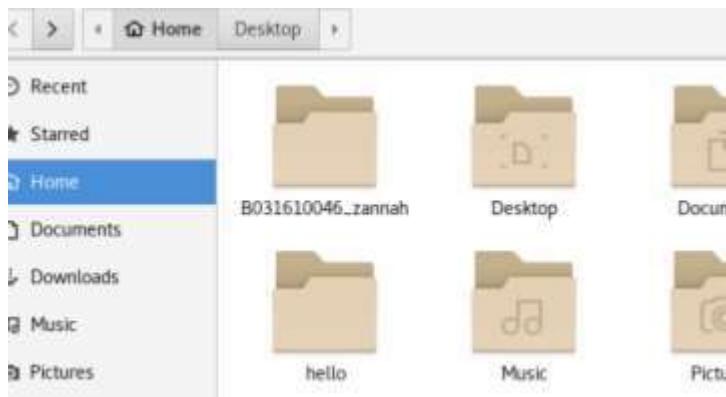


Figure 6.2.102 folder successfully created



Figure 6.2.103 file successfully created

## Step 6 : Fedora Server Testing

- a)Open the terminal and type the command “ sudo systemctl start sshd” and “systemctl status sshd” to make sure the ssh is active(running) in Fedora Server

```
[root@Nuqman ~]# systemctl start sshd
[root@Nuqman ~]# systemctl status sshd
● sshd.service - OpenSSH server daemon
  Loaded: loaded (/usr/lib/systemd/system/sshd.service; disabled; vendor prese>
  Active: active (running) since Mon 2018-10-22 16:35:11 +08; 18s ago
    Docs: man:sshd(8)
          man:sshd_config(5)
  Main PID: 2951 (sshd)
    Tasks: 1 (limit: 4449)
   Memory: 2.2M
  CGroup: /system.slice/sshd.service
          └─2951 /usr/sbin/sshd -D -oCiphers=aes256-gcm@openssh.com,chacha20-p>

Oct 22 16:35:11 Nuqman systemd[1]: Starting OpenSSH server daemon...
Oct 22 16:35:11 Nuqman sshd[2951]: Server listening on 0.0.0.0 port 22.
Oct 22 16:35:11 Nuqman sshd[2951]: Server listening on :: port 22.
Oct 22 16:35:11 Nuqman systemd[1]: Started OpenSSH server daemon.
Lines 1-15/15 (END)
```

Figure 6.2.104 to start the service ssh

- b)Type “ssh group10@192.168.9.146” to open ubuntu server

- c)Ubuntu server sucessfully log in into fedora server “

```
[group10@Nuqman ~]$ ssh group10@192.168.9.146
group10@192.168.9.146's password:
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.10.0-28-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

24 packages can be updated.
11 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

group10@group10:~$
```

group10@group10:~“

*Figure 6.2.105 open ubuntu server with ssh*

- d) At Documents ubuntu server, create folder “Workshop2\_zannah” and create file “b031610046.txt”

```
group10@group10:~$ cd Documents
group10@group10:~/Documents$ mkdir Workshop2_zannah
group10@group10:~/Documents$ cd Workshop2_zannah
group10@group10:~/Documents/Workshop2_zannah$ nano b031610046.txt
group10@group10:~/Documents/Workshop2_zannah$ █
```

*Figure 6.2.106 create the new folder*

```
group10@group10: ~/Documents/Workshop2_zannah
File Edit View Search Terminal Help
GNU nano 2.5.3           File: b031610046.txt           Modified
Hai..This is my file i created from ubuntu at fedora...█
```

*Figure*

*6.2.107 insert any word in text file*

- e) Check at PC ubuntu server that folder and file created success or not



*Figure 6.2.108 check the created file at PC ubuntu server*

f) The file success created and can check the contain in text file



*Figure 6.2.109 to check word in text file*

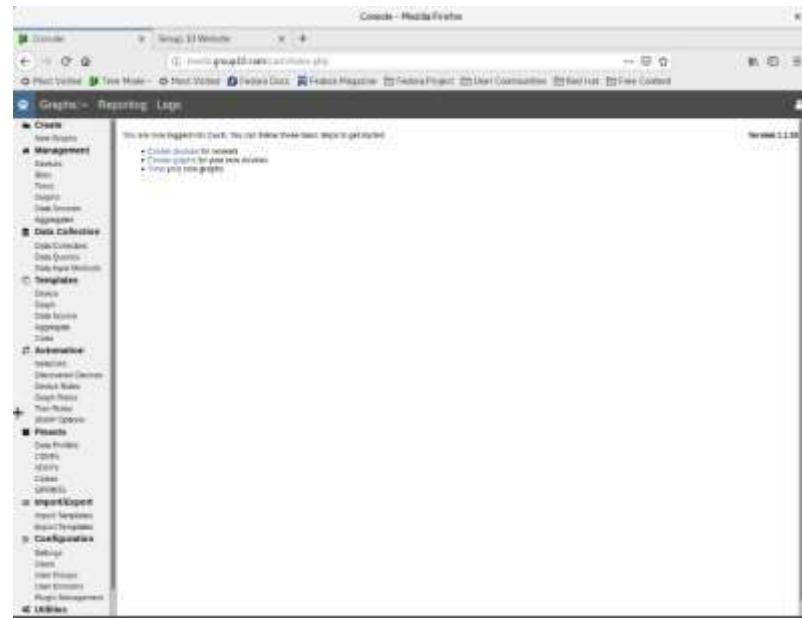
### **6.2.15 Network Management System**

1. Login to Cacti by entering the username and password



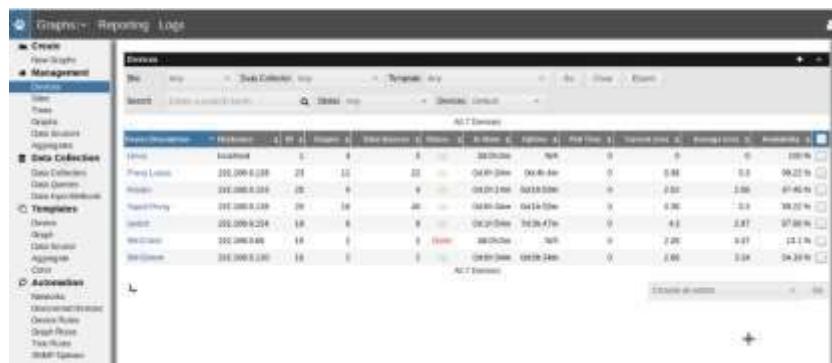
**Figure 6.2.110 show Login Page to Cacti**

2. Main Page for Cacti and each function is display on the left side



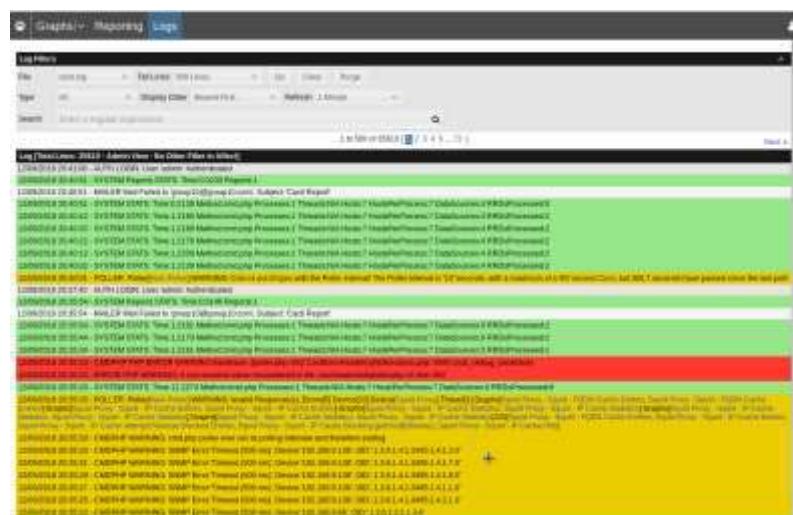
**Figure 6.2.111 show the Main Page of Cacti**

### 3. All device connected to Cacti including its details



**Figure 6.2.112 show the Device Connected to Cacti**

#### 4. Cacti Logs displaying all Logs that have been refresh in one minute



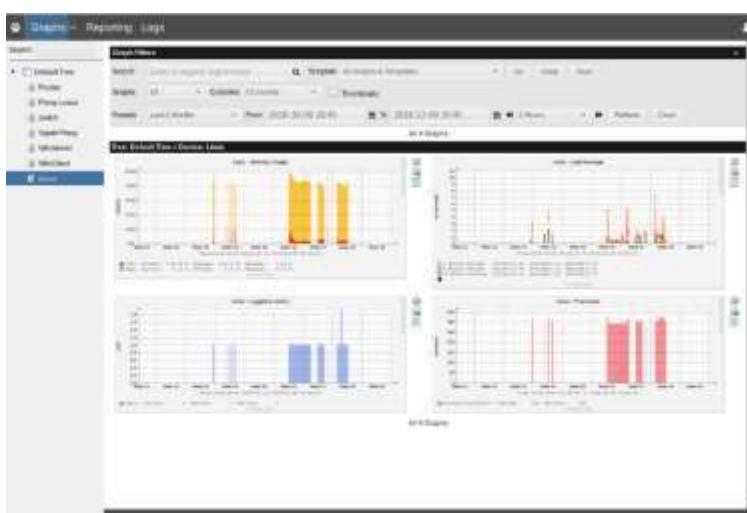
**Figure 6.2.113 show Cacti Logs**

## 5. Cacti displaying the default tree graph showing Linux



**Figure 6.2.114 show Default Tree Graph for Linux**

6. Cacti displaying the device of Linux graph



**Figure 6.2.115 show graph of Linux**

7. Cacti displaying the device of Windows Client graph



Figure 6.2.116 show graph of Windows Client

8. Cacti displaying the device of Windows Server graph



Figure 6.2.117 show graph of Windows Server

9. Cacti displaying the device of Switch graph



Figure 6.2.118 show graph of Switch

## 6.2.16 Port Security

**Step 1:** Used ping command to try connectivity between hosts. This to ensure that port security on port switch would frame receive data.

**Step 2:** Used command *show port security address* to display the type which is secure sticky

```
Group10Switch#sh port-security address
  Secure Mac Address Table

-----  
Vlan   Mac Address      Type            Ports      Remaining Age  
          (mins)  
-----  
 10    0015.5d09.8200  SecureSticky    Fa0/2      -  
 10    00ae.75b9.8293  SecureSticky    Fa0/2      -  
 10    6400.6a59.0afd  SecureSticky    Fa0/2      -  
 10    90b1.1c81.7172  SecureSticky    Fa0/2      -  
 10    da50.7abc.40d5  SecureSticky    Fa0/2      -  
 10    da89.b2d5.6d50  SecureSticky    Fa0/2      -  
 20    90b1.1c81.7068  SecureSticky    Fa0/3      -  
 30    90b1.1c81.7172  SecureSticky    Fa0/5      -  
 30    a08c.fd7f.6df6  SecureSticky    Fa0/5      -  
 40    6400.6a59.1634  SecureSticky    Fa0/7      -  
 80    90b1.1c81.7172  SecureSticky    Fa0/9      -  
-----  
Total Addresses in System (excluding one mac per port) : 6  
Max Addresses limit in System (excluding one mac per port) : 8192  
Group10Switch#
```

Figure 6.2.119 To display Mac Address

**Step 3:** Used command *show port security* to display list of port which is have been assigned and their security action.

```
Group10Switch#sh port-security
  Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action  
          (Count)        (Count)        (Count)  
-----  
  Fa0/1       5             0             0             Shutdown  
  Fa0/2       10            6             0             Shutdown  
  Fa0/3       1             1             0             Protect  
  Fa0/4       1             0             0             Protect  
  Fa0/5       2             2             0             Protect  
  Fa0/6       2             0             0             Protect  
  Fa0/7       1             1             0             Protect  
  Fa0/8       1             0             0             Protect  
  Fa0/9       1             1             0             Protect  
  Fa0/10      1             0             0             Protect  
  Fa0/11      1             0             0             Protect  
  Fa0/12      1             0             0             Protect  
  Fa0/13      1             0             0             Protect  
  Fa0/14      1             0             0             Protect  
-----  
Total Addresses in System (excluding one mac per port) : 6  
Max Addresses limit in System (excluding one mac per port) : 8192  
Group10Switch#
```

