



FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

SEMESTER 1 2020/2021

WORKSHOP II (BITU 3923)

BITC & BITZ

FINAL REPORT

PROJECT TITLE: DOMAIN NAME SERVICE (DNS)

GROUP NUMBER: 1

PREPARED BY:

NAME	MATRIC NO
NURUL AFIFAH BINTI AHMAD MAHIN	B031810378
AHMAD FARIS BIN MAZLAN	B031810253
AMIRAH SYAHIRAH BINTI ARIFFIN	B031810233
MUHAMMAD ARIQ BIN ADNAN	B031810393
AHMAD AKMAL HAZIM BIN ZULKIFLI	B031810402
TAN CHUN YONG	B031810217
SITI AISHAH BINTI SAHALUDIN	B031910192

SUPERVISOR: DR SHEKH FAISAL BIN ABDUL LATIP

: ERMAN BIN HAMID

EVALUATOR: ZAKIAH BINTI AYOP

: DR. NUR FADZILAH BINTI OTHMAN

Acknowledgements

Firstly, we would like to thank our supervisors for this project, Dr Shekh Faisal Bin Abdul Latip and Erman Bin Hamid for their valuable guidance and advice to finish Workshop II services. They inspired us much to work in a team for this project. Their willingness to motivate us contributed tremendously to our project. They also taught us that we must think outside the box and from our comfort zone and try to make our service better and excellent. All of this guidance helped us complete our project on time. We would also like to thank our evaluators for this workshop, Zakiah Binti Ayop and Dr Nur Fadzilah Binti Othman for taking the time to evaluate us. This evaluation gave us a deeper understanding of our services, network infrastructure and what we must add to our service to make it better than we already have.

We also would like to thank Universiti Teknikal Malaysia Melaka (UTeM) authority for providing us with the right environment and facilities to complete this project. Finally, an honourable mention goes to our families and friends that understand and support us in completing this project. With the help of them that are mentioned above, we overcame many problems that occurred during Workshop II and were able to complete our project successfully on time.

Abstract

In this Workshop II project, we have to define, implement and manage tasks which start from selecting a leader to lead this project from the beginning until the end of this project. A task has been given to each member and we create a schedule for the task to finish on time and who will do what service. It is very important to manage and organize every task given in order to avoid any problems and errors later on. Our main objective in this Workshop II is for this project to be successful and able to go through the obstacles and challenges faced while completing the task given. Next our objective also is to have a 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 in server Window and Debian in server Debian. We choose this server operating system because it has many benefits. Our group also was assigned to set up 18 services listed. The 10 services listed are Routing & NAT (Router), DNS (IPv4 & IPv6), DHCP (IPv4 & IPv6), Network Management System, AAA with radius, Secure FTP, Access Control List (ACL), Linux Email Server, Web, SSL & Virtual Hosting, Active Directory and IPSec site to site tunnelling for BITC. And, 8 services for BITZ which is IPSec VPN, User authentication, Windows hardening, Layer 2 Security, Samba, Audit compliances, IDS and Linux Hardening. During 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 II ini, kita harus menentukan, melaksanakan dan mengurus tugas yang bermula dari memilih pemimpin untuk memimpin projek ini dari awal hingga akhir projek ini. Tugas telah diberikan kepada setiap anggota dan kami membuat jadual agar tugas dapat diselesaikan tepat pada waktunya dan siapa yang akan melakukan perkhidmatan apa. Adalah sangat penting untuk mengurus dan mengatur setiap tugas yang diberikan untuk mengelakkan masalah dan kesilapan di kemudian hari. Objektif utama kami dalam Bengkel II ini adalah agar projek ini berjaya dan dapat melalui rintangan dan cabaran yang dihadapi semasa menyelesaikan tugas yang diberikan. Seterusnya objektif kami juga adalah untuk memiliki pemahaman yang lebih mendalam mengenai perkhidmatan mengenai cara kerjanya dan kami bersyukur untuk mengalami ini kerana ini membantu kami untuk lebih bersedia dalam latihan industri kami. Kumpulan kami telah memutuskan untuk menggunakan Windows Server 2012 di Window pelayan dan Debian di Debian pelayan. Kami memilih sistem operasi pelayan ini kerana mempunyai banyak faedah. Kumpulan kami juga ditugaskan untuk menyediakan 18 perkhidmatan yang disenaraikan. 10 perkhidmatan yang disenaraikan ialah Routing & NAT (Router), DNS (IPv4 & IPv6), DHCP (IPv4 & IPv6), Sistem Pengurusan Rangkaian, AAA dengan radius, Secure FTP, Daftar Kawalan Akses (ACL), Linux Email Server, Web, SSL & Virtual Hosting, Active Directory dan IPsec ke laman web tunneling untuk BITC. Dan, 8 perkhidmatan untuk BITZ iaitu IPsec VPN, Pengesahan pengguna, Pengerasan Windows, Keselamatan Lapisan 2, Samba, pematuhan Audit, IDS dan Pengerasan Linux. Semasa Bengkel II, kami menghadapi beberapa masalah tetapi masih berjaya mengatasinya dan membuat projek ini tepat pada waktunya dan berjaya menyelesaikan perkhidmatan.

1. CHAPTER 1: INTRODUCTION	1
1.1. Introduction	1
1.2. Objective	1
1.3. Project Plan/Schedule	2
1.3.1. Gantt chart of Project	2
1.3.2. Completion Date Every Task	2
1.3.3. Individual Task	3
1.4. Conclusion	5
2. CHAPTER 2: PROJECT REQUIREMENT	6
2.1. Introduction	6
2.2. Types of Operating System use in project	6
2.3. Operating system background	6
2.4. Operating system justification	7
2.5. Hardware requirement	8
2.6. Hardware justification	9
2.7. Conclusion	10
3. CHAPTER 3: DESIGN	10
3.1. Introduction	10
3.2. Security Policy	10
● Active Directory (AD) Policy	15
3.3. Physical Design	19
3.4. Logical (including Security) Design	20
3.5. Conclusion	21
4. CHAPTER 4: SERVICES	21
4.1. Introduction	21
4.2. List of services	22
4.3. Brief overview for services	22
4.3.1. Routing and NAT	22
4.3.2. DNS (IPv4 & IPv6)	23
4.3.3. Active Directory	23
4.3.4. DHCP (IPv4 & IPv6)	24
4.3.5. Web, SSL & Virtual Hosting	24
4.3.6. Linux Email Server	25
4.3.7. Access Control List	25

4.3.8.	IPSec Site-to-Site Tunneling	25
4.3.9.	Network Management System	26
4.3.10.	AAA (Authentication, Authorization and Accounting) using Radius	26
4.3.11.	Layer 2 Security - VLAN and Port Security	27
4.3.12.	Samba and Samba security	27
4.3.13.	User authentication user by integrating AD with linux	27
4.3.14.	IDS	28
4.3.15.	IPSec VPN server for remote employees	28
4.3.16.	Windows Server Hardening and Vulnerability Report	28
4.3.17.	Linux Server Hardening and Vulnerability Report	29
4.3.18.	Audit Compliance	29
4.4.	Conclusion	29
5.	CHAPTER 5: INSTALLATION AND CONFIGURATION	30
5.1.	Introduction	30
5.2.	Services and individual tasks	30
5.2.1.	Routing and NAT	31
5.2.2.	DNS (IPv4 & IPv6)	34
5.2.3.	Active Directory	52
5.2.4.	DHCP (IPv4 & IPv6)	73
5.2.5.	Web, SSL & Virtual Hosting	80
5.2.6.	Linux Email Server	91
5.2.7.	Access Control List	99
5.2.8.	IPSec Site-to-Site Tunneling	100
5.2.9.	Network Management System	101
5.2.10.	AAA (Authentication, Authorization and Accounting) using Radius	136
5.2.11.	Layer 2 Security - VLAN and Port Security	145
5.2.12.	Samba and Samba security	148
5.2.13.	User authentication user by integrating AD with linux	150
	Step 5: Create an Active Directory group which include AD users	153
5.2.14.	Intrusion Detection System (IDS) and Port Mirroring	159
5.2.15.	IPSec VPN server for remote employees	169
5.2.16.	Windows Server Hardening and Vulnerability Report	200
5.2.17.	Linux Server Hardening and Vulnerability Report	222
5.2.18.	Audit Compliance	230
1.0	SECURITY POLICY	231
1.1	Security Policy	231

1.1.1	Security policy document	231
1.1.2	Review and evaluation	231
2.0	ORGANISATIONAL SECURITY	232
2.1	Information security infrastructure	232
2.1.1	Management information security forum	232
2.1.2	Information security coordination	232
2.1.3	Allocation of information security responsibilities.	233
2.1.4	Authorisation process for information processing facilities	233
2.1.5	Security advise from supervisor	233
2.1.6	Independent review of information security	233
2.2	Security of third party	234
2.2.1	Security requirements in third party contracts	234
2.2.2	Identification of risks from third party	234
3.0	ASSET CLASSIFICATION AND CONTROL	234
3.1	Accountability of assets	234
3.2	Information classification	235
4.0	PERSONNEL SECURITY	236
4.1	Security in job definition and resourcing	236
4.1.1	Including security in job responsibilities	236
4.2	Responding security weakness	236
4.2.1	Reporting security weakness	236
4.2.2	Reporting software malfunctions	236
4.2.3	Reporting hardware malfunctions	237
4.2.4	Disciplinary process	237
5.0	PHYSICAL AND ENVIRONMENTAL SECURITY	237
5.1	Secure Area	237
5.1.1	Physical security Perimeter	237
5.1.2	Physical entry controls	238
5.1.3	Securing rooms and facilities	238
5.2	Equipment Security	238
5.2.1	Equipment siting and protection	239
5.2.2	Equipment Maintenance	239
5.2.3	Securing equipment off-premises	240
5.3	General Controls	240
5.3.1	Clear Desk and Clear Screen Policy	240
5.3.2	Removal of property	240

6.0	COMMUNICATION AND OPERATIONS MANAGEMENT	241
6.1	Operational Procedure and responsibilities	241
6.1.1	Documented Operating System	241
6.1.2	Segregation of duties	241
6.2	Protection Against Malicious Software	241
6.2.1	Control against malicious	242
6.3	Housekeeping	242
6.3.1	Information back-up	242
6.3.2	Fault Logging	242
6.4	Network Management	243
6.4.1	Network Controls	243
6.5	Exchange of Information and Software	243
6.5.1	Security of Media in transit	243
7.0	ACCESS CONTROL	244
7.1	User Access Control	244
7.1.1	User Registration	244
7.1.2	Privilege Management	244
7.1.3	User Password Management	244
7.2	User Responsibilities	245
7.2.1	Password use	245
7.2.2	Unattended User Equipment	245
7.3	Network Access Control	245
7.3.1	Segregation in networks	245
7.3.2	Node Authentication	246
7.3.3	Network Connection Protocols	246
7.3.4	Network Routing Control	246
7.3.5	Security of Network Services	247
7.4	Operating System Access Control	247
7.4.1	Automatic terminal identification	247
7.4.2	Terminal log-on procedures	248
7.4.3	User identification and Authorization	248
7.4.4	Use of System Utilities	248
7.4.5	Terminal Time-Out	249
7.5	Application Access Control	249
7.5.1	Sensitive System Isolation	249
7.6	Monitoring System Access and Use	249

7.6.1	Event Logging	249
7.6.2	Monitoring System Use	250
7.6.3	Message Authentication	250
7.6.4	Output Data Validation	250
8.0	SYSTEM DEVELOPMENT AND MAINTENANCE	250
8.1	Security in Application Systems	251
8.1.1	Input Data Validation	251
8.1.2	Message Authentication	251
8.1.3	Output Data Validation	251
8.2	Cryptographic Controls	251
8.2.1	Encryption	251
8.2.2	Digital Signatures	252
8.2.3	Key Management	252
8.3	Security in development and support process	252
8.3.1	Change control procedures	253
8.3.2	Technical review of operating system changes	253
8.3.3	Outsourced Software Development	253
9.0	COMPLIANCE	253
9.1	Aspects of Services Continuity Management	254
9.1.1	Testing, maintaining and re-accessing services	254
9.2	Compliance with Legal Requirements	254
9.2.1	Identification of Applicable legislation	254
9.2.2	Safeguarding of Organisational records	254
9.2.3	Data Protection and Privacy of Personal Information	254
9.2.4	Prevention of misuse of information processing facility	255
9.2.5	Collection of Evidence	255
9.3	Review of Security Policy and Technical Compliance	255
9.3.1	Compliance with Security Policy	255
9.3.2	Technical compliance checking	256
9.4	System Audit Considerations	256
9.4.1	System Audit Controls	256
5.3.	Conclusion	256
6.	CHAPTER 6: TESTING	256
6.1.	Introduction	256
6.2.	Services testing	257

6.2.1.	Routing and NAT	257
6.2.2.	DNS (IPv4 & IPv6)	259
6.2.3.	Active Directory	260
6.2.4.	DHCP (IPv4 & IPv6)	265
6.2.5.	Web, SSL and Virtual Hosting	269
6.2.6.	Linux Email Server	271
6.2.7.	Access Control List	272
6.2.8.	IPSec Site-to-Site Tunneling	278
6.2.9.	Network Management System	279
6.2.10.	AAA (Authentication, Authorization and Accounting) using Radius	286
6.2.11.	Layer 2 Security - VLAN and Port Security	287
6.2.12.	Samba and Samba security	290
6.2.13.	User authentication user by integrating AD with linux	293
6.2.14.	Intrusion Detection System (IDS) and Port Mirroring	296
6.2.15.	IPSec VPN server for remote employees	297
6.2.16.	Windows Server Hardening and Vulnerability Report	303
6.2.17.	Linux Server Hardening and Vulnerability Report	306
6.2.18.	Audit Compliance	309
1.0	SECURITY POLICY	310
1.1	Security Policy	310
1.1.1	Security policy document	310
1.1.2	Review and evaluation	310
2.0	ORGANISATIONAL SECURITY	311
2.1	Information security infrastructure	311
2.1.1	Management information security forum	311
2.1.2	Information security coordination	311
2.1.3	Allocation of information security responsibilities.	312
2.1.4	Authorisation process for information processing facilities	312
2.1.5	Security advise from supervisor	312
2.1.6	Independent review of information security	312
2.2	Security of third party	313
2.2.1	Security requirements in third party contracts	313
2.2.2	Identification of risks from third party	313
3.0	ASSET CLASSIFICATION AND CONTROL	313
3.1	Accountability of assets	313
3.2	Information classification	314

4.0	PERSONNEL SECURITY	315
4.1	Security in job definition and resourcing	315
4.1.1	Including security in job responsibilities	315
4.2	Responding security weakness	315
4.2.1	Reporting security weakness	315
4.2.2	Reporting software malfunctions	315
4.2.3	Reporting hardware malfunctions	316
4.2.4	Disciplinary process	316
5.0	PHYSICAL AND ENVIRONMENTAL SECURITY	316
5.1	Secure Area	316
5.1.1	Physical security Perimeter	316
5.1.2	Physical entry controls	317
5.1.3	Securing rooms and facilities	317
5.2	Equipment Security	317
5.2.1	Equipment siting and protection	318
5.2.2	Equipment Maintenance	318
5.2.3	Securing equipment off-premises	319
5.3	General Controls	319
5.3.1	Clear Desk and Clear Screen Policy	319
5.3.2	Removal of property	319
6.0	COMMUNICATION AND OPERATIONS MANAGEMENT	320
6.1	Operational Procedure and responsibilities	320
6.1.1	Documented Operating System	320
5.3.2	Removal of property	320
6.0	COMMUNICATION AND OPERATIONS MANAGEMENT	320
6.1	Operational Procedure and responsibilities	320
6.1.1	Documented Operating System	321
6.1.2	Segregation of duties	321
6.2	Protection Against Malicious Software	321
6.2.1	Control against malicious	321
6.3	Housekeeping	322
6.3.1	Information back-up	322
6.3.2	Fault Logging	322
6.4	Network Management	322
6.4.1	Network Controls	323
6.5	Exchange of Information and Software	323

6.5.1	Security of Media in transit	323
7.0	ACCESS CONTROL	323
7.1	User Access Control	323
7.1.1	User Registration	324
7.1.2	Privilege Management	324
7.1.3	User Password Management	324
7.2	User Responsibilities	324
7.2.1	Password use	325
7.2.2	Unattended User Equipment	325
7.3	Network Access Control	325
7.3.1	Segregation in networks	325
7.3.2	Node Authentication	326
7.3.3	Network Connection Protocols	326
7.3.4	Network Routing Control	326
7.3.5	Security of Network Services	327
7.4	Operating System Access Control	327
7.4.1	Automatic terminal identification	327
7.4.2	Terminal log-on procedures	327
7.4.3	User identification and Authorization	328
7.4.4	Use of System Utilities	328
7.4.5	Terminal Time-Out	328
7.5	Application Access Control	329
7.5.1	Sensitive System Isolation	329
7.6	Monitoring System Access and Use	329
7.6.1	Event Logging	329
7.6.2	Monitoring System Use	330
7.6.3	Message Authentication	330
7.6.4	Output Data Validation	330
8.0	SYSTEM DEVELOPMENT AND MAINTENANCE	330
8.1	Security in Application Systems	331
8.1.1	Input Data Validation	331
8.1.2	Message Authentication	331
8.1.3	Output Data Validation	331
8.2	Cryptographic Controls	331
8.2.1	Encryption	332
8.2.2	Digital Signatures	332

8.2.3	Key Management	332
8.3	Security in development and support process	332
8.3.1	Change control procedures	333
8.3.2	Technical review of operating system changes	333
8.3.3	Outsourced Software Development	333
9.0	COMPLIANCE	333
9.1	Aspects of Services Continuity Management	334
9.1.1	Testing, maintaining and re-accessing services	334
9.2	Compliance with Legal Requirements	334
9.2.1	Identification of Applicable legislation	334
9.2.2	Safeguarding of Organisational records	334
9.2.3	Data Protection and Privacy of Personal Information	334
9.2.4	Prevention of misuse of information processing facility	335
9.2.5	Collection of Evidence	335
9.3	Review of Security Policy and Technical Compliance	335
9.3.1	Compliance with Security Policy	335
9.3.2	Technical compliance checking	336
9.4	System Audit Considerations	336
9.4.1	System Audit Controls	336
6.3.	Conclusion	337
7.	CHAPTER 7: CONCLUSION	338
7.1.	Introduction	338
7.2.	Project advantages	339
7.3.	Project disadvantages	339
7.4.	Project limitation	339
7.5.	Conclusion	340
BIBLIOGRAPHY		340
APPENDIX		341

List of Figure

Figure 3.3.1	Physical Design.....	20
Figure 3.4.1	Logical Design.....	21
Figure 5.2.1.1	Configuration BGP on Router HQ.....	31
Figure 5.2.1.2	Configuration BGP on Router ISP	32
Figure 5.2.1.3	Configuration BGP on Router Branch.....	32
Figure 5.2.1.4	Configuration Dynamic NAT for client IT Department	33

Figure 5.2.1.5 Configuration Static NAT for Server Windows	33
Figure 5.2.1.6 Configuration Static NAT for Server Debian	33
Figure 5.2.1.7 Configuration Dynamic NAT for client Remote Access	34
Figure 5.2.2.1 Click on Add Roles and Features	34
Figure 5.2.2.2 Click on Next	35
Figure 5.2.2.3 Click on Role based installation	35
Figure 5.2.2.4 Click on Role server windows	36
Figure 5.2.2.5 Click on DNS Server	36
Figure 5.2.2.6 Click on Add Features	37
Figure 5.2.2.7 Click on Next	37
Figure 5.2.2.8 Click on install to install DNS Server	38
Figure 5.2.2.9 Click on New Host (A or AAA) to create forward zone IPv4	38
Figure 5.2.2.10 Fill in information for name and IP address for IPv4 DNS	39
Figure 5.2.2.11 The host www.group1.com for IPv4 is successfully created	39
Figure 5.2.2.12 Click on New Host (A or AAA) to create forward zone IPv6	40
Figure 5.2.2.13 Fill in information for name and IP address for IPv6 DNS	40
Figure 5.2.2.14 The host www.group1.com for IPv6 is successfully created	41
Figure 5.2.2.15 Fully configured forward zone for IPv4 and IPv6	41
Figure 5.2.2.16 Creating new zone for reverse lookup zone for DNS IPv4	41
Figure 5.2.2.17 New Zone Wizard for reverse lookup zone DNS IPv4	42
Figure 5.2.2.18 Choose primary zone for reverse lookup zone DNS IPv4	42
Figure 5.2.2.19 Choose to all DNS Servers running on domain group1.com	43
Figure 5.2.2.20 Click on IPv4 Reverse Lookup Zone	43
Figure 5.2.2.21 Identify the network ID for reverse lookup zone	44
Figure 5.2.2.22 Do not allow dynamic update	44
Figure 5.2.2.23 Click on Finish	45
Figure 5.2.2.24 Click on New Pointer (PTR)	45
Figure 5.2.2.25 Browse and map the hostname to the forward lookup zone	46
Figure 5.2.2.26 Creating new zone for reverse lookup zone for DNS IPv6	46
Figure 5.2.2.27 New Zone Wizard for reverse lookup zone DNS IPv6	47
Figure 5.2.2.28 Choose primary zone for reverse lookup zone DNS IPv6	47
Figure 5.2.2.29 Choose primary zone for reverse lookup zone DNS IPv6	48
Figure 5.2.2.30 Click on IPv6 Reverse Lookup Zone	48
Figure 5.2.2.31 Click on IPv4 Reverse Lookup Zone	49
Figure 5.2.2.32 Identify the network ID for reverse lookup zone	49
Figure 5.2.2.33 Click on Finish	50
Figure 5.2.2.34 Click on New Pointer (PTR)	50
Figure 5.2.2.35 Browse and map the hostname to the forward lookup zone	51
Figure 5.2.2.36 Fully configured reverse zone for IPv4 and IPv6	51
Figure 5.2.3.1 Add Roles and Features	52
Figure 5.2.3.2 Before you begin tab	52
Figure 5.2.3.3 Select installation type tab	53
Figure 5.2.3.4 Select destination server	53
Figure 5.2.3.5 Select server roles tab	54
Figure 5.2.3.6 Add feature	54
Figure 5.2.3.7 Select features tab	55
Figure 5.2.3.8 AD DS tab	55
Figure 5.2.3.9 Confirmation tab	56

Figure 5.2.3.10 Results tab	56
Figure 5.2.3.11 Flag information tab.....	57
Figure 5.2.3.12 Deployment configuration tab.....	57
Figure 5.2.3.13 Domain controller options tab.....	58
Figure 5.2.3.14 DNS options tab	58
Figure 5.2.3.15 Additional options tab	59
Figure 5.2.3.16 Paths tab	59
Figure 5.2.3.17 Review options tab.....	60
Figure 5.2.3.18 Prerequisites check tab	61
Figure 5.2.3.19 Active Directory Users and Computers.....	61
Figure 5.2.3.20 Creating organizational unit.....	61
Figure 5.2.3.21 Organizational unit tab	62
Figure 5.2.3.22 Organizational unit tab	62
Figure 5.2.3.23 User tab	63
Figure 5.2.3.24 User tab	63
Figure 5.2.3.25 Status of created user	64
Figure 5.2.3.26 List name of users created	64
Figure 5.2.3.27 Group Policy Management.....	65
Figure 5.2.3.28 Group Policy Management tab	65
Figure 5.2.3.29 Account lockout policy tab	66
Figure 5.2.3.30 Account lockout threshold properties tab.....	66
Figure 5.2.3.31 Account lockout duration properties tab.....	67
Figure 5.2.3.32 Setting for account lockout duration properties	67
Figure 5.2.3.33 Account lockout policy that been set up.....	68
Figure 5.2.3.34 Create GPO is selected.....	68
Figure 5.2.3.35 New GPO tab	69
Figure 5.2.3.36 Link enabled is selected	69
Figure 5.2.3.37 Security options tab.....	70
Figure 5.2.3.38 Interactive logon tab	70
Figure 5.2.3.39 Interactive logon tab	71
Figure 5.2.3.40 Status of second GPO that has been created.....	71
Figure 5.2.3.41 Report of first GPO.....	72
Figure 5.2.3.42 Report of second GPO	72
Figure 5.2.4 1 Installing new DHCP roles.....	73
Figure 5.2.4 2 Finish setup DHCP roles	74
Figure 5.2.4 3 Creating new scope for DHCP	74
Figure 5.2.4 4 Create DHCP scope name	75
Figure 5.2.4 5 Setup DHCP ipv4 range	75
Figure 5.2.4 6 Insert DHCP gateway	76
Figure 5.2.4 7 Select DHCP ip duration	76
Figure 5.2.4 8 Finish configure scope for DHCP	77
Figure 5.2.4 9 Finish DHCP setup.....	77
Figure 5.2.4 10 Insert ipv6 scope name	78
Figure 5.2.4 11 Ipv6 exclusion	79
Figure 5.2.4 12 Ipv6 DHCP finish query setup.....	79
Figure 5.2.5.1 Add roles and features	80
Figure 5.2.5.2 Select installation type.....	81
Figure 5.2.5.3 Select destination server	81

Figure 5.2.5.4 Select server roles.....	81
Figure 5.2.5.5 Include management tools if applicable.....	82
Figure 5.2.5.6 Installation Progress.....	82
Figure 5.2.5.7 verify installation succeeds.....	83
Figure 5.2.5.7 SSL certificate	84
Figure 5.2.5.8 Add website.....	84
Figure 5.2.5.8 Website added	84
Figure 5.2.5.9 HTML file ate wwwroot	85
Figure 5.2.5.10 Default document at IIS	85
Figure 5.2.5.11 Directory browsing at IIS	86
Figure 5.2.5.12 Directory HTML file.....	86
Figure 5.2.5.13 SSL Settings	87
Figure 5.2.5.14 Create new host AAA	87
Figure 5.2.5.15 New host created	88
Figure 5.2.5.16 New Zone Wizard.....	89
Figure 5.2.5.17 Primary Zone.....	89
Figure 5.2.5.18 Zone Name	90
Figure 5.2.5.19 Completing New Zone.....	90
Figure 5.2.5.20 Zone details.....	91
Figure 5.2.5.21 Host Properties	91
Figure 5.2.6.1 nano/etc/hosts.....	92
Figure 5.2.6.2 /etc/postfix/main.cf.....	93
Figure 5.2.6.3 /etc/postfix/main.cf 2.....	93
Figure 5.2.6.4 10-auth.conf	94
Figure 5.2.6.5 10-mail.conf.....	95
Figure 5.2.6.6 10-master.conf	96
Figure 5.2.6.7 Maildirmake	96
Figure 5.2.6.8 Admin mail login.....	97
Figure 5.2.6.9 Edit domain	98
Figure 5.2.6.10 Login screen.....	98
Figure 5.2.7.1 Acl command	99
Figure 5.2.7.2 List of acl command	99
Figure 5.2.8 1 Create ISAKMP phase 1 policy	100
Figure 5.2.8 2 Create an encryption method	100
Figure 5.2.8 4 Configure and Define a pre-shared key	100
Figure 5.2.8 5 Create an access-list.....	100
Figure 5.2.8 6 Create the transform set.....	101
Figure 5.2.8 7 Create the Crypto Map	101
Figure 5.2.8 8 Apply the crypto map to the outgoing interface.....	101
Figure 5.2.9.1 Install components for installation Nagios Core	102
Figure 5.2.9.2 Install latest release of Nagios Core	102
Figure 5.2.9.3 Extract downloaded file	103
Figure 5.2.9.4 Navigate the nagios source code directory	103
Figure 5.2.9.5 Compile Nagios Core main program	103
Figure 5.2.9.6 Create Nagios user and group	103
Figure 5.2.9.7 Add web server user and www-data.....	104
Figure 5.2.9.8 Install Nagios main program, CGIs and HTML files	104
Figure 5.2.9.9 Install Nagios service configuration files and enable run on system boot....	104

Figure 5.2.9.10 Install and configure permissions on the directory	104
Figure 5.2.9.11 Run make command with install-config option.....	105
Figure 5.2.9.12 Install apache configuration file for nagios	105
Figure 5.2.9.13 Install apache configuration file for nagios	105
Figure 5.2.9.14 Create apache user for authentication.....	105
Figure 5.2.9.15 Set the ownership of the nagios Apache configuration	105
Figure 5.2.9.16 Set the ownership of the nagios Apache configuration	106
Figure 5.2.9.17 Set the ownership of the nagios Apache configuration	106
Figure 5.2.9.18 Start nagios core service	106
Figure 5.2.9.19 Check nagios service status.....	106
Figure 5.2.9.20 Access to nagios website	107
Figure 5.2.9.21 Web interface of nagios core.....	107
Figure 5.2.9.22 Install nagios plugins	108
Figure 5.2.9.23 Extract the plugins.....	108
Figure 5.2.9.24 Compile and install plugins.....	108
<i>Figure 5.2.9.25 Run make and make install for plugins.....</i>	109
Figure 5.2.9.26 Restart nagios	109
Figure 5.2.9.27 Localhost service status is OK.....	110
Figure 5.2.9.28 Download MIB Browser	111
Figure 5.2.9.29 Run sudo apt update before installing java.....	111
Figure 5.2.9.30 Install Java	112
Figure 5.2.9.31 Latest java version	112
Figure 5.2.9.32 Run browser.sh	112
Figure 5.2.9.33 Interface of MIB Browser	113
Figure 5.2.9.34 Install SNMP and libraries	114
Figure 5.2.9.35 Make a copy of the file	114
Figure 5.2.9.36 Command to modify the file.....	114
Figure 5.2.9.37 Edit the configuration file	115
<i>Figure 5.2.9.38 Restart service on Linux.....</i>	115
Figure 5.2.9.39 Restart service snmp on systemd system	116
Figure 5.2.9.40 Test snmpwalk in command line.....	116
Figure 5.2.9.41 Input the community string for read and write	117
Figure 5.2.9.42 Verify information is same with the one configured n snmpd.conf.....	118
Figure 5.2.9.43 Reconfigure nagios plugins	118
Figure 5.2.9.44 Enter root and make install nagios plugin	118
Figure 5.2.9.45 check_snmp plugin is available	119
Figure 5.2.9.46 Configure SNMP on router HQ	119
Figure 5.2.9.47 Configure SNMP on router Branch	119
Figure 5.2.9.48 Configure management ip for vlan SwitchHQ	120
Figure 5.2.9.49 Configure community string for vlan SwitchHQ.....	120
Figure 5.2.9.50 Configure community string for vlan SwitchBranch.....	120
Figure 5.2.9.51 Configure community string for vlan SwitchBranch.....	120
Figure 5.2.9.52 Uncomment a line for switch.cfg	121
Figure 5.2.9.53 Edit configuration for file switch.cfg	128
Figure 5.2.9.54 Get update before install PNP4Nagios	128
Figure 5.2.9.55 Perform all the command for installation.....	131
Figure 5.2.9.56 Edit configuration file for windows.cfg.....	134
Figure 5.2.9.57 Edit configuration file for WorkshopII.cfg	135

Figure 5.2.10.1 Add roles	136
Figure 5.2.10.2 Server pool.....	136
Figure 5.2.10.3 Add features.....	137
Figure 5.2.10.4 Install Roles and Features.....	137
Figure 5.2.10.5 group1IntegrateAD user	138
Figure 5.2.10.6 Radius group.....	138
Figure 5.2.10.7 Group member	139
Figure 5.2.10.8 HQ router properties.....	140
Figure 5.2.10.9 Radius Clients	140
Figure 5.2.10.10 Network policies	140
Figure 5.2.10.11 Group HQ overview.....	141
Figure 5.2.10.12 Group select.....	141
Figure 5.2.10.13 Attribute information	142
Figure 5.2.10.14 Vendor specific information	143
Figure 5.2.10.15 Accounting	143
Figure 5.2.10.16 Settings log file.....	143
Figure 5.2.10.17 Log file	144
Figure 5.2.10.18 AAA configure	145
Figure 5.2.10.19 AAA debug	145
Figure 5.2.11.1 Configure Port for Windows Server	146
Figure 5.2.11.2 Configure Port for Debian Server	146
Figure 5.2.11.3 Configure Port for ITDepartment	146
Figure 5.2.11.4 Configure Port for Remote Access	146
Figure 5.2.11.5 disable unused ports for SwitchHQ	147
Figure 5.2.11.6 disable unused ports for SwitchBranch.....	147
Figure 5.2.11.7 create new VLAN for unusedports	147
Figure 5.2.11.8 Assign unused port to new VLAN for SwitchHQ	147
Figure 5.2.11.9 Assign unused port to new VLAN for SwitchBranch	147
Figure 5.2.11.10 Change VLAN status	147
Figure 5.2.11.11 Securing trunk port.....	148
Figure 5.2.12.1 Installing Samba.....	148
Figure 5.2.12.2 Installing Samba client	149
Figure 5.2.13.1 Update for the system	151
Figure 5.2.13.2 Upgrade for the system	151
Figure 5.2.13.3 Download PBIS package.....	152
Figure 5.2.13.4 Change Execute Permission	152
<i>Figure 5.2.13.5 Installation of PBIS Open Edition.....</i>	153
<i>Figure 5.2.13.6 Create AD group with users</i>	154
Figure 5.2.13.7 Joining system to Active Directory	154
Figure 5.2.13.8 Configure login settings	154
Figure 5.2.13.9 Change directory and Open common session file.....	155
Figure 5.2.13.10 Editing common session file	155
Figure 5.2.13.11 Installation of lightdm.....	156
Figure 5.2.13.12 Change directory and Open configuration file	156
Figure 5.2.13.13 Editing configuration file	157
<i>Figure 5.2.13.14 Open sudoers file</i>	158
<i>Figure 5.2.13.15 Update sudoers file on Debian</i>	158
Figure 5.2.14.1: Install build-essential	159

Figure 5.2.14.2: Install libpcap-dev.....	159
Figure 5.2.14.3: Install libpcre3-dev	159
Figure 5.2.14.4: Install libdumbnet-dev	159
Figure 5.2.14.5: Install bison flex.....	159
Figure 5.2.14.6: Create ~snort_src folder.....	160
Figure 5.2.14.7: Go to the ~snort_src folder.....	160
Figure 5.2.14.8: Download DAQ 2.0.7	160
Figure 5.2.14.9: Extract daq-2.0.7.tar.gz	160
Figure 5.2.14.10: Go to the daq-2.0.6 folder.....	160
Figure 5.2.14.11: Unpack and configure daq-2.0.7.....	160
Figure 5.2.14.12: Make the daq-2.0.7	161
Figure 5.2.14.13: Install the daq-2.0.7	161
Figure 5.2.14.14: Install zlib1g-dev.....	161
Figure 5.2.14.15: Download snort-2.9.17	161
Figure 5.2.14.16: Extract snort-2.9.17.tar.gz	161
Figure 5.2.14.17: Go to snort-2.9.17 and configure the snort	161
Figure 5.2.14.18: Make the snort-2.9.17	162
Figure 5.2.14.19: Install the snort-2.9.17	162
Figure 5.2.14.20: Command to update the shared library.....	162
Figure 5.2.14.21: Create a symlink.....	162
Figure 5.2.14.22: Group add snort	162
Figure 5.2.14.22: Create user	163
Figure 5.2.14.23: Create rules file	163
Figure 5.2.14.24: Create dynamic rules file	163
Figure 5.2.14.25: Create a log file	163
Figure 5.2.14.26: Change permission for snort file	163
Figure 5.2.14.27: Set permission for log file	163
Figure 5.2.14.28: Set permission for dynamic rules file	163
Figure 5.2.14.29: Change ownership for snort file	164
Figure 5.2.14.30: Change ownership for log file	164
Figure 5.2.14.31: Change ownership for dynamic rules file	164
Figure 5.2.14.32: Create a white and black file in rules	164
Figure 5.2.14.33: Command to copy the configuration	164
Figure 5.2.14.34: Installation complete.....	165
Figure 5.2.14.35: Open the configuration file.....	165
Figure 5.2.14.36: Insert the Debian IP address	165
Figure 5.2.14.37: Insert external network address with !\$HOME_NET	166
Figure 5.2.14.38: Change the path to the rules files	166
Figure 5.2.14.39: Set the absolute path appropriately	166
Figure 5.2.14.40: Comment all the include line except local.rules	166
Figure 5.2.14.41: Command for testing configuration.....	167
Figure 5.2.14.42: Result for configuration.....	167
Figure 5.2.14.43: Open our local rules	167
Figure 5.2.14.44: Custom snort rules	168
Figure 5.2.14.45: Setup source port.....	169
Figure 5.2.14.46: Result after setup source and destination port.....	169
<i>Figure 5.2.15.1 : Go to website and click download</i>	170
Figure 5.2.15.2 : Download SoftEther VPN	170

Figure 5.2.15.3 : Choose requirement	171
<i>Figure 5.2.15. 4 : Download section.....</i>	171
Figure 5.2.15.5: Choose software component to install.....	172
<i>Figure 5.2.15.6 : Agree to End user Agreement</i>	172
Figure 5.2.15.7 : Important Notice	173
Figure 5.2.15.8 : Path Selection	173
Figure 5.2.15.9 : Wait for installation	174
Figure 5.2.15.10 : Finish installation	174
Figure 5.2.15.11 SoftEther VPN Server Manager Interface	175
Figure 5.2.15.12 : Select local host	176
Figure 5.2.15.13 : Set up local host.....	177
Figure 5.2.15.14 : Set administrator password	177
Figure 5.2.15.15 : Set up bridge.....	178
Figure 5.2.15.16 : Set up confirmation notice	178
Figure 5.2.15.17 : Set up Virtual Hub Name.....	178
Figure 5.2.15.18 : Disable VPN Azure Services	179
Figure 5.2.15.19 : Create a new user	180
<i>Figure 5.2.15.20 : Set up new user</i>	180
Figure 5.2.15.21 : Confirmation alert of user created	181
Figure 5.2.15.22 : Manage user	181
Figure 5.2.15.23 : Set up local bridge.....	182
Figure 5.2.16.24: Manage Virtual Hub.....	183
Figure 5.2.15.25: Choose Virtual NAT and Virtual DHCP Server (SecureNAT).....	183
Figure 5.2.15.26: Enable SecueNAT	184
Figure 5.2.15.27: Enable SecureNAT alert.....	184
Figure 5.2.15.28: IP address provided by SecureNAT.....	184
Figure 5.2.15.29 : Select Encryption and Network.....	185
Figure 5.2.15.30 : Modify encryption algorithm name	186
Figure 5.2.15.31 : Select IPsec / L2TP Setting	186
Figure 5.2.15.32 : Virtual Hub is created	187
Figure 5.2.15.33: Go to website and click download	187
Figure 5.2.15.34 : Download SoftEther VPN	188
Figure 5.2.15.35 : Choose requirement	188
Figure 5.2.15.36 : Download section	189
Figure 5.2.15.37 : Choose software component to install	189
Figure 5.2.15.38 : Agree to End User Agreement.....	189
Figure 5.2.15.39 : Important Notice	190
Figure 5.2.15.40 : Path Selection	191
Figure 5.2.15.41 : Wait for installation	191
Figure 5.2.15.42 : Finish installation	192
Figure 5.2.15.43 : GUI of SoftEther VPN Client Manager	192
Figure 5.2.15.44 : Create new Virtual Network Adapter.....	192
Figure 5.2.15.45 : Set up Virtual Network Adapter name.....	193
Figure 5.2.15.46 : New virtual network adapter	193
Figure 5.2.15.47 : Set up VPN Connection.....	194
Figure 5.2.15.48 : VPN Connection created	195
Figure 5.2.15.49 : GUI of SoftEther VPN Client Manager	196

Figure 5.2.15.52 : Create new Virtual Network Adapter.....	196
Figure 5.2.15.50 : Set up Virtual Network Adapter name.....	197
Figure 5.2.15.51 : New virtual network adapter	197
Figure 5.2.15.52 : Set up VPN Connection.....	198
Figure 5.2.15.53 : VPN Connection created.....	199
1. Configure Audit Policy.....	200
Figure 5.2.16.1 Local Security Policy	200
Figure 5.2.16.2 Audit privilege use	201
Figure 5.2.16.3 Audit privilege use Properties	201
Figure 5.2.16.4 Audit Policy use - Success, Failure	202
Figure 5.2.16.5 Add Roles and Features Wizard.....	202
Figure 5.2.16.6 Confirm installation selections	203
Figure 5.2.16.7 Installation progress	203
3. Configure Windows Firewall	203
Figure 5.2.16.8 Windows Firewall with Advanced Security.....	204
Figure 5.2.16.9 Domain Profile.....	204
Figure 5.2.16.10 Windows Firewall with Advanced Security after enabling	205
4. Disable Automatic.....	205
Figure 5.2.16.11 services.msc	205
Figure 5.2.16.12 Print Spooler Properties	206
Figure 5.2.16.13 Distributed Transaction Coordinator	206
Figure 5.2.16.14 services.msc	207
Figure 5.2.16.15 Windows Error Reporting Service.....	207
Figure 5.2.16.16 services.msc	208
Figure 5.2.16.17 Secure Socket Tunneling Protocol Service.....	208
Figure 5.2.16.18 services.msc	209
Figure 5.2.16.19 NetLogon Properties	209
Figure 5.2.16.20 Welcome to the Security Configuration Wizard.....	210
Figure 5.2.16.21 Configuration Action	210
Figure 5.2.16.22 Select Server.....	211
Figure 5.2.16.23 Processing Security Configuration Database.....	212
Figure 5.2.16.24 Role-Based Service Configuration.....	212
Figure 5.2.16.25 Select Server Roles.....	212
Figure 5.2.16.26 Select Client Features	213
Figure 5.2.16.27 Select Administration and Other Options	214
Figure 5.2.16.28 Handling Unspecified Services	214
Figure 5.2.16.29 Confirm Service Changes.....	215
Figure 5.2.16.30 Network Security	215
Figure 5.2.16.31 Network Security Rules	215
Figure 5.2.16.32 Registry Settings	216
Figure 5.2.16.33 Require SMB Security Signatures	216
Figure 5.2.16.34 Outbound Authentication Methods	217
Figure 5.2.16.35 Outbound Authentication using Domain Accounts	217
Figure 5.2.16.36 Registry Settings Summary	218
Figure 5.2.16.37 Audit Policy	218
Figure 5.2.16.38 System Audit Policy.....	219
Figure 5.2.16.39 Audit Policy Summary	219
Figure 5.2.16.40 Save Security Policy.....	220

Figure 5.2.16.41 Security Policy File Name.....	220
Figure 5.2.16.42 Apply Security Policy	221
Figure 5.2.16.43 Completing the Security Configuration Wizard	221
Figure 5.2.17.1: apt update	222
Figure 5.2.17.2: apt upgrade	223
Figure 5.2.17.3: Reboot	223
Figure 5.2.17.4: Daily update	223
Figure 5.2.17.5: apt install ufw	223
Figure 5.2.17.6: ufw status	224
Figure 5.2.17.7: ufw default deny incoming	224
Figure 5.2.17.8: ufw allow ssh.....	224
Figure 5.2.17.9: ufw enable.....	224
Figure 5.2.17.10: Set password expiration	225
Figure 5.2.17.11: Password expiration	225
Figure 5.2.17.12: Install libpam-cracklib	226
Figure 5.2.17.13: Password configuration file.....	226
Figure 5.2.17.14: Install nmap	227
Figure 5.2.17.15: Identify open port.....	227
Figure 5.2.17.16: Disable CUPS	228
Figure 5.2.17.17: List the port	228
Figure 5.2.17.18: Bluetooth configuration file	228
Figure 5.2.17.19: Add “rfkill block bluetooth”	229
Figure 5.2.17.20: Bluetooth main file.....	229
Figure 5.2.17.21: Add command	229
Figure 5.2.17.22: Bluetooth status.....	230
Figure 6.2.1.1 sh ip bgp summary on Router HQ	257
Figure 6.2.1.2 sh ip bgp summary on Router ISP.....	258
Figure 6.2.1.3 sh ip bgp summary on Router Branch	258
Figure 6.2.1.4 sh ip nat translation on Router HQ	259
. Figure 6.2.1.5 sh ip nat translation on Router Branch.....	259
Figure 6.2.2.1 nslookup from client IT Department.....	259
Figure 6.2.2.2 nslookup from client Remote Access.....	260
Figure 6.2.3.1 Ping in cmd	261
Figure 6.2.3.2 System tab	261
Figure 6.2.3.3 System properties tab	262
Figure 6.2.3.4 Computer name/domain changes tab.....	262
Figure 6.2.3.5 Username and password entered.....	262
Figure 6.2.3.6 Domain successfully join	263
Figure 6.2.3.7 Command to apply GPO	263
Figure 6.2.3.8 Testing of the first GPO	264
Figure 6.2.3.9 Account is being locked.....	264
Figure 6.2.3.10 Testing of the second GPO	265
Figure 6.2.4 1 ipconfig IPv4 remote.....	266
Figure 6.2.4 2 ipconfig IPv4 ITDepartment	266
igure 6.2.4 3 Address Lease IPv4 remote	267
Figure 6.2.4 4 Address Lease IPv4 ITDepartment.....	267
Figure 6.2.4 5 ipconfig IPv6.....	269
Figure 6.2.4 6 Address Lease IPv6	269

Figure 6.2.5.1 Web	270
Figure 6.2.5.2 SSL	270
Figure 6.2.5.3 Virtual Host	271
Figure 6.2.6.1 Inbox	271
Figure 6.2.6.2 Success send.....	272
Figure 6.2.7.1 Test nagios before apply acl rule 1	273
Figure 6.2.7.2 Test nagios after apply acl rule 1	273
Figure 6.2.7.3 Test linux emails before apply acl rule 1	274
Figure 6.2.7.4 Test linux emails after apply acl rule 1	274
Figure 6.2.7.5 Test ftp before apply acl rule 2	275
Figure 6.2.7.6 Test ftp after apply acl rule 2	275
Figure 6.2.7.7 Setup to connect ssh.....	275
Figure 6.2.7.8 Test ssh before apply acl rule 3.....	276
Figure 6.2.7.9 Test ssh after apply acl rule 3.....	276
Figure 6.2.7.10 Setup to connect telnet.....	277
Figure 6.2.7.11 Test telnet before apply acl rule 4.....	277
Figure 6.2.7.12 Test telnet after apply acl rule 4.....	278
Figure 6.2.8 3 Tunnel is active	278
Figure 6.2.8 2 Current IPSec configuration	279
Figure 6.2.8 3 Ipsec mapping table	279
Figure 6.2.9.1 Status monitoring for localhost	280
Figure 6.2.9.2 Status monitoring for Router HQ	281
Figure 6.2.9.3 Status monitoring for Router Branch	281
Figure 6.2.9.4 Status monitoring for Switch HQ.....	282
Figure 6.2.9.5 Status monitoring for Switch Branch.....	282
Figure 6.2.9.6 Status monitoring for Server Debian.....	283
Figure 6.2.9.7 Status monitoring for Server Windows.....	283
Figure 6.2.9.8 Stop service FTP Server	284
Figure 6.2.9.9 Status FTP is critical.....	284
Figure 6.2.9.10 Start service FTP Server	284
Figure 6.2.9.11 Status FTP is OK.....	285
Figure 6.2.9.12 Stop service Web Server.....	285
Figure 6.2.9.13 Status Web service is critical.....	286
Figure 6.2.9.14 Start service Web Server.....	286
Figure 6.2.9.15 Status Web service is OK.....	286
Figure 6.2.10.1 privilege level 15	287
Figure 6.2.10.2 privilege level 1	287
Figure 6.2.11.1 sh port-security for SwitchHQ	288
Figure 6.2.11.2 sh port-security for SwitchBranch	288
Figure 6.2.11.3 sh port-security address SwitchHQ	288
Figure 6.2.11.4 sh port-security address SwitchBranch.....	288
Figure 6.2.11.5 sh int trunk SwitchHQ	289
Figure 6.2.11.6 sh int trunk SwitchBranch	289
Figure 6.2.11.7 sh vlan for SwitchHQ	289
Figure 6.2.11.8 sh vlan for SwitchBranch	289
Figure 6.2.12.1 Running IP address.....	291
Figure 6.2.12.2 Entering username and password to access	291
Figure 6.2.12.3 Share files in samba folder	292

Figure 6.2.12.4 Connect to server	292
Figure 6.2.12.5 Enter credentials	292
Figure 6.2.12.6 Share folder in Debian.....	293
Figure 6.2.13.1 Re-joining AD domain group	293
Figure 6.2.13.2 Login successful for AD account	294
Figure 6.2.13.3 Check connected Debian system	294
<i>Figure 6.2.13.4 Verify invalid account</i>	295
Figure 6.2.13.5 Verify AD domain on Debian Server.....	295
Figure 6.2.13.6 Leave domain on Debian.....	295
Figure 6.2.14.1: Command to run IDS for port enp0s9	296
Figure 6.2.14.2: The output of the log that receives the data on port enp0s9	297
Figure 6.2.15.1 : GUI of SoftEther VPN Client Manager.....	298
Figure 6.2.15.2 : Connect to VPN.....	299
Figure 6.2.15.3 : Connection successful.....	299
Figure 6.2.15.4 : Verify VPN Connection.....	300
Figure 6.2.15.5 : Verify IP address	300
Figure 6.2.15.6 : GUI of SoftEther VPN Client Manager.....	301
Figure 6.2.15.7 : Properties of G1-OutsideNet	302
Figure 6.2.15.8 : Connect to VPN.....	302
Figure 6.2.15.9 : Connection successful.....	303
Figure 6.2.15.10 : Verify ip address in cmd	303
Figure 6.2.16.1 Audit privilege use	304
Figure 6.2.16.2 Windows Firewall with Advanced Security.....	304
Figure 6.2.16.3 Password Policy	305
Figure 6.2.16.4 Account Lockout Policy	305
Figure 6.2.16.5 Kerberos Policy	306
Figure 6.2.17.1: Password expiration	307
Figure 6.2.17.2: Password length.....	307
Figure 6.2.17.3: ufw status	307
Figure 6.2.17.4: Bluetooth status	308
Figure 6.2.17.5: CUPS	308
Figure 6.2.17.6: Open port	309

1. CHAPTER 1: INTRODUCTION

1.1. Introduction

Subject BITU 3923, Workshop II is introduced to all FTMK Bachelor Degree students. This subject is a prerequisite for BITC and BITZ students to act as a platform to prepare before undergoing their Final Year Project and Industrial Training. This subject trains students to work in a group and is required to develop a project based on their major.

This project required students to design, install, maintain and secure the network environment with stated basic client applications and services by using the equipment provided such as three servers, one network interface card (NIC), one router (2 Fast Ethernet), one wireless router and many more.

In this scenario, company XYZ is expanding with approximately 100 employees and is in the process of setting up a new IT department. The company is divided into two sites. The HQ site, where the main server is homed and the clients connect to and the remote site (Branch).The sites are connected with a simple point-to-point tunnel that can be used to carry IPv6 packets between the sites. We have to set up the infrastructure for company XYZ that covers all networking functions for internal and external IT communications, user management, port management, security, remote access to the network for telecommuters and network monitoring. Apart from that, the company also wants to provide several services to their employees, such as email and web services.

1.2. Objective

1. To setup and secure a network infrastructure using the available tool.
2. To maintain and control the secure network services infrastructure.
3. To implement designated network and security services.

1.3. Project Plan/Schedule

1.3.1. Gantt chart of Project

Weeks	ITEM	ACTION
2-3	<p>Project Proposal Includes:</p> <ol style="list-style-type: none"> 1. Executive Summary 2. Organization Chart 3. Network Design (Logical and Physical) 4. VLSM Addressing 5. Gantt charts and project distribution. <p>Device Setup Student must ensure that the provided PCs can be access from home using remote desktop connection such as VNC/TeamViewer/AnyDesk or others account which has been setup by the Supervisor.</p>	<p>Proposal Submission Log Book Review Test Connection</p>
6-7	Progress I Presentation of project progress: setup minimum 30% services.	Present Progress I Log Book Review
11	<p>Progress II Presentation of project progress: completed all services 100%.</p> <p>Each individual in the group is required to demonstrate their individual and group task respectively with the supervisor</p>	Present Progress III Log Book Review
12	Video & Poster Video and poster preparation involves ONE (1) services that has been set. Video and poster (softcopy) should be presented to supervisor for the purpose of evaluation at week 12-13	Video & Poster submission Log Book Review
13	Demonstration Each individual in the group is required to demonstrate their individual and group task respectively with the evaluator	
14	Workshop II Competition Video is pre-evaluated by the juries. Only poster is evaluated in an online session by the juries on the competition day.	Workshop II Competition
Study Week	Final Report, Peer Assesment Report, and Log Book	Final Report, Peer Assesment Report, and Log Book Submission

Table 1.3.1.1 Gantt Chart of Project

1.3.2. Completion Date Every Task

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V				
NO	TASK	OCTOBER				NOVEMBER				DECEMBER				JANUARY											
		2	3	4	1	2	3	4	5	1	2	3	4	1	2	3	4	W8	W9	W10	W11	W12	W13	W14	W15
7	PLANNING	W1	W2	W3	W4	W5	W6	W7																	
8	1 BRIEFING OF WORKSHOP																								
9	2 ASSIGNED TO SUPERVISOR																								
10	3 VERIFY PROJECT TITLE AND SYNOPSIS																								
11	4 SUBMISSION OF PROPOSAL																								
12	BITC SERVICES																								
13	1 VLSM ADDRESSING																								
14	2 INTERVLAN																								
15	3 ROUTING, NAT																								
16	4 DNS																								
17	5 ACTIVE DIRECTORY																								
18	6 DHCP																								
19	7 WEB, SSL, VH																								
20	8 LINUX EMAIL SERVER																								
21	9 ACCESS CONTROL LIST																								
22	10 IPSEC SITE-TO-SITE TUNNELING																								
23	11 NETWORK MONITORING SYSTEM																								
24	11 AAA USING RADIUS																								
25	BITZ SERVICES																								
26	1 LAYER 2 SECURITY																								
27	2 SAMBA AND SAMBA SECURITY																								
28	3 USER AUTHENTICATION WITH AD																								
29	4 IDS PORT MIRRORING																								
30	5 IPSEC VPN SERVER EEMOTE EMPLOYEE																								
31	6 WINDOWS SERVER HARDENING																								
32	7 LINUX SERVER HARDENING																								
33	8 AUDIT COMPLIANCE																								
34																									

Table 1.3.2.1 Completion Date Every Task

1.3.3. Individual Task

No	PERSON IN CHARGE	SERVICES
BITC SERVICES		
1.	Nurul Afifah Binti Ahmad Mahin	<ul style="list-style-type: none"> • Routing & NAT • DNS (IPv4 & IPv6) • Network Management System
2.	Ahmad Faris Bin Mazlan	<ul style="list-style-type: none"> • DHCP (IPv4 & IPv6) • IPSec site-to-site Tunneling
3.	Amirah Syahirah Binti Ariffin	<ul style="list-style-type: none"> • Active Directory • Access Control List (ACL)
4.	Muhammad Ariq Bin Adnan	<ul style="list-style-type: none"> • AAA (Authentication, Authorization and Accounting) using Radius • Linux Email Server • Web, SSL & Virtual Hosting
BITZ SERVICES		
5.	Ahmad Akmal Hazim Bin Zulkifli	<ul style="list-style-type: none"> • Samba and Samba security services • Audit Compliance • Layer 2 security
6.	Tan Chun Yong	<ul style="list-style-type: none"> • IPSec VPN server for remote employees • Windows Hardening and Vulnerability Report • User authentication user by integrating AD with linux
7.	Siti Aishah Binti Sahaludin	<ul style="list-style-type: none"> • IDS • Linux Server Hardening and Vulnerability Report

Table 1.3.3.1 Completion Date Every Task

1.4. Conclusion

At the end of this project, the benefits that we will get based on this progress of workshop 2 is to apply the theory that we have learnt for this project. We will be able to do a network design based on the situation that has been given and develop an organizational security policy. We should understand and analyze network services, application performance, network traffic and protocols, network-troubleshooting concepts and network security concepts. Besides that, after we finish workshop 2 we will be able to understand and use the knowledge of network devices.

At the end of this project, the benefits that we will get based on this progress of workshop 2 is to apply the theory of functioning such as router and switch. During this course, we are exposed to handling the real situation to work in a group such as discussing and getting the solution with other opinions from team members to complete the task successfully.

Moreover, we will use several software such as Virtual Box, GNS3 and VNC. By using the software provided, we have the ability to install, configure, set up, monitor and maintain our own network given the necessary network equipment. We will use a varied type of operating system such as Microsoft Windows 2012, Debian. We also can design our own network and maintain a good network environment.

Furthermore, in Workshop 2, we will learn to set up some security configuration such as server hardening, port security, access control list (ACL), and so forth to enhance the security level of our network and protect the network being accessed or hacked by unauthorized access. To give an opportunity to apply the concept or knowledge that we learned during the lecture such as Computer Organization and Architecture, Operating System, Local Area Network (LAN), Wide Area Network (WAN), Network analysis and Design, and so on.

2. CHAPTER 2: PROJECT REQUIREMENT

2.1. Introduction

The secure network infrastructure will be designed by using the available tools. Workshop II, are required to use different operating platforms. We are using two different operating systems which are Windows Server 2012 and Debian 10 Buster for setup on the servers and Windows 10 Pro for the client PC using virtual machines that are provided by UTeM and personal lab computers. All Linux operating systems do not require any license as it is provided as open source and able to download through online. By using the equipment above, are required to design, set up, maintain and monitor a network environment with basic server applications and fundamental services. Besides that, we are setting up 18 services and it will be divided among the servers. There are 10 services of computer networking and 8 services of network security. The servers will be using mainstream operating systems to simulate real environment and superior services for the users. It is very important to make sure that the network system operates at the desired performance and the technologies used will be the best possible, depending on the allocated budget. , will explain our selection in the next section.

2.2. Types of Operating System use in project

An operating system is a program that acts as an interface between the user and the computer hardware and controls the execution of all kinds of programs. It is to manage the computer's memory, processes, software and hardware. To let the user gain a good experience when they operate the computer, a high-quality operating system is needed to integrate network services infrastructure to suit the network environment and security policies that have been set. It is very important to make sure that the network system operations are doing. Hence, by choosing 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. The operating systems used in the project are Windows Server 2012 and Debian 10 Buster.

2.3. Operating system background

2.3.1. Windows Server 2012

Windows Server 2012, formerly codenamed Windows Server 8, is the latest version of Windows Server. The successor of Windows Server 2008 R2, its improvements include overall upgrades in cloud computing and storage infrastructure. Those enhancements are Graphical user interface (GUI), which it was made with the Metro structure language so it has the same look and feel from Windows 8 except if introduced in Server Core mode and administrators can switch between Server Core and the Server with GUI choices without a full reinstallation. Next, address management which has an IP address management (IPAM) role for discovering, monitoring, auditing and managing the network's IP address space. Other than that, hyper-V which offers a scalable, virtual extensible switch that allows a virtual network to extend its functionality in ways that were difficult or impossible to achieve in previous versions.

2.3.2. Debian 10 Buster

Debian is an openly accessible computer operating system that utilizes the Linux kernel and other program components acquired from the GNU project. Debian can be downloaded over the Internet or can be purchased on CD-ROM. It is created by more than 500 contributors who comprise the Debian Project. Debian's attention to detail allows us to produce a high-quality, stable, and scalable distribution. Installations can be easily configured to serve many roles, from stripped-down firewalls to desktop scientific workstations to high-end network servers. Debian is especially popular among advanced users because of its technical excellence and its deep commitment to the needs and expectations of the Linux community.

2.4. Operating system justification

In Workshop 2, our group has chosen this particular operating system as its cover all function and features that needed in our network design such as:

2.4.1. Windows Server 2012

- Full GUI support features. It contains a server manager that makes it easy to deploy roles and services.
- Hyper-V features. Hyper-V is a Microsoft virtualization platform that acts and functions like a Virtualbox.
- The features and functions can be easily updated by Microsoft from time to time.

2.4.2. Debian 10 Buster

- Debian is Free software. Debian is made of free and open source software and will always be 100% free. Free for anyone to use, modify, and distribute.
- Debian is the seed and base for many other distributions. Many of the most popular Linux distributions, like Ubuntu, Knoppix, PureOS, SteamOS or Tails, choose Debian as a base for their software. Debian is providing all the tools so everyone can extend the software packages from the Debian archive with their own packages for their needs.
- Debian is a stable and secure Linux based operating system. Debian is an operating system for a wide range of devices including laptops, desktops and servers. Users like its stability and reliability since 1993.

2.5. Hardware requirement

2.5.1. Windows Server 2012

Server Requirement

Processor	2GHz
Memory	2GB
Disk Space	50 GB

2.5.2. Debian 10 Buster

Server Requirement	
Processor	2GHz
Memory	2GB
Disk Space	30 GB

2.6. Hardware justification

2.6.1. Servers

- a. There are two servers which will be installed which are Windows Server 2012 and Debian 10 Buster.
- b. In Windows Server 2012, we installed DNS (IPv4 & IPv6), DHCP, Active Directory, web, SSL & Virtual Hosting, AAA, Windows Hardening and Audit Compliance.
- c. For Debian 10 Buster, we installed Network Management System, IDS, Linux Email Server, User authentication integrate AD with linux, Samba and Samba Security, SSH and FTP Server

2.6.2. Router

To set IP addresses and to make connections between servers and clients and to route information to servers. , are also using cisco router in our workshop project. Model router is Cisco 3725.

2.6.3. Switch

The switch is used to connect all the three servers and the client is using Cisco switch IOSvL2 version qcows2 in our workshop project.

2.7. Conclusion

As the conclusion, before installing an Operating System, one should ensure that the computer meets the requirements. It can be complicated to integrate two different types of Operating System with 18 different services and configuration in a network infrastructure. must consider the compatibility and performance of the server and decide which service belongs to which server. Besides, must list out and research about the hardware requirements to make sure of the network. Also must make sure those requirements are suitable and afford to support our services for each server before installing it. After all these considerations, we would expect a secured network infrastructure with good performance and minimum downtime. Perfect settings can make a strong connection over the internet.

3. CHAPTER 3: DESIGN

3.1. Introduction

In this workshop II, we need to define, design, implement and manage network services. Every group needs to implement their own network design which needs to be applied in real devices. Stated in the requirements, that need us to design the network that include three different servers, three cisco router, two cisco switch and two client host for the design.

3.2. Security Policy

Security Policy is a set of security objectives for a company, rules of behaviour for users and administrators, and system requirements. These objectives, rules, and requirements collectively ensure the security of a network, the data, and the computer systems in an organization. On the overall of the security policy must able to accomplish several tasks, such as:

- It demonstrates an organization's commitment to security.
- It ensures consistency in system operations, software and hardware acquisition.

- It sets the rules for expected behavior.

3.2.1. General

- **Email Policy**

The purpose of this is to ensure the proper use of the email system and make users aware of what situation is considered acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within the networks.

- i. All use of email must be consistent with the policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
- ii. All the data contained within an email message or an attachment must be secured according to the Data Protection Standard.
- iii. Users are prohibited from automatically forwarding the email to any third party email system. Individual messages which are forwarded by the user must not contain any confidential information.
- iv. The email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.
- v. Using a reasonable amount of resources for personal emails is acceptable.

- **Password Protection Policy**

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

- i. All users-level and system-level passwords length must have a minimum of 8 characters.
- ii. The password must include a mix of numbers, uppercase and lowercase letters.
- iii. Avoid passwords based on easily identifiable piece of information
- iv. Do not provide any hint for the password.
- v. Passwords must not be shared with anyone, including supervisors and co-workers. All passwords are to be treated as sensitive information.

3.2.2. Network Security

- **Remote Policy**

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

- i. It is the responsibility of Group 1 with remote access privileges to Group 1's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to our network.
- ii. General access to the Internet for recreational use through our network is strictly limited to our group members (Authorized Users). When accessing our network from a personal computer, Authorized Users are responsible for preventing access to any computer resources or data by non-Authorized Users.
- iii. Secure remote access must be strictly controlled with encryption and strong passphrases.
- iv. 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 Group's 1 Networks.

- **Router and Switch Security Policy**

The purpose of this policy is to describe a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity.

- i. The enable password on the router HQ must be kept in a secure encrypted form.
- ii. The router HQ must have the enable password set.
- iii. All routing updates shall be done using secure routing updates.
- iv. Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.
- v. Only routers HQ use RADIUS for all user authentications.

3.2.3. Server Security

- **Server Security Policy**

This policy is to establish standards for the base configuration of internal server equipment on internal networks. Effective implementation of this policy will minimize unauthorized access to proprietary information and technology.

- i. All internal servers deployed at network Group 1 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.

- ii. Access to services should be logged and/or protected through access control methods such as a web application firewall, if possible.
- iii. Services and applications that will not be used must be disabled where practical.
- iv. Always use standard security principles of least required access to perform a function.
- v. Servers should be physically located in an access-controlled environment.
- vi. If a methodology for secure channel connection is available privileged access must be performed over secure channels, for example encrypted network connections using SSH or IPsec.
- vii. All security-related events on critical or sensitive systems must be logged as follows:
 - a. Weekly full backups of logs will be retained for at least 1 month.
 - b. Monthly full backups will be retained for a minimum of 1 years.

- **Software Installation Policy**

This policy is to outline the requirements around installation software on the computing devices. To minimize the risk of loss of program functionality, the exposure of sensitive information contained within the computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

- i. 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.
- ii. The Information Technology Department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

3.2.4. Application Security

- **Virtual Hosting**

Name-based and IP-based virtual hosting can be combined: a server may have multiple IP addresses and serve multiple names on some or all of those IP addresses. This technique can be useful when using SSL/TLS with wildcard certificates. 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 about web servers, but the principle does carry over to other internet services.

- **DNS Services Policy**

- i. All DNS servers in the network perform standard DNS resolution.
- ii. All DNS servers are configured to listen on all their IP addresses.
- iii. DNS servers are configured to listen on specified IP addresses.

- **Active Directory (AD) Policy**

Administrator is in charge of managing users that are created in the Active Directory. The users in Active Directory are regular users and they have their own password and can be able to log into the IT Department and Remote Access pc. Passwords are created by using uppercase character, lowercase character and number and the maximum password age is 42 days. After 42 days, users need to set up their new passwords.

- **VLAN Service Policy**

- i. VLAN security is applied to create an external VLAN for managing switches.

- ii. VLAN must have at least one active port for a service policy to be configured on.

- **Secure Shell Services Policy**

Secure Shell (SSH) is a protocol for secure remote login and other secure network services over an insecure network.

- **Virtual Private Network (VPN) Services Policy**

- i. Unauthorized users are not allowed to access internal networks.
- ii. VPN gateway should be set up by a network operational group.
- iii. VPN users should be auto disconnected after some time of inactivity.

- **SSL (Secure Sockets Layer)**

SSL is used to provide the security protocol used by the Internet to provide easy access to the websites.

- i. HTTP is insecure and is subject to eavesdropping attacks which can let attackers gain access to online accounts and sensitive information.
- ii. Data or posted that is sent through the browser using HTTPS can ensure that information is encrypted and secure.

- **ACL Policy**

An ACL policy is a set of rules, or permissions, that specify the conditions necessary to perform an operation on a protected object.

An ACL policy identifies the operations permitted on a protected object and lists the identities such as users and groups that can protect object space and ACL policies are defined in the master authorization database. Each ACL policy has a unique name or label. Each ACL policy can be applied to one or more objects. An ACL policy consists of one or more entries that include user and group designations and their specific permissions.

- **Samba Policy**

There are three levels at which security principles must be observed in order to render a site at least moderately secure. They are the perimeter firewall, the configuration of the host server that is running Samba, and Samba itself.

Samba permits a most flexible approach to network security. As far as possible Samba implements the latest protocols to permit more secure MS Windows file and operations. Samba can be secured from connections that originate from outside the local network. Another method by which Samba may be secured is by setting Access Control Entries (ACEs) in an Access Control List (ACL) on the shares themselves.

The Server Message Block (SMB) Protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol. The set of message packets that defines a particular version of the protocol is called a dialect. The Common Internet File System (CIFS) Protocol is a dialect of SMB.

For the security part, the authentication for users to access the shared folder is implemented. Only the valid user(s) can access the shared folder. Besides that, ACL for certain network addresses is also set up to secure the network established between Samba Server and client. Lastly, for this project, permission for shared folders and files are set up and defined for each shared folders and

files. Permissions are defined to restrict client's action on the shared folders and files.

- **Authentication User by Integrate AD with Linux Policy**

- i. Join Linux, and UNIX systems to Active Directory. Transforming the host system into an Active Directory client enables users to secure when using the same authentication and policy services currently deployed for AD.
- ii. Login using username and password that have been set at AD in Windows server. If the username and password are correct, the user can access their account in debian server.
- iii. Active Directory uses LDAP (Lightweight Directory Access Protocol) which is an application protocol for querying and modifying items in directory service providers.

- **Hardening Services Policy**

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

- i. Harden Windows Server
 - a. Passwords must have at least 10 characters including numbers, uppercase and lowercase words to produce a strong password.
 - b. Passwords must be renewed after 42 day.
 - c. Enabled password complexity requirements
 - d. Do not store password using reversible encryption
 - e. Configure Account Lockout Policy set the account lockout with 3 attempts and 2 minutes duration session.
 - f. Disable unnecessary services such as Print Spooler and Distributed Coordinator Properties.

- g. Enable necessary services such as NetLogon and Windows Error Reporting.

- ii. Harden Debian Server

- a. Passwords must have at least 8 characters including numbers, uppercase and lowercase words to produce a strong password.
- b. Passwords must be renewed after 4 months.
- c. Disable unnecessary services such as CUPS service using IPP.

3.3. Physical Design

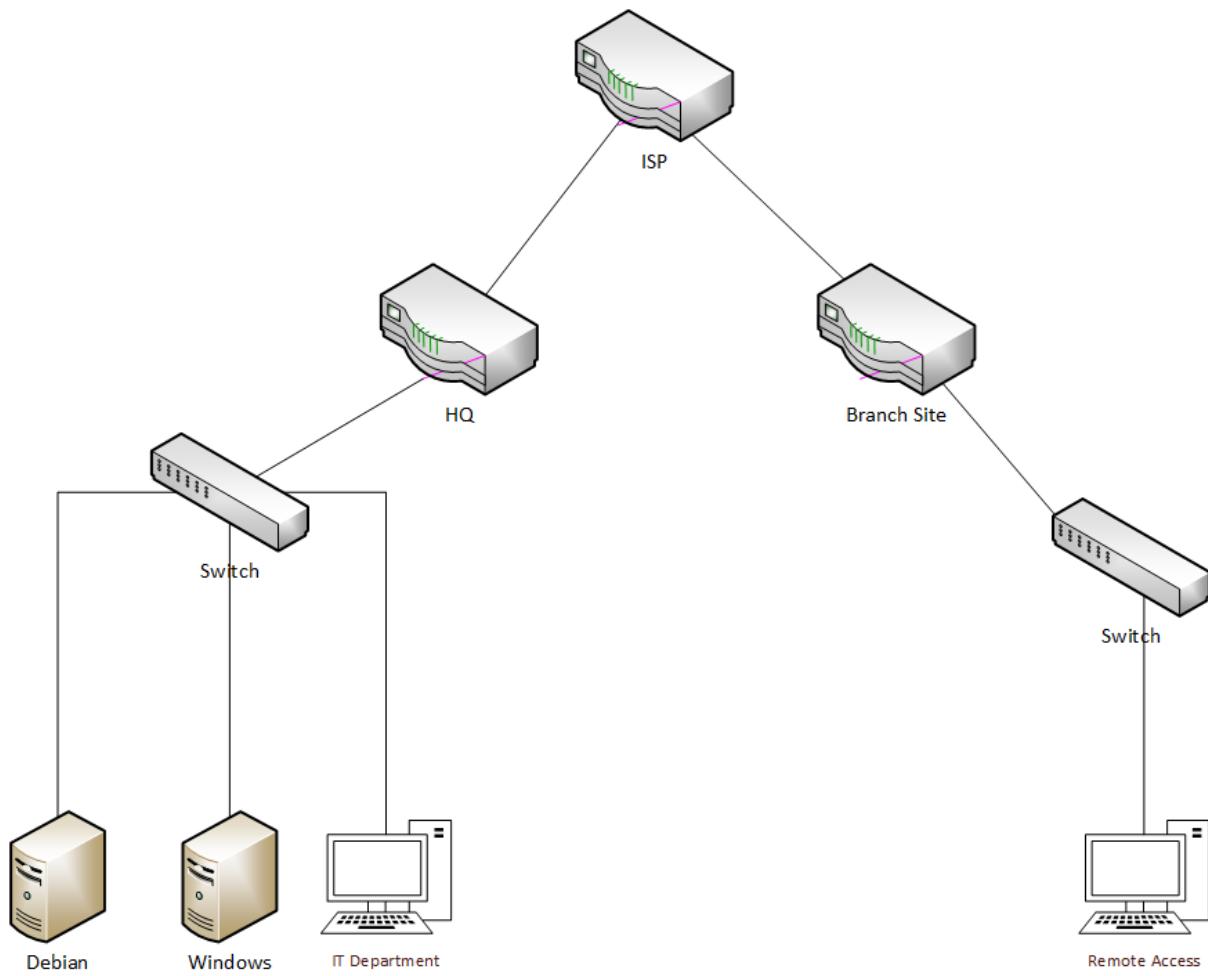


Figure 3.3.1 Physical Design

3.4. Logical (including Security) Design

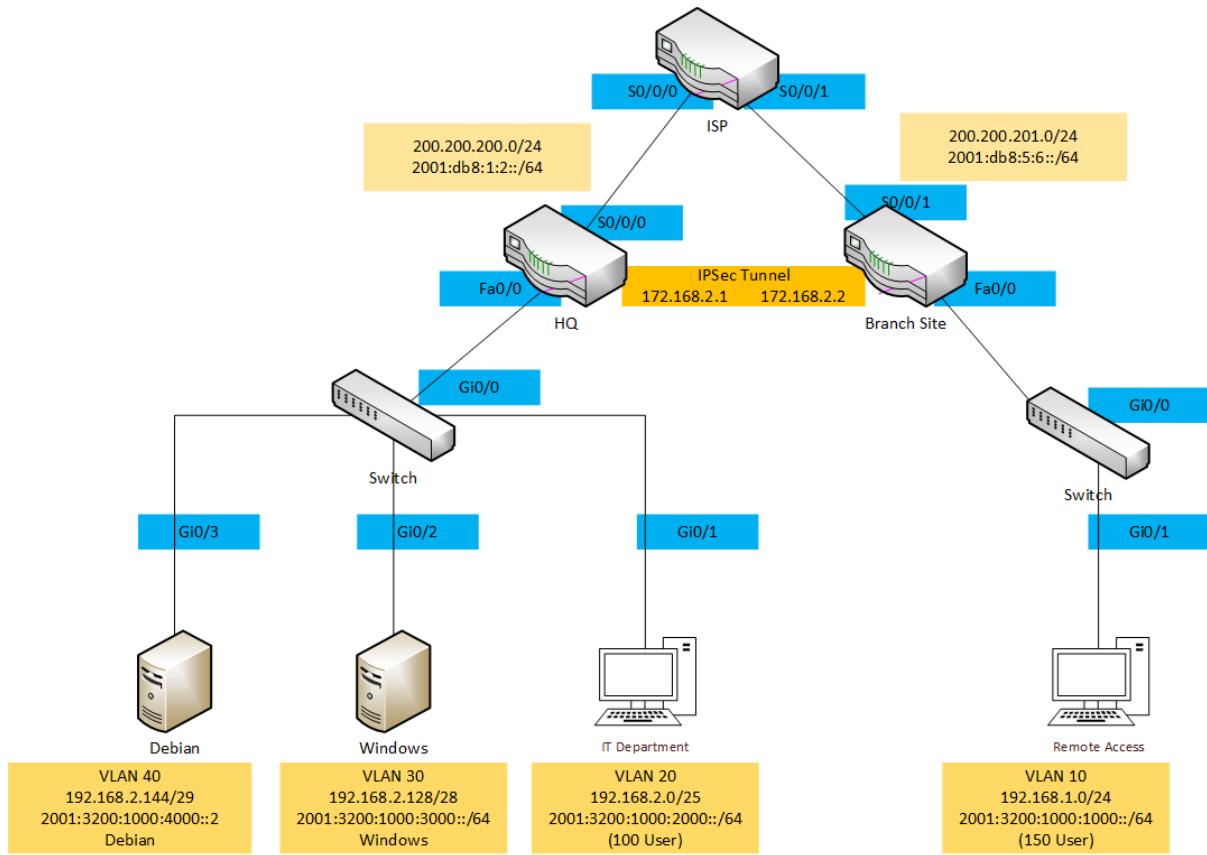


Figure 3.4.1 Logical Design

3.5. Conclusion

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

4. CHAPTER 4: SERVICES

4.1. Introduction

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

4.2. List of services

4.2.1. BITC Services

1. Routing & NAT
2. DNS (IPv4 & IPv6)
3. Active Directory
4. DHCP (IPv4 & IPv6)
5. Web, SSL & Virtual Hosting
6. Linux Email Server
7. Access Control List
8. IPSec site-to-site Tunneling
9. Network Management System
10. AAA (Authentication, Authorization and Accounting) using Radius

4.2.2. BITZ Services

1. Layer 2 Security - VLAN and Port Security
2. Samba and Samba Security
3. User authentication user by integrating AD with Linux
4. IDS
5. IPSec VPN server for remote employees
6. Windows Server Hardening and Vulnerability Report
7. Linux Server Hardening and Vulnerability Report
8. Audit Compliance

4.3. Brief overview for services

4.3.1. Routing and NAT

Routing is the process of selecting paths in a network along which to send network traffic. Routing directs packet forwarding, the transit of logically addressed packets from their source toward their ultimate destination through intermediate nodes. The routing process directs forwarding on the basis of routing tables which maintain a record of the routes to various

network destinations. The routing service provided by the router allows a client to access and receive resources from remote networks.

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

4.3.2. DNS (IPv4 & IPv6)

Domain Name System (DNS) is a hierarchical distributed naming system for computers, services or any resource connected to the Internet or a private network. It associates information with domain names assigned to each of the participating entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for the purpose of locating computer services and devices worldwide.

The client side of the DNS is called a DNS resolver. It is responsible for initiating and sequencing the queries that ultimately lead to a full resolution (translation) of the resource sought, in which translation of a domain name into an IP address. Forward DNS zone contains the record for the mapping of domain names to IP addresses or other information. Reverse zone is finding the DNS name associated with an IP address.

4.3.3. Active Directory

Active Directory is a directory service and it provides authentication and authorization functions, as well as providing a framework. It is also a distributed, hierarchical database structure that shares infrastructure

information for locating, securing, managing, and organizing computer and network resources.

4.3.4. DHCP (IPv4 & IPv6)

The Dynamic Host Configuration Protocol (DHCP) is a network service that enables host computers to be automatically assigned settings from a server as opposed to manually configuring each network host. Computers configured to be DHCP clients need no control over the settings they receive from the DHCP server and the configuration is transparent to the computer's user. It is also a communications protocol that lets network administrators centrally manage and automate the assignment of Internet Protocol (IP) addresses in an organization's network. When a computer uses a static IP address, it means that the computer is manually configured to use a specific IP address.

DHCP has a number of advantages:

- No need to manually configure each client with an IP address.
- Don't need to keep a record of the IP addresses that are needed to be assigned.
- Can automatically assign a new IP address if move a client to a different subnet

4.3.5. Web, SSL & Virtual Hosting

Web server is a system that delivers content or services to end users over the internet. A web server consists of a physical server, server operating system (OS) and software used to facilitate HTTP communication. A web server is also known as an internet server. Every web server has an IP address and possibly a domain name.

Secure Sockets Layer (SSL) is a 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.

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.

4.3.6. Linux Email Server

An email server is an application that is used to transfer mails from one user to another. A mail server handles both sending and receiving mails using protocols such as SMTP (Simple Mail Transfer Protocol) or ESMTP (Extended SMTP) for sending mails and POP3 (Post Office Protocol 3) or IMAP (Internet Message Access Protocol) for receiving mails.

4.3.7. Access Control List

The Access Control List (ACL) are 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.

4.3.8. IPSec Site-to-Site Tunneling

IPsec is a group of protocols that are used together to set up encrypted connections between devices. It helps keep data sent over public networks secure. IPsec is often used to set up VPNs, and it works by encrypting IP packets, along with authenticating the source where the packets come from. A virtual private network (VPN) is an encrypted connection between two or more computers. VPN connections take place over public networks, but the data exchanged over the VPN is still private because it

is encrypted. VPNs make it possible to securely access and exchange confidential data over shared network infrastructure, such as the public Internet. For instance, when employees are working remotely instead of in the office, they often use VPNs to access corporate files and applications.