Figure 6.2.120 To display the Secure port

**Step 4:** To display port security information about specific interface ,used command *show port-security interface fa0/5* .

```
Group10Switch#show port-security interface fa0/5
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode        : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 2
Total MAC Addresses   : 1
Configured MAC Addresses : 0
Sticky MAC Addresses  : 1
Last Source Address:Vlan : 90b1.1c81.7172:30
Security Violation Count : 0
```

```
Group10Switch#
```

*Figure 6.2.121 To display port security information*

**Step 5:** To display port security information about specific interface used command *show port-security interface fa0/5*.

```
Group10Switch#sh port-security interface fa0/5
Port Security          : Enabled
Port Status            : Secure-down
Violation Mode        : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 2
Total MAC Addresses   : 1
Configured MAC Addresses : 0
Sticky MAC Addresses  : 1
Last Source Address:Vlan : 90b1.1c81.7172:30
Security Violation Count : 0
```

*Figure 6.2. 122 To display port security information*

## 6.2.17 Linux Server Hardening

### 6.2.17.1 Testing Ubuntu Server hardening

#### 1. System update

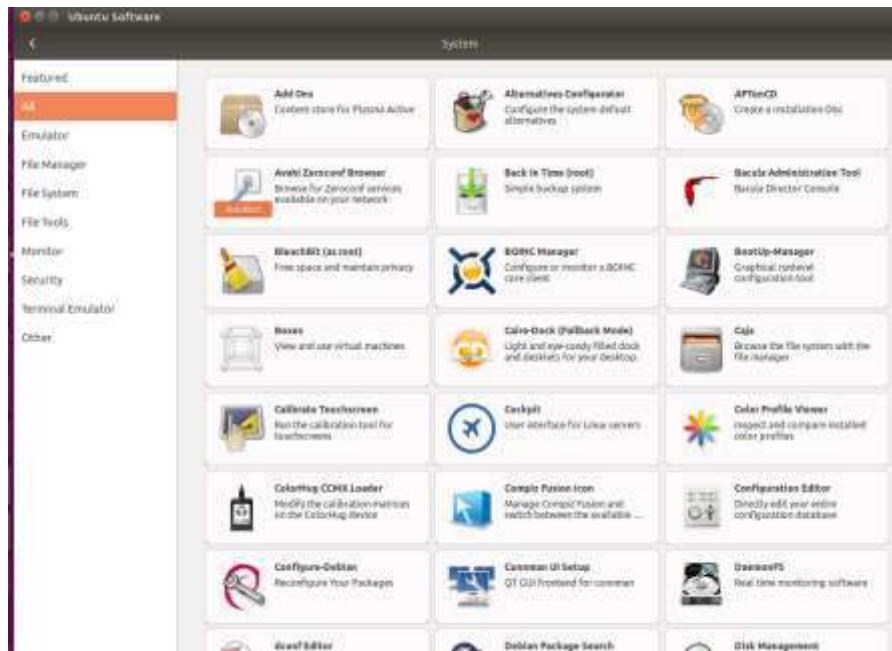


Figure 6.2.123 system update

## 2. Check disable service

```
root@group10:~# echo "manual">> /etc/init/cups.override
root@group10:~# sudo service cups stop
root@group10:~# nmap -v -sT localhost

Starting Nmap 7.01 ( https://nmap.org ) at 2018-12-07 11:32 +08
Initiating Connect Scan at 11:32
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 22/tcp on 127.0.0.1
Discovered open port 143/tcp on 127.0.0.1
Discovered open port 3306/tcp on 127.0.0.1
Discovered open port 53/tcp on 127.0.0.1
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 587/tcp on 127.0.0.1
Discovered open port 993/tcp on 127.0.0.1
Discovered open port 25/tcp on 127.0.0.1
Completed Connect Scan at 11:32, 0.01s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000073s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
143/tcp   open  imap
587/tcp   open  submission
993/tcp   open  imaps
3306/tcp  open  mysql

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
root@group10:~# █
```

Figure 6.2.124 To display port have disable

## 3. Check password change

```
group10@group10:~$ sudo chage -l group10
[sudo] password for group10:
Last password change : Nov 26, 2018
Password expires     : Mei 25, 2019
Password inactive    : Jun 24, 2019
Account expires       : Jun 10, 2036
Minimum number of days between password change : 0
Maximum number of days between password change : 180
Number of days of warning before password expires : 14
group10@group10:~$ █
```

Figure 6.2.125 To display password information

## 4. Check disable bluetooth

```
group10@group10:~$ sudo service bluetooth status
● bluetooth.service - Bluetooth service
  Loaded: loaded (/lib/systemd/system/bluetooth.service; enabled; vendor preset: enabled)
  Active: inactive (dead)
    Docs: man:bluetoothd(8)
group10@group10:~$ █
```

Figure 6.2.126 check status bluetooth

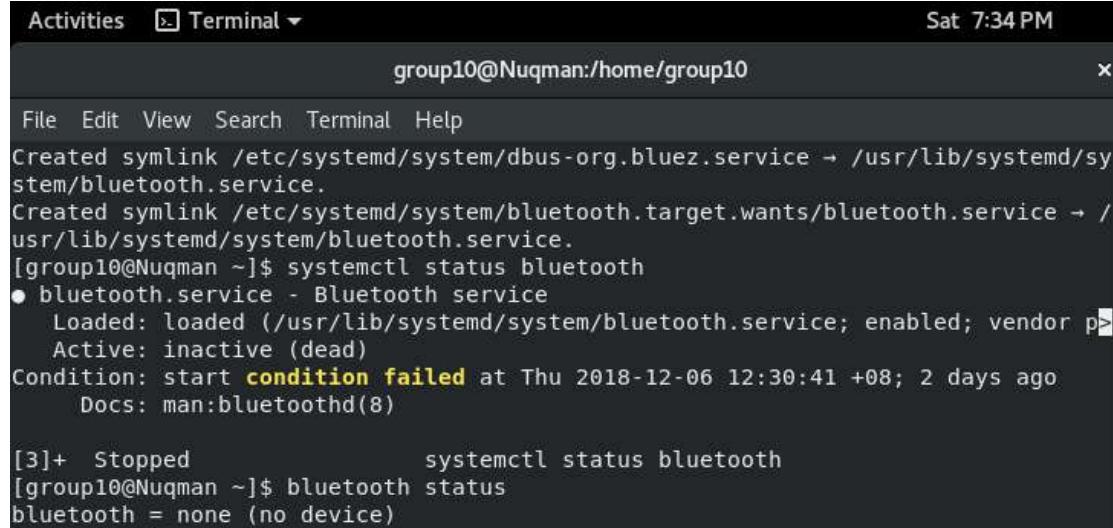
### 6.2.19.2 Testing Fedora Server

#### 1. Check password change

```
[root@Nuqman ~]# chage -l group10
Last password change : Dec 30, 2018
Password expires     : Jan 29, 2019
Password inactive   : Feb 28, 2019
Account expires      : Apr 04, 2019
Minimum number of days between password change : 5
Maximum number of days between password change : 30
Number of days of warning before password expires : 25
```

Figure 6.2.127 To display password information

#### 2. Check disable bluetooth



The screenshot shows a terminal window titled "group10@Nuqman:/home/group10". The window title bar also displays the date and time as "Sat 7:34 PM". The terminal content includes:

```
File Edit View Search Terminal Help
Created symlink /etc/systemd/system/dbus-org.bluez.service → /usr/lib/systemd/system/bluetooth.service.
Created symlink /etc/systemd/system/bluetooth.target.wants/bluetooth.service → /usr/lib/systemd/system/bluetooth.service.
[group10@Nuqman ~]$ systemctl status bluetooth
● bluetooth.service - Bluetooth service
  Loaded: loaded (/usr/lib/systemd/system/bluetooth.service; enabled; vendor p>
  Active: inactive (dead)
Condition: start condition failed at Thu 2018-12-06 12:30:41 +08; 2 days ago
  Docs: man:bluetoothd(8)

[3]+  Stopped                  systemctl status bluetooth
[group10@Nuqman ~]$ bluetooth status
bluetooth = none (no device)
```

Figure 6.2.128 To display status bluetooth

#### 4. Scanning the port and service

```
[root@Nuqman ~]# nmap -v -sT localhost
Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-29 12:47 +08
Initiating Connect Scan at 12:47
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 22/tcp on 127.0.0.1
Discovered open port 3306/tcp on 127.0.0.1
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 199/tcp on 127.0.0.1
Discovered open port 631/tcp on 127.0.0.1
Completed Connect Scan at 12:47, 0.04s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00027s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
199/tcp   open  smux
631/tcp   open  ipp
3306/tcp  open  mysql

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
  Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
[root@Nuqman ~]# █
```

*Figure 6.2.129 port scanning*

## 6.2.18 Intrusion Detection System (IDS) & Port Mirror

### Intrusion Detection System Testing

**Step 1** :Start Snort service and check status snort

**Step 2** :Verify snort installation using *snort -V*

```
=====
Snort exiting
group10@group10:~/snort_src$ udo nano /lib/systemd/system/snort.service
The program 'udo' is currently not installed. You can install it by typing:
sudo apt install udo
group10@group10:~/snort_src$ sudo nano /lib/systemd/system/snort.service
group10@group10:~/snort_src$ sudo systemctl daemon-reload
group10@group10:~/snort_src$ sudo systemctl start snort
group10@group10:~/snort_src$ sudo systemctl status snort
● snort.service - Snort NIDS Daemon
  Loaded: loaded (/lib/systemd/system/snort.service; disabled; vendor preset: e
  Active: active (running) since Isn 2018-10-29 21:32:07 UTC; 8s ago
    Main PID: 5649 (snort)
      CGroup: /system.slice/snort.service
              └─5649 /usr/local/bin/snort -q -u snort -g snort -c /etc/snort/snort.

okt 29 21:32:07 group10 systemd[1]: Started Snort NIDS Daemon.

group10@group10:~/snort_src$
```

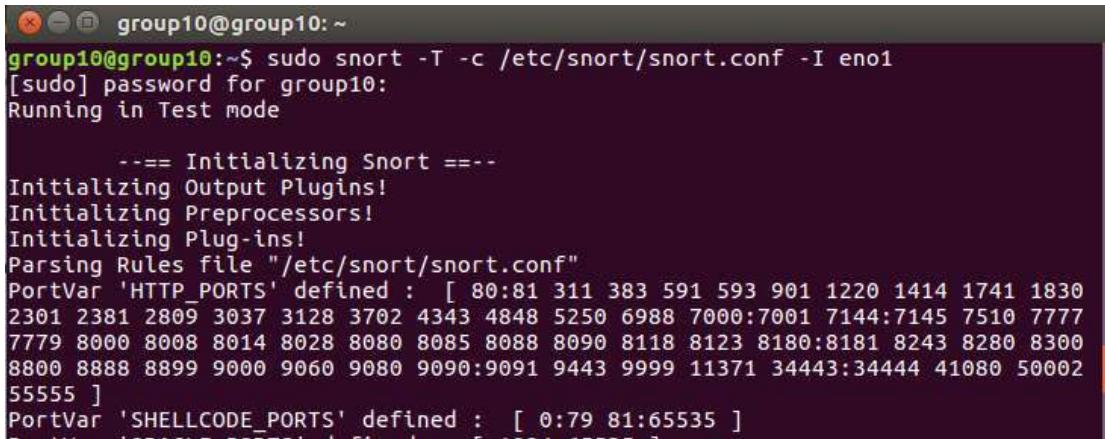
Figure 6.2.130 run command check status snort

```
group10@group10:~/snort_src/snort-2.9.12$ snort -V
      -*> Snort! <*-
o",,-~ Version 2.9.12 GRE (Build 325)
     By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
     Copyright (C) 2014-2018 Cisco and/or its affiliates. All rights reserved.
     Copyright (C) 1998-2013 Sourcefire, Inc., et al.
     Using libpcap version 1.7.4
     Using PCRE version: 8.38 2015-11-23
     Using ZLIB version: 1.2.8

group10@group10:~/snort_src/snort-2.9.12$
```