4.3.9. Network Management System

An NMS is a system designed for monitoring, maintaining, and optimizing a network. It includes both hardware and software, but most often an NMS refers to the software used to manage a network. Network management systems provide multiple services such as network monitoring, device detection and performance analysis.

- **Network monitoring** - NMS software monitors network hardware to ensure all devices are operating correctly and are not near or at full capacity. Alerts can be sent to network administrators if a problem is detected.

- **Device detection** - When a new device is connected to the network, the NMS detects it so that it can be recognized, configured, and added to the network. This is also called device provisioning.
- **Performance analysis** - NMS can gauge the current and historical performance of a network. This includes the overall performance of the network as well as individual devices and connections. For example, the NMS may detect aspects of a network where throughput is nearing the maximum bandwidth available. The data can be used to optimize the flow of traffic and recommend the addition of new hardware if needed

4.3.10. AAA (Authentication, Authorization and Accounting) using Radius

RADIUS (Remote Authentication Dial in User Service) is a networking protocol that provides centralized Authentication, Authorization and Accounting (AAA) management for computers to connect and use a network service. RADIUS is a security service for authenticating and authorizing dial-up users. A typical enterprise network may need an access server attached to a modem pool, along with a RADIUS server to provide authentication services.

4.3.11. Layer 2 Security - VLAN and Port Security

A VLAN (virtual LAN) is a subnetwork that can group collections of devices on separate physical local area networks. The purpose is to improve the performance of a network and security. Port security is to secure the network by preventing unknown devices from forwarding packets.

4.3.12. Samba and Samba security

Samba is an open-source software that runs on Unix or Linux-based platforms. There are four types of security modes for Samba, Share-level, User-level, Server-level, and Domain-level, collectively known as security levels. It also can communicate with Windows clients like a native application. Since 1992, Samba has provided secure, stable, and fast file and print services for all clients using the Server Message Block (SMB)/Common Internet File System protocol (CIFS), such as all versions of DOS and Windows, OS/2, Linux, and many others.

4.3.13. User authentication user by integrating AD with linux

Active Directory (AD) serves as a central location for network administration and security. It is responsible for authenticating and authorizing all users and computers within a Windows domain type network, assigning and enforcing security policies for all computers in a network, and installing or updating software on network computers. The active directory uses Lightweight Directory Access Protocol (LDAP) version 2, three, and DNS. At this project, we need to integrate Active Directory with Linux.

4.3.14. IDS

An intrusion detection system (IDS) is a type of security software designed to automatically alert administrators when someone or something is trying to compromise an information system through malicious activities or security policy violations. An IDS works by monitoring system activity by examining vulnerabilities in the system, files integrity, and analyzing patterns based on already known attacks. It also automatically monitors the Internet to search for any of the latest threats, resulting in a future attack. Port Mirroring, also known as SPAN (Switched Port Analyzer), monitors network traffic. With port mirroring enabled, the switch sends a copy of all network packets seen on one port (or an entire VLAN) to another port, where the packet can be analyzed.

4.3.15. IPsec VPN server for remote employees

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 fulfill security requirements or 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).

4.3.16. Windows Server Hardening and Vulnerability Report

Windows Server hardening involves identifying and remediating security vulnerabilities. Hardening Windows Server 2012 operating systems is the best practice you can implement immediately to reduce the attack surface by disabling functionality that is not required while maintaining the

minimum needed functionality. This service is to implement security procedures from the initial installation. New machines need to install on an isolated network, well protected from possible hostile traffic until the operating system is hardened. Step to harden the Windows Server: i. Configure a security policy ii. Disable or delete unnecessary accounts, ports, and services iii. Uninstall Unnecessary Applications iv. Configure the Windows 2012 Firewall v. Configure Auditing vi. Disable unnecessary shares vii. Configure Encryption on 2012 server viii. Least Privilege.

4.3.17. Linux Server Hardening and Vulnerability Report

Linux OS Server may have some security flaws that can be manipulated by the intruder to steal information. By server hardening, it improves the server security and makes the server more secure. Hardened servers make it more resistant to security issues and threats. Keeping software updated, disable unnecessary service are some of the methods to harden the server.

4.3.18. Audit Compliance

A cybersecurity audit compliance addresses how well your company identifies, detects, protects, responds, and recovers from breaches and other incidents. Precisely, you are expecting to document compliance in the following areas:

- Risk management, including hardware, software, assets, and system interconnections. The risk level must communicate to all stakeholders throughout the organization.
- Configuration management is including settings and baselines for all information systems as well as routine audit procedures.
- Implement training in security and privacy.

4.4. Conclusion

Each service needs their own functionalities and services also need different types of software or packages to be installed on the server. Service can be simple but it can be very important such as some services need to interconnect with other

services so the service can have the functionality. Every configuration needs to be precise and detail all of the services will be fully operational.

5. CHAPTER 5: INSTALLATION AND CONFIGURATION

5.1. Introduction

This chapter presents the installation and the configuration of the services, which we had installed and configured in our network. This chapter will show how each service is installed and configured.

5.2. Services and individual tasks

No	PERSON IN CHARGE	SERVICES
BITC SERVICES		
1.	Nurul Afifah Binti Ahmad Mahin	<ul style="list-style-type: none"> • Routing & NAT • DNS (IPv4 & IPv6) • Network Management System
2.	Ahmad Faris Bin Mazlan	<ul style="list-style-type: none"> • DHCP (IPv4 & IPv6) • IPSec site-to-site Tunneling
3.	Amirah Syahirah Binti Ariffin	<ul style="list-style-type: none"> • Active Directory • Access Control List (ACL)
4.	Muhammad Arij Bin Adnan	<ul style="list-style-type: none"> • AAA (Authentication, Authorization and Accounting) using Radius • Linux Email Server • Web, SSL & Virtual Hosting
BITZ SERVICES		
5.	Ahmad Akmal Hazim Bin Zulkifli	<ul style="list-style-type: none"> • Samba and Samba security services • Audit Compliance • Layer 2 security
6.	Tan Chun Yong	<ul style="list-style-type: none"> • IPSec VPN server for remote employees • Windows Hardening and Vulnerability Report • User authentication user by integrating AD with linux
7.	Siti Aishah Binti Sahaludin	<ul style="list-style-type: none"> • IDS

- | | | |
|--|--|---|
| | | <ul style="list-style-type: none"> • Linux Server Hardening and Vulnerability Report |
|--|--|---|

5.2.1. Routing and NAT

Step 1: Configure BGP routing for Router HQ

```

router bgp 50001
no synchronization
bgp log-neighbor-changes
neighbor 2001:DB8:1:2::2 remote-as 50002
neighbor 200.200.201.2 remote-as 50002
no auto-summary
!
address-family ipv6
neighbor 2001:DB8:1:2::2 activate
network 2001:DB8:1:2::/64
network 2001:3200:1000:2000::/64
network 2001:3200:1000:3000::/64
network 2001:3200:1000:4000::/64
exit-address-family
!
```

Figure 5.2.1.1 Configuration BGP on Router HQ

Step 2: Configure BGP routing for Router ISP

```
router bgp 50002
  no synchronization
  bgp log-neighbor-changes
  network 200.200.200.0
  network 200.200.201.0
  neighbor 2001:DB8:1:2::1 remote-as 50001
  neighbor 2001:DB8:5:6::6 remote-as 50003
  neighbor 200.200.200.6 remote-as 50003
  neighbor 200.200.201.1 remote-as 50001
  no auto-summary
  !
  address-family ipv6
    neighbor 2001:DB8:1:2::1 activate
    neighbor 2001:DB8:5:6::6 activate
    network 2001:DB8:1:2::/64
  exit-address-family
!
```

Figure 5.2.1.2 Configuration BGP on Router ISP

Step 3: Configure BGP routing for Router Branch

```
router bgp 50003
  no synchronization
  bgp log-neighbor-changes
  neighbor 2001:DB8:5:6::5 remote-as 50002
  neighbor 200.200.200.5 remote-as 50002
  no auto-summary
  !
  address-family ipv6
    neighbor 2001:DB8:5:6::5 activate
    network 2001:DB8:5:6::/64
    network 2001:3200:1000:1000::/64
  exit-address-family
!
```

Figure 5.2.1.3 Configuration BGP on Router Branch

NAT

Step 4: Configuration Dynamic NAT on client IT Department in Router HQ

```

HQ#conf t
Enter configuration commands, one per line. End with CNTL/Z.
HQ(config)#access-list 20 permit 192.168.2.0 0.0.0.127
HQ(config)#+$nt 200.200.201.100 200.200.201.200 netmask 255.255.255.0
HQ(config)#ip nat inside source list 20 pool NAT-POOL-ITDepartment

HQ(config)#int f0/0.20
HQ(config-subif)#ip nat inside

*Mar 1 00:15:35.539: %LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, chan
ged state to up
HQ(config-subif)#int f0/0.30
HQ(config-subif)#ip nat inside
HQ(config-subif)#int f0/0.40
HQ(config-subif)#ip nat inside
HQ(config-subif)#int s0/0
HQ(config-if)#ip nat outside

```

Figure 5.2.1.4 Configuration Dynamic NAT for client IT Department

Step 5: Configuration Static NAT on Server Windows in Router HQ

```

HQ#conf t
Enter configuration commands, one per line. End with CNTL/Z.
HQ(config)#ip nat inside source static 192.168.2.130 200.200.201.30

HQ(config)#int f0/0.30
HQ(config-subif)#ip nat inside
HQ(config-subif)#int s0/0
HQ(config-if)#ip nat outside

```

Figure 5.2.1.5 Configuration Static NAT for Server Windows

Step 6: Configuration Static NAT on Server Debian in Router HQ

```

HQ#conf t
Enter configuration commands, one per line. End with CNTL/Z.
HQ(config)#ip nat inside source static 192.168.2.146 200.200.201.40

HQ(config)#int f0/0.40
HQ(config-subif)#ip nat inside
HQ(config-subif)#int s0/0
HQ(config-if)#ip nat outside

```

Figure 5.2.1.6 Configuration Static NAT for Server Debian

Step 7: Configuration Dynamic NAT on client Remote Access in Router Branch

```

Branch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Branch(config)#access-list 10 permit 192.168.1.0 0.0.0.255
Branch(config)#$ss 200.200.200.100 200.200.200.250 netmask 255.255.255.0
Branch(config)#ip nat inside source list 10 pool NAT-POOL-RemoteAccess

Branch(config)#int f0/0.10
Branch(config-subif)#ip nat inside

*Mar 1 00:43:01.419: %LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, chan-
ged state to up
Branch(config-subif)#int s0/1
Branch(config-if)#ip nat outside

```

Figure 5.2.1.7 Configuration Dynamic NAT for client Remote Access

5.2.2. DNS (IPv4 & IPv6)

Step 1: Click on Add Roles and Features

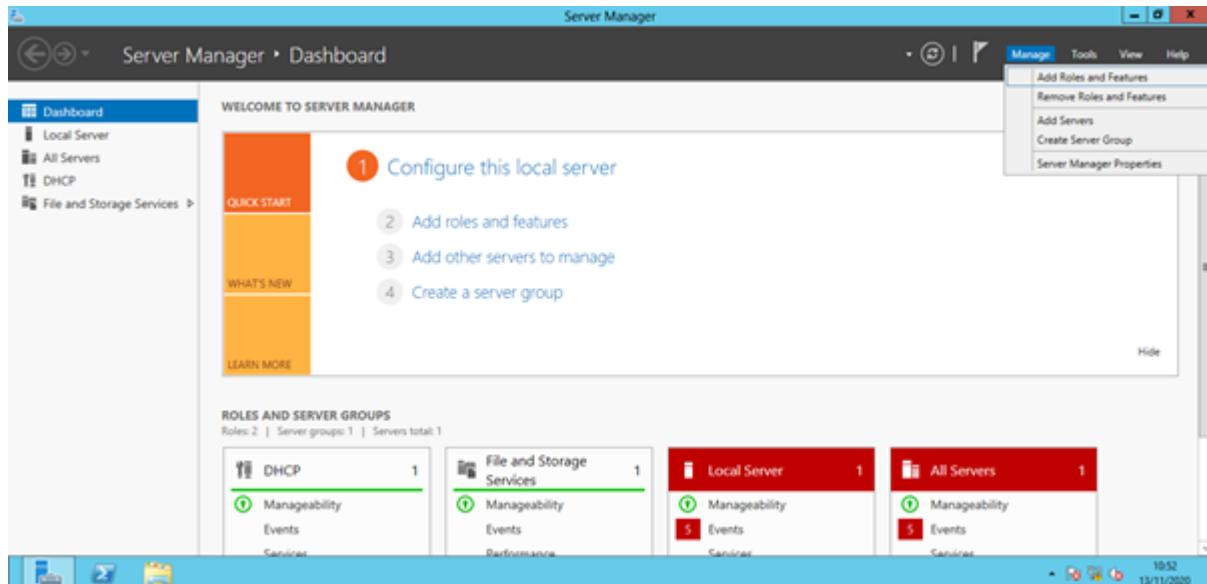


Figure 5.2.2.1 Click on Add Roles and Features

Step 2: Click on Next

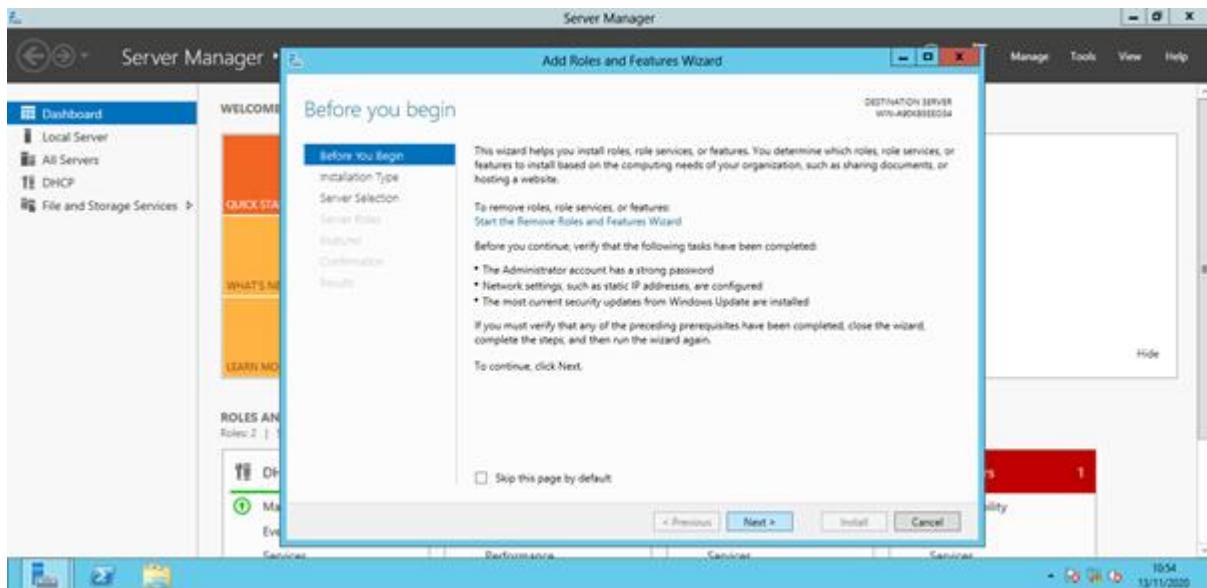


Figure 5.2.2.2 Click on Next

Step 3: Click on Role Based installation

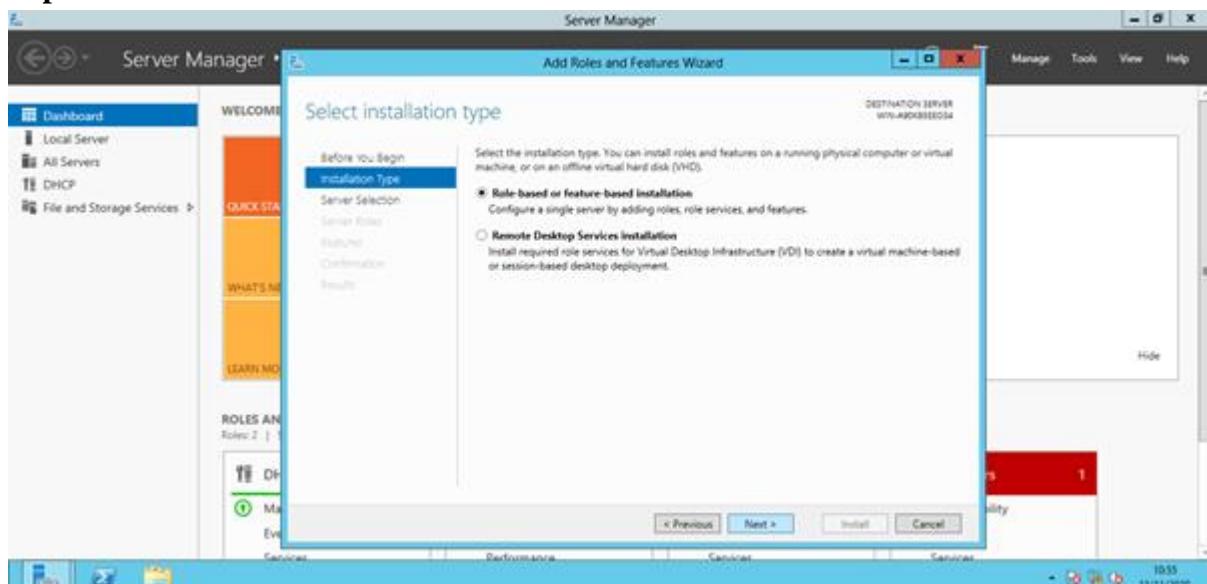


Figure 5.2.2.3 Click on Role based installation

Step 4: Click on Next again

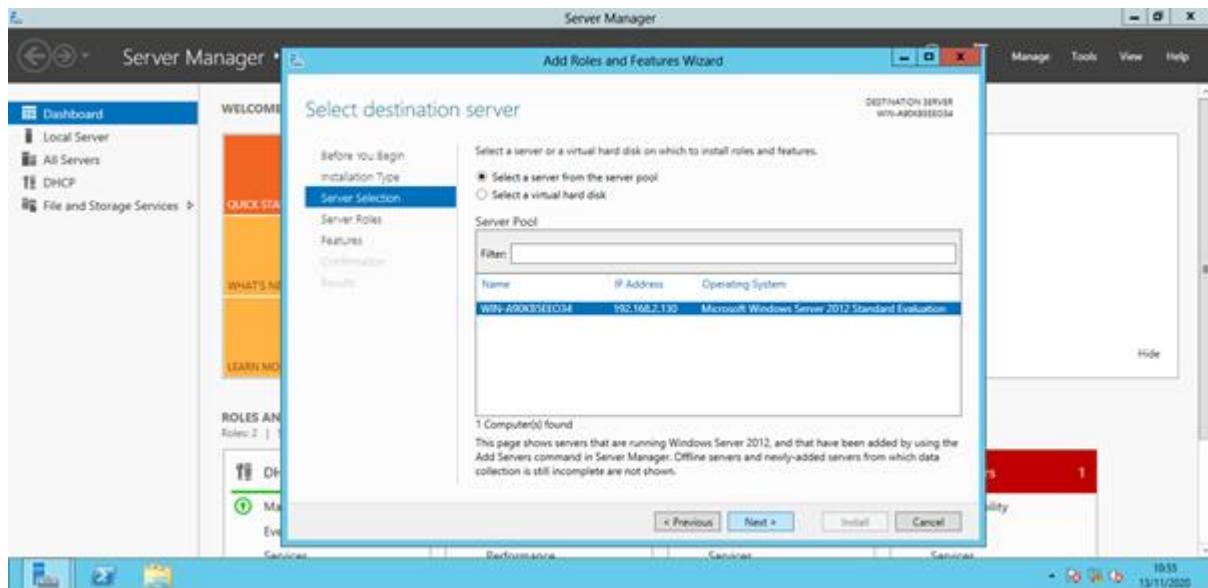


Figure 5.2.2.4 Click on Role server windows

Step 5: Choose DNS Server

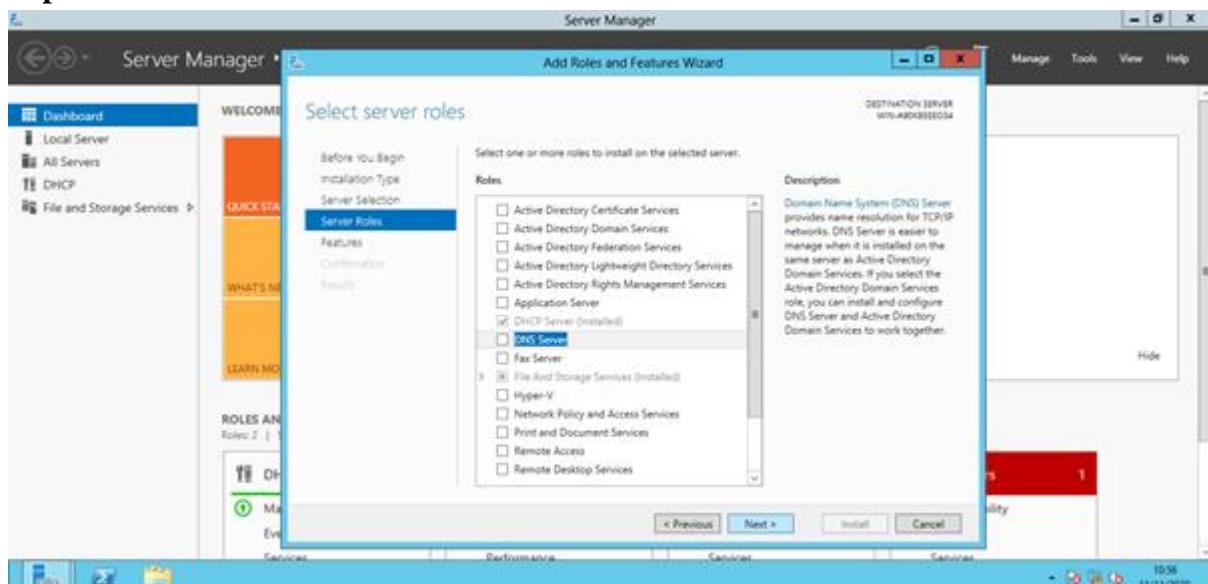


Figure 5.2.2.5 Click on DNS Server

Step 6: Click on Add Features

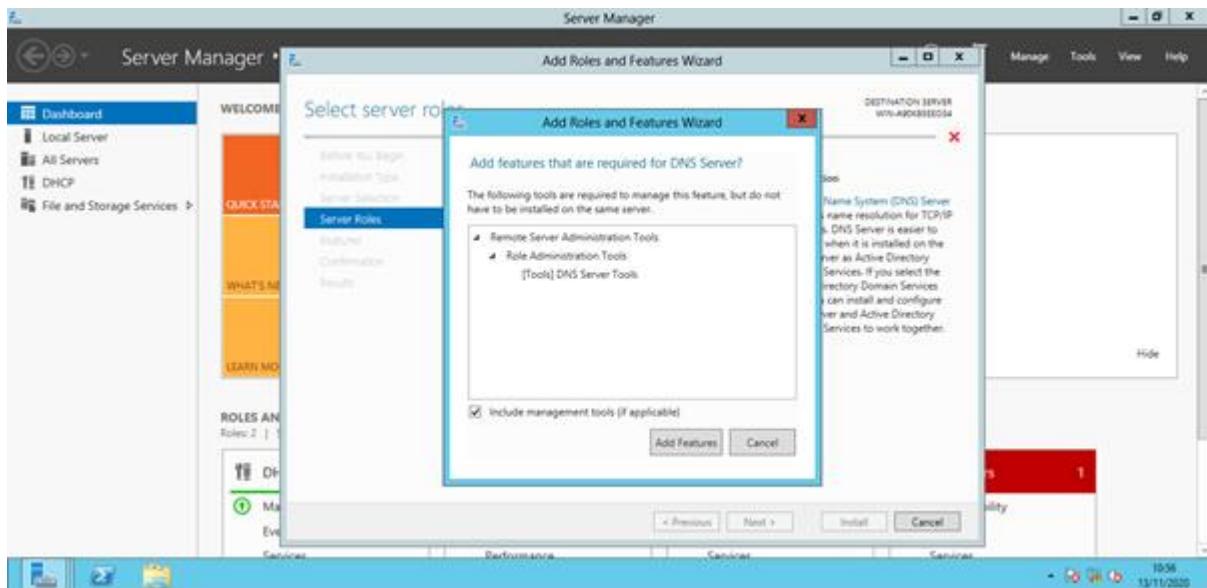


Figure 5.2.2.6 Click on Add Features

Step 7: Click on Next

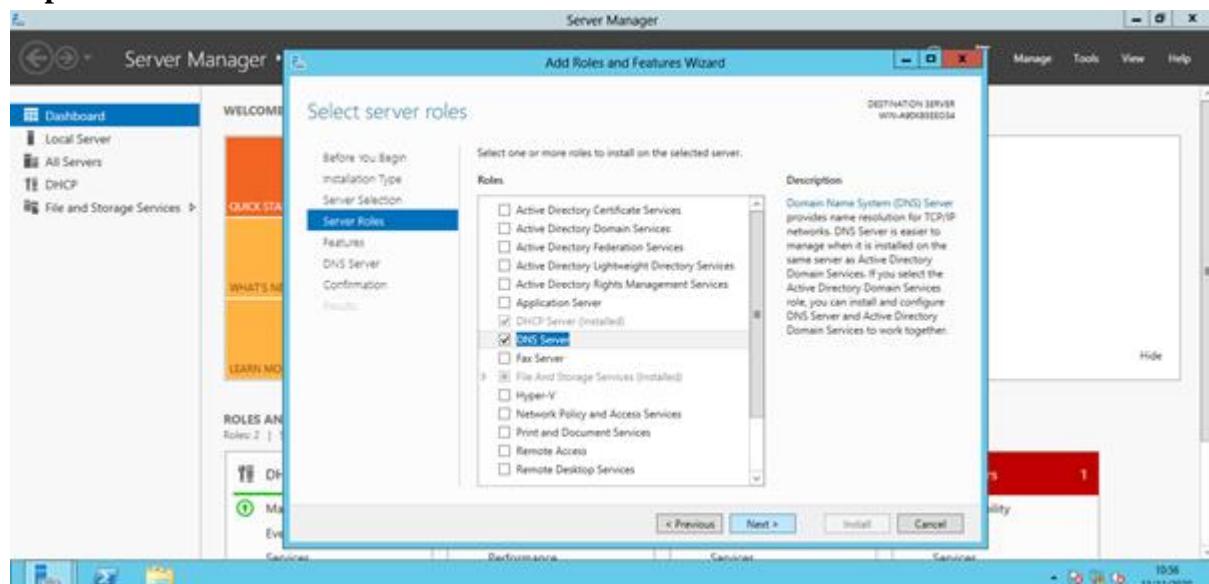


Figure 5.2.2.7 Click on Next

Step 8: Click on Next until the installation part. Click on install to install DNS Server. Wait until the installation finishes and close the window.

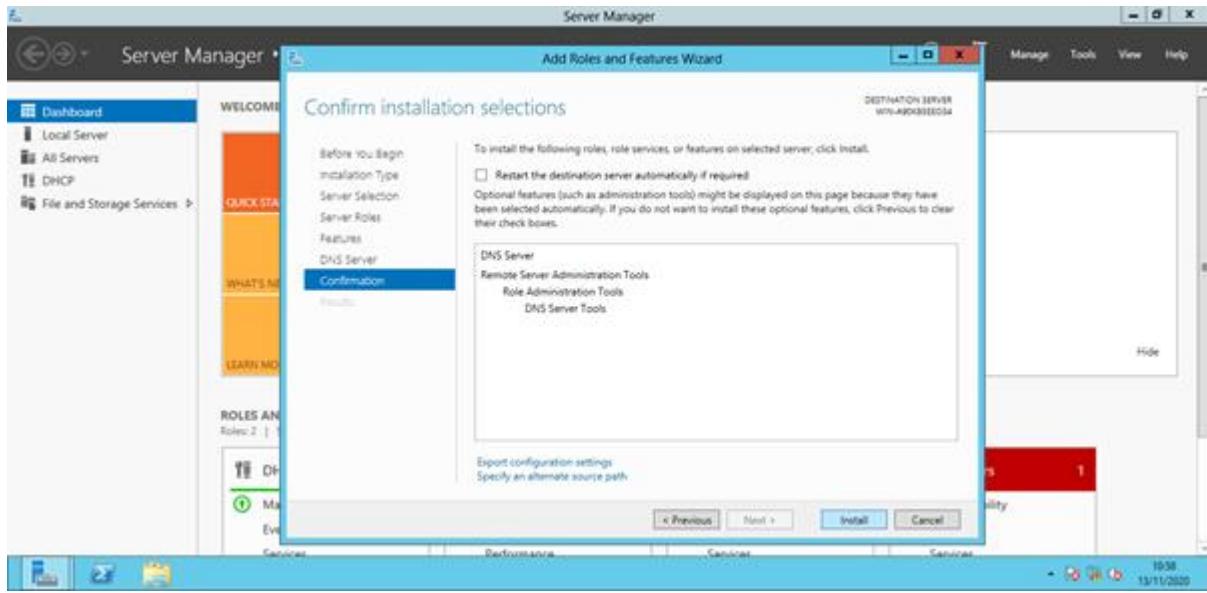


Figure 5.2.2.8 Click on install to install DNS Server

Step 9: Create Forward Lookup zones DNS for IPv4 and IPv6. Click on the domain name which is group1.com and click on New Host (A or AAA) to create forward lookup zone IPv4.

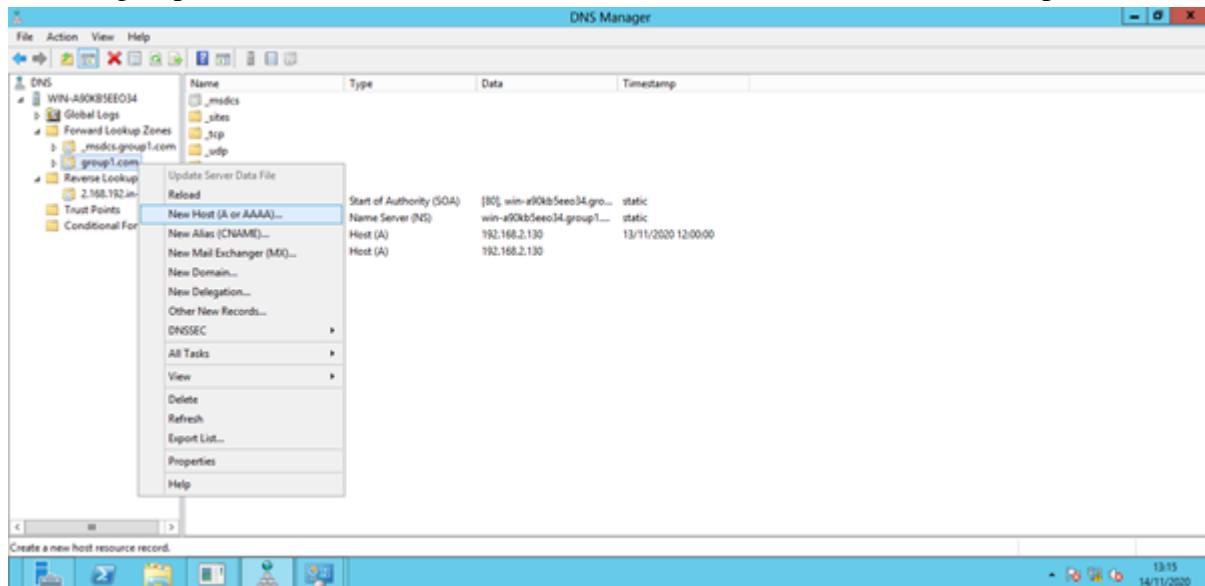


Figure 5.2.2.9 Click on New Host (A or AAA) to create forward zone IPv4

Step 10: Fill in the name and IP address that we want to translate the domain into IP address for IPv4.

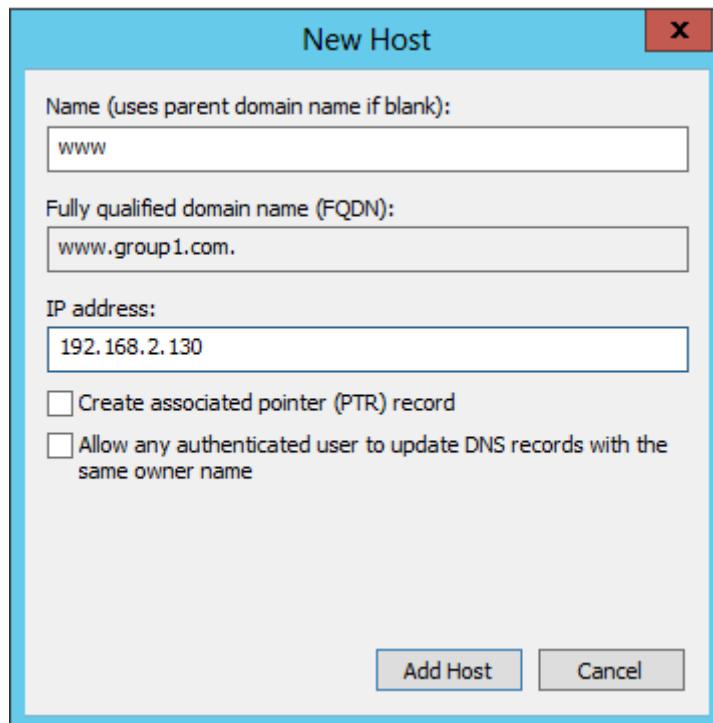


Figure 5.2.2.10 Fill in information for name and IP address for IPv4 DNS

Step 11: The host for IPv4 which is www.group1.com is successfully created.

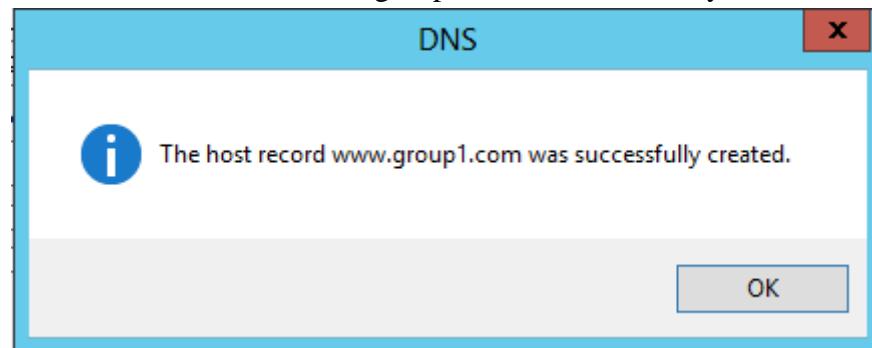


Figure 5.2.2.11 The host www.group1.com for IPv4 is successfully created

Step 12: Click on the domain name which is group1.com and click on New Host (A or AAA) to create forward lookup zone IPv6.

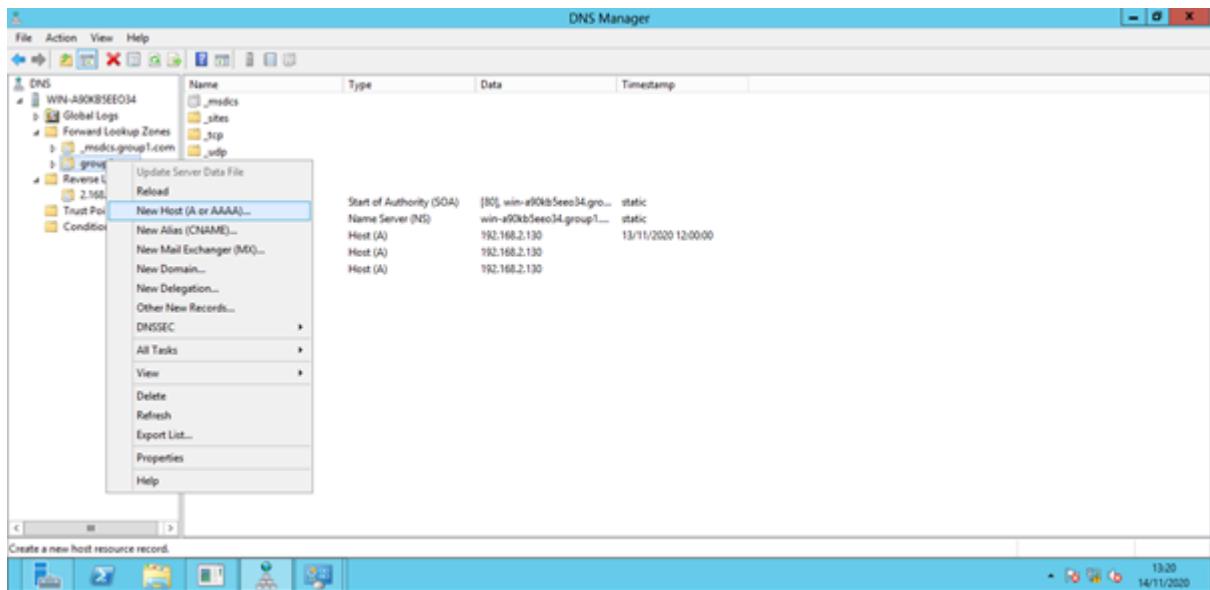


Figure 5.2.2.12 Click on New Host (A or AAAA) to create forward zone IPv6

Step 13: Fill in the name and IP address that we want to translate the domain into IP address for IPv6.

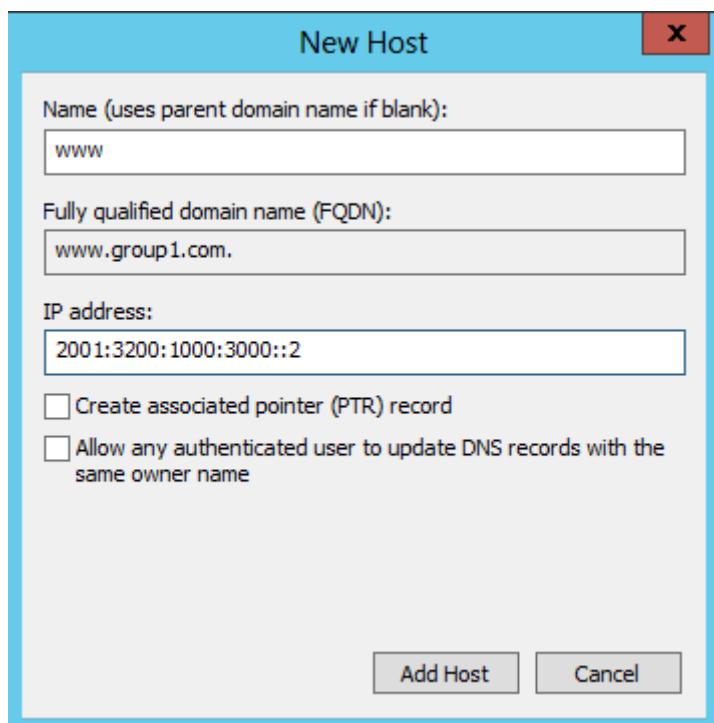


Figure 5.2.2.13 Fill in information for name and IP address for IPv6 DNS

Step 14: The host for IPv6 which is www.group1.com is successfully created.

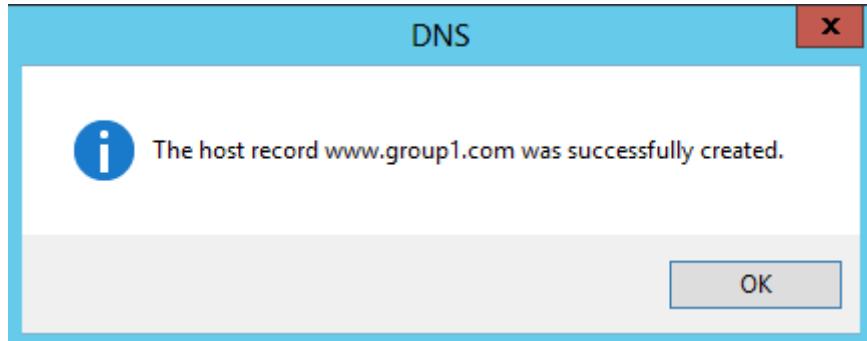


Figure 5.2.2.14 The host www.group1.com for IPv6 is successfully created

Step 15: Repeat the same step to create another forward zone for IPv4 and IPv6. Below is the fully configured forward zone for IPv4 and IPv6.

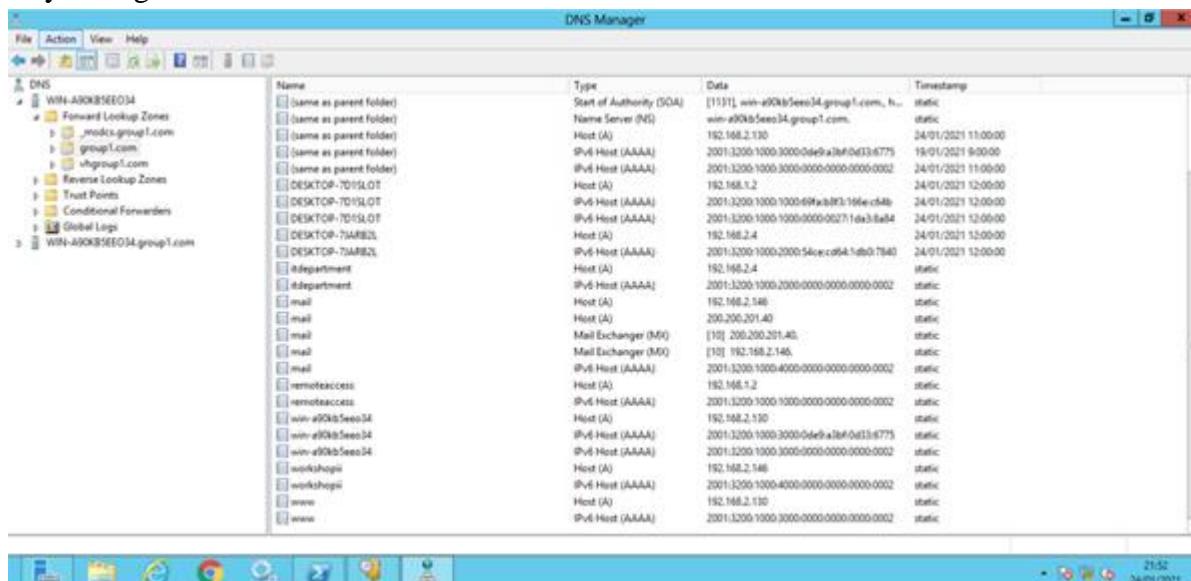


Figure 5.2.2.15 Fully configured forward zone for IPv4 and IPv6

Step 16: Create Reverse Lookup Zones DNS for IPv4 and IPv6. Click on the Reverse Lookup Zones and right click and click on New Zone. This one we create a reverse lookup zone for IPv4.

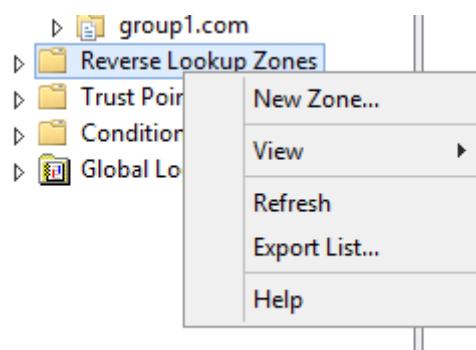


Figure 5.2.2.16 Creating new zone for reverse lookup zone for DNS IPv4

Step 17: Click on Next



Figure 5.2.2.17 New Zone Wizard for reverse lookup zone DNS IPv4

Step 18: Click on Next

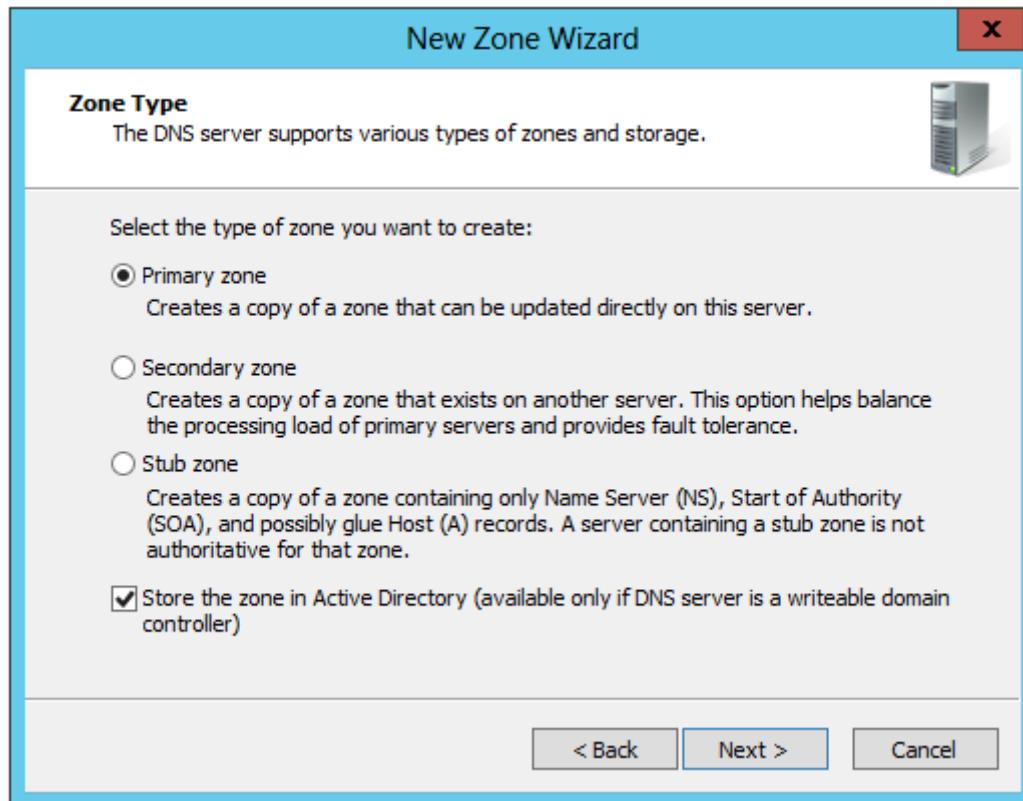


Figure 5.2.2.18 Choose primary zone for reverse lookup zone DNS IPv4

Step 19: Click on to all DNS Servers running on domain controllers in group1.com

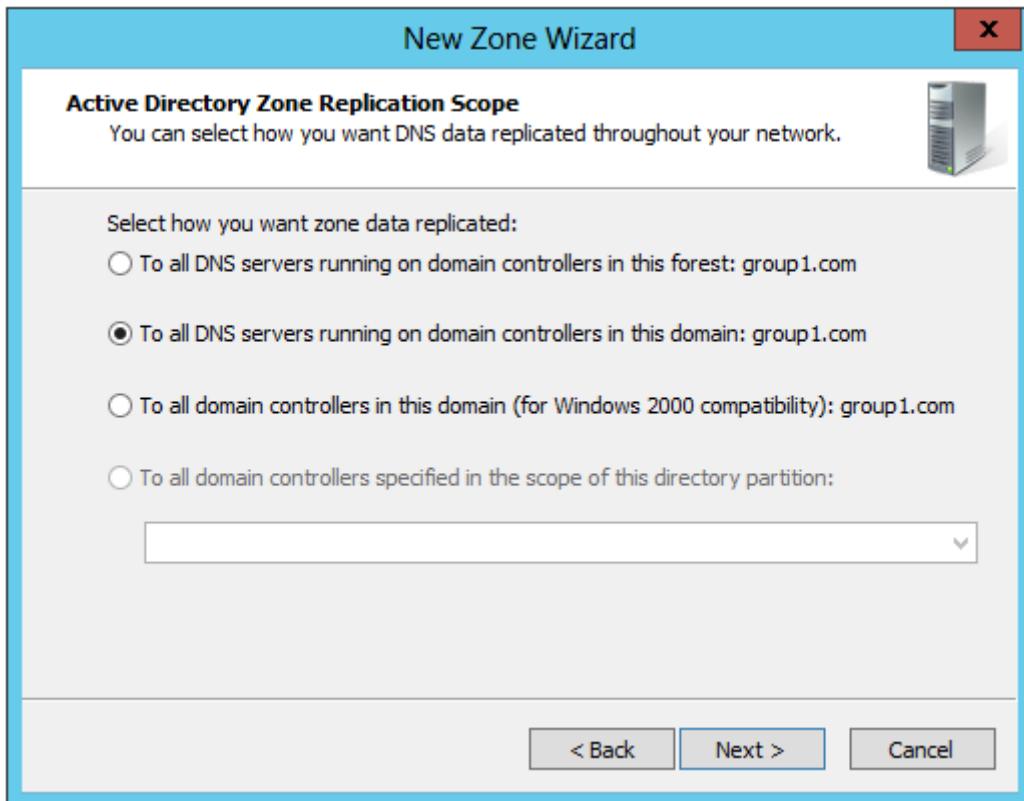


Figure 5.2.2.19 Choose to all DNS Servers running on domain group1.com

Step 20: Click on IPv4 Reverse Lookup Zone

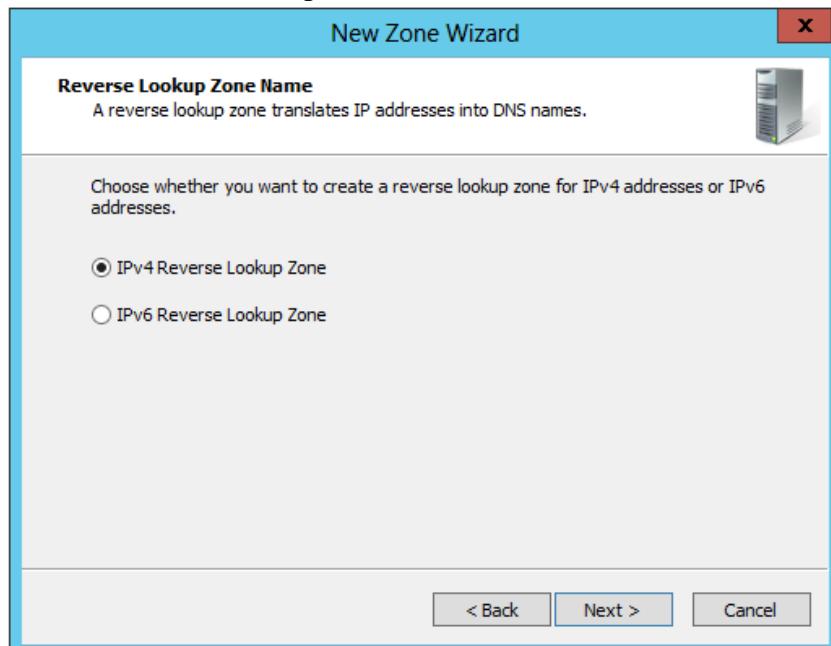


Figure 5.2.2.20 Click on IPv4 Reverse Lookup Zone

Step 21: Identify the network ID for the reverse lookup zone.

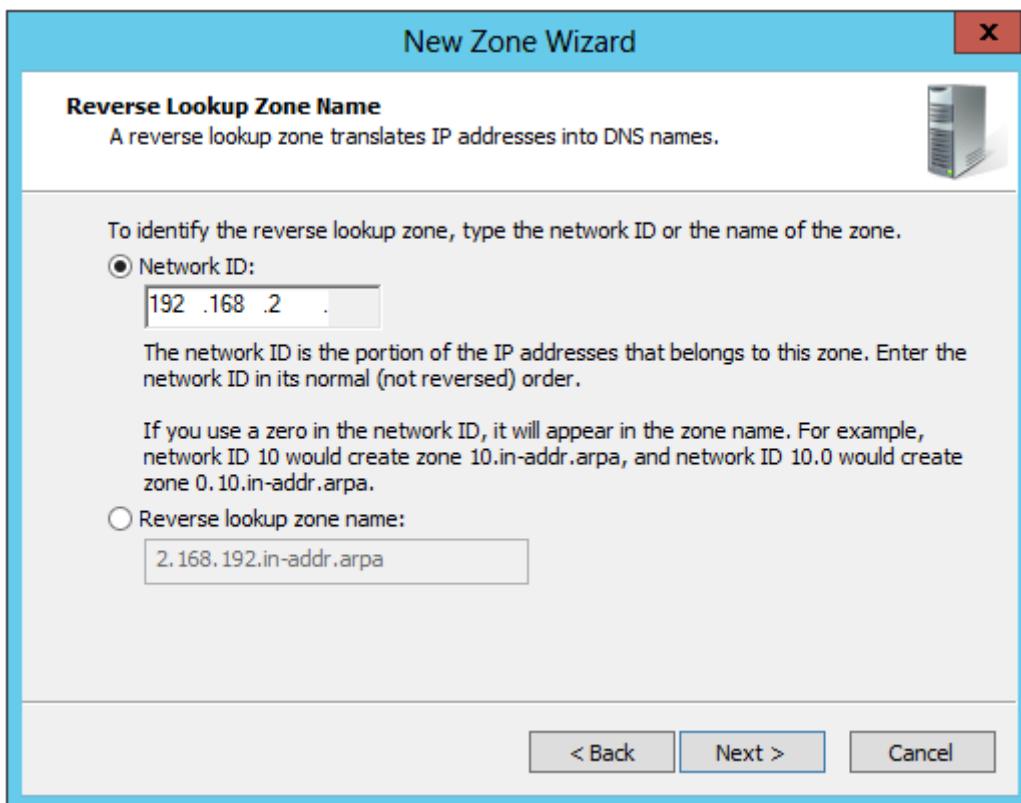


Figure 5.2.21 Identify the network ID for reverse lookup zone

Step 22: Identify the network ID for the reverse lookup zone.

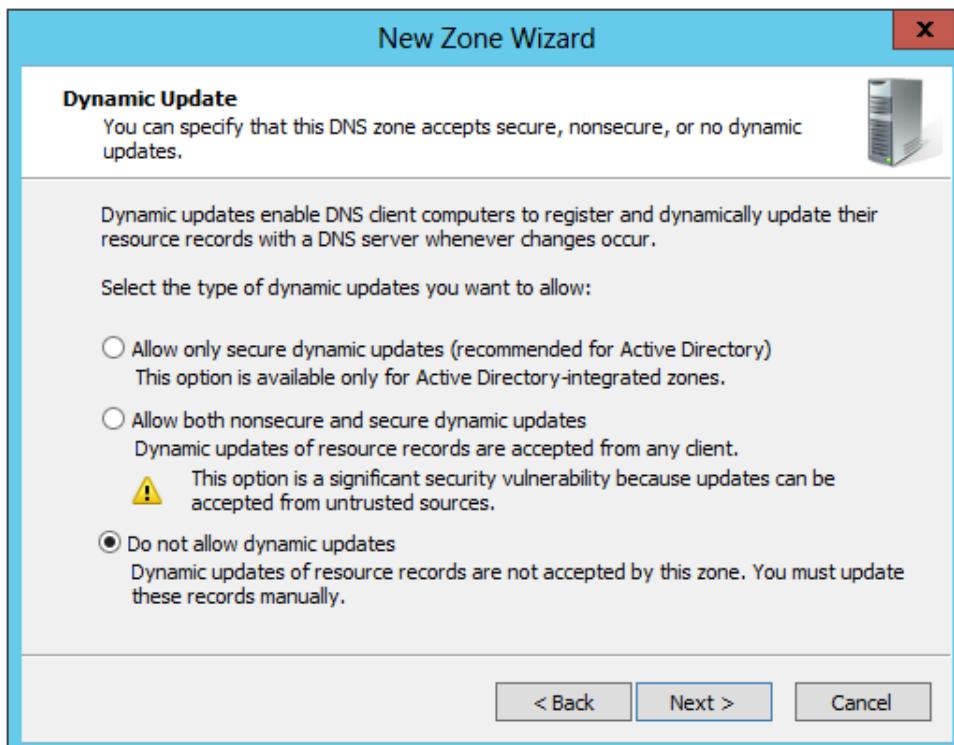


Figure 5.2.22 Do not allow dynamic update

Step 23: Click on Finish

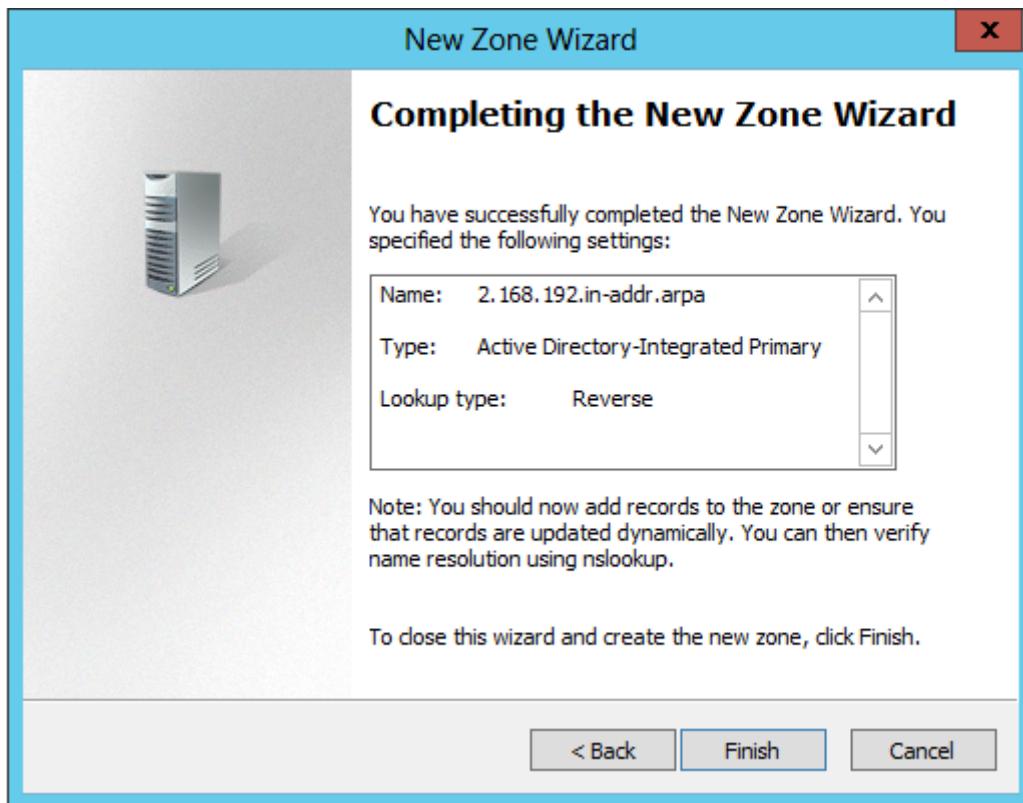


Figure 5.2.23 Click on Finish

Step 24: Click on New Pointer (PTR)

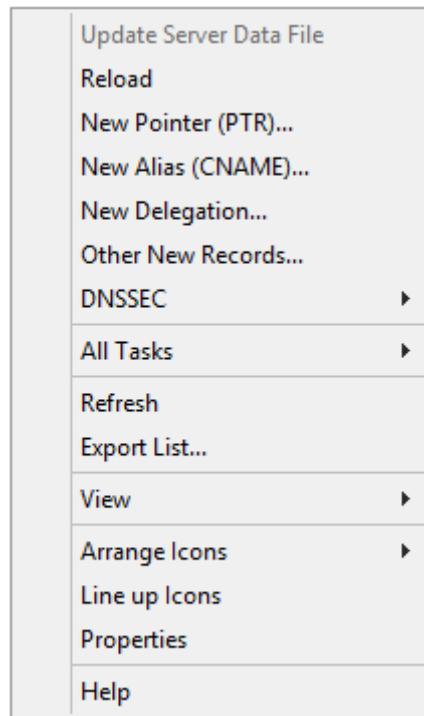


Figure 5.2.24 Click on New Pointer (PTR)

Step 25: Click on browse and map the hostname to the forward lookup zone.

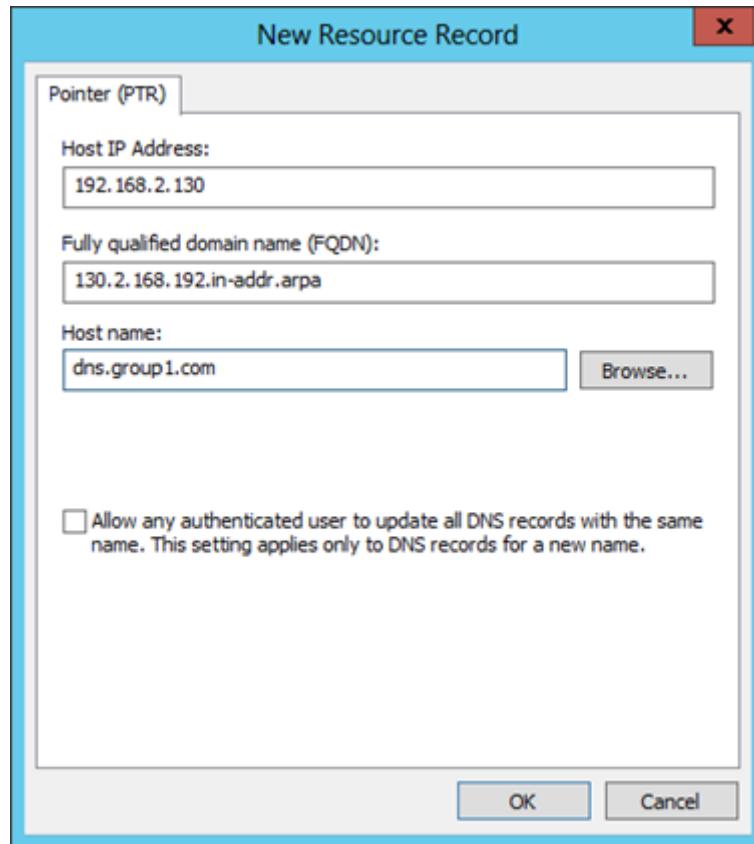


Figure 5.2.25 Browse and map the hostname to the forward lookup zone.

Step 26: Create Reverse Lookup Zones DNS for IPv4 and IPv6. Click on the Reverse Lookup Zones and right click and click on New Zone. This one we create a reverse lookup zone for IPv6.

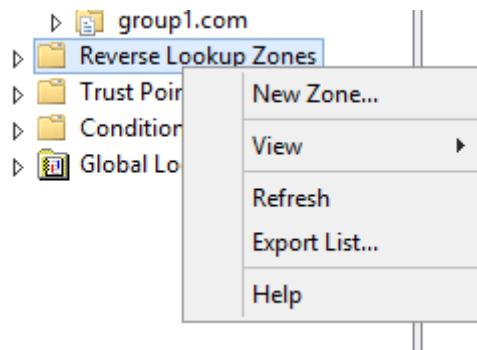


Figure 5.2.26 Creating new zone for reverse lookup zone for DNS IPv6

Step 27: Click on Next



Figure 5.2.2.27 New Zone Wizard for reverse lookup zone DNS IPv6

Step 28: Click on Next

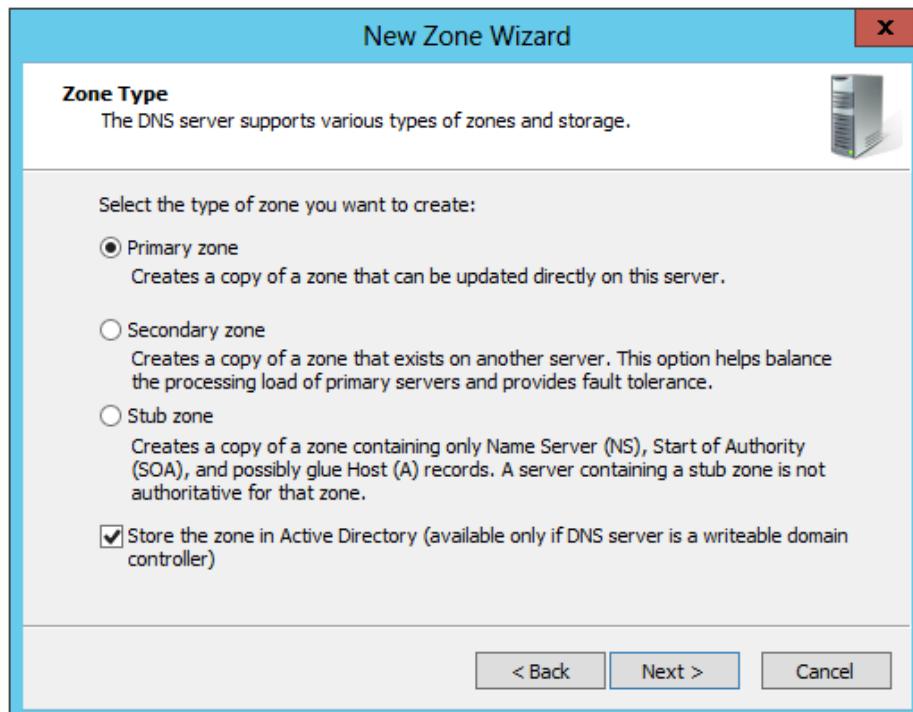


Figure 5.2.2.28 Choose primary zone for reverse lookup zone DNS IPv6

Step 29: Click on Next



Figure 5.2.2.29 Choose primary zone for reverse lookup zone DNS IPv6

Step 30: Click on Next

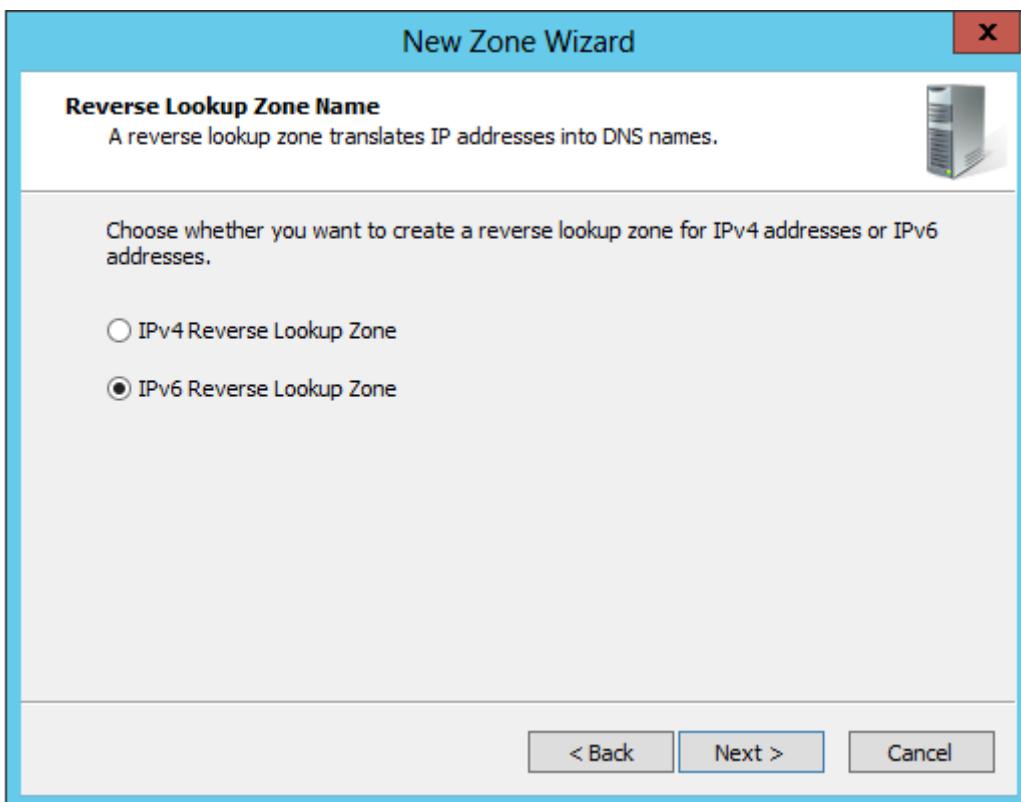


Figure 5.2.2.30 Click on IPv6 Reverse Lookup Zone

Step 31: Click on Next

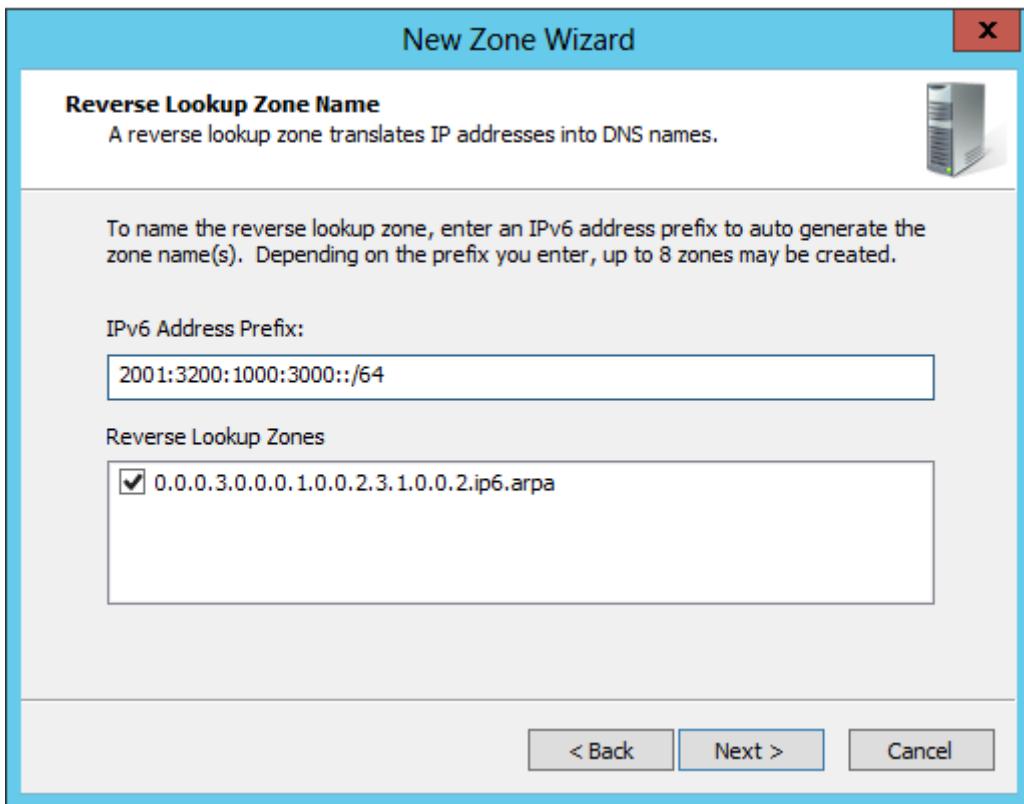


Figure 5.2.2.31 Click on IPv4 Reverse Lookup Zone

Step 32: Identify the network ID for the reverse lookup zone.



Figure 5.2.32 Identify the network ID for reverse lookup zone

Step 33: Click on Finish

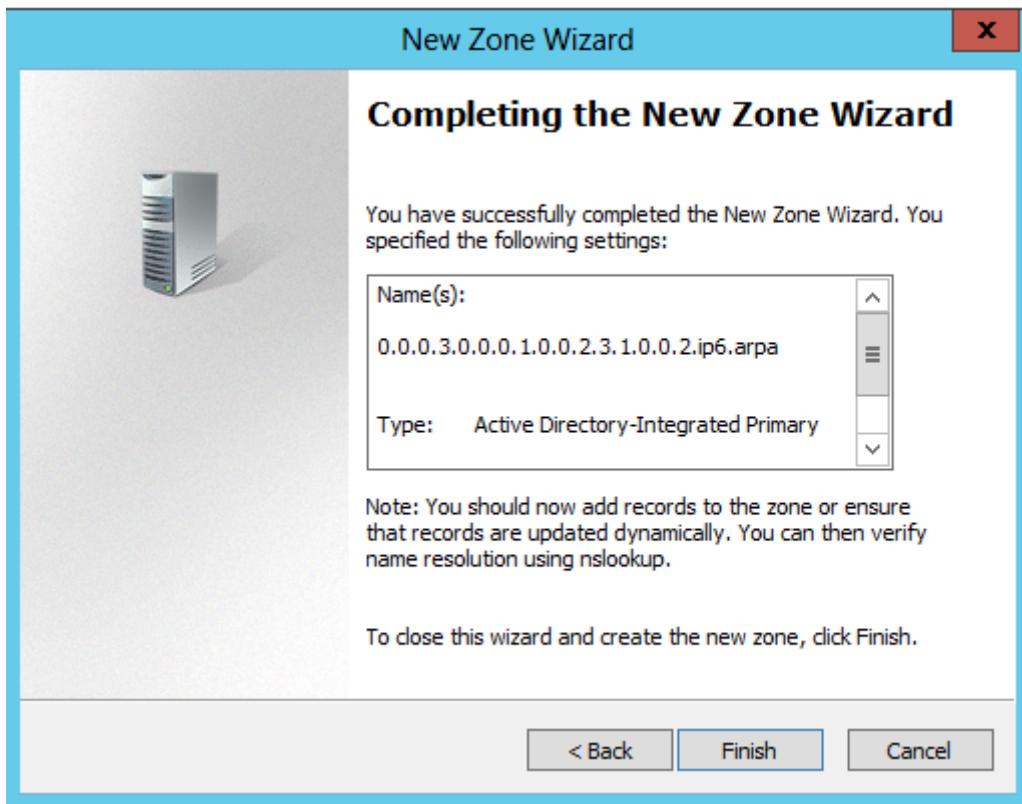


Figure 5.2.33 Click on Finish

Step 34: Click on New Pointer (PTR)

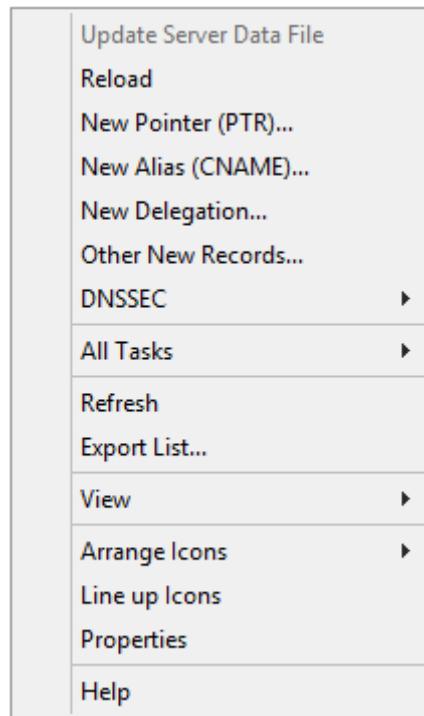


Figure 5.2.34 Click on New Pointer (PTR)

Step 35: Click on browse and map the hostname to the forward lookup zone.

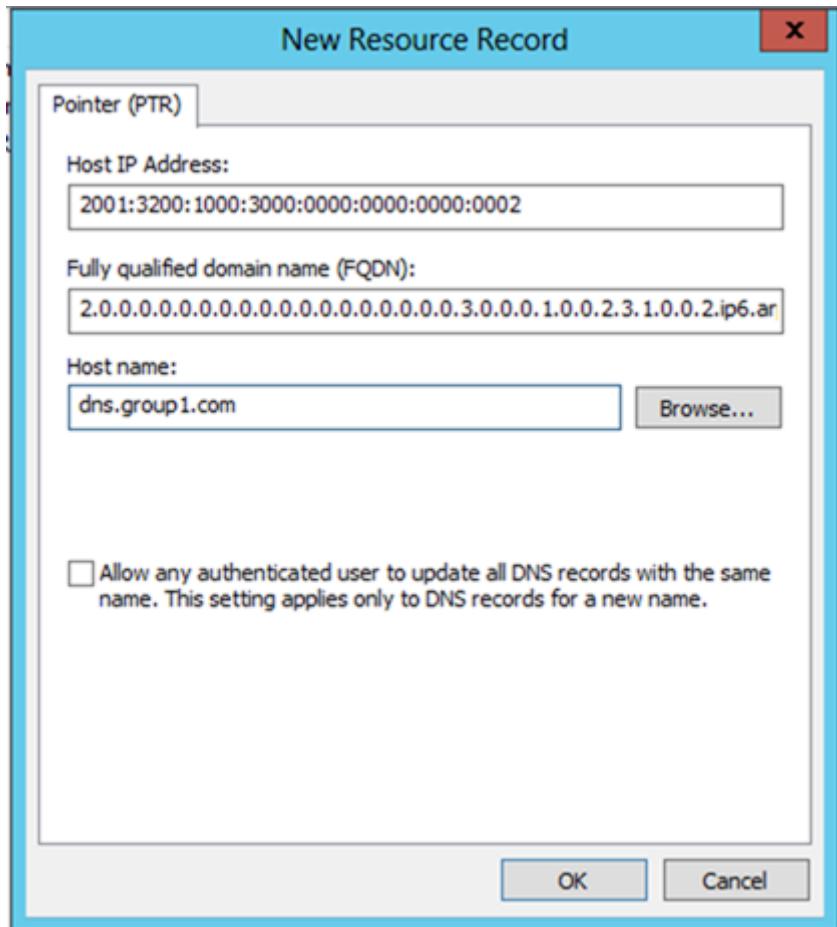


Figure 5.2.35 Browse and map the hostname to the forward lookup zone.

Step 36: Repeat the same step to create another forward zone for IPv4 and IPv6. Below is the fully configured reverse zone for IPv4 and IPv6.

The screenshot shows the Windows DNS Manager application window. The left pane displays a tree view of DNS objects under the root node 'WIN-A90KBSE0I04'. The 'Forward Lookup Zones' node has three children: '_msdcv.group1.com', 'group1.com', and 'vhggroup1.com'. The 'Reverse Lookup Zones' node has four children: '0.0.0.1.0.0.0.1.0.0.2.3.1.0.0.2.ip6.arpa', '0.0.0.2.0.0.0.1.0.0.2.3.1.0.0.2.ip6.arpa', '0.0.0.3.0.0.0.1.0.0.2.3.1.0.0.2.ip6.arpa', and '0.0.0.4.0.0.0.1.0.0.2.3.1.0.0.2.ip6.arpa'. Below these are entries for '1.168.192.in-addr.arpa', '2.168.192.in-addr.arpa', and '201.200.200.in-addr.arpa'. The 'Trust Points', 'Conditional Forwarders', and 'Global Logs' nodes are also listed. The right pane lists the details of a selected DNS record: Name '2001:3200:1000:3000:0000:0000:0000:0002', Type 'Pointer (PTR)', Data 'win-a90kbse0i04.group1.com.', and Timestamp '19/01/2021 12:00:00'.

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[redacted]	static
(same as parent folder)	Name Server (NS)	win-a90kbse0i04.group1.com.	static
2001:3200:1000:3000:0000:0000:0000:0002	Pointer (PTR)	win-a90kbse0i04.group1.com.	static
2001:3200:1000:3000:0de9:a9f:0d3:6775	Pointer (PTR)	win-a90kbse0i04.group1.com.	19/01/2021 12:00:00

Figure 5.2.2.36 Fully configured reverse zone for IPv4 and IPv6

5.2.3. Active Directory

Step 1: Go to manage and click add roles and features.

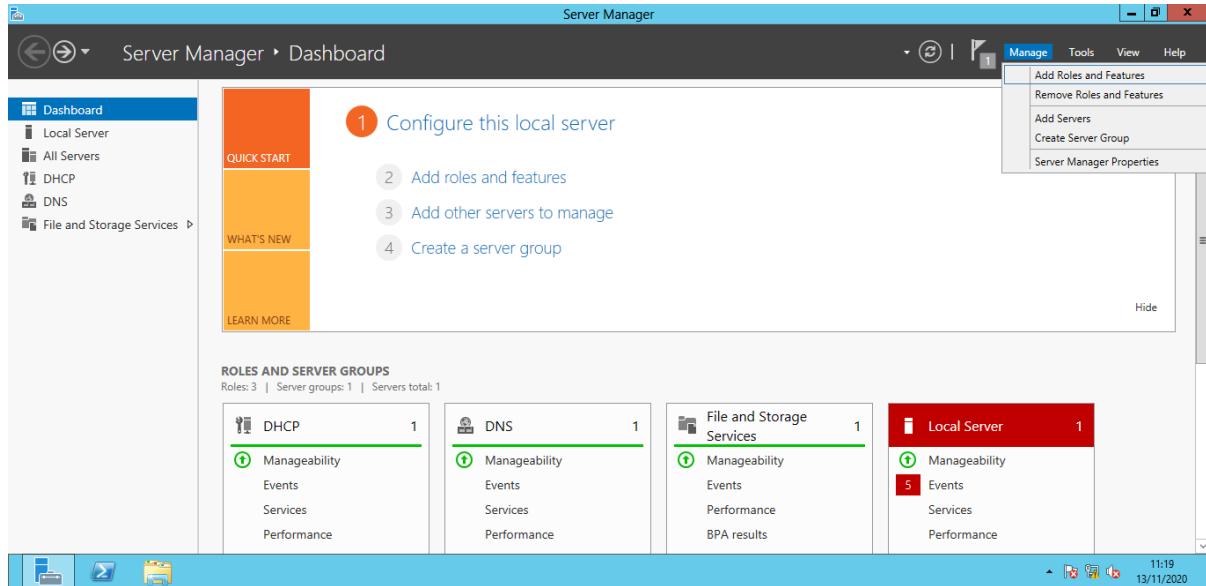


Figure 5.2.3.1 Add Roles and Features

Step 2: Click next.