Figure 6.2.131 Check verifying of snort

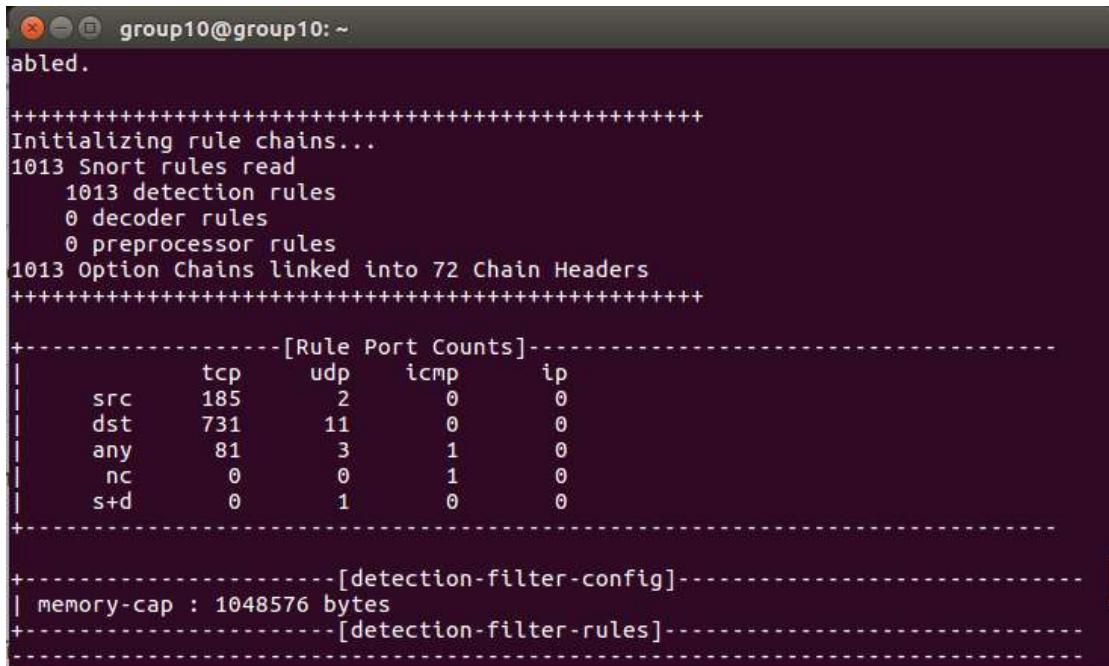
**Step 3:** Test configuration file using `sudo snort -T -c /etc/snort/snort.conf -I eno1`



```
group10@group10:~$ sudo snort -T -c /etc/snort/snort.conf -I eno1
[sudo] password for group10:
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 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 'SHELLCODE_PORTS' defined : [ 0:79 81:65535 ]
```

Figure 6.2.131 Test the configuration file



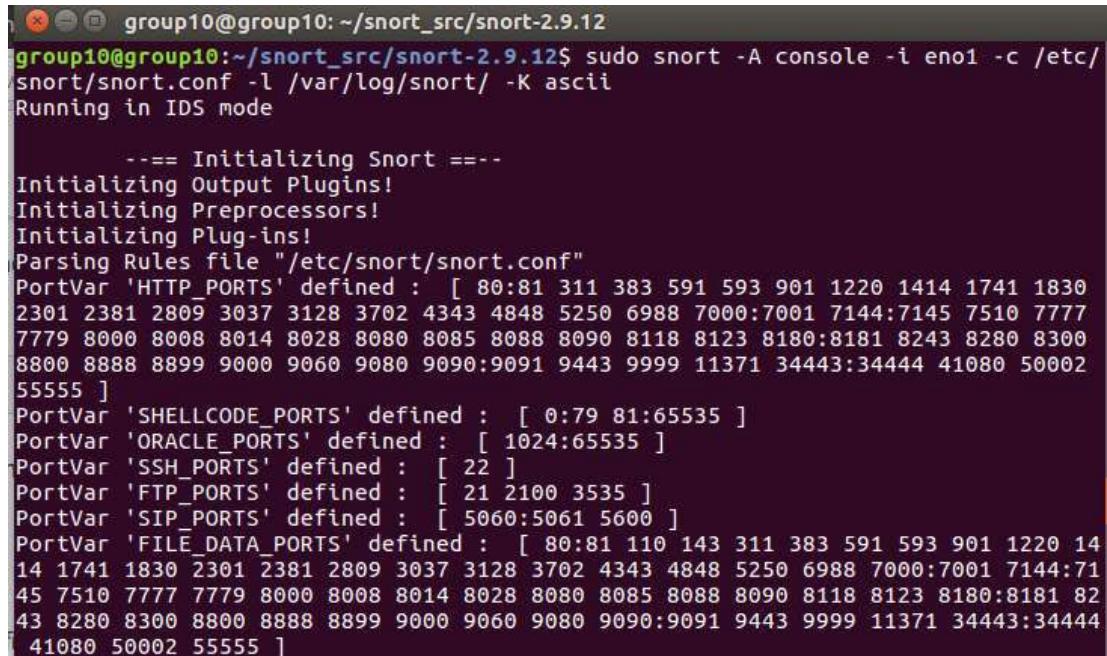
```
group10@group10:~$ sudo snort -T -c /etc/snort/snort.conf -I eno1
[...]
abled.

+++++
Initializing rule chains...
1013 Snort rules read
  1013 detection rules
    0 decoder rules
    0 preprocessor rules
1013 Option Chains linked into 72 Chain Headers
++++

-----[Rule Port Counts]-----
|      tcp      udp      icmp      ip
| src    185       2        0        0
| dst    731      11        0        0
| any     81       3        1        0
| nc      0        0        1        0
| s+d     0        1        0        0
+-----[detection-filter-config]-----
| memory-cap : 1048576 bytes
+-----[detection-filter-rules]-----
|
```

Figure 6.2.132 Test snort

**Step 4** :Run snort in console mode



```
group10@group10:~/snort_src/snort-2.9.12$ sudo snort -A console -i eno1 -c /etc/snort/snort.conf -l /var/log/snort/ -K ascii
Running in IDS mode

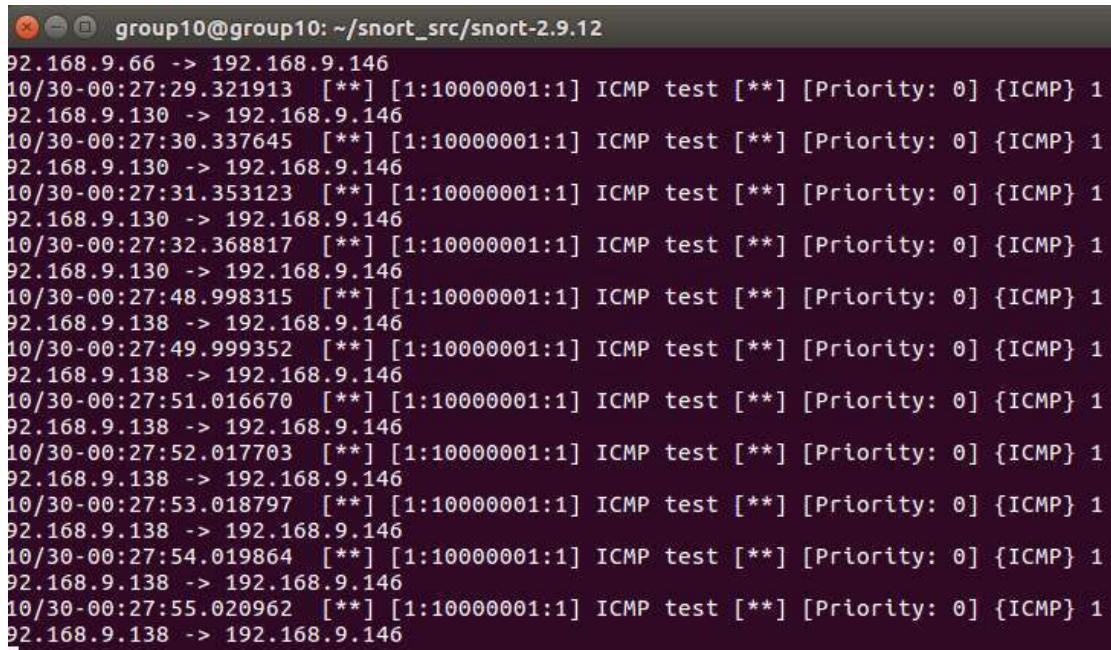
     === Initializing Snort ===
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined : [ 80:81 311 383 591 593 901 1220 1414 1741 1830
2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 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 '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 14
14 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:71
45 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 82
43 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444
41080 50002 55555 ]
```

Figure 6.2.133 Run Snort in Console mode

**Step 5** :Using `sudo snort -A console -i eno1 -c /etc/snort/snort.conf -l /var/log/snort/ -K ascii` command in Ubuntu while ping 192.168.9.130 from Window Server.

- `-A console` means that messages will show up on screen
- `-i eno1` specifies the interface snort is listening on
- `-c /etc/snort/snort.conf` specifies the configuration file you are running. This would include the custom snort rules that were added earlier.
- `-l /var/log/snort` specifies the directory where the logs will be located
- `-K ascii` specifies how the log files will be written. Ascii can easily be opened up by a text editor or by the command “`cat`”.

**Step 6** :The system sucessfully detect.



```
group10@group10: ~/snort_src/snort-2.9.12
92.168.9.66 -> 192.168.9.146
10/30-00:27:29.321913 [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 1
92.168.9.130 -> 192.168.9.146
10/30-00:27:30.337645 [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 1
92.168.9.130 -> 192.168.9.146
10/30-00:27:31.353123 [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 1
92.168.9.130 -> 192.168.9.146
10/30-00:27:32.368817 [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 1
92.168.9.130 -> 192.168.9.146
10/30-00:27:48.998315 [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 1
92.168.9.138 -> 192.168.9.146
10/30-00:27:49.999352 [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 1
92.168.9.138 -> 192.168.9.146
10/30-00:27:51.016670 [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 1
92.168.9.138 -> 192.168.9.146
10/30-00:27:52.017703 [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 1
92.168.9.138 -> 192.168.9.146
10/30-00:27:53.018797 [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 1
92.168.9.138 -> 192.168.9.146
10/30-00:27:54.019864 [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 1
92.168.9.138 -> 192.168.9.146
10/30-00:27:55.020962 [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 1
92.168.9.138 -> 192.168.9.146
```

*Figure 6.2.144 Check test Detection ICMP*

```

Copyright (C) 2014-2018 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.7.4
Using PCRE version: 8.38 2015-11-23
Using ZLIB version: 1.2.8

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SOF Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>

Commencing packet processing (pid=17688)
12/01/09:08:18.195454 [**] [1:18000008:0] HTTP Packet Found [**] [Priority: 0] [TCP] 2007:facc:3::2:33622 -> 2007:facc:2::2:80
12/01/09:08:19.197291 [**] [1:18000008:0] HTTP Packet Found [**] [Priority: 0] [TCP] 2007:facc:3::2:33622 -> 2007:facc:2::2:80
12/01/09:08:21.245290 [**] [1:18000008:0] HTTP Packet Found [**] [Priority: 0] [TCP] 2007:facc:3::2:33622 -> 2007:facc:2::2:80
12/01/09:08:23.531796 [**] [1:18000001:1] Window Server [**] [Priority: 0] [ICMP] 192.168.9.130 -> 192.168.9.146
12/01/09:08:23.531920 [**] [1:18000001:1] Window Server [**] [Priority: 0] [ICMP] 192.168.9.130 -> 192.168.9.146
12/01/09:08:23.532146 [**] [1:18000001:1] Window Server [**] [Priority: 0] [ICMP] 192.168.9.146 -> 192.168.9.130
12/01/09:08:23.532234 [**] [1:18000001:1] Window Server [**] [Priority: 0] [ICMP] 192.168.9.146 -> 192.168.9.130
12/01/09:08:24.548443 [**] [1:18000001:1] Window Server [**] [Priority: 0] [ICMP] 192.168.9.130 -> 192.168.9.146
12/01/09:08:24.548593 [**] [1:18000001:1] Window Server [**] [Priority: 0] [ICMP] 192.168.9.130 -> 192.168.9.146
12/01/09:08:24.548773 [**] [1:18000001:1] Window Server [**] [Priority: 0] [ICMP] 192.168.9.146 -> 192.168.9.130
12/01/09:08:24.548785 [**] [1:18000001:1] Window Server [**] [Priority: 0] [ICMP] 192.168.9.146 -> 192.168.9.130
12/01/09:08:25.277224 [**] [1:18000008:0] HTTP Packet Found [**] [Priority: 0] [TCP] 2007:facc:3::2:33622 -> 2007:facc:2::2:80
12/01/09:08:25.559966 [**] [1:18000001:1] Window Server [**] [Priority: 0] [ICMP] 192.168.9.130 -> 192.168.9.146
12/01/09:08:25.560884 [**] [1:18000001:1] Window Server [**] [Priority: 0] [ICMP] 192.168.9.130 -> 192.168.9.146
12/01/09:08:25.560884 [**] [1:18000001:1] Window Server [**] [Priority: 0] [ICMP] 192.168.9.146 -> 192.168.9.130
12/01/09:08:25.560981 [**] [1:18000001:1] Window Server [**] [Priority: 0] [ICMP] 192.168.9.146 -> 192.168.9.130
12/01/09:08:26.585195 [**] [1:18000001:1] Window Server [**] [Priority: 0] [ICMP] 192.168.9.130 -> 192.168.9.146
12/01/09:08:26.585345 [**] [1:18000001:1] Window Server [**] [Priority: 0] [ICMP] 192.168.9.130 -> 192.168.9.146
12/01/09:08:26.585489 [**] [1:18000001:1] Window Server [**] [Priority: 0] [ICMP] 192.168.9.146 -> 192.168.9.130
12/01/09:08:26.585523 [**] [1:18000001:1] Window Server [**] [Priority: 0] [ICMP] 192.168.9.146 -> 192.168.9.130
12/01/09:08:29.108539 [**] [1:18000001:1] Window Server [**] [Priority: 0] [ICMP] 192.168.9.130 -> 192.168.9.146
12/01/09:08:29.166679 [**] [1:18000001:1] Window Server [**] [Priority: 0] [ICMP] 192.168.9.130 -> 192.168.9.146
12/01/09:08:29.166932 [**] [1:18000001:1] Window Server [**] [Priority: 0] [ICMP] 192.168.9.146 -> 192.168.9.130
12/01/09:08:29.168949 [**] [1:18000001:1] Window Server [**] [Priority: 0] [ICMP] 192.168.9.146 -> 192.168.9.130
12/01/09:08:29.197118 [**] [1:10000008:0] HTTP Packet Found [**] [Priority: 0] [TCP] 192.168.9.3:41766 -> 157.240.13.55:80
12/01/09:08:29.278709 [**] [1:18000008:0] HTTP Packet Found [**] [Priority: 0] [TCP] 192.168.9.3:41766 -> 157.240.13.55:80
12/01/09:08:29.346886 [**] [1:18000008:0] HTTP Packet Found [**] [Priority: 0] [TCP] 192.168.9.3:41766 -> 157.240.13.55:80
12/01/09:08:30.126274 [**] [1:18000001:1] Window Server [**] [Priority: 0] [ICMP] 192.168.9.130 -> 192.168.9.146

```

Figure 6.2.145 Check Detection HTTP

```

12/07/08:37:54.550183 [**] [1:18000007:0] SSH Packet found [**] [Priority: 0] [TCP] 192.168.9.138:13760 -> 192.168.9.146:22
12/07/08:37:55.580393 [**] [1:18000012:1] Ubuntu Server pinging Fedora Server [**] [Priority: 0] [ICMP] 192.168.9.146 -> 192.168.9.1
38
12/07/08:37:55.580393 [**] [1:18000002:1] Fedora Server Pinging ubuntu Server [**] [Priority: 0] [ICMP] 192.168.9.146 -> 192.168.9.1
38
12/07/08:37:55.581343 [**] [1:18000012:1] Ubuntu Server pinging Fedora Server [**] [Priority: 0] [ICMP] 192.168.9.138 -> 192.168.9.1
46
12/07/08:37:55.581343 [**] [1:18000002:1] Fedora Server Pinging ubuntu Server [**] [Priority: 0] [ICMP] 192.168.9.138 -> 192.168.9.1
46
12/07/08:37:55.582266 [**] [1:18000007:0] SSH Packet found [**] [Priority: 0] [TCP] 192.168.9.138:13760 -> 192.168.9.146:22
12/07/08:37:55.695337 [**] [1:18000007:0] SSH Packet found [**] [Priority: 0] [TCP] 192.168.9.138:13760 -> 192.168.9.146:22
12/07/08:37:55.696378 [**] [1:18000007:0] SSH Packet found [**] [Priority: 0] [TCP] 192.168.9.138:13760 -> 192.168.9.146:22
12/07/08:37:55.696393 [**] [1:18000007:0] SSH Packet found [**] [Priority: 0] [TCP] 192.168.9.138:13760 -> 192.168.9.146:22
12/07/08:37:55.696969 [**] [1:18000007:0] SSH Packet found [**] [Priority: 0] [TCP] 192.168.9.138:13760 -> 192.168.9.146:22
12/07/08:38:12.615181 [**] [1:18000007:0] SSH Packet found [**] [Priority: 0] [TCP] 192.168.9.138:13760 -> 192.168.9.146:22
12/07/08:38:12.616337 [**] [1:18000007:0] SSH Packet found [**] [Priority: 0] [TCP] 192.168.9.138:13760 -> 192.168.9.146:22
12/07/08:38:16.615094 [**] [1:18000007:0] SSH Packet found [**] [Priority: 0] [TCP] 192.168.9.138:13760 -> 192.168.9.146:22
12/07/08:38:16.616308 [**] [1:18000007:0] SSH Packet found [**] [Priority: 0] [TCP] 192.168.9.138:13760 -> 192.168.9.146:22
12/07/08:38:16.942654 [**] [1:18000007:0] SSH Packet found [**] [Priority: 0] [TCP] 192.168.9.138:13760 -> 192.168.9.146:22
12/07/08:38:16.943884 [**] [1:18000007:0] SSH Packet found [**] [Priority: 0] [TCP] 192.168.9.138:13760 -> 192.168.9.146:22
12/07/08:38:17.670953 [**] [1:18000007:0] SSH Packet found [**] [Priority: 0] [TCP] 192.168.9.138:13760 -> 192.168.9.146:22

```

Figure 6.2.146 Check Detection SSH

```
group10@group10:~$ sudo ls /var/log/snort
192.168.9.130      snort.log.1542233021  snort.log.1542233460
192.168.9.138      snort.log.1542233246  snort.log.1542233489
192.168.9.146      snort.log.1542233270  snort.log.1542233515
192.168.9.66       snort.log.1542233272  snort.log.1542233625
snort.log.1540848238  snort.log.1542233329  snort.log.1542233993
snort.log.1540848727  snort.log.1542233417  snort.log.1542234125
snort.log.1541024190  snort.log.1542233457
group10@group10:~$ sudo ls /var/log/snort/192.168.9.66
ICMP_ECHO  ICMP_ECHO_REPLY
group10@group10:~$
```

Figure 6.2.147 Command to check the save log file

### 6.2.19 Router Hardening

- **Password Encryptions**

**Step 1:** Login to router device. Type **show run** to check the password encryptions service on device.

```
! username group10 privilege 15 secret 5 $1$w8Fx$QpefyR51M2Oq6r34Nre4c0
```

Figure 6.2.148 Password Encryptions Router

- **Password minimal length**

**Step 1:** Login to router device. Type **show run** to check the password minimal length service on device.

```
security passwords min-length 8
```

Figure 6.2.149 Password Minimal Length Router

- **Login Failure**

**Step 1** Login to router device. Type **show run** to check the login failure service on device.

```
security authentication failure rate 3 log
```

Figure 6.2.150 Login Failure Router

- **Password implementation at line console**

**Step 1** Login to router device. Type **show run** to check the login failure service on device.

```
! line con 0
  exec-timeout 3 0
  password 7 01322717480F025E731F1A5C
  logging synchronous
```

Figure 6.2.151 Password implementation at line console

- **Execution timeout for 3 minutes**

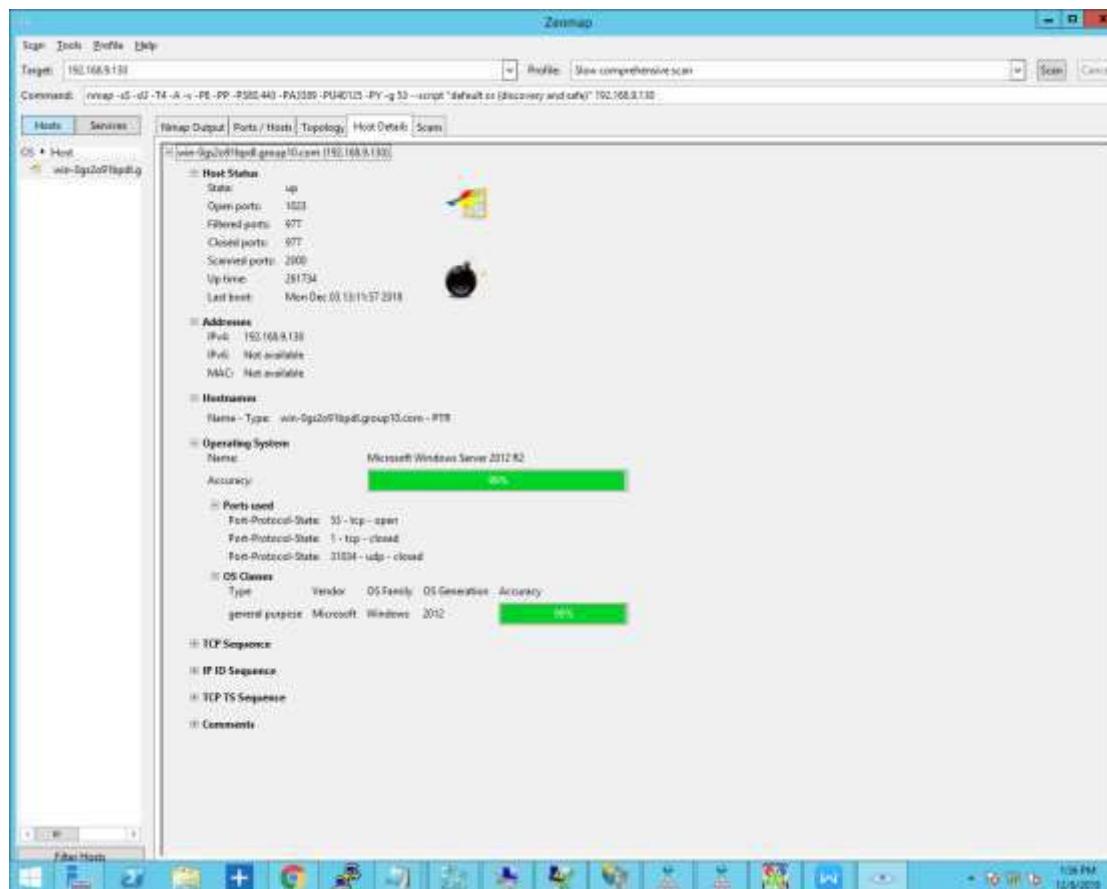
**Step 1 :** Login to router device. Type **show run** to check the login failure service on device.

```
exec-timeout 3 0
```

Figure 6.2.152 Execution timeout for 3 minutes Router

## Testing For Window Server Hardening

Step 1: Open Zenmap to scan port



**Figure 6.2.153 Port scanning status**

As shown in the result in Figure , 1000 ports were scanned, 21 ports were opened, 0 ports were closed and 976 ports were filtered before hardening process. The ports are opened means that an application is actively accepting TCP connection. Besides, it shows services available for use on the network. A closed port means it is accessible but there is no application listening on it. Filtered ports that Nmap cannot determine whether the port is opened or closed because packet filtering prevents its probes from reaching the port.