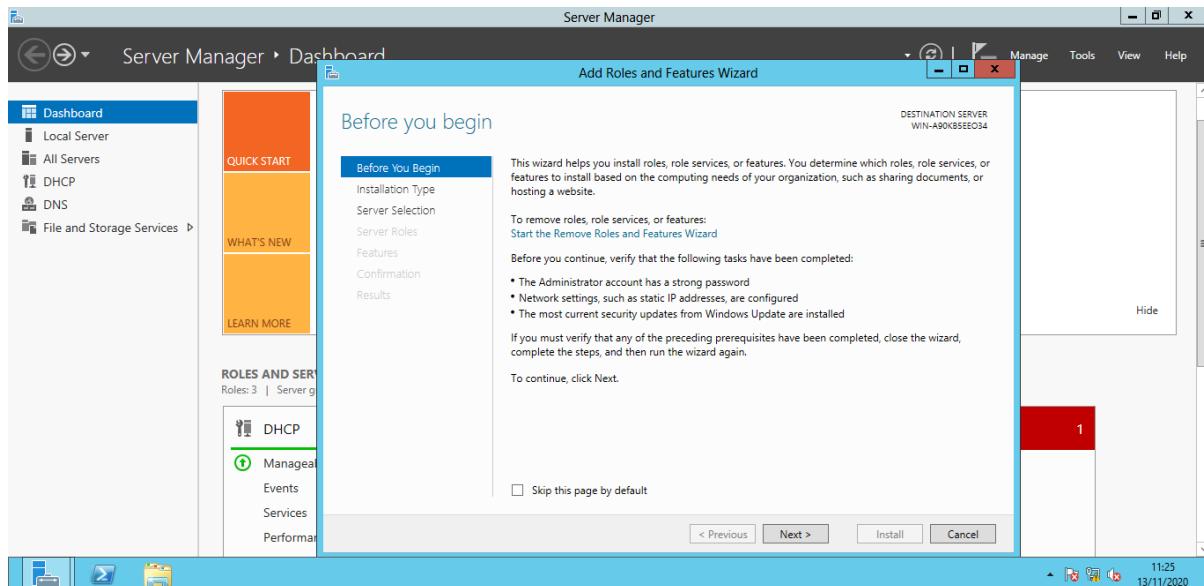


Figure 5.2.3.2 Before you begin tab

Step 3: Choose role-based or future-based installation and click next.

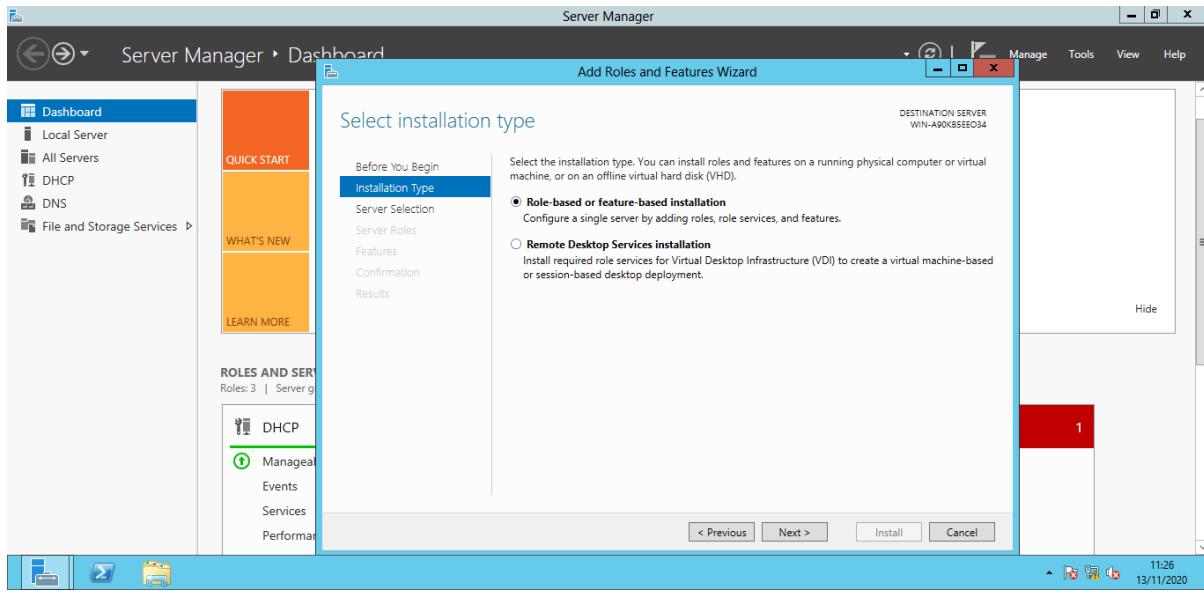


Figure 5.2.3.3 Select installation type tab

Step 4: Choose select a server from the server pool and click next.

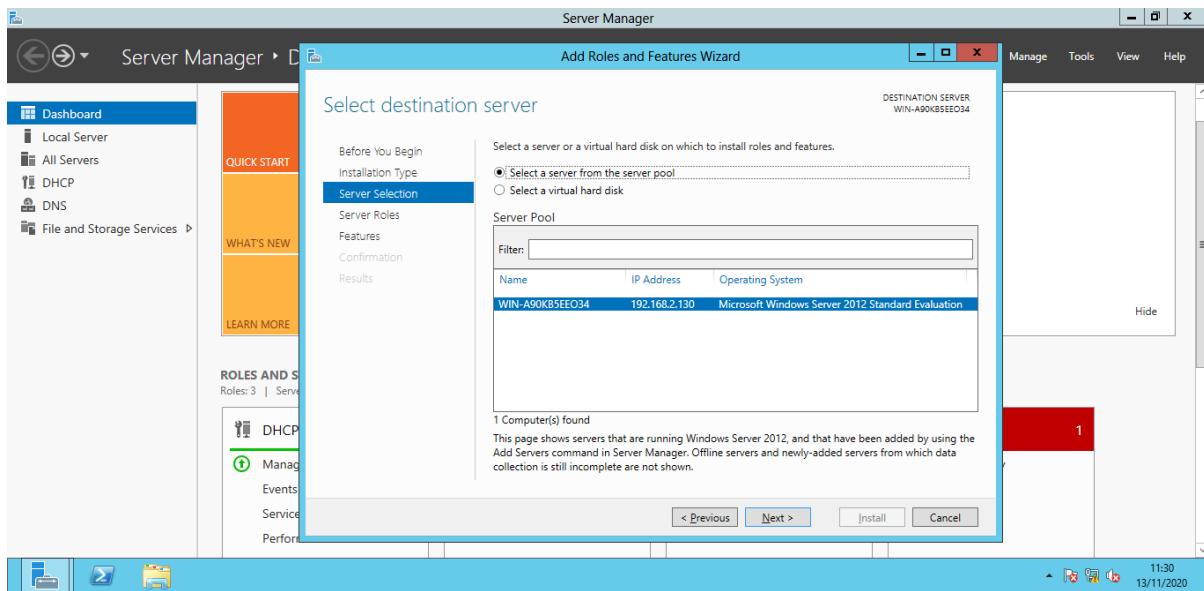


Figure 5.2.3.4 Select destination server

Step 5: Choose Active Directory Domain Services and click next.

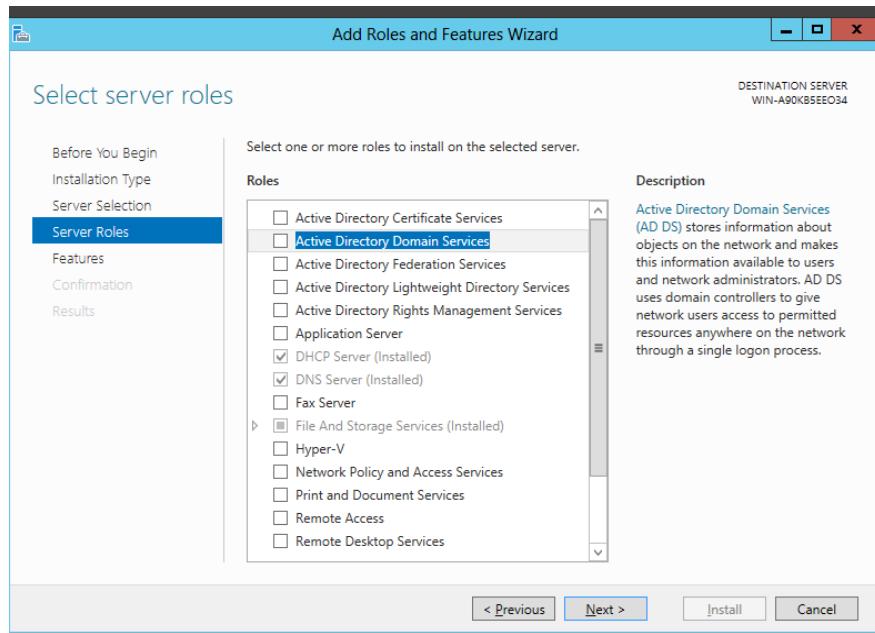


Figure 5.2.3.5 Select server roles tab

Step 6: Then click add features.

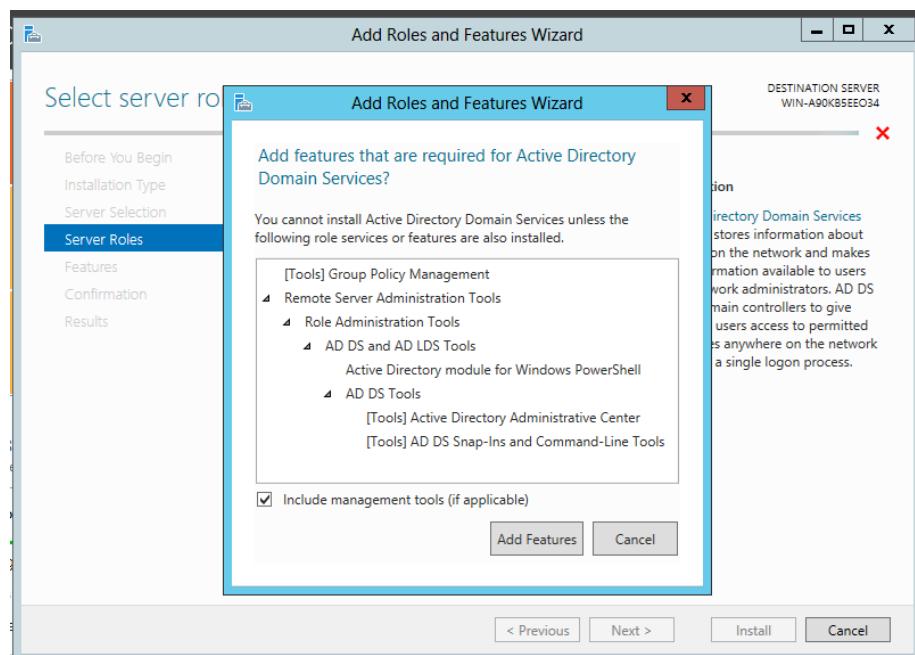


Figure 5.2.3.6 Add feature

Step 7: Choose .NET Framework 3.5 Features and click next.

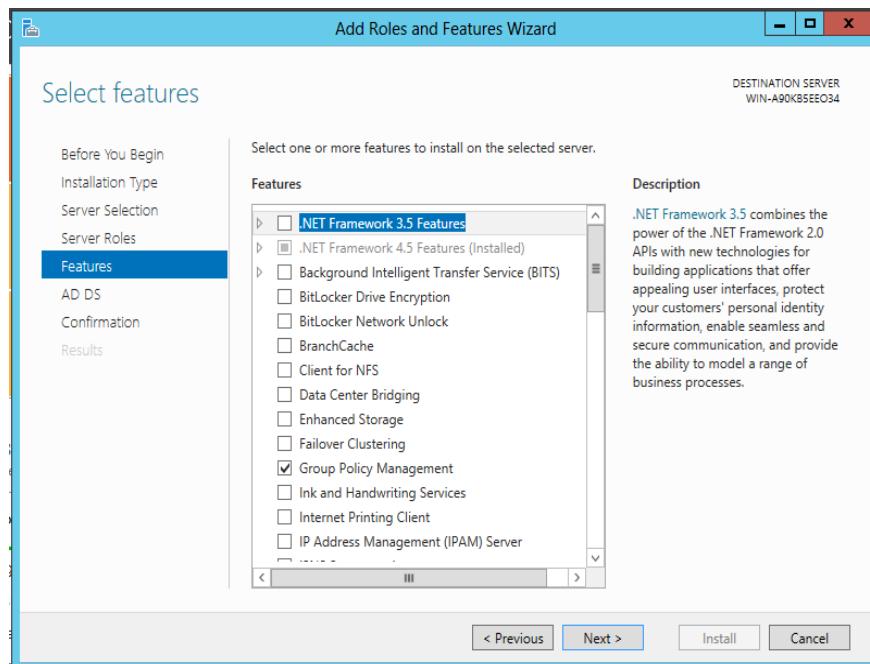


Figure 5.2.3.7 Select features tab

Step 8: Click next.

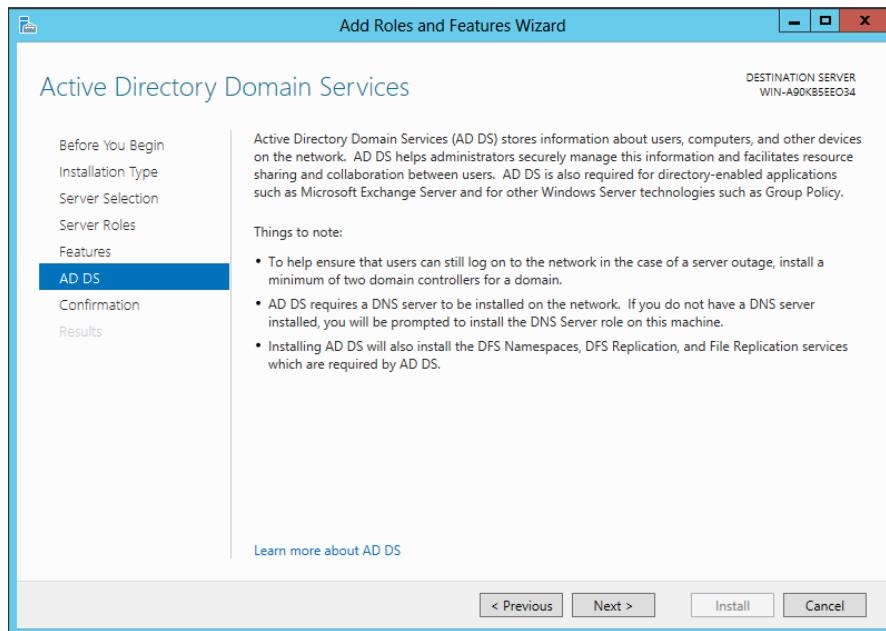


Figure 5.2.3.8 AD DS tab

Step 9: Click install.

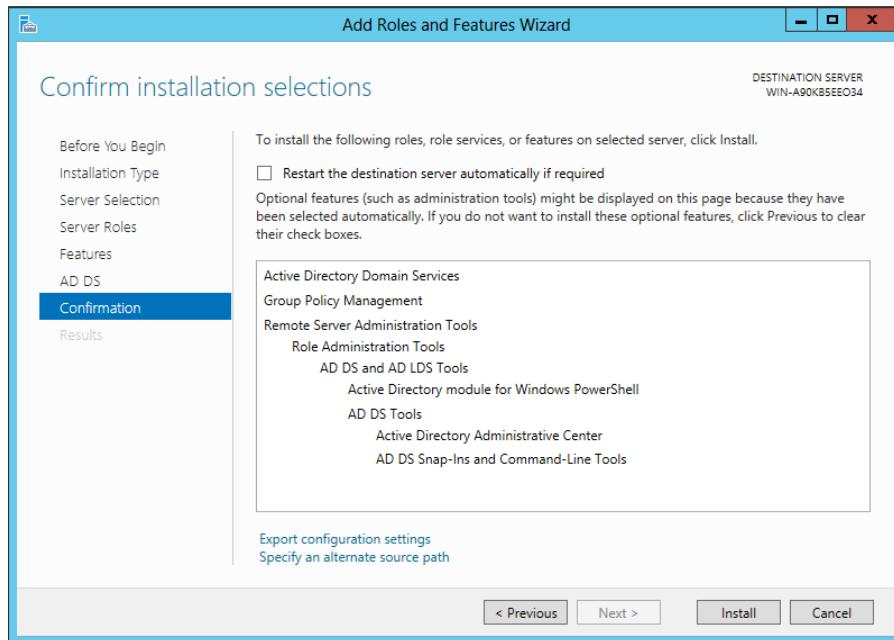


Figure 5.2.3.9 Confirmation tab

Step 10: Installation completed

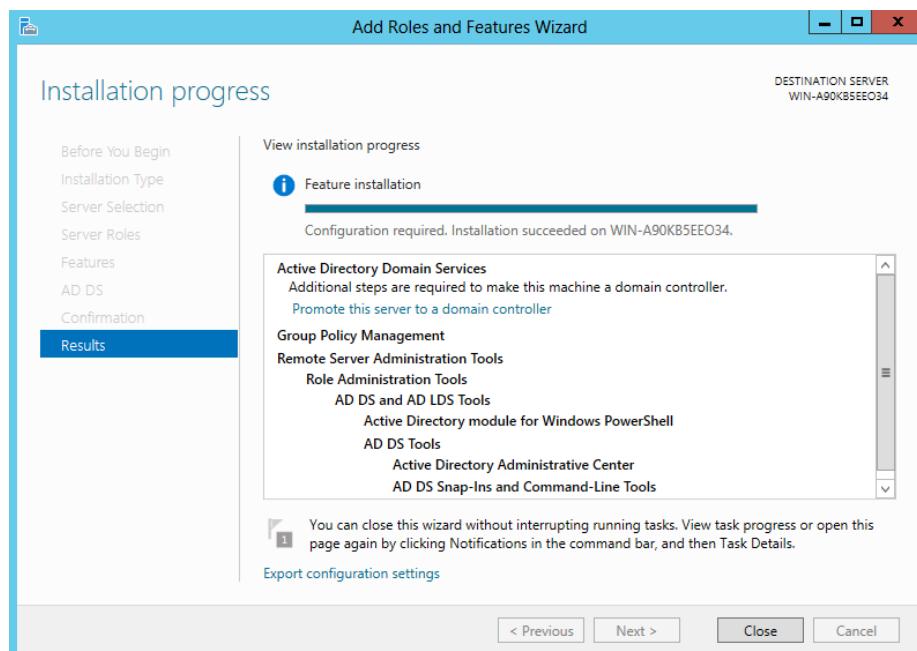


Figure 5.2.3.10 Results tab

Step 11: Click at the Promote this server to a domain controller.

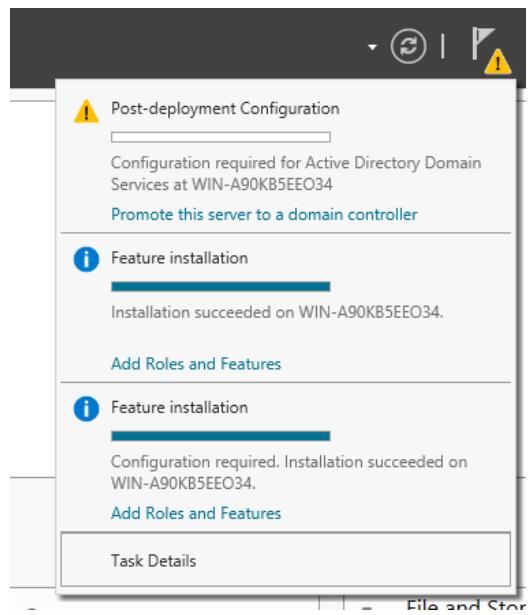


Figure 5.2.3.11 Flag information tab

Step 12: Choose add a new forest and add root domain name.

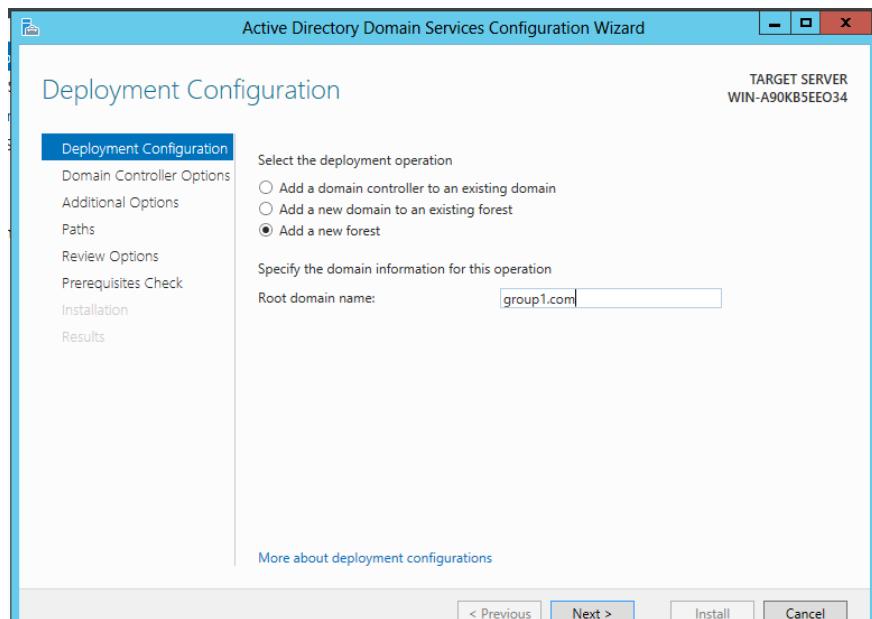


Figure 5.2.3.12 Deployment configuration tab

Step 13: Add password

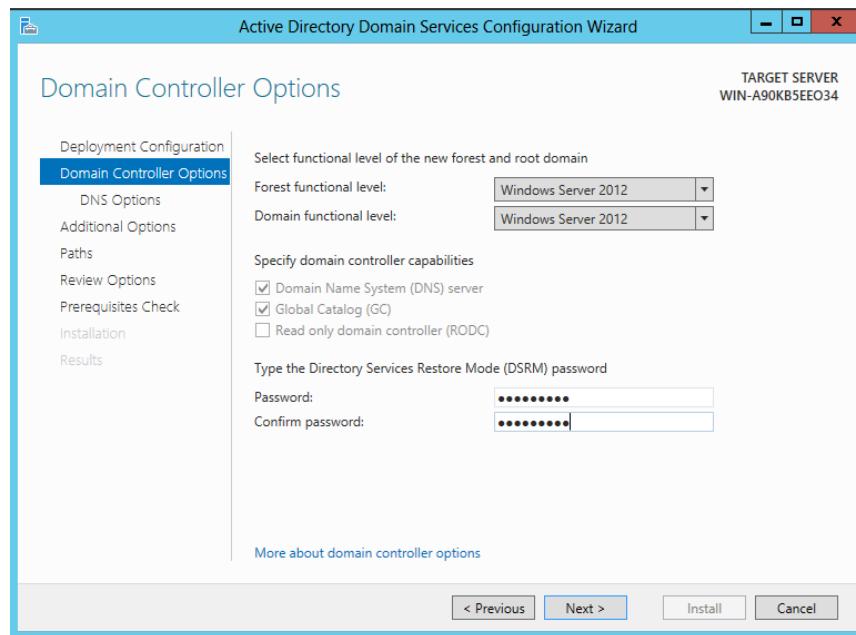


Figure 5.2.3.13 Domain controller options tab

Step 14: Click next

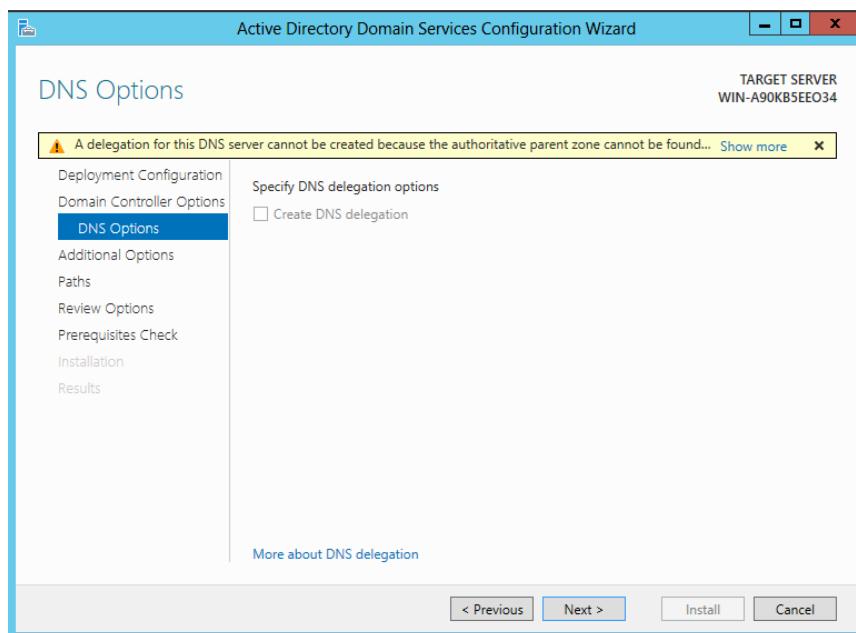


Figure 5.2.3.14 DNS options tab

Step 15: The NetBIOS domain name will automatically created and click next

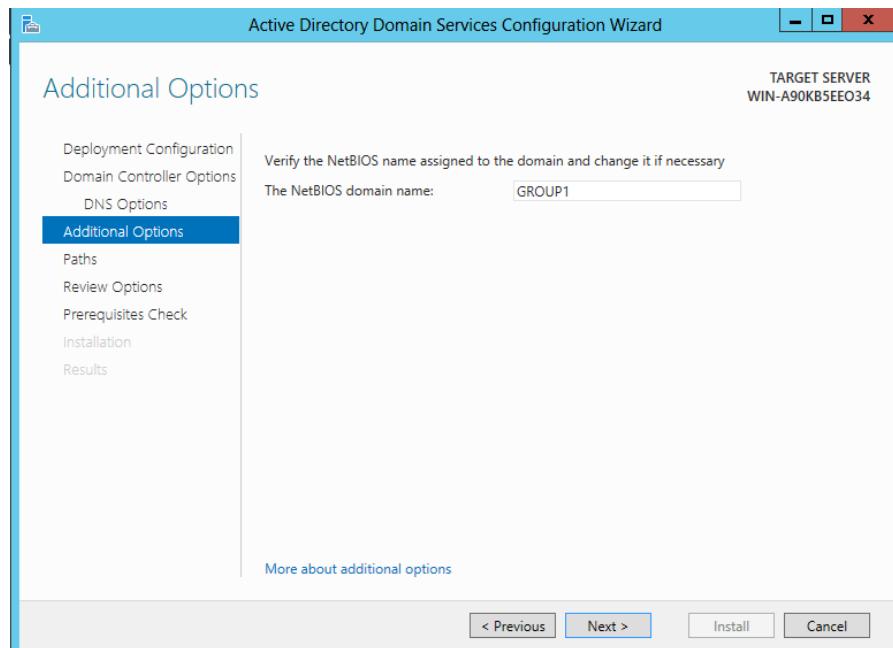


Figure 5.2.3.15 Additional options tab

Step 16: Use the default folder location and click next

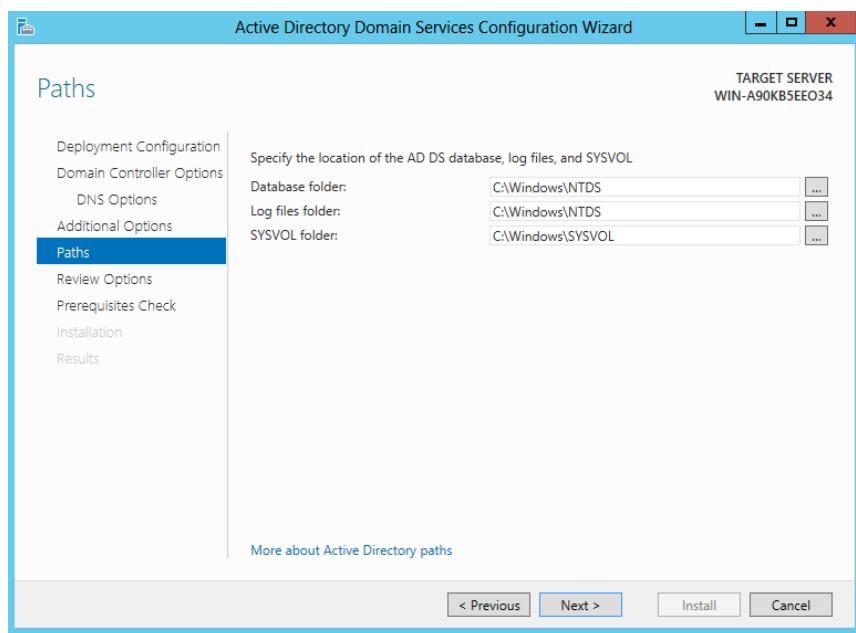


Figure 5.2.3.16 Paths tab

Step 17: Click next

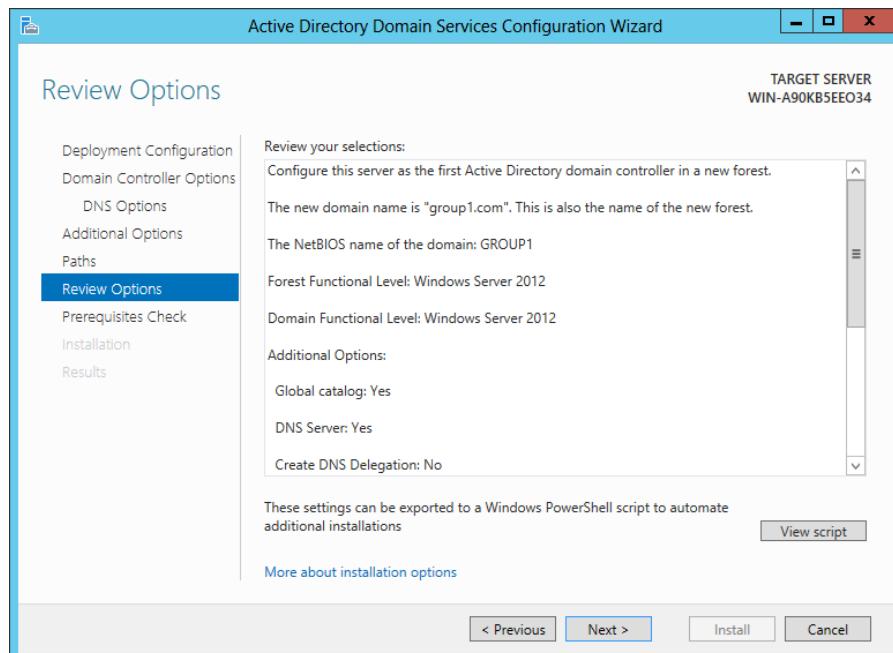


Figure 5.2.3.17 Review options tab

Step 18: Click install and it will automatically restart.

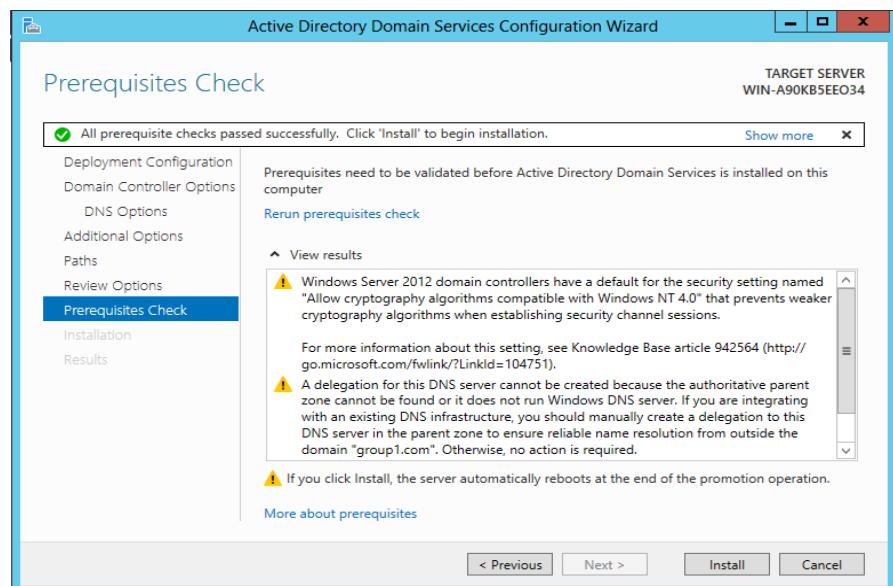


Figure 5.2.3.18 Prerequisites check tab

Step 19: Click at Active Directory Users and Computers

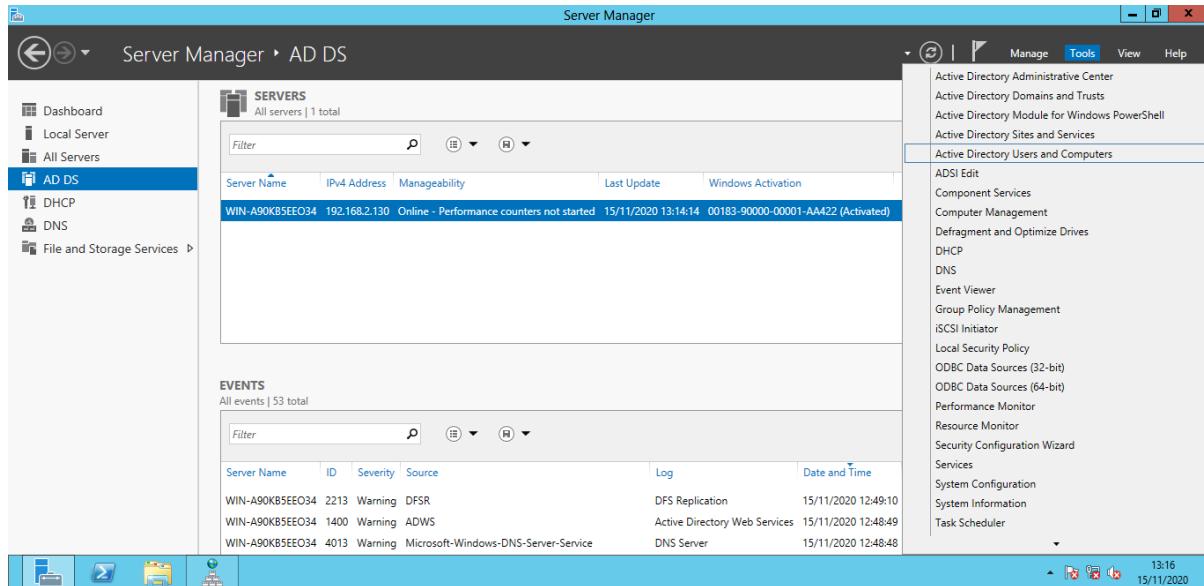


Figure 5.2.3.19 Active Directory Users and Computers

Step 20: Create new organizational unit inside group1.com

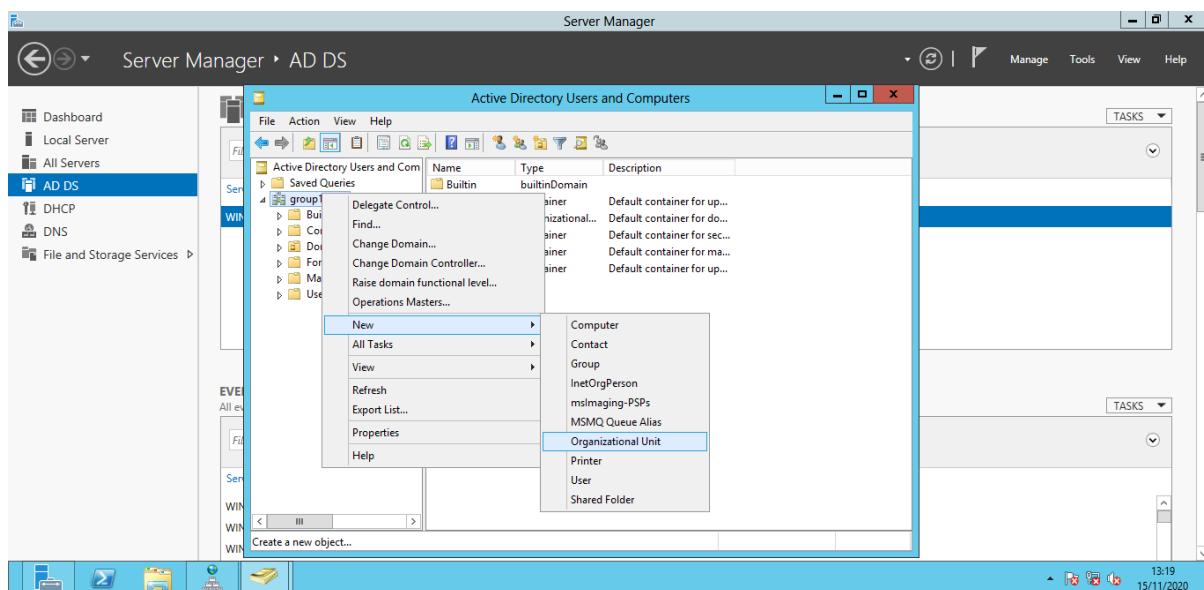


Figure 5.2.3.20 Creating organizational unit

Step 21: Add the name of the organizational unit which is ITDepartment then click ok.

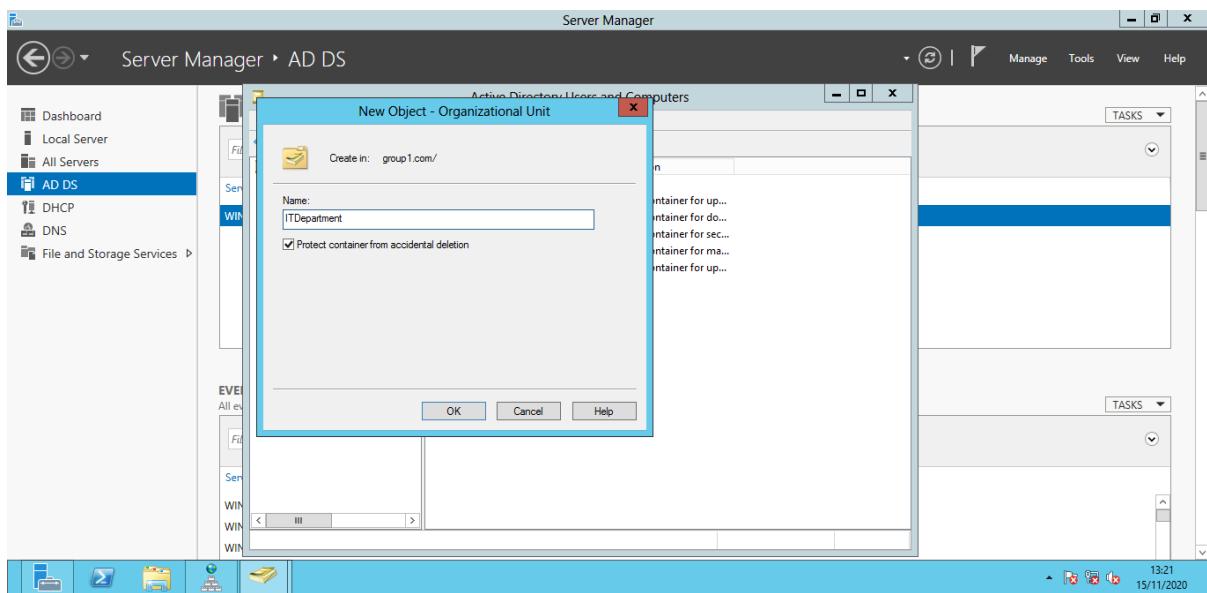


Figure 5.2.3.21 Organizational unit tab

Step 22: Create new organizational unit named Users inside ITDepartment

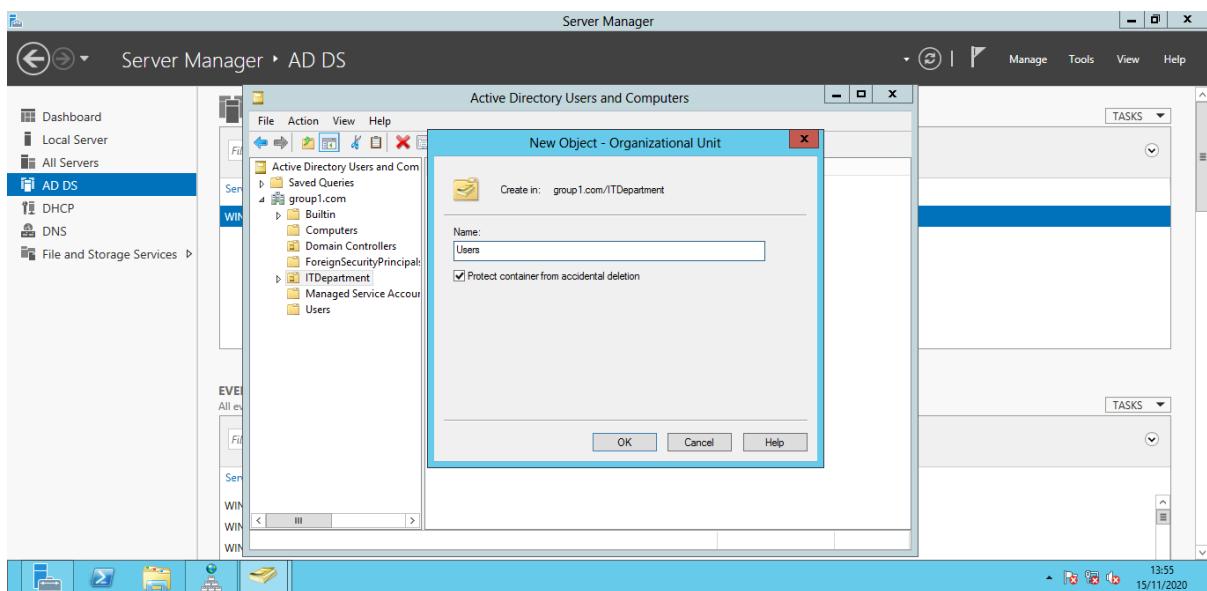


Figure 5.2.3.22 Organizational unit tab

Step 23: Create a new user named Amirah inside Users organizational unit and click next.