The open ports are explained as the following:

- Port 53

Used by TCP/ UDP protocol for DNS is used for domain name resolution.

- Port 80,443,992,5555

Used by TCP/ UDP protocol for Hypertext Transfer Protocol(HTTP)

- Port 443

Used by TCP for HTTP services for IIS

- Port 88

Used by TCP/ UDP protocol for Kerberos authentication system.

- Port 135, 49153,49154,49155, 49158

Used by TCP/ UDP protocol for Microsoft EPMAP( End Point Mapper), also known as DCE/RPC Locator Service, used to remotely manage services including DHCP server, DNS server and WINS.

Also used by DCOM.

- Port 139

Used by TCP/ UDP protocol for NetBIOS session Service.

- Port 389, 636, 3268, 3269

Used by TCP for Lightweight Directory Access Protocol services (LDAP). LDAP is an Internet protocol used by MS Active Directory, as well as some email programs to look up contact information from a server.

- Port 445

Used by TCP for Microsoft-DS services. It is used for direct TCP/IP MS Networking access without the need for a NetBIOS layer.

- Port 464

Used by TCP/ UDP protocol for Kerberos password

- Port 593, 49157

Used for ncacn\_http that identifies the Microsoft Internet Information Server (IIS) as the protocol family for the endpoint.

### 6.2.21 Authentication user by Integrating AD with Linux

1. After reboot, select the login. Enter the username and password of active directory account. Login successful.

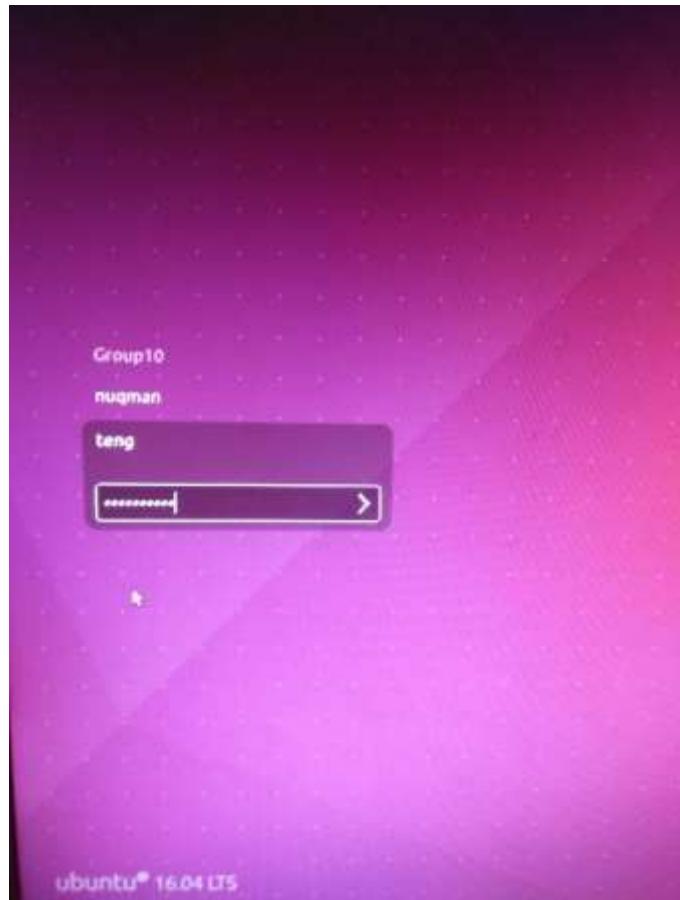
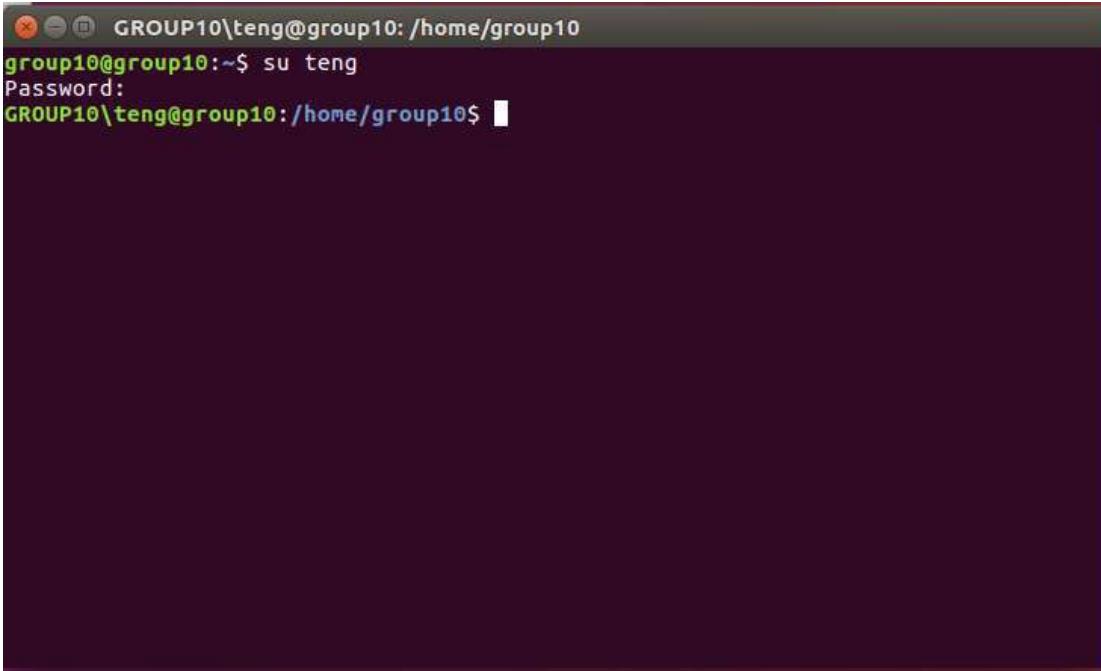


Figure 6.2.154: Login page (Ubuntu)

2. Successfully change user to Active Directory account.



GROUP10\teng@group10: /home/group10  
group10@group10:~\$ su teng  
Password:  
GROUP10\teng@group10:/home/group10\$

Figure 6.2.155: Change to Active Directory user (Ubuntu)

3. Join in Active Directory domain.

```
[group10@Nuqman ~]$ realm join Group10.com  
Password for Administrator:  
[group10@Nuqman ~]$
```

Figure 6.2. 156: Join Active Directory (Fedora)

4. Verify it's possible to get an Active Directory user info or not.

```
[group10@Nuqman ~]$ id GROUP10\\Administrator  
uid=919400500(administrator@groupl0.com) gid=919400513(domain users@groupl0.com) groups=919400513  
(domain users@groupl0.com),919400512(domain admins@groupl0.com),919400519(enterprise admins@groupl0.com),919400520(group policy creator owners@groupl0.com),919400572(denied rodc password replication group@groupl0.com),919400518(schema admins@groupl0.com)
```

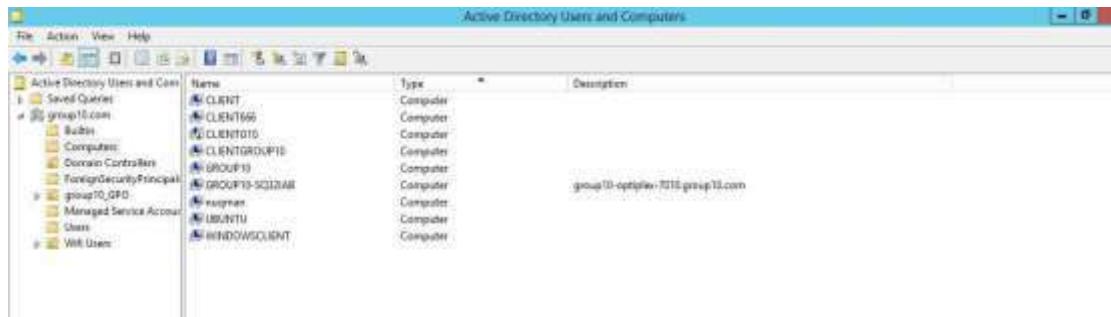
Figure 6.2. 157: Check Active Directory group (Fedora)

5. Verify it's possible to switch to an Active Directory user or not.

```
[group10@Nuqman ~]$ su GROUP10\\Administrator  
Password:  
[administrator@groupl0.com@Nuqman group10]$
```

Figure 6.2. 158: Change to Active Directory (Fedora)

6. On the Window Server side, we can see how many pc is connected.

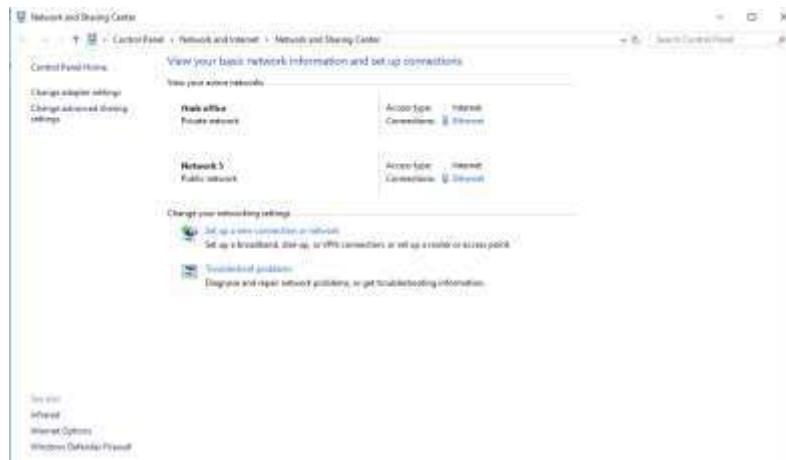


**Figure 6.2.159: Window Server Active Directory Users and Computers**

### 6.2.22 IPSec

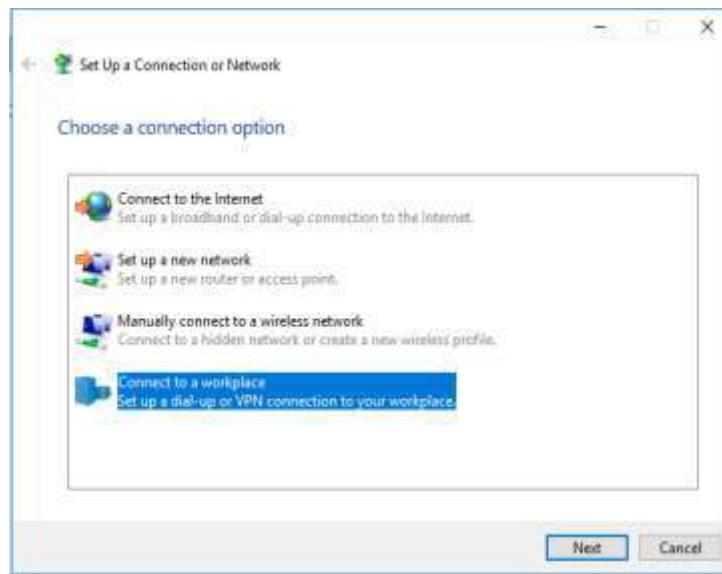
#### Testing IPSec VPN for remote employee

1. Open Network and Sharing Center > Set up a new connection or network.



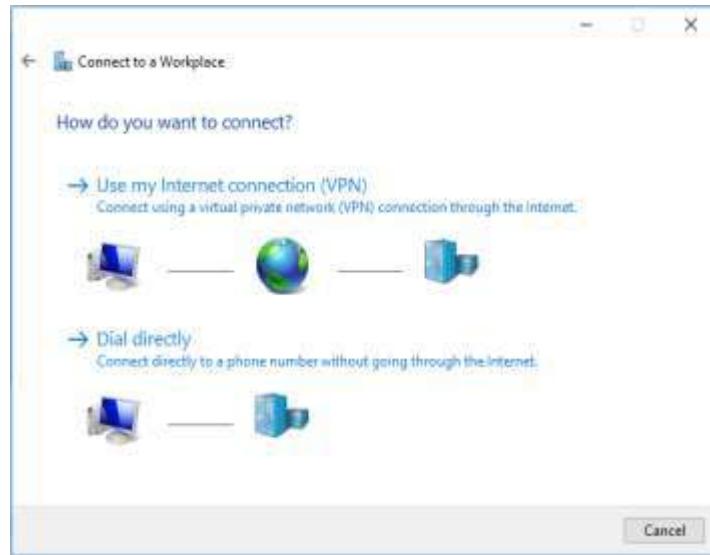
*Figure 6.2.160: Set up a new connection*