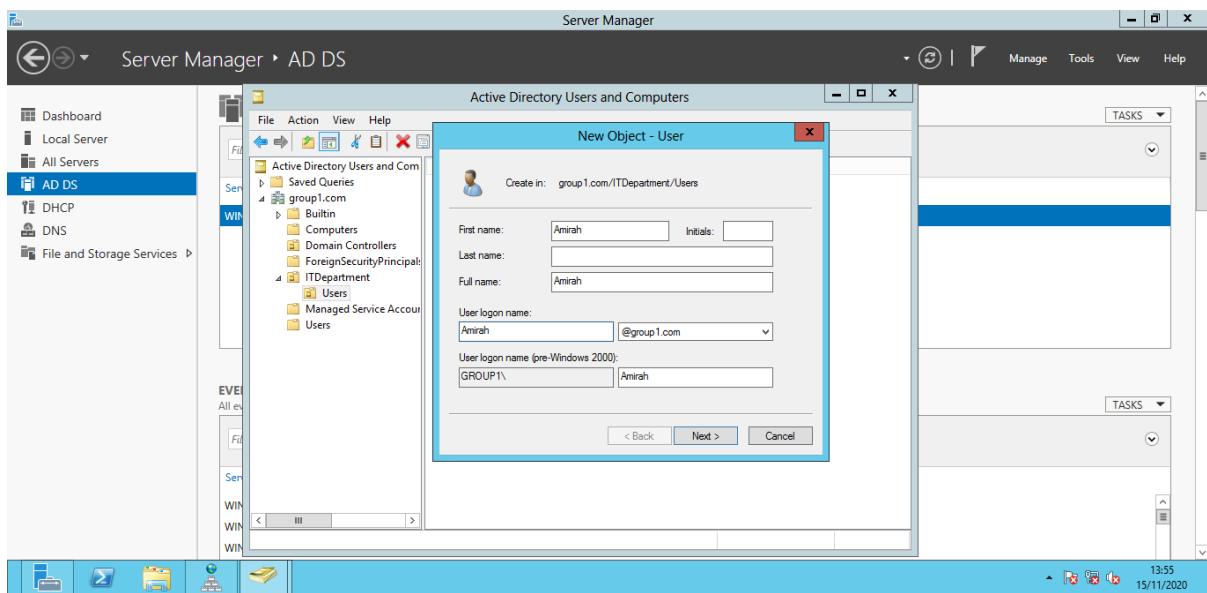


Figure 5.2.3.23 User tab

Step 24: Add password, choose the setting for password and click next

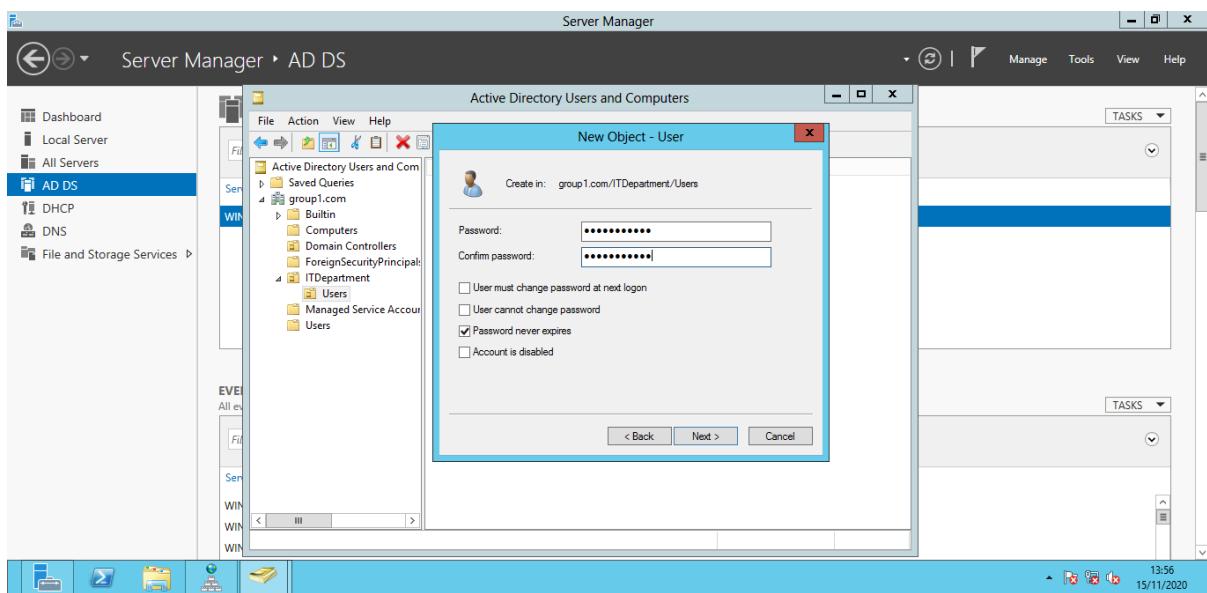


Figure 5.2.3.24 User tab

Step 25: The status of the user that has been added shows and click finish

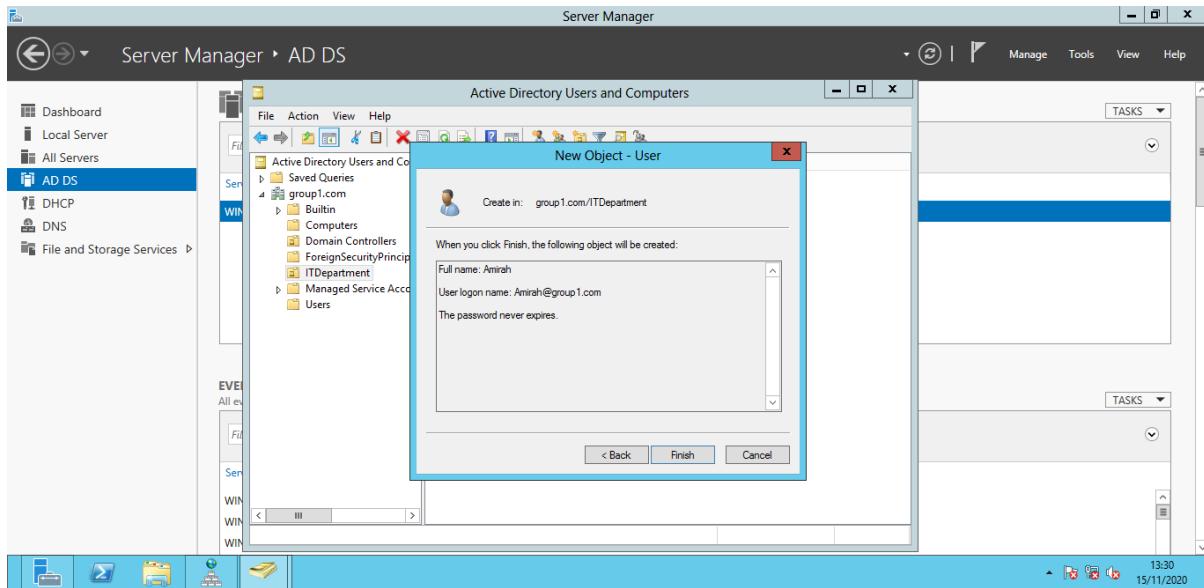


Figure 5.2.3.25 Status of created user

Step 26: Repeat steps 23-25 with different users named Afifahh, Aishah, Ariq, Faris, Yong and Hazim. All the users that have been created appear in Users organizational unit under ITDepartment.

Active Directory Users and Computers			
	Name	Type	Description
Active Directory Users and Computers	Aishah	User	
Saved Queries	Ariq	User	
group1.com	Faris	User	
Builtin	Hazim	User	
Computers	Amirah	User	
Domain Controllers	Afifahh	User	
ForeignSecurityPrincipals	Group1	User	
ITDepartment	Yongg	User	
LostAndFound			
Managed Service Accounts			
Program Data			
System			
Users			
NTDS Quotas			
TPM Devices			

Figure 5.2.3.26 List name of users created

Step 27: To create the first GPO policy, go to the Group Policy Management

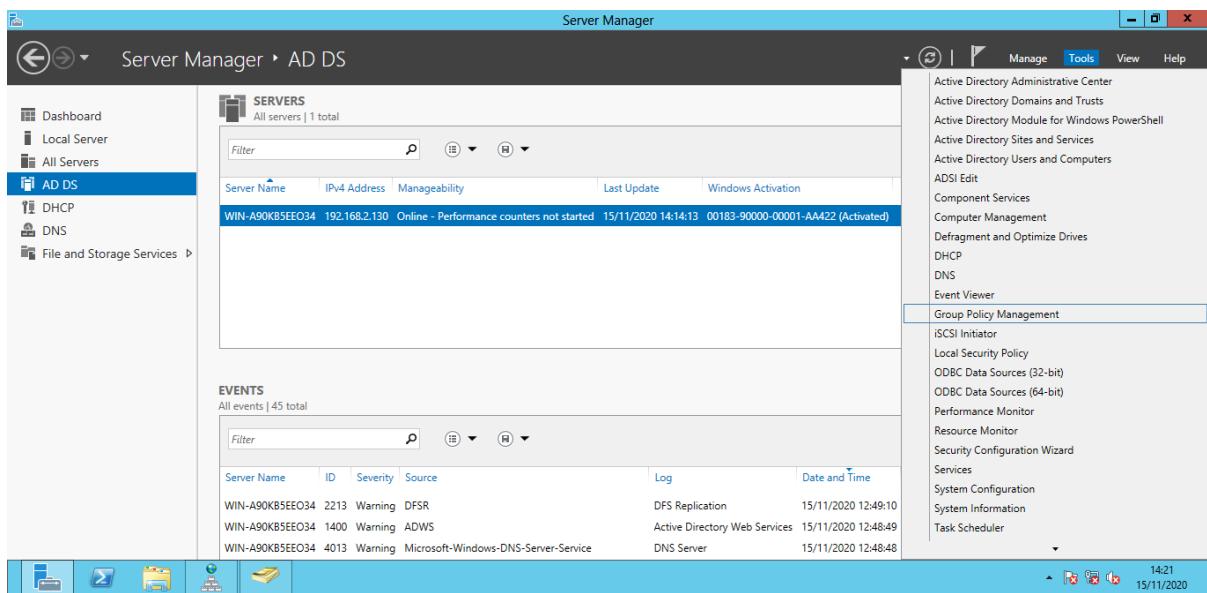


Figure 5.2.3.27 Group Policy Management

Step 28: Click edit at Default Domain Policy

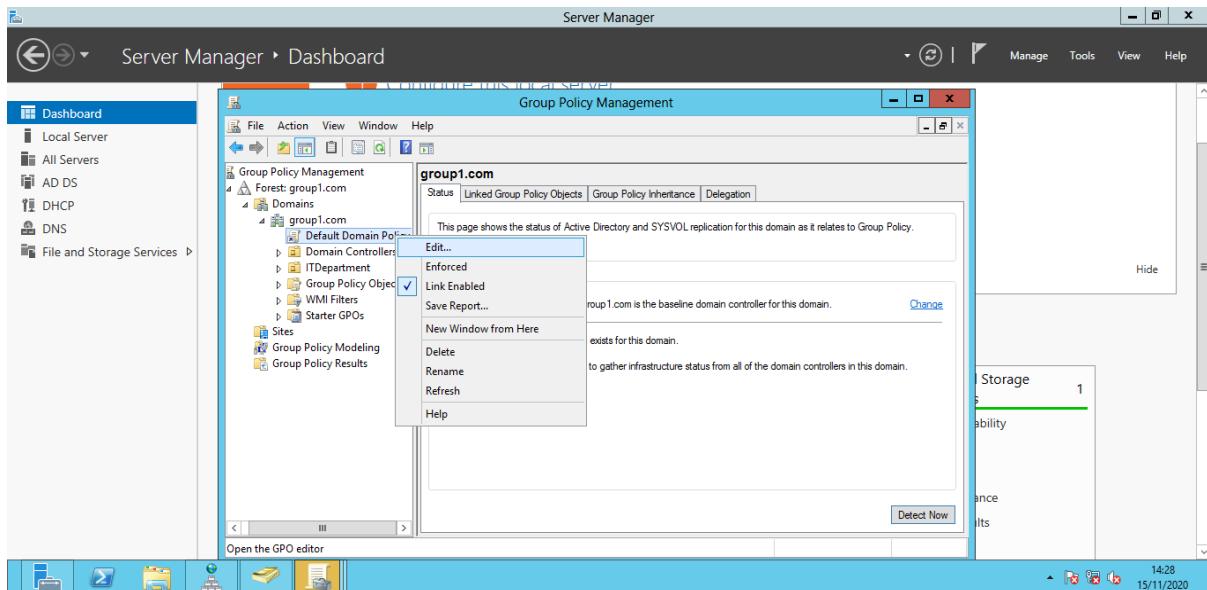


Figure 5.2.3.28 Group Policy Management tab

Step 29: Under Account Policies click Account Lockout Policy.

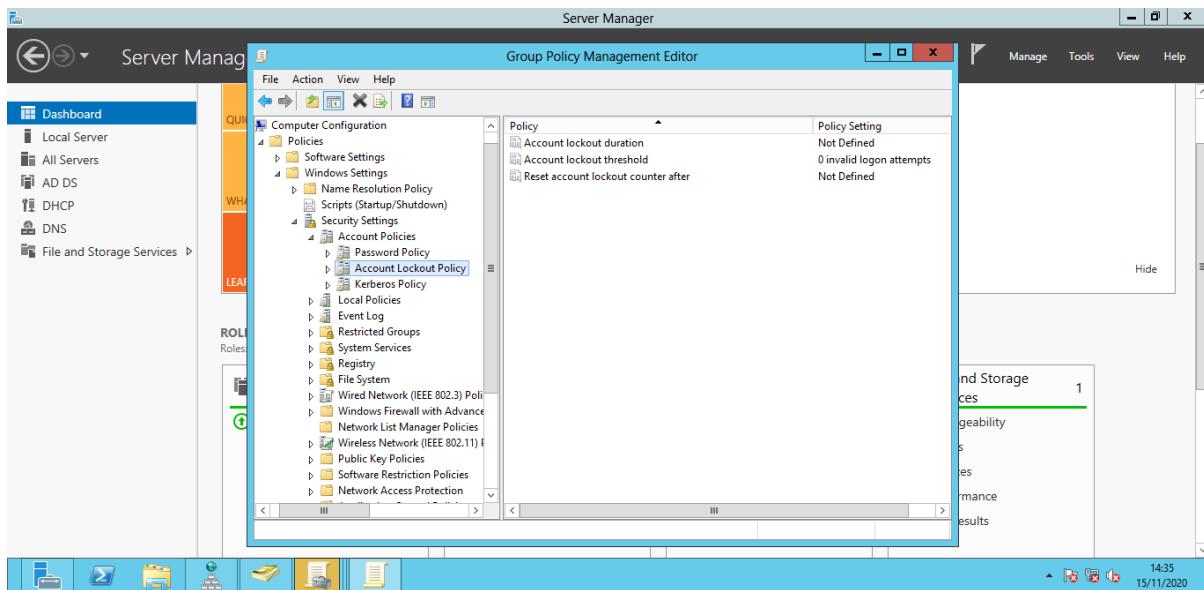


Figure 5.2.3.29 Account lockout policy tab

Step 30: Click at the Account lockout threshold Properties, choose 3, click apply and ok.

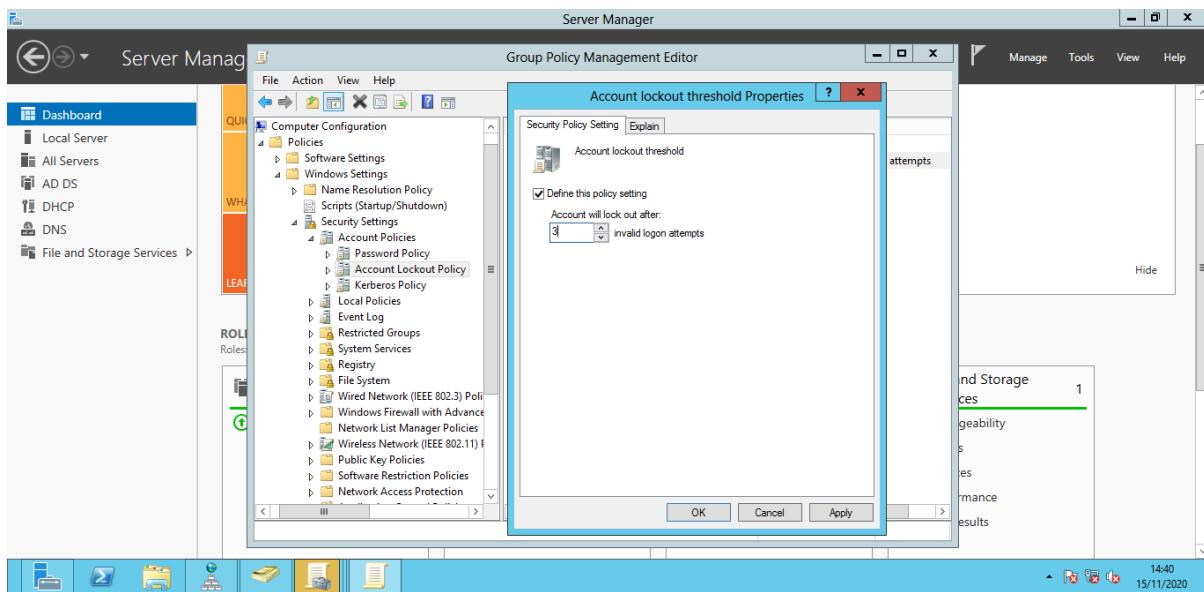


Figure 5.2.3.30 Account lockout threshold properties tab

Step 31: Click at the Account lockout duration Properties and choose 2 minutes, click apply and ok.

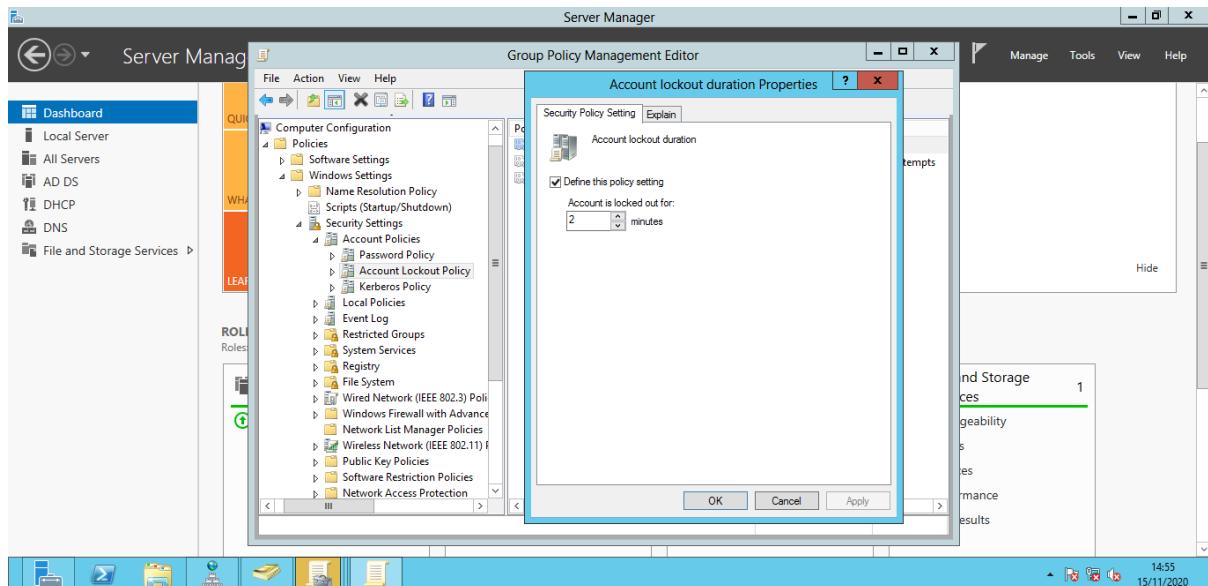


Figure 5.2.3.31 Account lockout duration properties tab

Step 32: Then click ok for the suggested value for Reset account lockout which is 2 minutes.

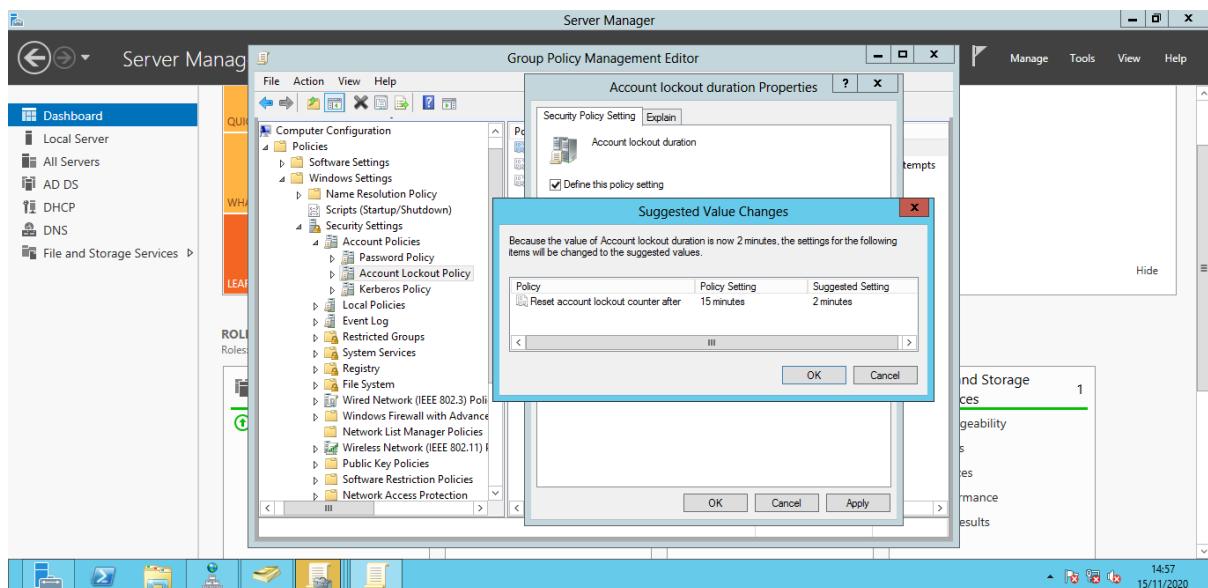


Figure 5.2.3.32 Setting for account lockout duration properties

Step 33: It is shown the policy setting that has been selected.

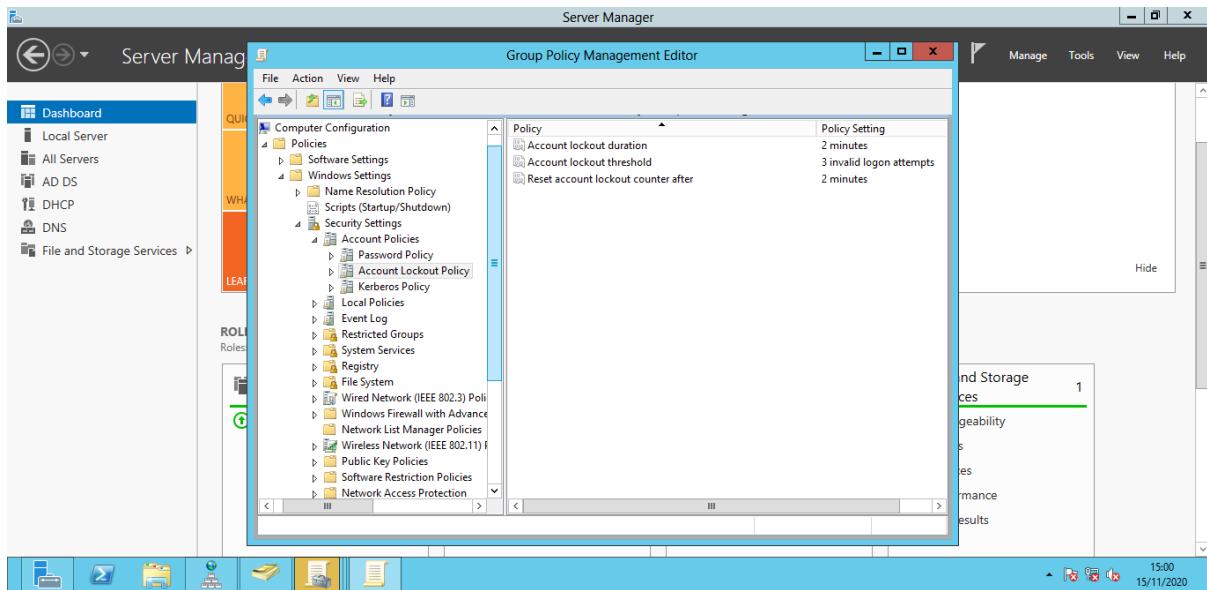


Figure 5.2.3.33 Account lockout policy that been set up

Step 34: To create the second GPO, click create GPO under group1.com.

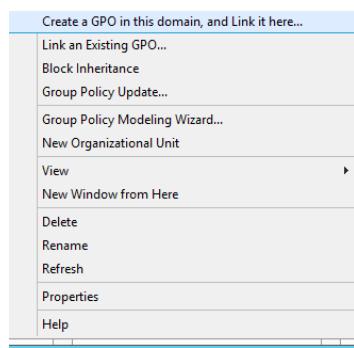


Figure 5.2.3.34 Create GPO is selected

Step 35: Name the second GPO as GROUP 1 LOGON BANNER and click ok

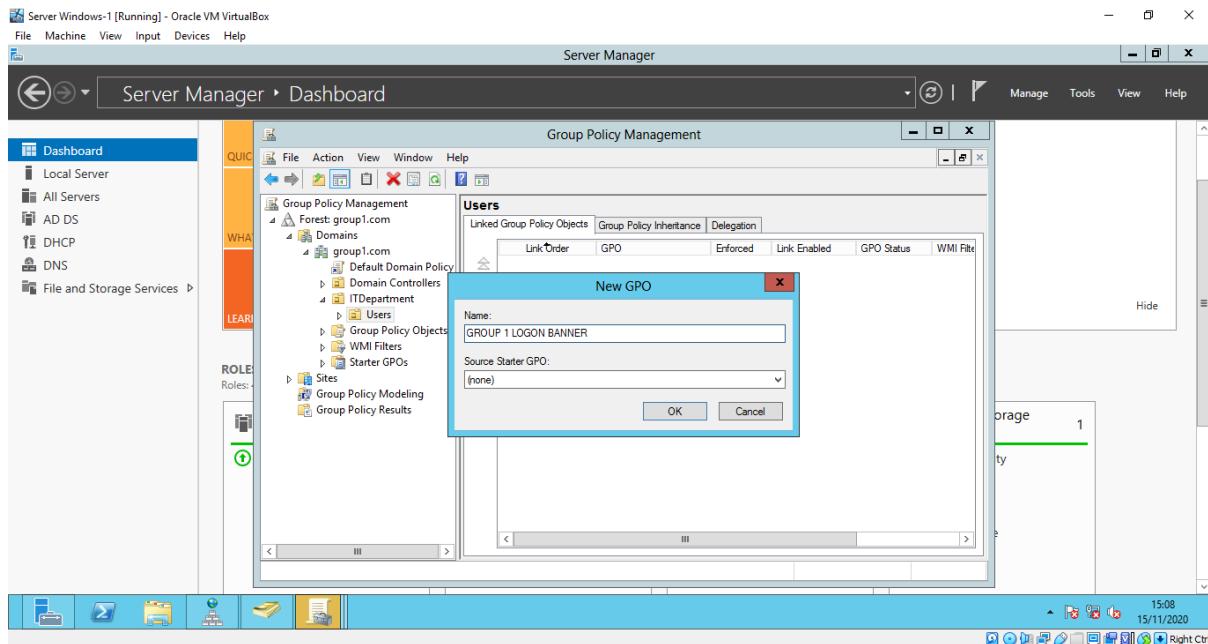


Figure 5.2.3.35 New GPO tab

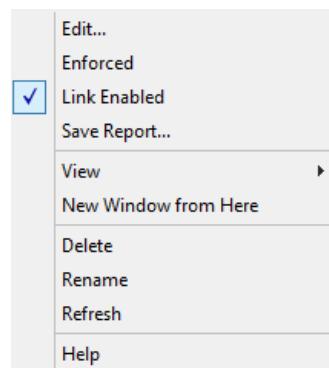


Figure 5.2.3.36 Link enabled is selected

Step 37: Click Security Options under Local Policies

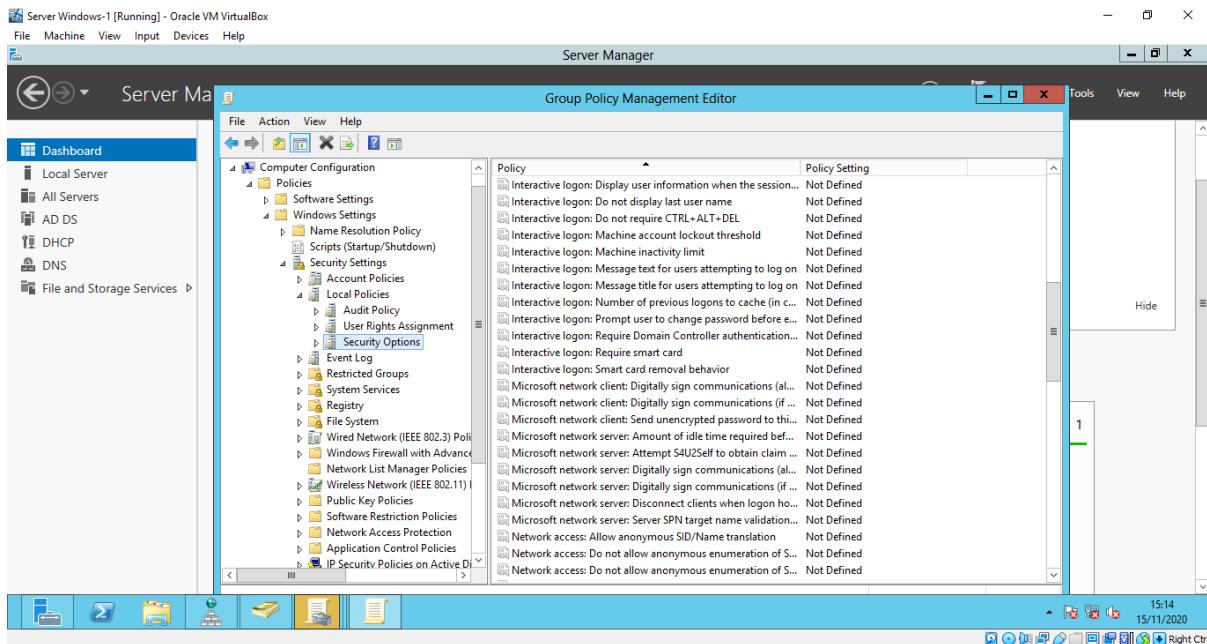


Figure 5.2.3.37 Security options tab

Step 38: Choose Interactive logon as shown below, type the text, click apply and ok

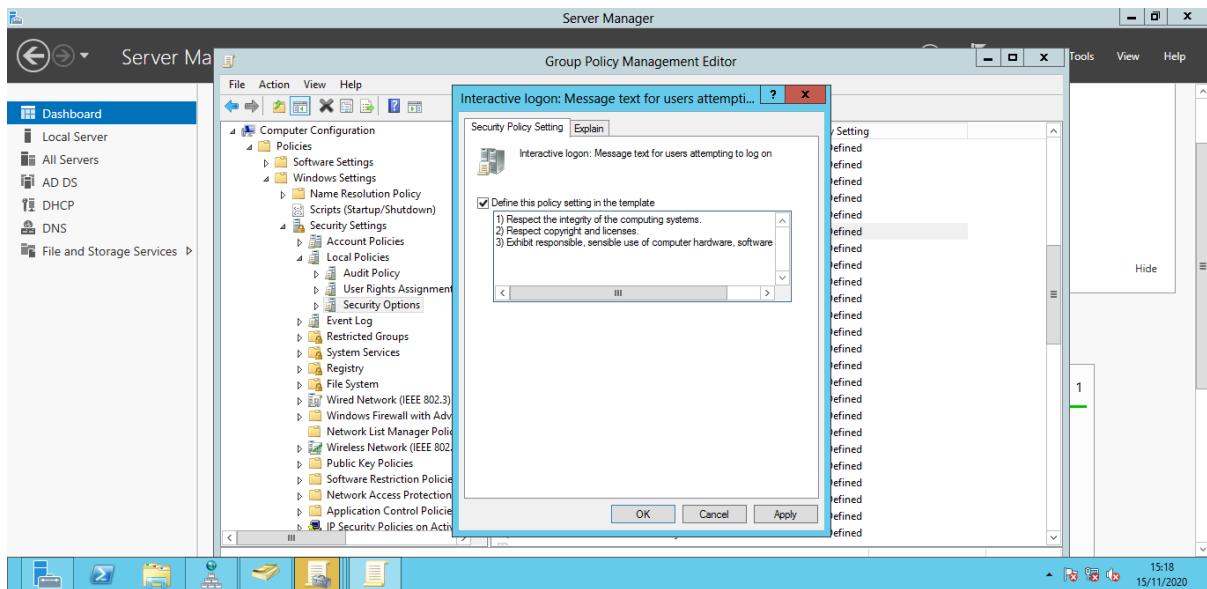


Figure 5.2.3.38 Interactive logon tab

Step 39: Choose Interactive logon as shown below, type the text, click apply and ok

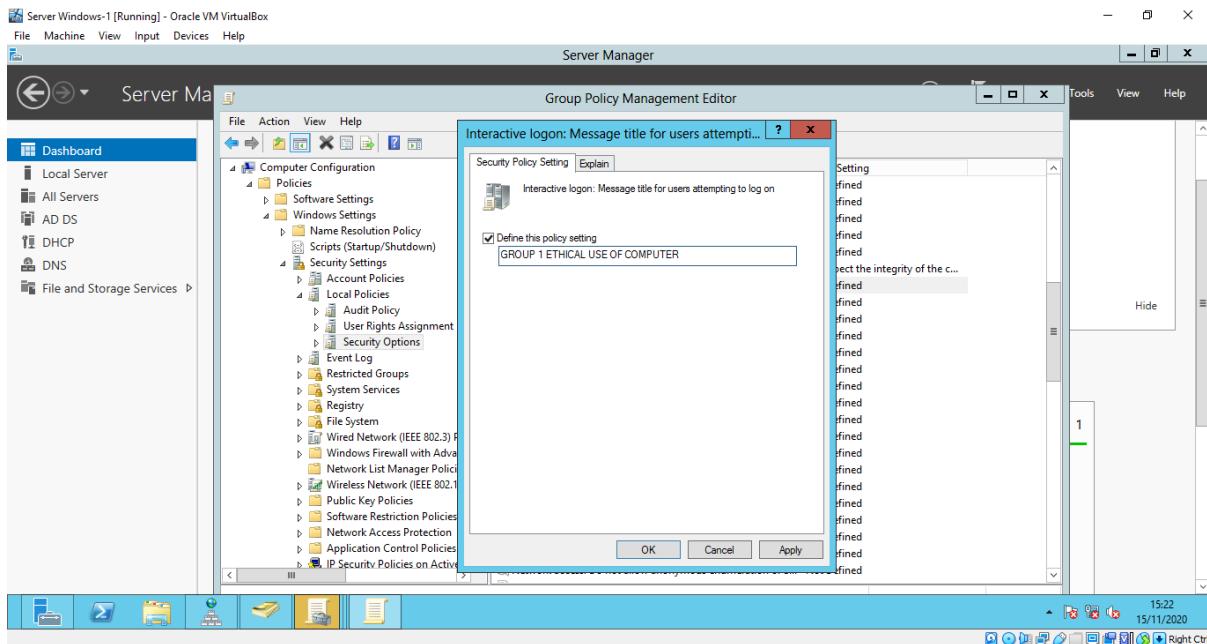


Figure 5.2.3.39 Interactive logon tab

Step 40: Both status of the policy setting are defined

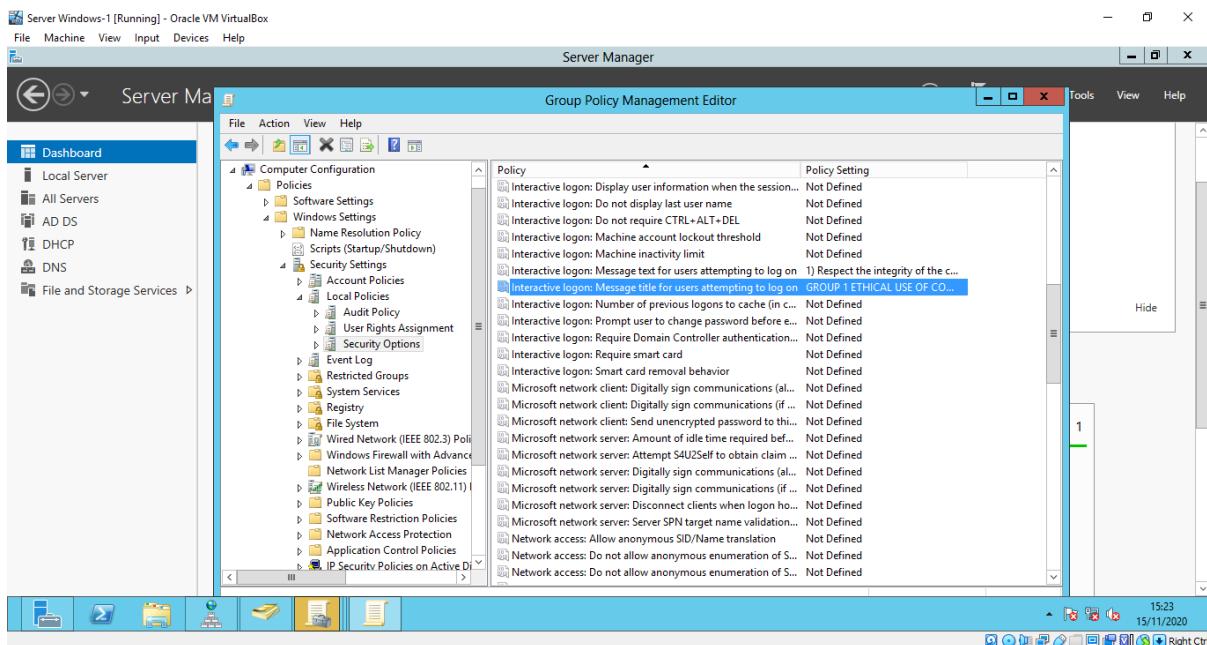


Figure 5.2.3.40 Status of second GPO that has been created

Step 41: The report of the first GPO

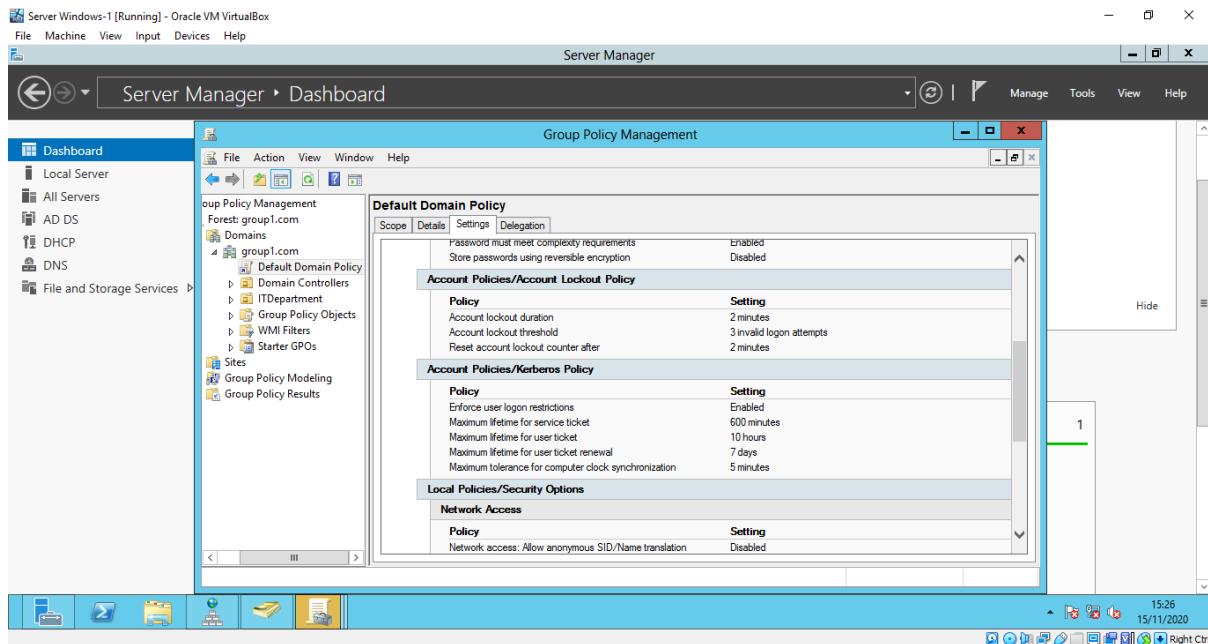


Figure 5.2.3.41 Report of first GPO

Step 42: The report of the second GPO

The screenshot shows the 'GROUP 1 LOGON BANNER' report. The 'Policies' section is selected, showing 'Windows Settings' and 'Security Settings'. Under 'Local Policies/Security Options', the 'Interactive Logon' section is expanded, showing two policies: 'Interactive logon: Message text for users attempting to log on' and 'Interactive logon: Message title for users attempting to log on'. Both policies have their settings defined. The 'User Configuration' section shows 'No settings defined.'