2. Choose to connect to a workplace.



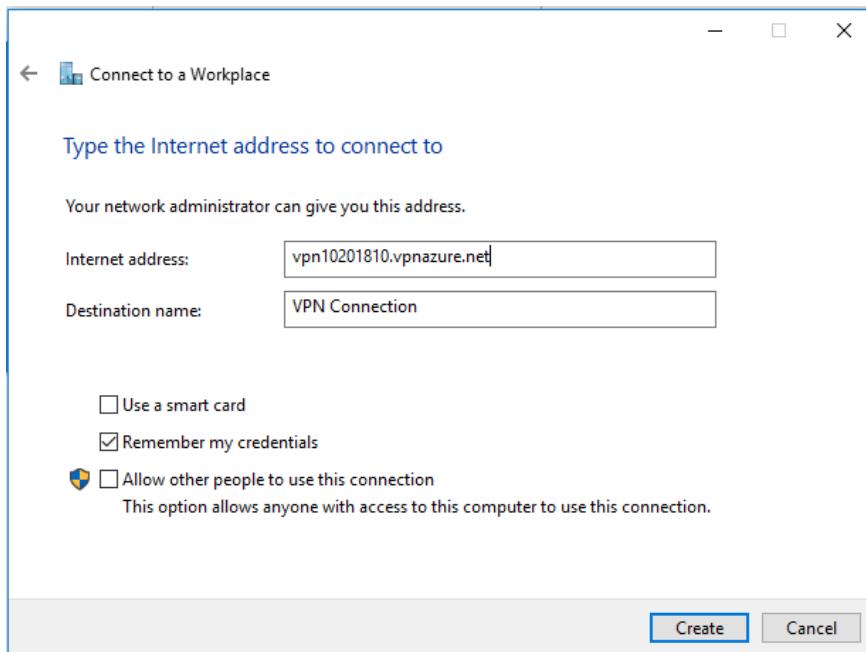
*Figure 6.2. 161: Set up a new connection 2*

3. Choose to use my internet connection.



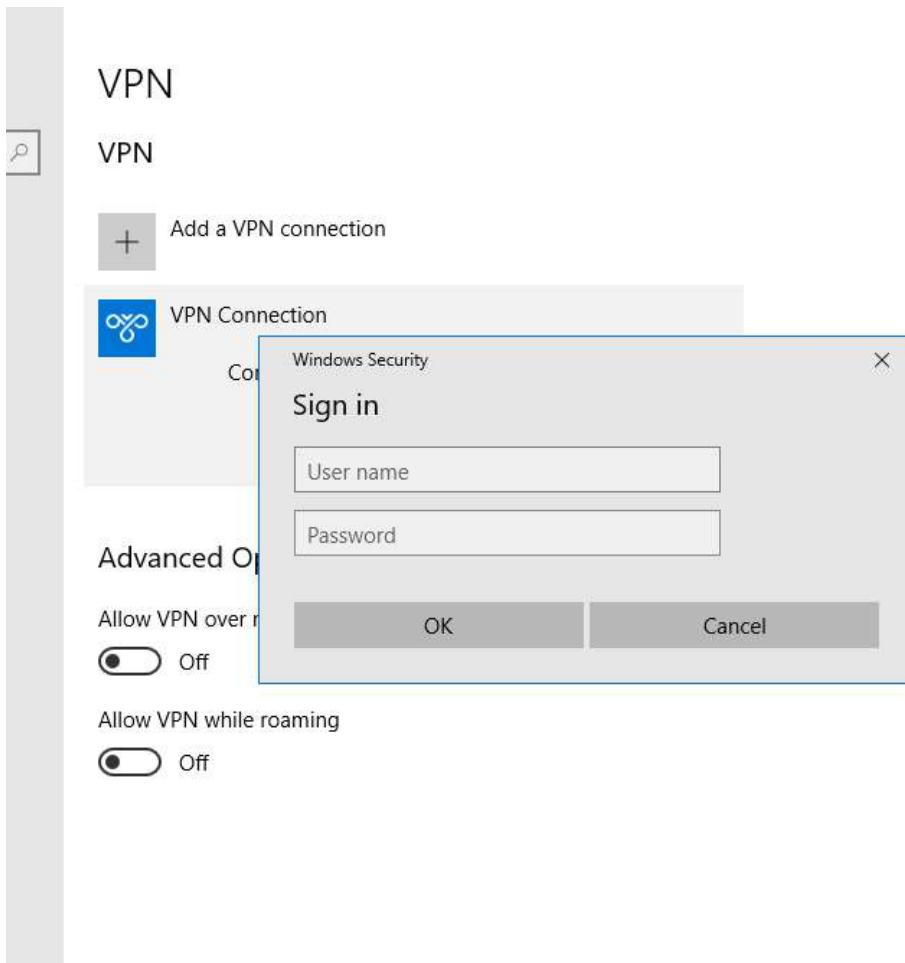
*Figure 6.2. 162: Set up a new connection 3*

4. Insert name of the internet address.



*Figure 6.2. 163: Set up a new connection 4*

5. Go to VPN tab and choose VPN connection that created and insert the username and password.



*Figure 6.2. 164 Login to VPN*

6. VPN connection is established.

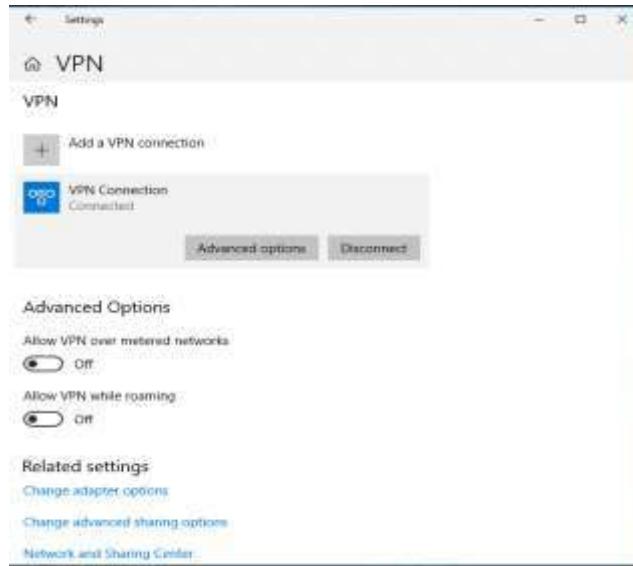


Figure 6.2.165: VPN show connected

7. Ping the device on workplace with result of successful.

```
C:\Users\User>ping 192.168.9.130

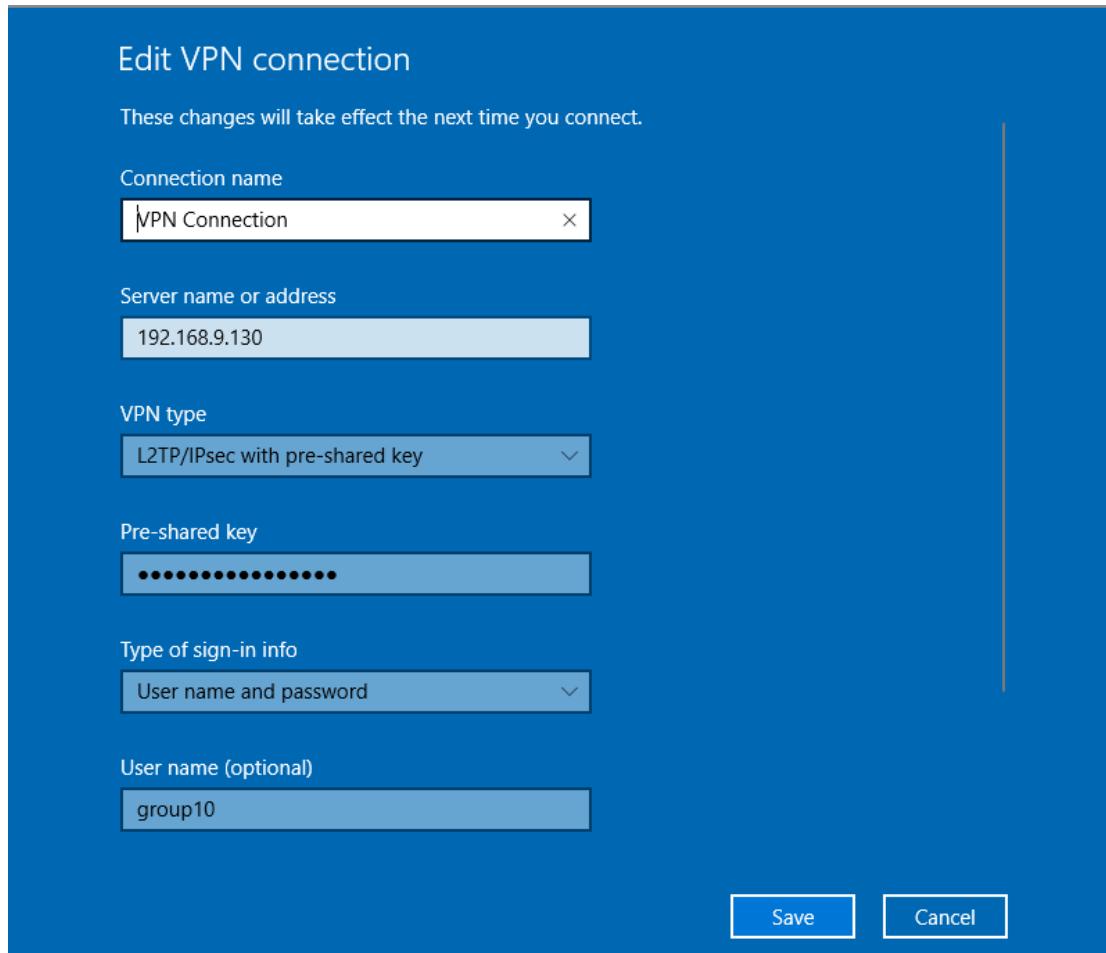
Pinging 192.168.9.130 with 32 bytes of data:
Reply From 192.168.9.130: bytes=32 time=470ms TTL=127
Reply From 192.168.9.130: bytes=32 time=435ms TTL=127
Reply From 192.168.9.130: bytes=32 time=432ms TTL=127
Reply From 192.168.9.130: bytes=32 time=430ms TTL=127

Ping statistics for 192.168.9.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 430ms, Maximum = 470ms, Average = 441ms

C:\Users\User>
```

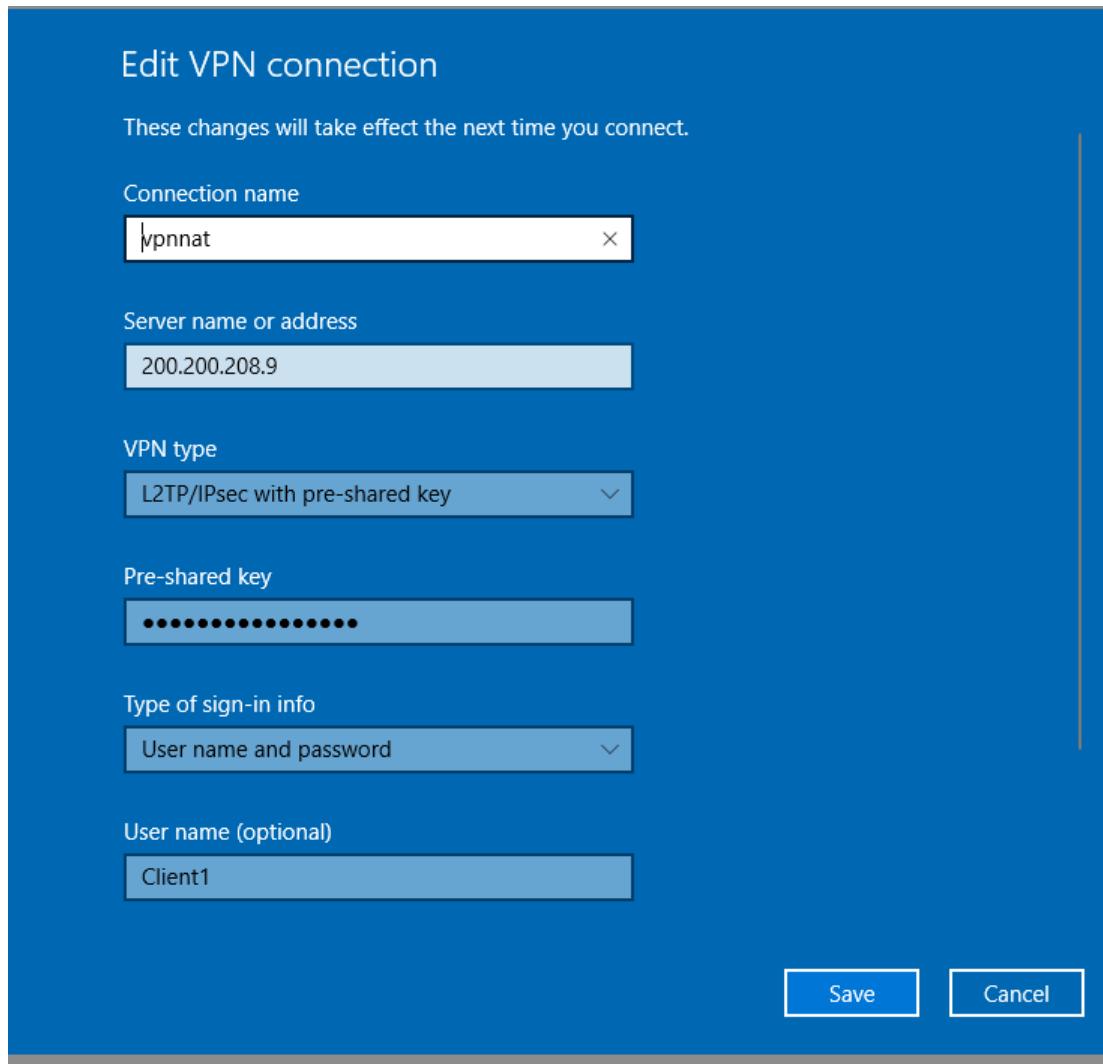
Figure 6.2. 166: Try to ping Window Server

8. While under no internet circumstances, just type the IP address of the VPN server and connect.



*Figure 6.2. 167: Set up a new connection without internet.*

9. While connecting to the other side of island after doing NAT, just type their Public IP address to connect.



*Figure 6.2. 168: Set up a new connection without internet to another island.*

### 6.2.23 Samba Security Services

1. Go to Window Client which IP address is 192.168.9.2 and connect to samba on fedora 192.168.9.138.

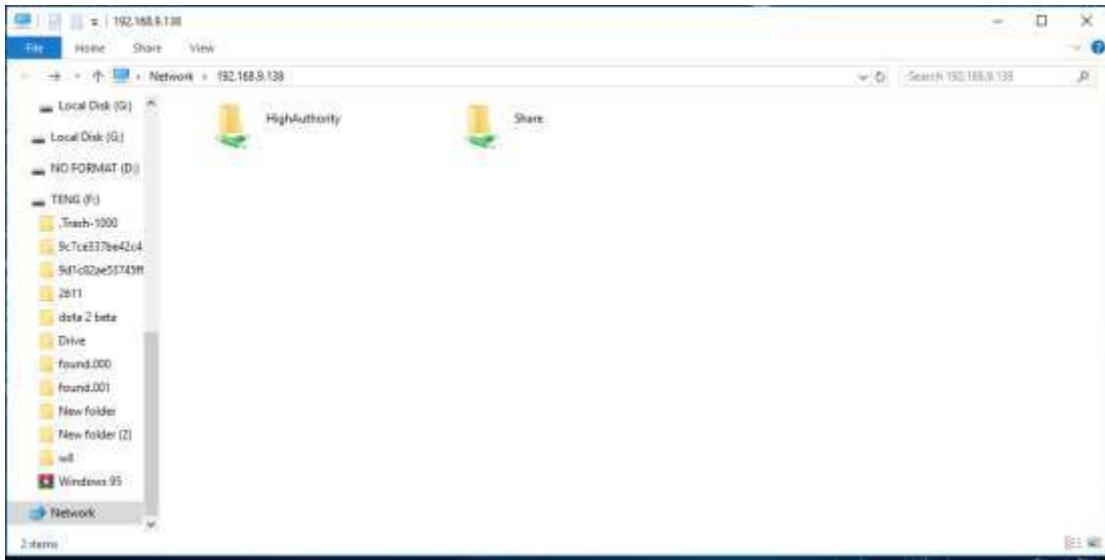


Figure 6.2. 169: On Window 192.168.9.2

2. Try to connect to HighAuthority. It shows access denied due to High Authority only allow IP address with 192.168.9.66.

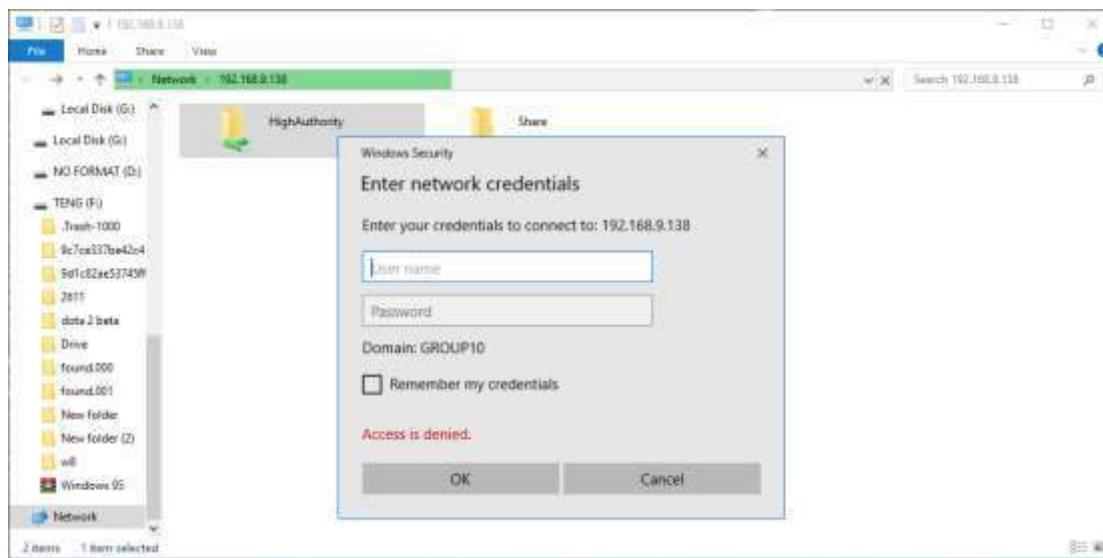


Figure 6.2.170: On Window 192.168.9.2

3. But when go to Share file, it will be allowed.

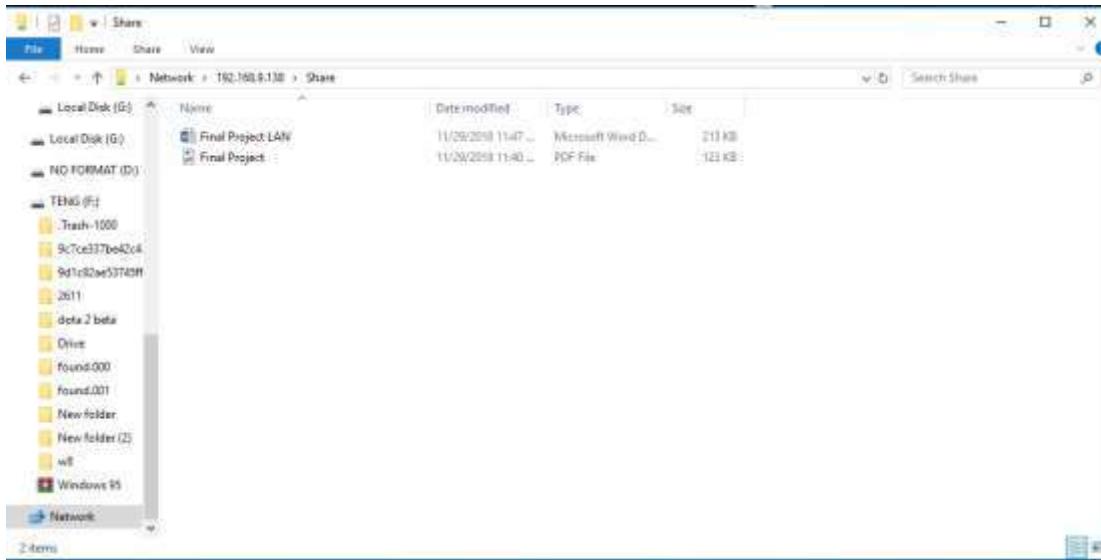


Figure 6.2. 171: On Window 192.168.9.2

4. Next test on HighAuthority in Window Client with IP address 192.168.9.66. In this, higher authority will have permission on read, write and execute. Therefore gello.txt can be created.

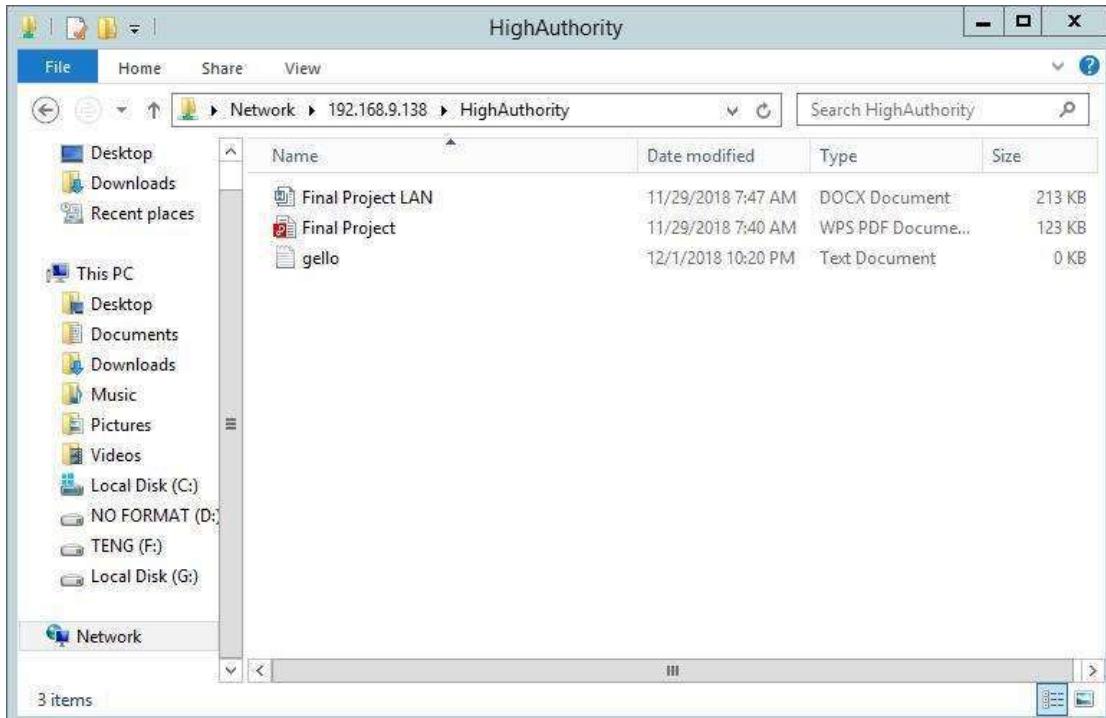


Figure 6.2. 172: On Window 192.168.9.66

### 6.2.24 Active Directory

Step 1 : Open up **System Properties** by right-click on **My Computer** and click on **Properties** then click on **Change Settings**. Then click on **Change** to proceed.