Figure 5.2.3.42 Report of second GPO

5.2.4. DHCP (IPv4 & IPv6)

DHCP IPV4

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

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

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

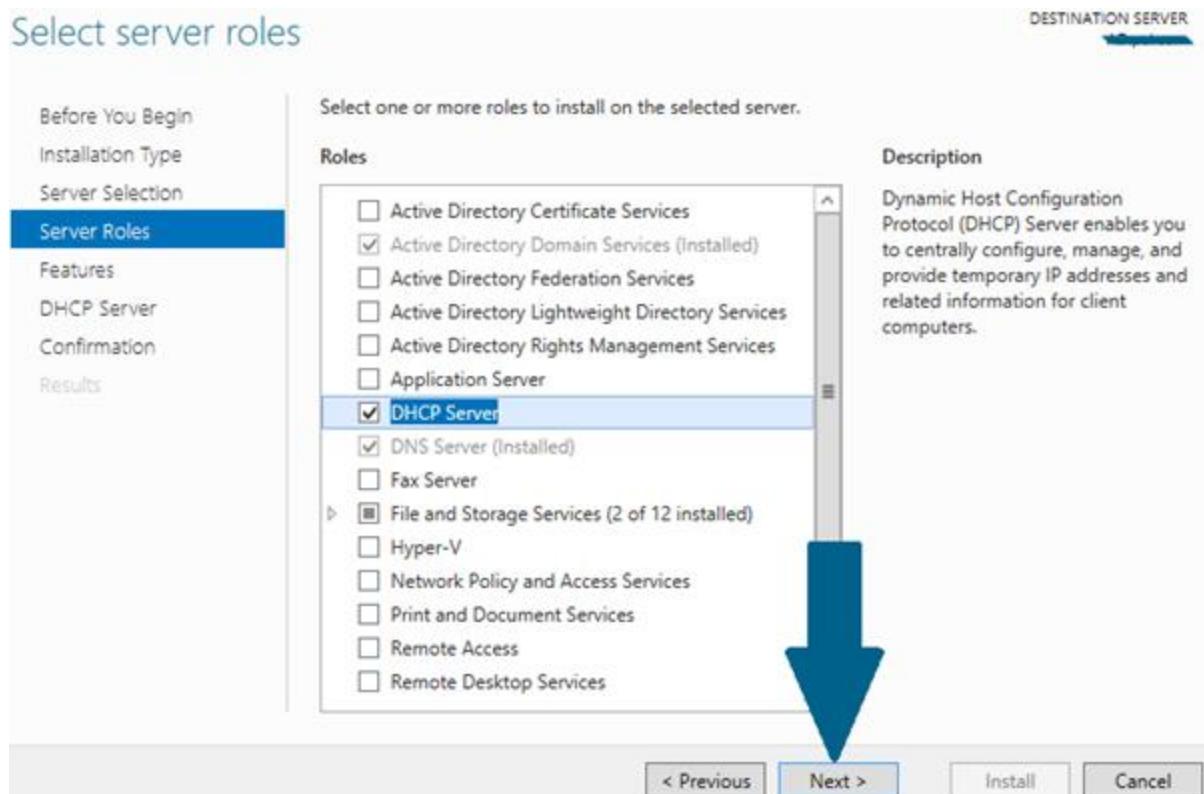


Figure 5.2.4 1 Installing new DHCP roles

Step 4: Then, wait until the installation is completed.

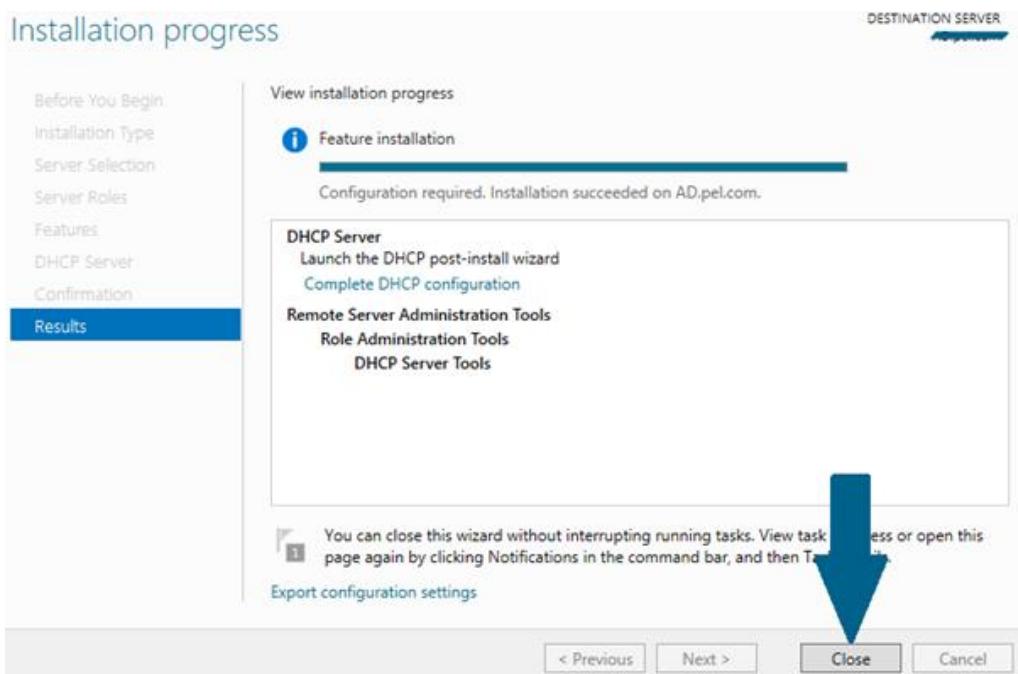


Figure 5.2.4 2 Finish setup DHCP roles

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

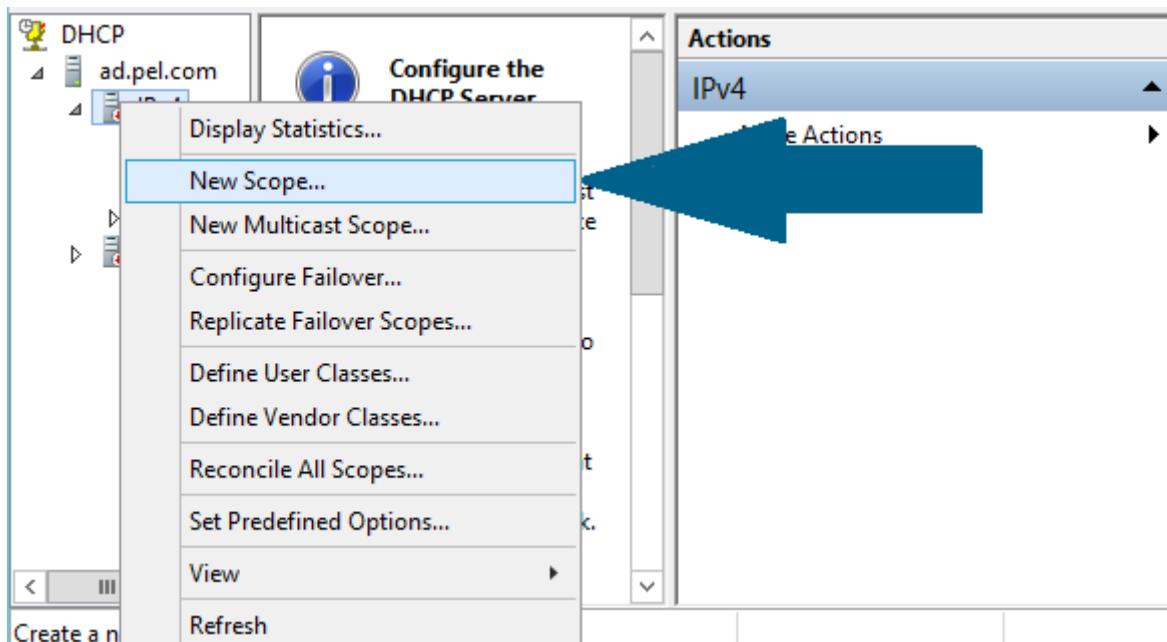


Figure 5.2.4 3 Creating new scope for DHCP

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

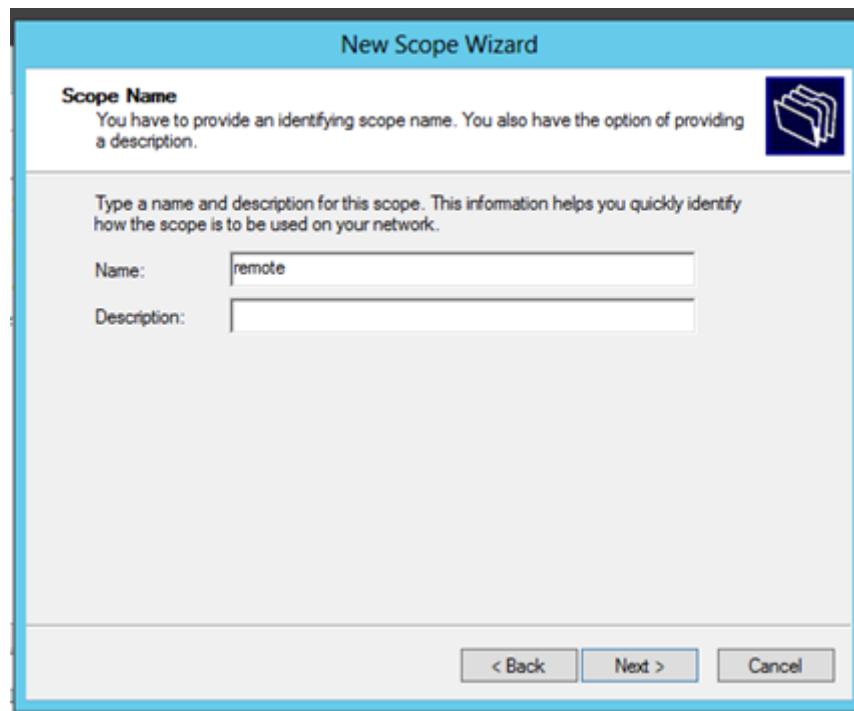


Figure 5.2.4 4 Create DHCP scope name

Step 7: Then, Insert ip address range for ipv4.

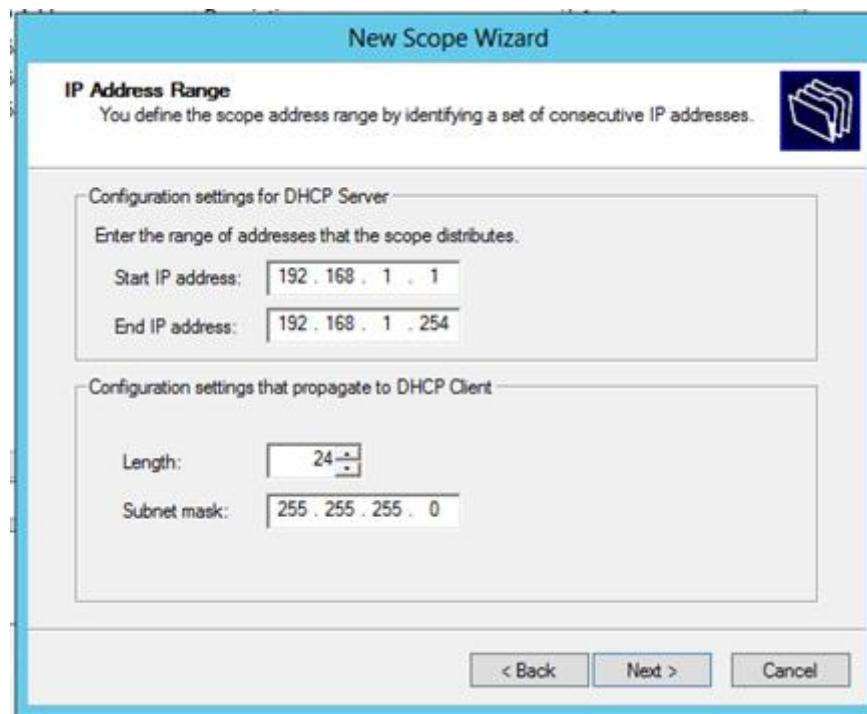


Figure 5.2.4 5 Setup DHCP ipv4 range

Step 8: Then insert default gateway for router.

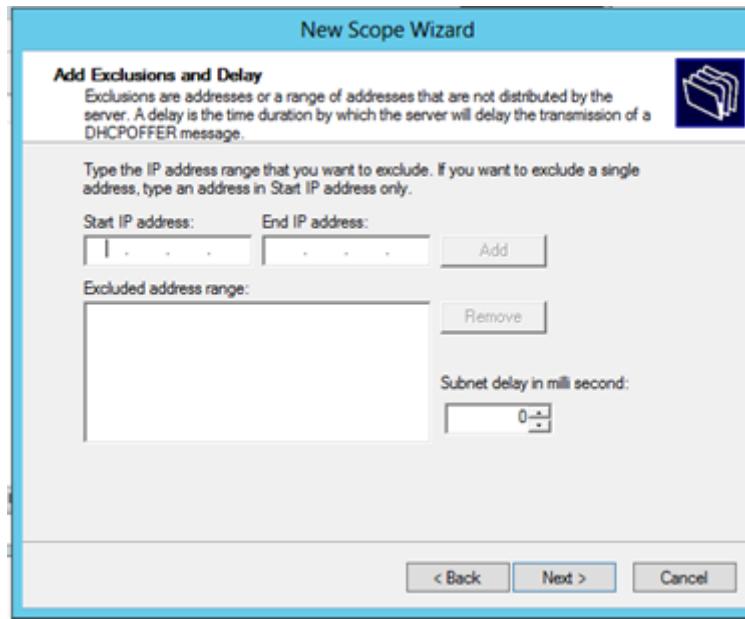


Figure 5.2.4 6 Insert DHCP gateway

Step 9: Select lease duration for DNS (example 8 days)



Figure 5.2.4 7 Select DHCP ip duration

Step 10: Then, select “Yes, I want to configure these option”

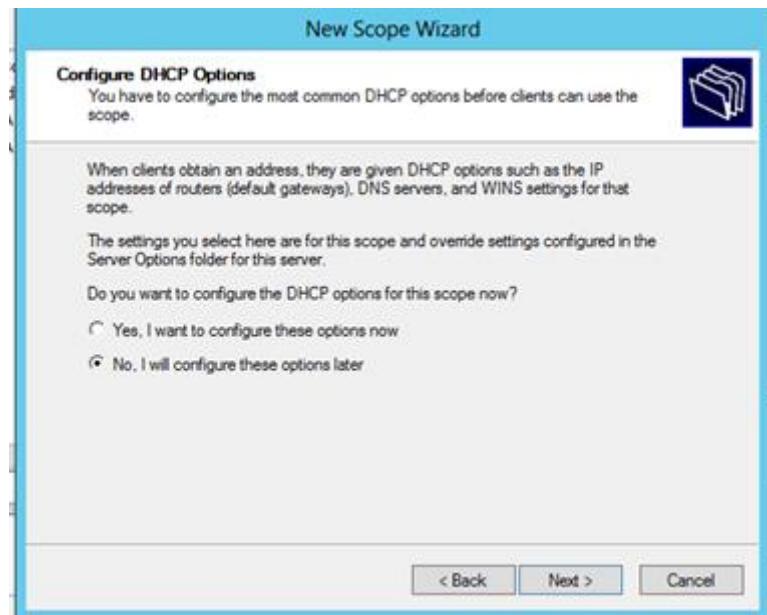


Figure 5.2.4 8 Finish configure scope for DHCP

Step 11: Click next on the next page.

Step 12: Then click “Yes” and finish the setup for Ipv4.



Figure 5.2.4 9 Finish DHCP setup

DHCP IPV6

Step 1: Now create new scope for ipv6

Step 2: Insert name as “group1” for remote pc then click next.

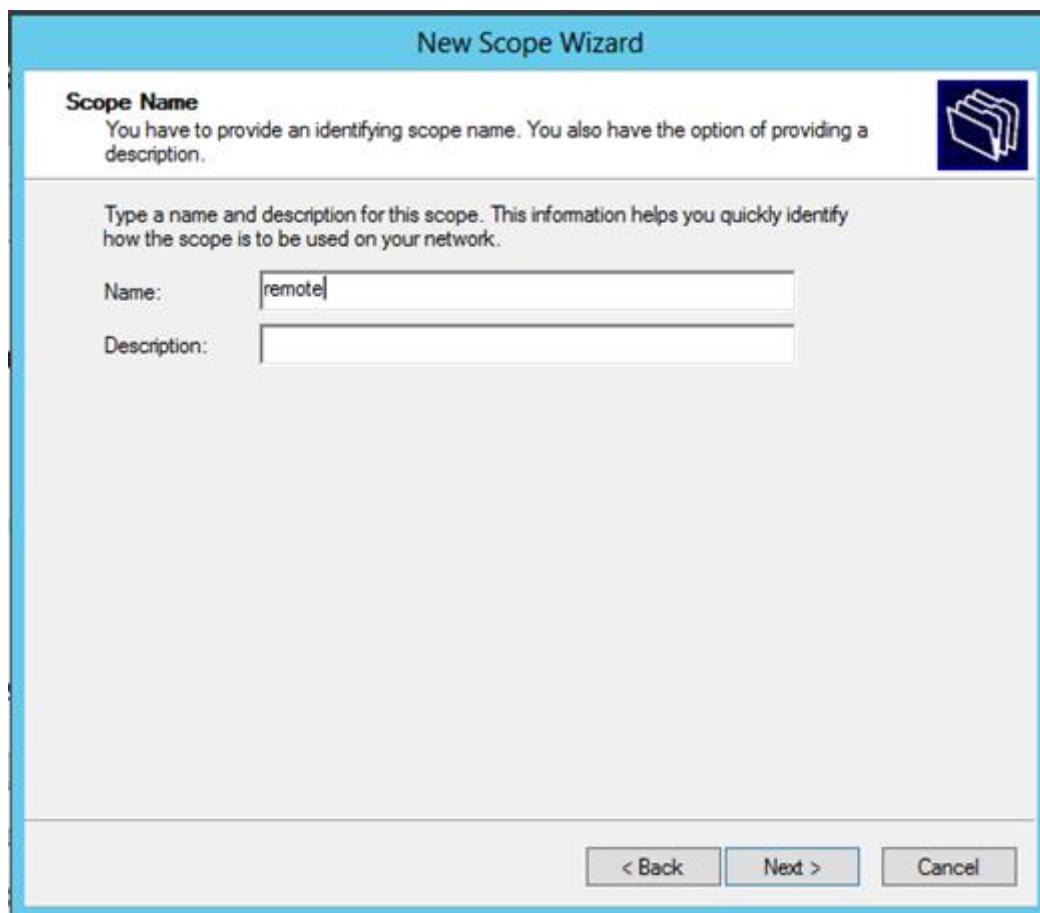


Figure 5.2.4 10 Insert ipv6 scope name

Step 3: Insert prefix with (2001:3200:1000:1000::/64). Then, click next.

Step 4: Exclude the ip in the figure and just click next the next step and click finish.

Start IP Address	End IP Address	Description
2001:3200:1000:1000:0:2f:ffff:ffff	2001:3200:1000:1000:ffff:ffff:ffff:ffff	IP Addresses excluded from distribution

Figure 5.2.4 11 Ipv6 exclusion

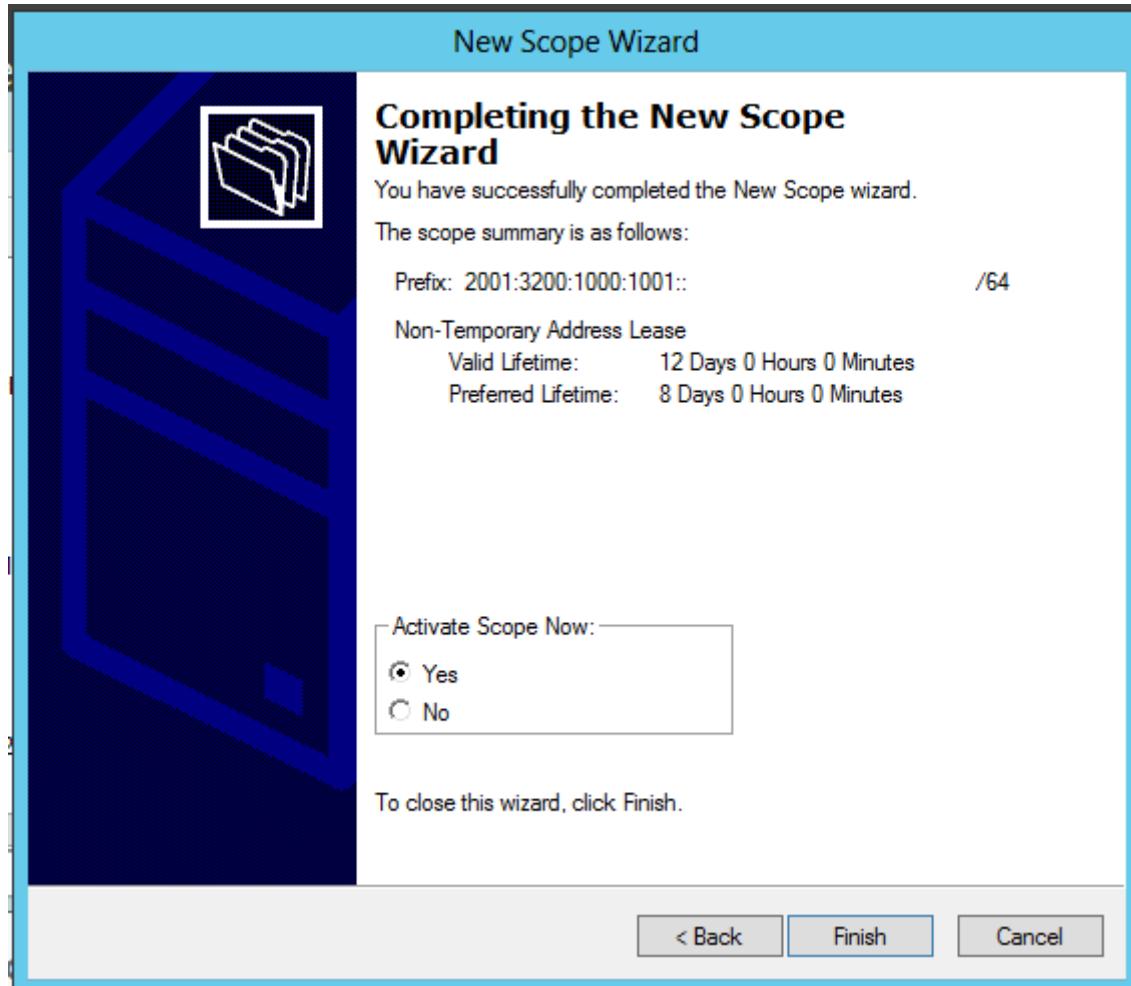


Figure 5.2.4 12 Ipv6 DHCP finish query setup

5.2.5. Web, SSL & Virtual Hosting

IIS (Internet Information Services) installation

Step 1: Open the Server Manager and click Add Roles and Features

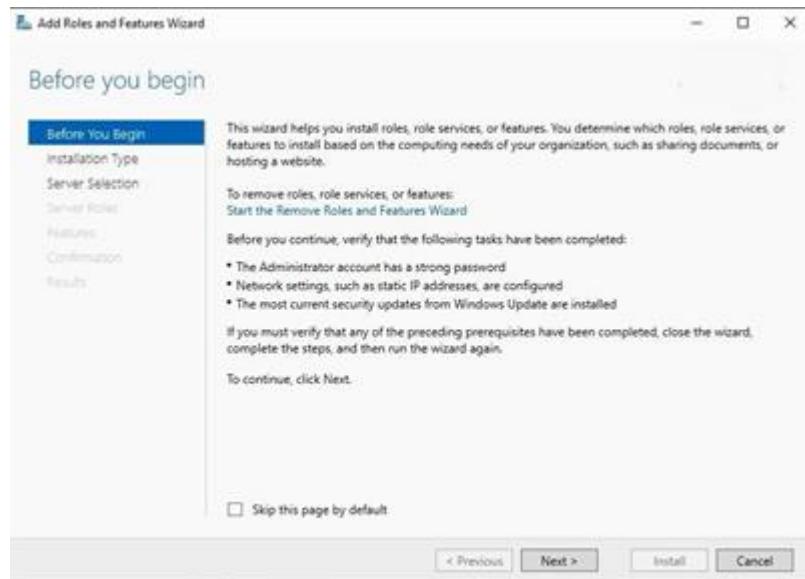


Figure 5.2.5.1 Add roles and features

Step 2: On the Installation Type page, select Role-based or feature-based installation to configure a single server. Click Next.

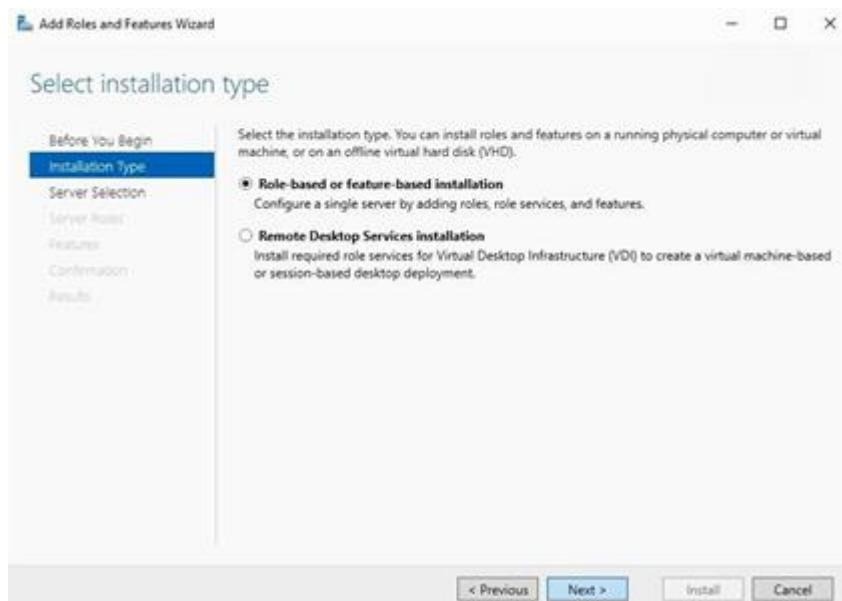


Figure 5.2.5.2 Select installation type

Step 3: On the **Server Selection** page, select **Select a server from the server pool**, and then select a server; or select **Select a virtual hard disk server**, select a server to mount the VHD on, and then select a VHD file. Click **Next**.

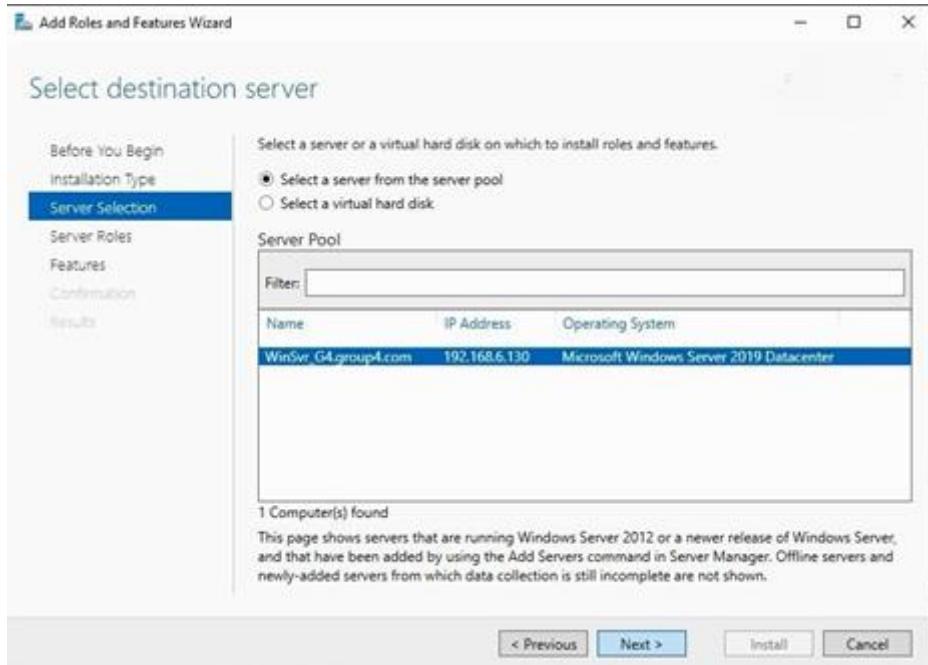


Figure 5.2.5.3 Select destination server

Step 4: On the **Server Roles** page, select **web Server (IIS)**

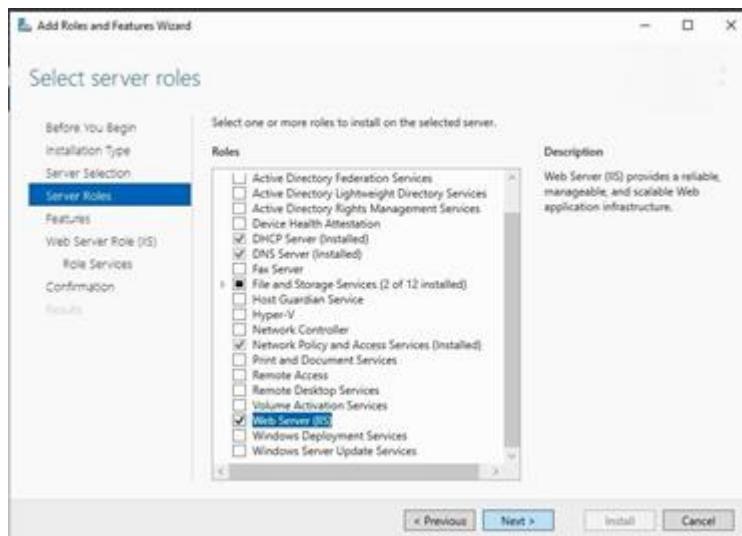


Figure 5.2.5.4 Select server roles

Step 5: In the **Add Roles and Features** wizard, click **Add Features** if , want to install the IIS Management Console. If, do not want to install the Management Console, uncheck **Include management tools (if applicable)**, and then click **Continue**.

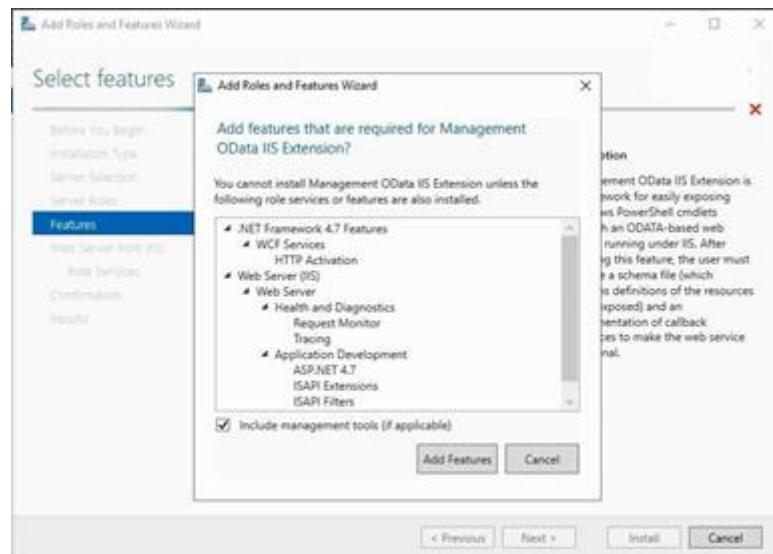


Figure 5.2.5.5 Include management tools if applicable

Step 6: The Installation Progress page is displayed. , can close the wizard without interrupting running tasks. , can view task progress or open the page again by clicking Notifications in the notification area, and then clicking Task Details.

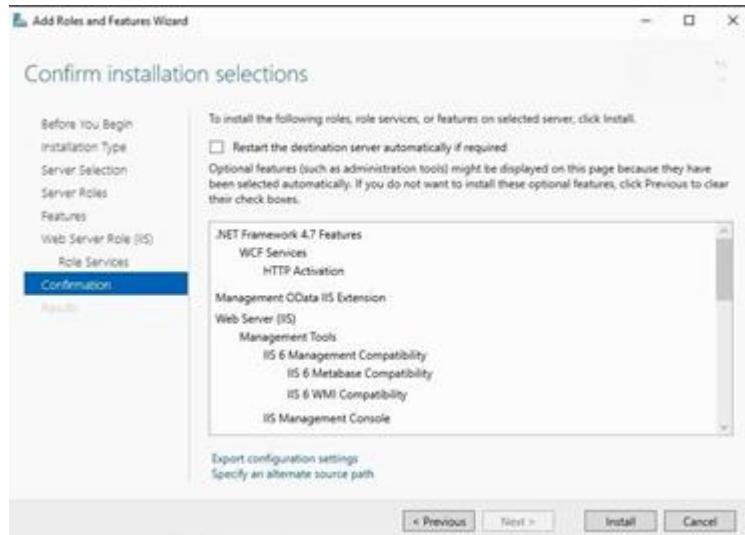


Figure 5.2.5.6 Installation Progress

Step 7: On the **Results** page, verify that the installation succeeds, and then click **Close**.