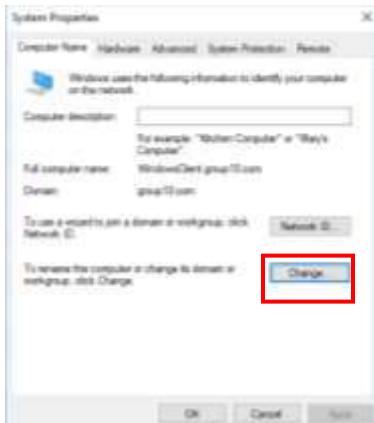


Figure 6.2. 173: System Properties Information

Step 2 : By default, the client is on **Workgroup** as shown in the figure below. Click on the **Domain** checkbox, enter your domain name and click **OK** to proceed.

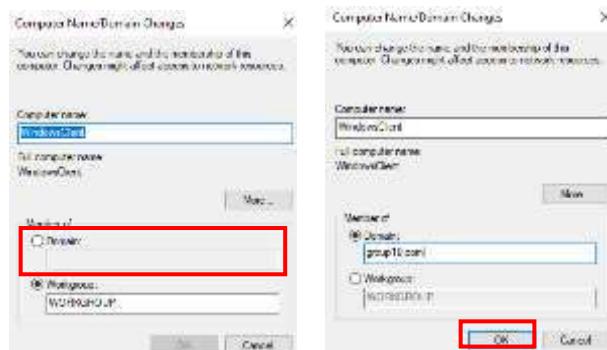


Figure 6.2. 174: Computer Name/Domain Changes

Step 3: A popup windows will appear prompting for **username** and **password**. Enter the information on the Active Directory account created and press the **OK** button to proceed.



*Figure 6.2. 174: Username and Password authentication for AD*

Step 4 : A message will appear welcoming you to the Domain once you have entered the correct username and password as shown in the figure below. You must restart your PC for the changes to apply.



*Figure 6.2. 175: Restart computer*

### 6.2.25 Vlan Security

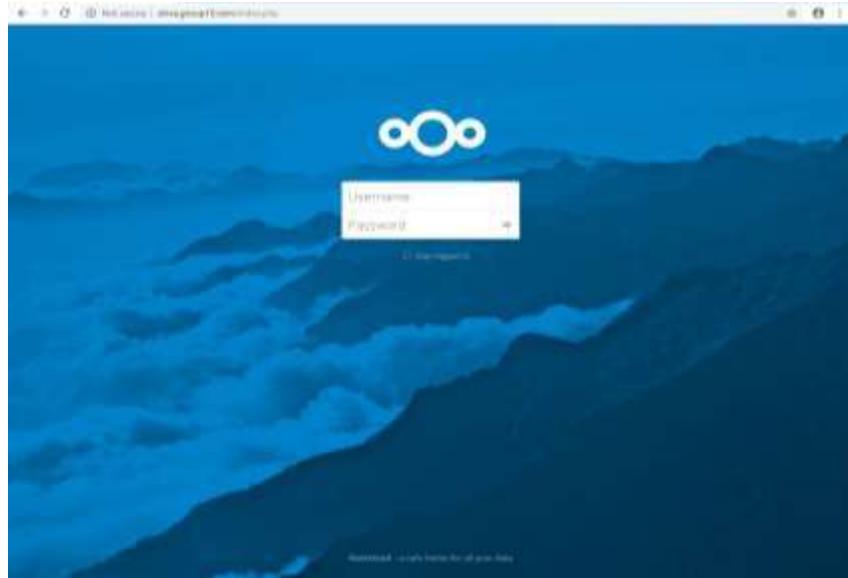
Then view the VLAN table to ensure all the unused port is in the right VLAN.

VLAN Name	Status	Ports
1 default	active	Fa0/24, Gi0/1, Gi0/2
5 TRUNK	active	
10 WINSERVER	active	Fa0/1, Fa0/2
20 FEDORA	active	Fa0/3, Fa0/4
30 UBUNTU	active	Fa0/5, Fa0/6
40 CLIENT_WIRED	active	Fa0/7
50 CLIENT_AP	active	Fa0/15
80 Unusedport	suspended	Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/13, Fa0/14, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/21 Fa0/22
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

Figure 6.2. 176: List of VLAN

### 6.2.26 Cloud Server

Step1: Open drive.group10.com at web browser and login into the NextCloud server.



*Figure 6.2. 177: Homepage of drive.group10.com*

Step 2: Upload any file you desired to store into the cloud server

A screenshot of the NextCloud file list interface. The left sidebar shows navigation links like "All files", "Favorites", "Shared with me", "Shared with others", "Shared by link", and "Tags". The main area displays a list of files and folders. There are three items listed: "Document" (uploaded 5 minutes ago), "Photo" (uploaded 5 minutes ago), and "share" (uploaded 2 minutes ago). Each item has a preview thumbnail, a file name, a date uploaded, and a "More" options menu icon.

*Figure 6.2. 178: List of there file stored inside the cloud server*

## 6.2.27 Media Streaming Server

### Configuring Subsonic

Step 1: Open **Subsonic** web page by entering the IP Address and the port number as shown in the figure below. Then enter you username along with your password to continue.



Figure 6.2. 179: Subsonic Login Page

Step 2: Go to the left bar and click on **Settings** and navigate to the **Media Folders** tabs.

Step 3: Add your **media paths** in the folder form as shown in the figure below and then click the **Scan media folders now** to scan the media into the subsonic library.

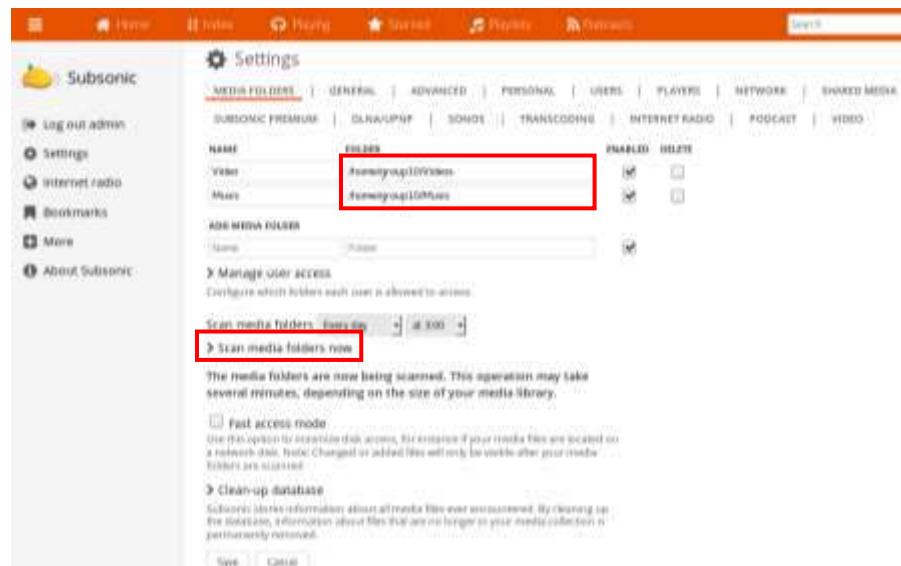


Figure 6.2. 180: Subsonic Setting Page

Step 4: Go to the Home page and your media will be listed as show in the figure below.

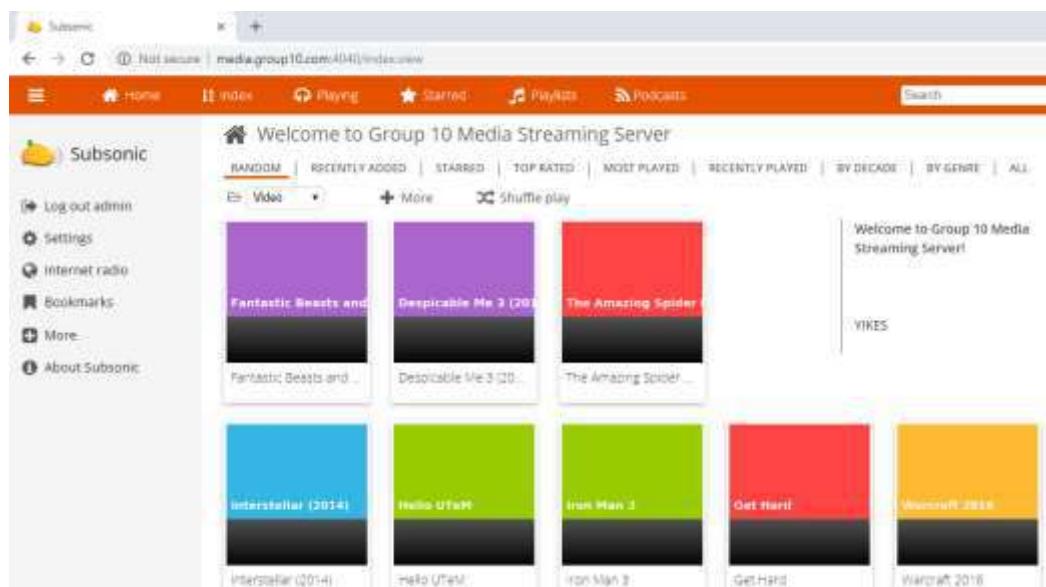


Figure 6.2. 181: Subsonic Homepage

## **CHAPTER 7**

### **CONCLUSION**

#### **7.1 Introduction**

Through these numerous weeks, a lot of things have been studied such as method to setup, configure, maintain and troubleshoot and all the basic of the services in this Workshop 2. All the lesson learnt from this Workshop 2 will be applied for industrial training. In order to run this Workshop 2 with successfully our group choose a leader to lead this project and starting to define, implement and manage this Workshop 2 from beginning until the ned of the project. Tasks have been distributed equally to each member and a schedule has been created to mange the flow of it. This is very important in managing and organizing every task in order to prevent the error from occurring before the due date. Overall our group has successfully done all of the services before the due date.

This network is suitable for Small and Medium Enterprise Business since it is easy to manage and implement. Furthermore, this network includes all the basic service (such as DNS, DHCP, Email, SFTP, Proxy Server and etc.) that needs to run the business. Hopefully we can achieve our goals or objective that is to make this project a success and able go through the obstacles and challenges faces in completing the task given. We are so grateful being given this as this will bring us more prepared for an industrial training.

## **7.2 Project Advantages**

There are a lot of advantages to implement this project. The most important of this project is providing an experience during the working environment on computer networking and security. Besides that, this project also provides other advantages which are:

1. Learn how to design the network infrastructure for this project.
2. learn how to implement designated network services.
3. To learn configuration and installation of the services in a server.
4. To integrate network services infrastructure to suit the network environment.
5. To maintain and control the network services infrastructure.
6. To increase the communication between network student and security student in developing a good network environment
7. To troubleshoot and overcome any problems during settings up the services.
8. To build team work between network student and security student in a group.

## **7.3 Project Disadvantages**

Even through, this project also gives disadvantages to us to archive the successful. This project disadvantage which are:

1. Lack of knowledge about some of the services.
2. The servers that were provided were old and caused many problems during the progress of Workshop 2.
3. Some of the network equipment is not in a good condition, it may work as well as expected.

## **7.4 Project Limitation**

There was some project limitation that was caused, and we had to adapt and work harder to succeed in this project. These limitations were:

1. The network was only implemented in wired environment.
2. All the equipment that has been given to each group is not in very good conditions.
3. We are not really exposed to large network set ups and management.
4. The wireless technology was not implemented in this project due to the problem in the wireless device.

## **7.5 Conclusion**

As a conclusion from this Workshop 2, there are a lot of things that have been learnt and some improvement can be made to make it an excellent infrastructure. We had learnt to identify, install, set up, configure and even troubleshoot the services in order to make our network infrastructure run smoothly. We are very grateful to be able to do Workshop 2 as it involved a lot of practical that can be implemented in real network environment.

Workshop 2 requires us to control and monitor the network infrastructure throughout the progress to make sure it in good conditions and run smoothly. Furthermore, we need to secure our network infrastructure to make it more reliable. This project requires us to install 30 services consist of 18 network service and 12 security services. By completing this workshop, we can gain knowledge in theoretical and practical about all services needed in order to provide a good and secure networking environment for an organization.