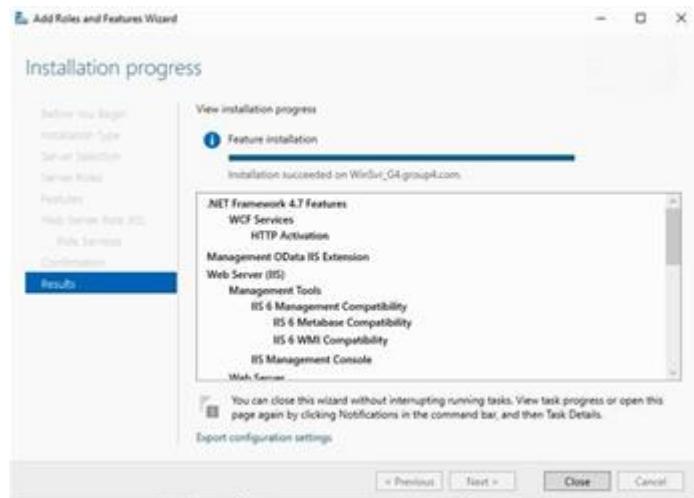


Figure 5.2.5.7 verify installation succeeds

SSL (Secure Socket Layer) Installation and Configuration

1. In Confirm installation selections, click **Install**. Do not close the wizard during the installation process. When installation is complete, click **Configure Active Directory Certificate Services on the destination server**. The AD CS Configuration wizard opens. Read the credentials information and, if needed, provide the credentials for an account that is a member of the Enterprise Admins group. Click **Next**.
2. In **Role Services**, click **Certification Authority**, and then click **Next**.
3. On the **Setup Type** page, verify that **Enterprise CA** is selected, and then click **Next**.
4. In **Confirmation**, click **Configure** to apply ,r selections, and then click **Close**.
5. Open Internet Information Services (IIS) then click on Server Certificates.
6. Create Domain Certificate in Server Certificates
7. Fill up the form then click button Next.
8. Select Certification Authority and fill up Friendly Name then click button Finish
9. Certificate has been created on the list Server Certificates

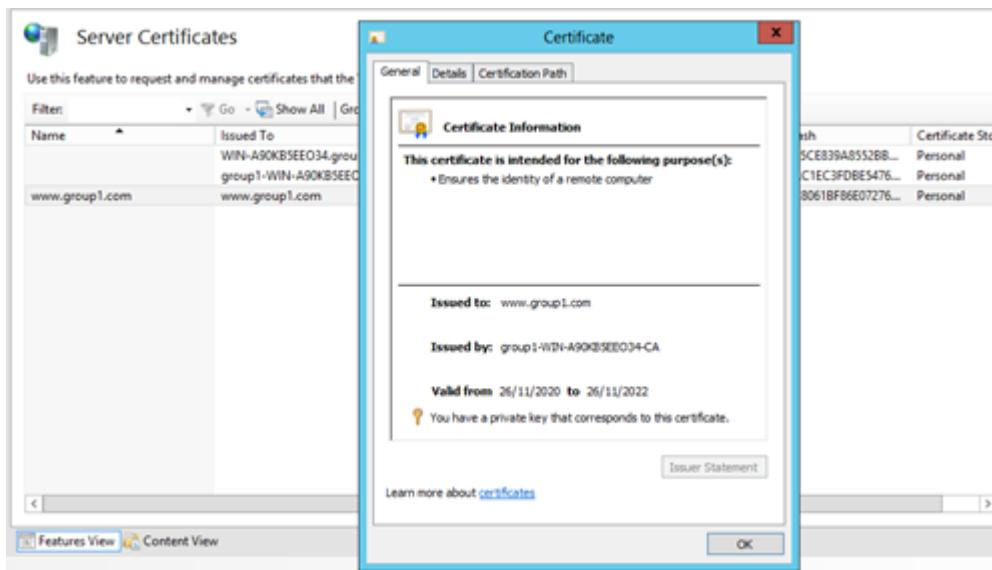


Figure 5.2.5.7 SSL certificate

Add website Web & SSL

Step 1: Open IIS manager and click add website

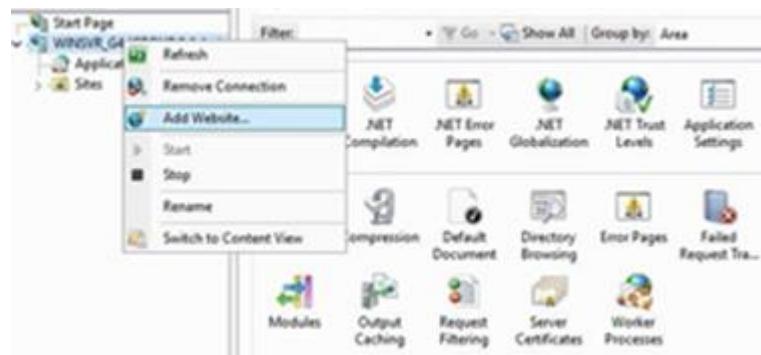


Figure 5.2.5.8 Add website

Step 2: Add website for Ipv4

Sites				
Name	ID	Status	Binding	Path
Default Web Site	1	Started (ht...)	*:81 (http)	%SystemDrive%\inetpub\wwwroot
group1vh	4	Started (ht...)	vhgroup1.com on *:80 (http)	C:\inetpub\wwwroot\vhgp1
group1web.com	2	Started (ht...)	www.group1.com on *:80 (http)	C:\inetpub\wwwroot\WebSSL
group1webSSL	3	Started (ht...)	www.group1.com on *:443 (https)	C:\inetpub\wwwroot\SSL

Figure 5.2.5.8 Website added

Step 3: Create folder and default document and save as html file in the directory intetpub/wwwroot

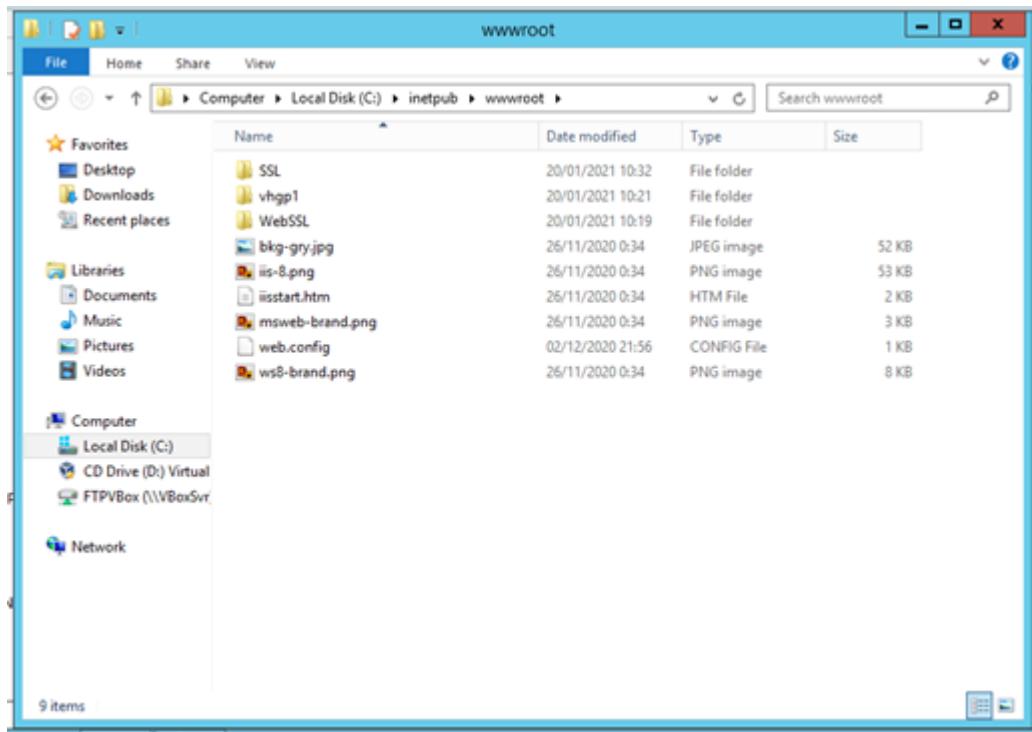


Figure 5.2.5.9 HTML file ate wwwroot

Step 4: Add default document that already created at wwwroot in IIS Default Document

The screenshot shows the "Default Document" section of the IIS Manager. The title bar says "Default Document". Below it is a descriptive text: "Use this feature to specify the default file(s) to return when a client does not request a specific file. Set default documents in order of priority." A table lists the default documents:

Name	Entry Type
table.html	Local
WebSSL	Local
Default.htm	Inherited
Default.asp	Inherited
index.htm	Inherited
index.html	Inherited
iisstart.htm	Inherited

Figure 5.2.5.10 Default document at IIS

Step 5: Enable Directory Browsing at IIS

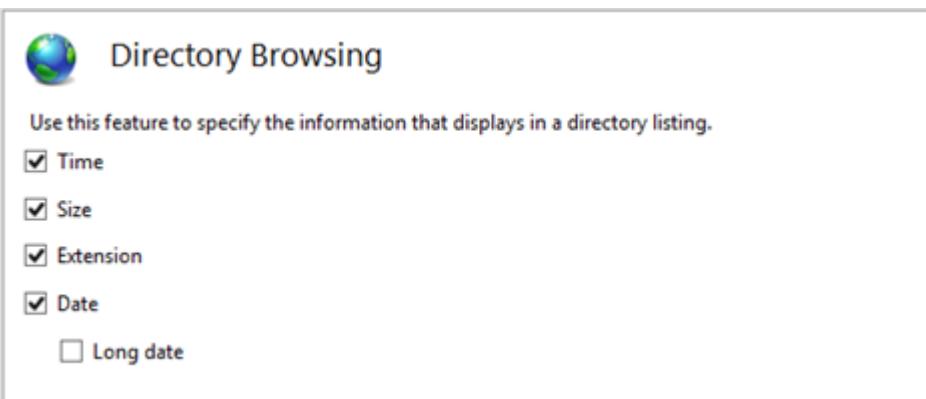


Figure 5.2.5.11 Directory browsing at IIS

Step 6: Click on advance to see the directory for website

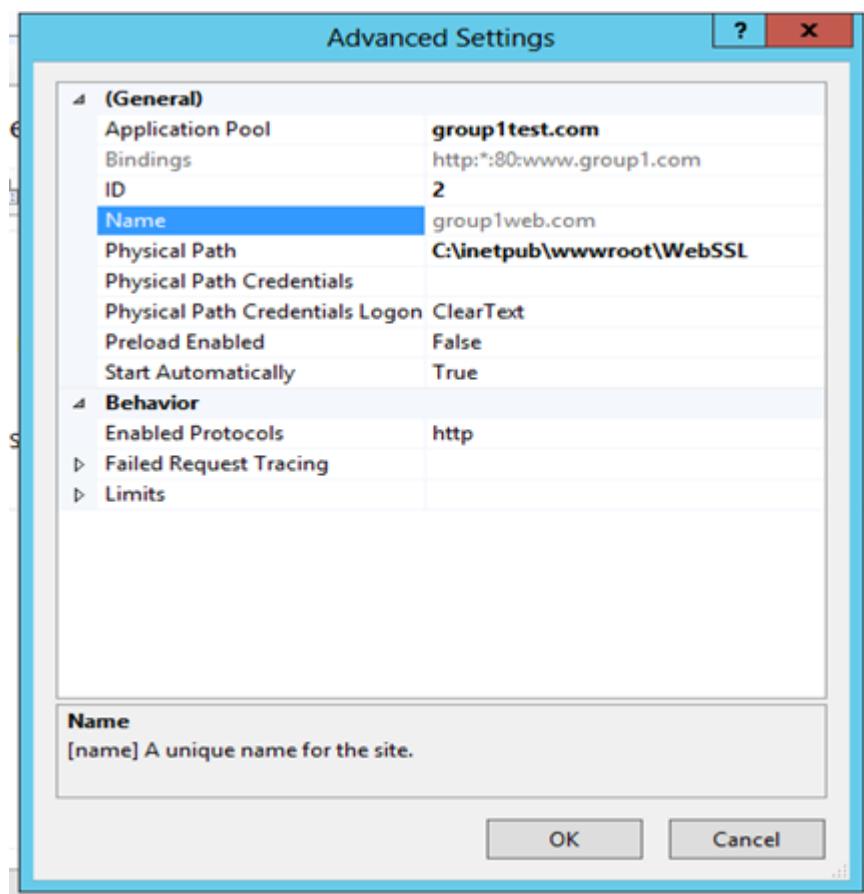


Figure 5.2.5.12 Directory HTML file

Step 7: Tick the Require SSL for SSL website



Figure 5.2.5.13 SSL Settings

Step 8: Open DNS manager. Then go to forward lookup zone. Find group1.com. Then create new host AAA which is www for web

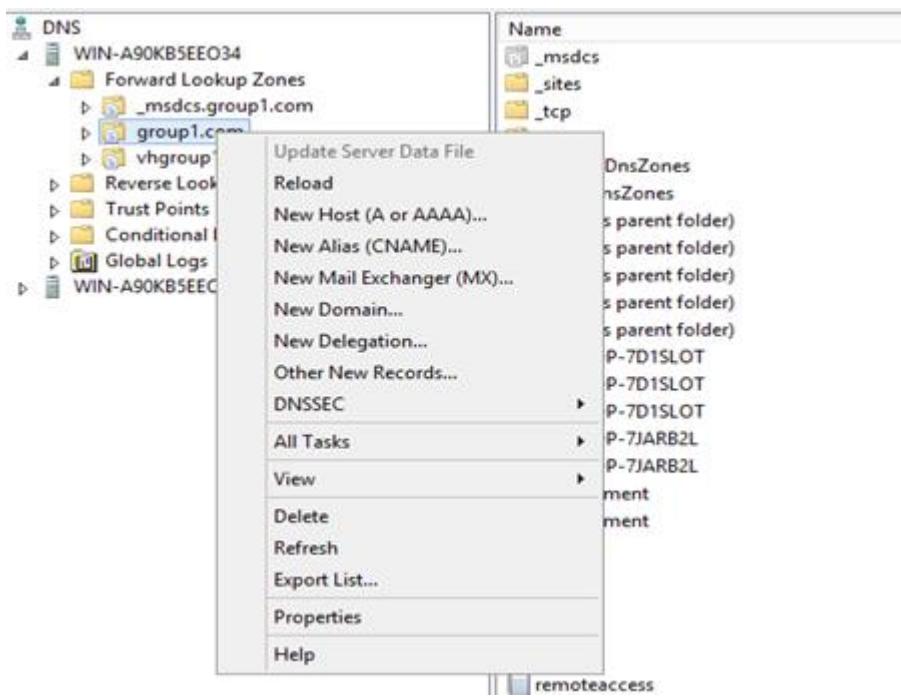


Figure 5.2.5.14 Create new host AAA

Step 9: Create the www for web

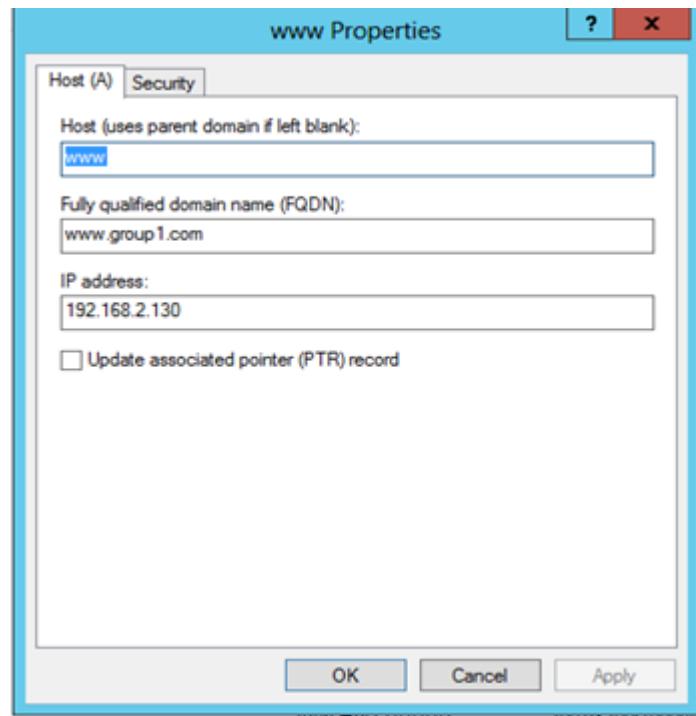


Figure 5.2.5.15 New host created

5.2.5.4 Virtual hosting

Step 1: Go to Server Manager > Tools > Internet Information (IIS) Manager and at the connection column double-click WIN to expand it. Then, right-click on Sites and select Add Website

Step 2: Add virtual website

Step 3: Create the directory for the website. Then, create new html file for the site and add default document to the site.

Step 4: Open DNS Manager, create new Forward Lookup Zone.



Figure 5.2.5.16 New Zone Wizard

Step 5: Select zone type as Primary Zone



Figure 5.2.5.17 Primary Zone

Step 6: Choose “To all DNS servers running on domain controller this domain: group1.com”

Step 7: Enter zone name as vhgroup1.com



Figure 5.2.5.18 Zone Name

Step 8: Choose “Allow both nonsecure and secure dynamic updates”

Step 9: Complete New Zone Creation



Figure 5.2.5.19 Completing New Zone

Step 10: Right click on the zone and choose new host

Step 11: Add the host details and click add host button

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[2] win-a90kb5eo34.group1.com, host...	static
(same as parent folder)	Name Server (NS)	win-a90kb5eo34.group1.com.	static
(same as parent folder)	Host (A)	192.168.2.130	static

Figure 5.2.5.20 Zone details

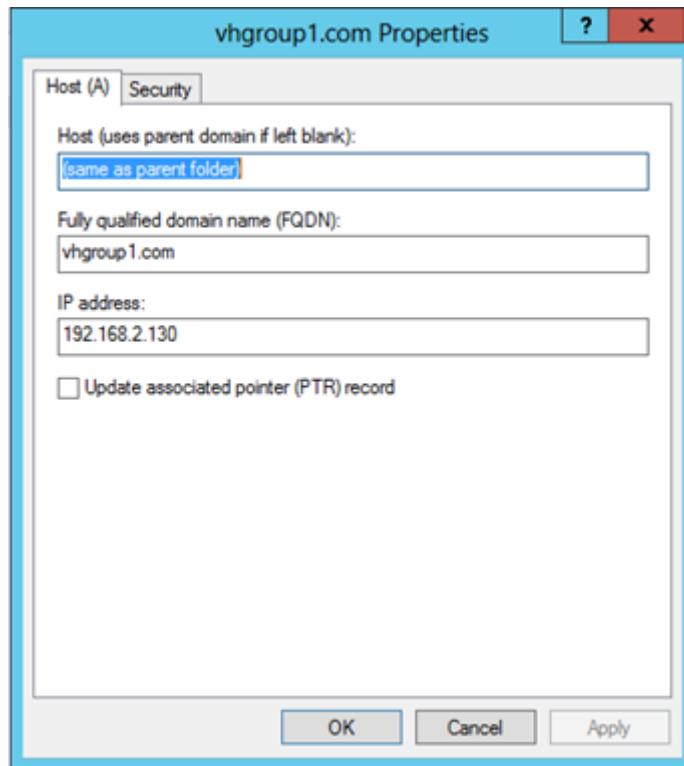


Figure 5.2.5.21 Host Properties

5.2.6. Linux Email Server

Step 1: Go to terminal and write the command **nano /etc/hosts**

- Write – ip address mail.group1.com

```

debian@WorkshopII: ~
File Edit View Search Terminal Help
GNU nano 3.2          /etc/hosts

127.0.0.1 localhost
127.0.1.1 workshopii.group1.com WorkshopII
192.168.2.146 mail.group1.com
200.200.201.40 mail.group1.com
# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

[ File '/etc/hosts' is unwritable ]
^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 5.2.6.1 nano/etc/hosts

Step 2: Postfix installation, **apt install postfix -y**, go to internet site and change the name to mail.group1.com then write **/etc/init.d/postfix start** and **systemctl enable postfix**

Step 3: Get into postfix main.cf, write **nano /etc/postfix/main.cf** and change the following command

- **smtpd_banner = \$myhostname ESMTP**
- **myhostname = mail.group1.com**
- **mydomain = group1.com**
- **myorigin = \$mydomain**
- **mydestination = \$myhostname, \$mydomain, mail.group1.com, localhost**
- **home_mailbox = Maildir/**

and then write command **/etc/init.d/postfix reload**

```

debian@WorkshopII: ~
File Edit View Search Terminal Help
GNU nano 3.2          /etc/postfix/main.cf
# See /usr/share/postfix/main.cf.dist for a commented, more complete version

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

smtpd_banner = $myhostname ESMTP
biff = no

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

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

readme_directory = no

[ File '/etc/postfix/main.cf' is unwritable ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell ^L Go To Line

```

Figure 5.2.6.2 /etc/postfix/main.cf

```

debian@WorkshopII: ~
File Edit View Search Terminal Help
GNU nano 3.2          /etc/postfix/main.cf
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_un$ 
myhostname = mail.group1.com
mydomain = group1.com
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = $mydomain
mydestination = $myhostname, $mydomain, mail.group1.com, localhost
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all
home_mailbox = Maildir/

^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 5.2.6.3 /etc/postfix/main.cf 2

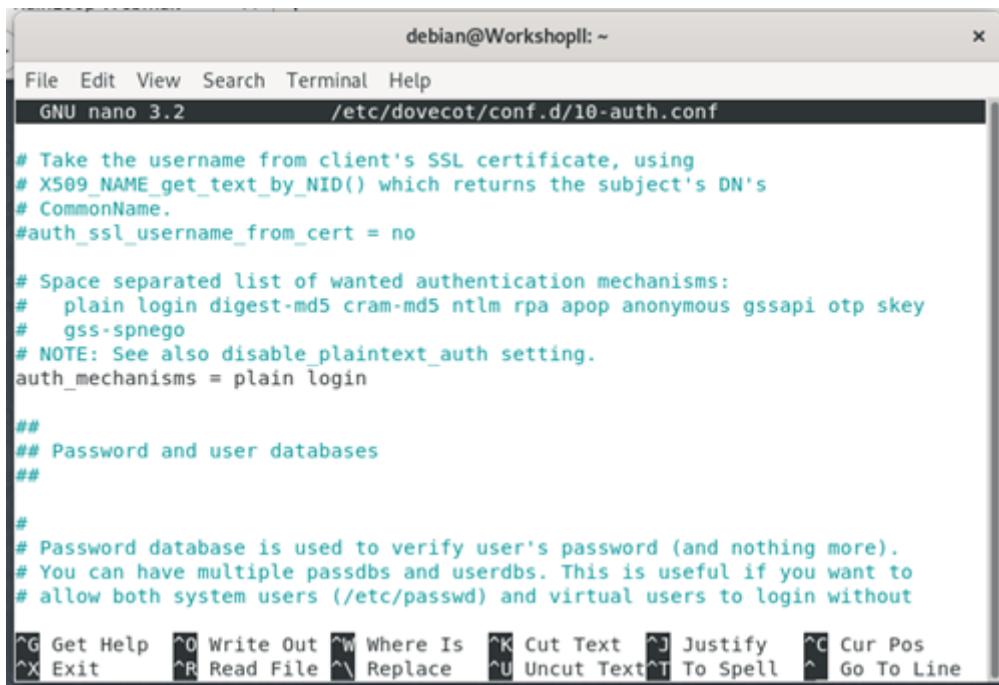
Step 4: Dovecot installation, write command **apt install dovecot-core dovecot-imapd –y** then enable dovecot with this command **systemctl enable dovecot**

Step 5: Get into dovecot dovecot.conf, **nano /etc/dovecot/dovecot.conf**

- Remove # at **Listen = *, ::**

Step 6: Write command **nano /etc/dovecot/conf.d/10-auth.conf** and remove # at this command

- **disable_plaintext_no = no**
- **auth_mechanisms = plain login**



```

debian@WorkshopII: ~
File Edit View Search Terminal Help
GNU nano 3.2          /etc/dovecot/conf.d/10-auth.conf

# 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

##
## Password and user databases
##


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

^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 5.2.6.4 10-auth.conf

Step 7: Write command **nano /etc/dovecot/conf.d/10-mail.conf**

- Remove # at **mail_location = mailldir:~/Maildir**

```
debian@WorkshopII: ~
File Edit View Search Terminal Help
GNU nano 3.2          /etc/dovecot/conf.d/10-mail.conf

#
# 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

# 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
# namespaces you'll typically want to enable ACL plugin also, otherwise all

^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 5.2.6.5 10-mail.conf

Step 8: Write command **nano /etc/dovecot/conf.d/10-master.conf** and go to service auth and remove the # and add another command

- **unix_listener /var/spool/postfix/private/auth {**

mode = 0666

user = postfix

group = postfix

}

```

debian@WorkshopII: ~
File Edit View Search Terminal Help
GNU nano 3.2          /etc/dovecot/conf.d/10-master.conf

#mode = 0666
#user =
#group =
}

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

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

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

```

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

Figure 5.2.6.6 10-master.conf

Step 9: Start the dovecot, `systemctl start dovecot` then write command `/etc/init.d/dovecot start` and write `telnet ipaddress imap`. And write command under telnet

- **A1 LOGIN username password**
- **A2 LIST “” “”**
- **A3 EXAMINE INBOX**
- **A4 LOGOUT**

Step 10: Write command to make directory for mail at dovecot.

```

debian@WorkshopII:~$ sudo mailldirmake.dovecot /etc/skel/Maildir/.Drafts
debian@WorkshopII:~$ sudo mailldirmake.dovecot /etc/skel/Maildir/.Sent
debian@WorkshopII:~$ sudo mailldirmake.dovecot /etc/skel/Maildir/.Trash
debian@WorkshopII:~$ sudo mailldirmake.dovecot /etc/skel/Maildir/.Archive
debian@WorkshopII:~$ sudo mailldirmake.dovecot /etc/skel/Maildir/.Templates
debian@WorkshopII:~$ sudo cp -r /etc/skel/Maildir/home/myuser/
cp: missing destination file operand after '/etc/skel/Maildir/home/myuser/'
Try 'cp --help' for more information.
debian@WorkshopII:~$ sudo cp -r /etc/skel/Maildir/home/myuser/
sudo: cp-r: command not found
debian@WorkshopII:~$ sudo cp -r /etc/skel/Maildir/home/Afifahh/
cp: missing destination file operand after '/etc/skel/Maildir/home/Afifahh/'
Try 'cp --help' for more information.
debian@WorkshopII:~$ sudo cp -r /etc/skel/Maildir /home/Afifahh/
debian@WorkshopII:~$ sudo cp -r /etc/skel/Maildir /home/Aishah/
debian@WorkshopII:~$ sudo cp -r /etc/skel/Maildir /home/Amirahh/
debian@WorkshopII:~$ sudo cp -r /etc/skel/Maildir /home/Faris/
debian@WorkshopII:~$ sudo cp -r /etc/skel/Maildir /home/Hazim/
debian@WorkshopII:~$ sudo cp -r /etc/skel/Maildir /home/Yongg/
debian@WorkshopII:~$ /etc/init.d/dovecot restart
[ ok ] Restarting dovecot (via systemctl): dovecot.service.

```

Figure 5.2.6.7 Mailldirmake

Step 11: Curl installation, **apt install apache2 php libapache2-mod-php php-curl php-xml -y** then write this command

- **mkdir /var/www/html/mail/**
- **cd /var/www/html/mail/**
- **apt install curl**
- **curl -sL <https://repository.rainloop.net/installer.php> | php**

Step 12: Open the browser and write **mail.group1.com/mail/?admin** and enter the username and password **admin 12345**

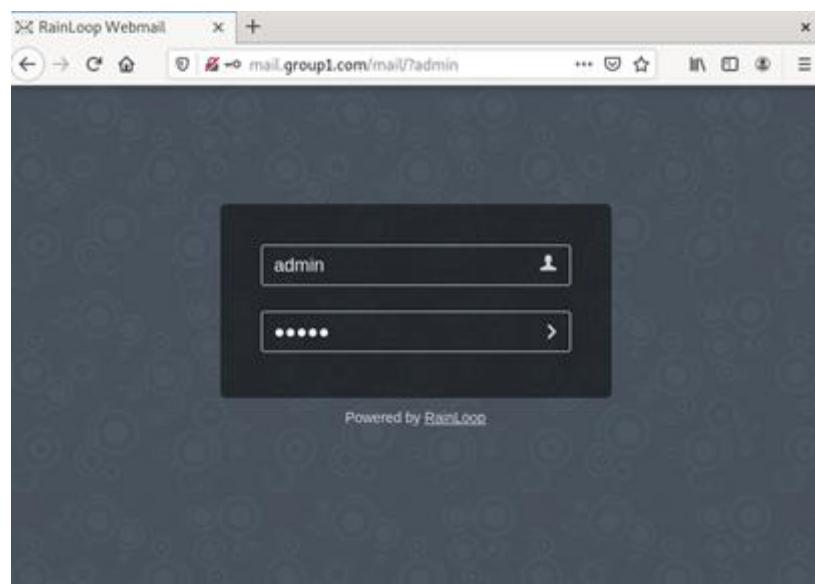


Figure 5.2.6.8 Admin mail login

Step 13: Add domain

- **domain = group1.com**
- **server = mail.group1.com**
- **Tick up user short login**
- **SMTP tick use php mail() function**

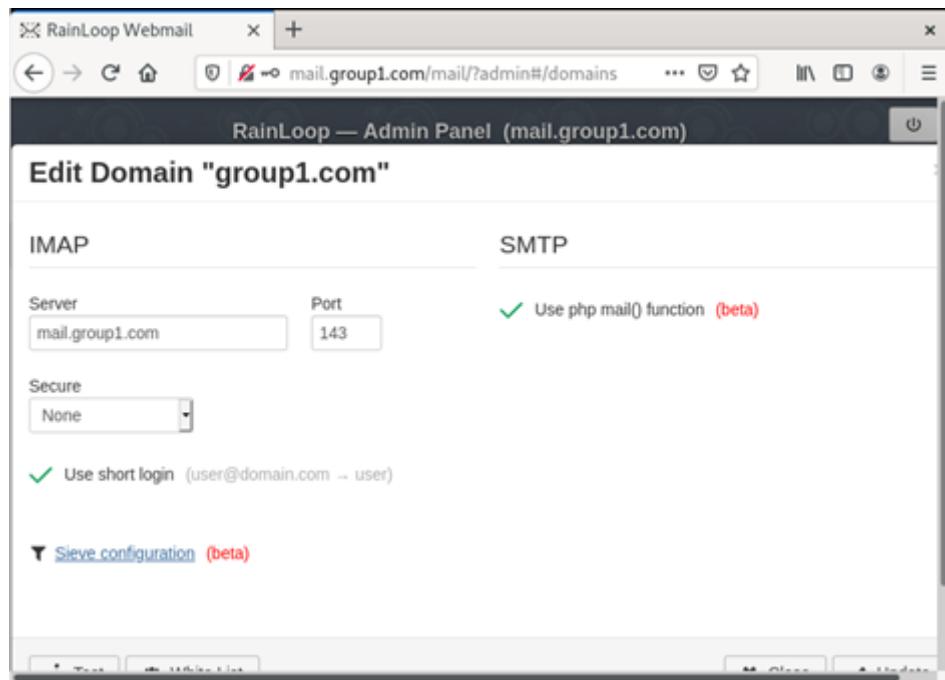


Figure 5.2.6.9 Edit domain

Step 14: Fill up the default domain with **group1.com** and tick **Try to determine user domain**

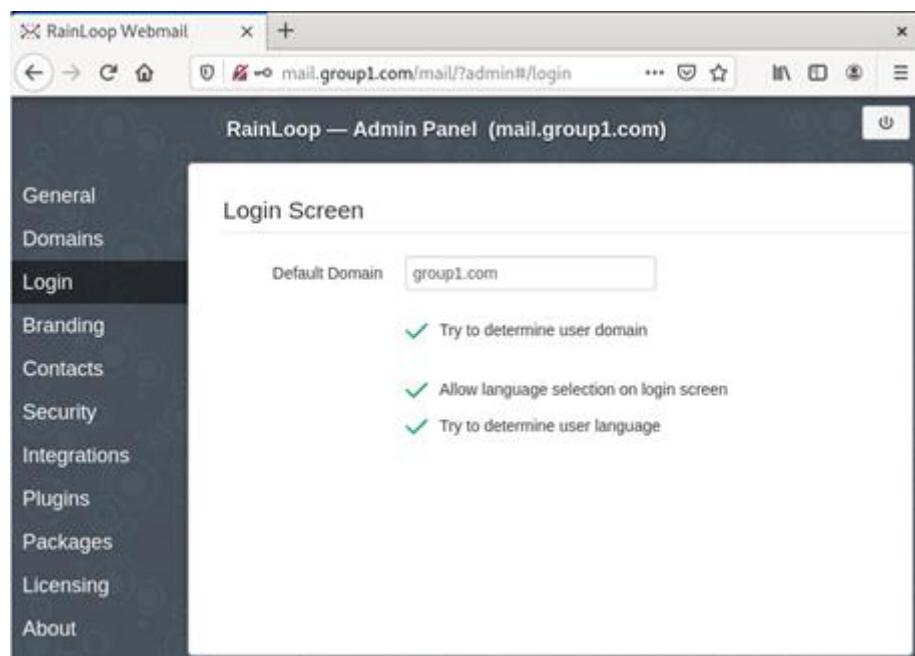


Figure 5.2.6.10 Login screen

5.2.7. Access Control List

Step 1: Configuration at router Branch to limit the usage of certain services at RemoteAccess client pc.

- Rule 1: Deny http, port 80 in RemoteAccess client
- Rule 2: Deny ftp, port 21 in RemoteAccess client.
- Rule 3: Deny ssh, port 22 in RemoteAccess client.
- Rule 4: Deny telnet, port 23 in RemoteAccess client.

```
Branch(config)#ip access-list extended DENY_HTTP_EMAIL_SSH_TELNET
Branch(config-ext-nacl)#$2.168.1.0 0.0.0.255 host 200.200.201.40 eq 80
Branch(config-ext-nacl)#$2.168.1.0 0.0.0.255 host 200.200.201.40 eq 21
Branch(config-ext-nacl)#$2.168.1.0 0.0.0.255 host 200.200.201.40 eq 22
Branch(config-ext-nacl)#$2.168.1.0 0.0.0.255 host 192.168.2.129 eq 23
Branch(config-ext-nacl)#permit ip any any
Branch(config-ext-nacl)#int f0/0.10
Branch(config-subif)#ip access-group DENY_HTTP_EMAIL_SSH_TELNET in
```

Figure 5.2.7.1 Acl command

Step 2: do sh access-list to list out the acl command that has been created

```
Extended IP access list DENY_HTTP_EMAIL_SSH_TELNET
    10 deny tcp 192.168.1.0 0.0.0.255 host 200.200.201.40 eq www
    20 deny tcp 192.168.1.0 0.0.0.255 host 200.200.201.40 eq ftp
    30 deny tcp 192.168.1.0 0.0.0.255 host 200.200.201.40 eq 22
    40 deny tcp 192.168.1.0 0.0.0.255 host 192.168.2.129 eq telnet
    50 permit ip any any
```

Figure 5.2.7.2 List of acl command

5.2.8. IPSec Site-to-Site Tunneling

Go to Branch router configuration

Step 1 : Create an ISAKMP phase 1 policy.

```
crypto isakmp policy 10
```

Figure 5.2.8 1 Create ISAKMP phase 1 policy

Step 2 : Create an encryption method to be used for Phase 1. This encryption method is to secure and encrypt our packet and connection between the tunnel.

```
encr aes 256
```

Figure 5.2.8 2 Create an encryption method

Step 4 : Create the pre share key authentication with our peer (Next group router). The peer's pre-shared key is set to bitu3923 and its public IP address is 200.200.201.1. Every time the router try to establish a tunnel with the other group router (200.200.201.1), this pre shared key will be used.

```
authentication pre-share
group 5
crypto isakmp key bitu3923 address 200.200.201.1
```

Figure 5.2.8 4 Configure and Define a pre-shared key

Step 5 : Create an access-list and define the traffic we would like the router to pass through the VPN tunnel. In this configuration it would be traffic from one network to the other, 200.200.201.1 to 200.200.200.6.

```
ip access-list extended VPN-TRAFFIC
 permit gre host 200.200.201.1 host 200.200.200.6
```

Figure 5.2.8 5 Create an access-list

Step 6 : Create the transform set used to protect our data. We've named this VPN-SET.

```
crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
```

Figure 5.2.8 6 Create the transform set

Step 7 : Create the Crypto Map and connects the previously defined ISAKMP and Ipsec configuration together. We've named our crypto map VPN-MAP. The ipsec-isakmp tag tells the router that this crypto map is an IPSec crypto map.

```
crypto map VPN-MAP 10 ipsec-isakmp
description VPN connection to HQ
set peer 200.200.201.1
set transform-set VPN-SET
set pfs group5
match address VPN-TRAFFIC
```

Figure 5.2.8 7 Create the Crypto Map

Step 8 : Apply the crypto map to the outgoing interface of the router to another router. Here, the outgoing interface is Serial 0/1.

```
!
interface Serial0/1
ip address 200.200.200.6 255.255.255.0
ip nat outside
ip virtual-reassembly
ipv6 address 2001:DB8:5:6::6/64
clock rate 2000000
crypto map VPN-MAP
!
```

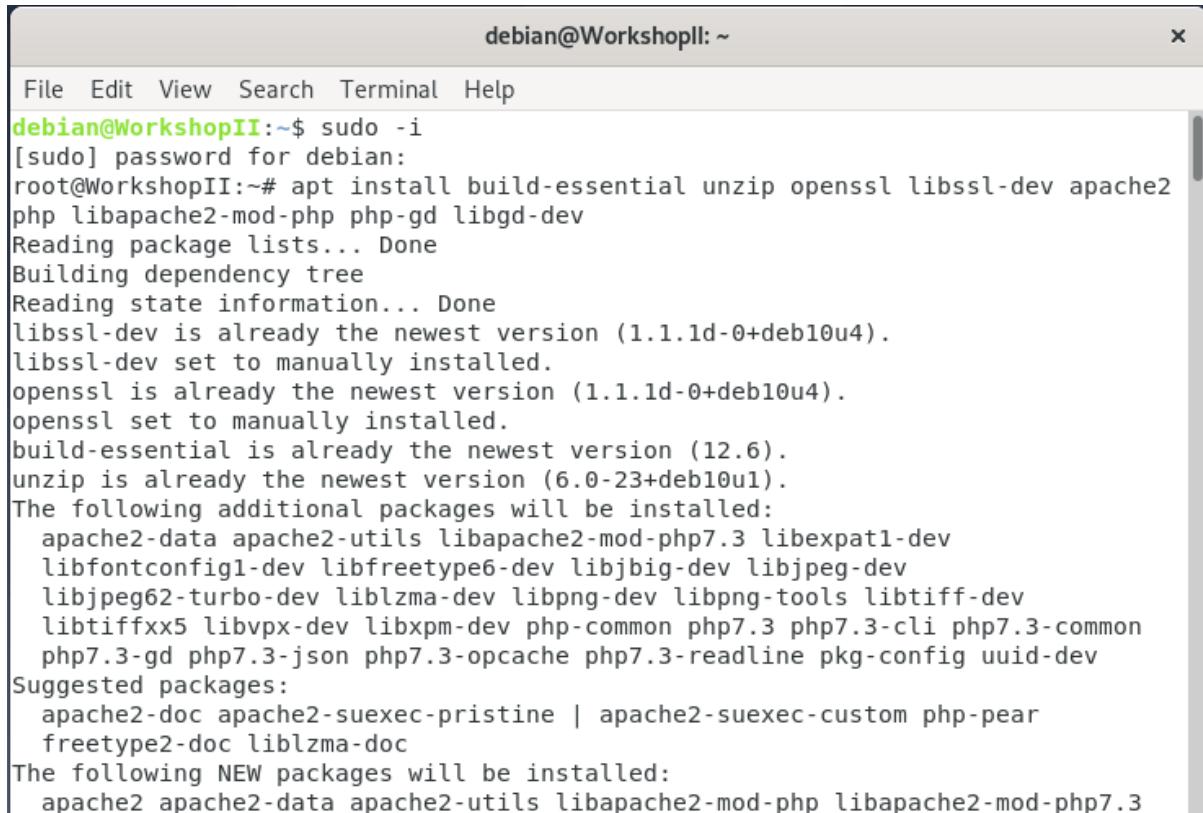
Figure 5.2.8 8 Apply the crypto map to the outgoing interface

Step 8 : Repeat the same process in the HQ Router using Branch Router as peer.

5.2.9. Network Management System

Install Nagios Core

Step 1: Install some components of LAMP/LEMP Stack, APache/Nginx and PHP.



```
debian@WorkshopII:~$ sudo -i
[sudo] password for debian:
root@WorkshopII:~# apt install build-essential unzip openssl libssl-dev apache2
php libapache2-mod-php php-gd libgd-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
libssl-dev is already the newest version (1.1.1d-0+deb10u4).
libssl-dev set to manually installed.
openssl is already the newest version (1.1.1d-0+deb10u4).
openssl set to manually installed.
build-essential is already the newest version (12.6).
unzip is already the newest version (6.0-23+deb10u1).
The following additional packages will be installed:
 apache2-data apache2-utils libapache2-mod-php7.3 libexpat1-dev
 libfontconfig1-dev libfreetype6-dev libjbig-dev libjpeg-dev
 libjpeg62-turbo-dev liblzma-dev libpng-dev libpng-tools libtiff-dev
 libtiffxx5 libvpx-dev libxpm-dev php-common php7.3 php7.3-cli php7.3-common
 php7.3-gd php7.3-json php7.3-opcache php7.3-readline pkg-config uuid-dev
Suggested packages:
 apache2-doc apache2-suexec-pristine | apache2-suexec-custom php-pear
 freetype2-doc liblzma-doc
The following NEW packages will be installed:
 apache2 apache2-data apache2-utils libapache2-mod-php libapache2-mod-php7.3
```

Figure 5.2.9.1 Install components for installation Nagios Core

Step 2: Install latest release of Nagios Core



```
debian@WorkshopII:~$ wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.6.tar.gz? -P /tmp
--2020-12-22 11:02:34-- https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.6.tar.gz?
Resolving assets.nagios.com (assets.nagios.com)... 2600:3c00::f03c:91ff:fedf:b821, 72.14.181.71
Connecting to assets.nagios.com (assets.nagios.com)|2600:3c00::f03c:91ff:fedf:b821|:443... failed: No route to host.
Connecting to assets.nagios.com (assets.nagios.com)|72.14.181.71|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11333414 (11M) [application/x-gzip]
Saving to: '/tmp/nagios-4.4.6.tar.gz?'
nagios-4.4.6.tar.gz 100%[=====] 10.81M 3.03MB/s in 4.4s
2020-12-22 11:02:43 (2.43 MB/s) - '/tmp/nagios-4.4.6.tar.gz?' saved [11333414/11333414]
```

Figure 5.2.9.2 Install latest release of Nagios Core

Step 3: Extract file downloaded

```
debian@WorkshopII:~$ cd /tmp  
debian@WorkshopII:/tmp$ tar xzf nagios-4.4.6.tar.gz
```

Figure 5.2.9.3 Extract downloaded file

Step 4: Navigate to the Nagios source code directory and run configure script to adapt Nagios to our system

```
debian@WorkshopII:/tmp$ cd nagios-4.4.6  
debian@WorkshopII:/tmp/nagios-4.4.6$ ./configure --with-httpd-conf=/etc/apache2/  
sites-enabled  
checking for a BSD-compatible install... /usr/bin/install -c  
checking build system type... x86_64-pc-linux-gnu  
checking host system type... x86_64-pc-linux-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 make sets $(MAKE)... yes  
checking whether ln -s works... yes  
checking for strip... /usr/bin/strip  
checking how to run the C preprocessor... gcc -E  
checking for grep that handles long lines and -e... /usr/bin/grep  
checking for egrep... /usr/bin/grep -E  
checking for ANSI C header files... yes  
checking whether time.h and sys/time.h may both be included... yes  
checking for evdev.h that is DONTY 1 compatible... yes
```

Figure 5.2.9.4 Navigate the nagios source code directory

Step 5: To compile Nagios Core main program and CGIs, execute the command below

```
debian@WorkshopII:/tmp/nagios-4.4.6$ make all  
cd ./base && make  
make[1]: Entering directory '/tmp/nagios-4.4.6/base'  
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o nagios.o nagios.c  
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o broker.o broker.c  
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o nebmods.o nebmods.c  
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o ..../common/shared.o ..../common/shared.c  
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o query-handler.o query-handler.c  
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o workers.o workers.c  
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o checks.o checks.c  
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o config.o config.c  
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o commands.o commands.c  
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o events.o events.c  
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o flapping.o flapping.c  
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o logging.o logging.c  
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o macros-base.o ..../common/macros.c  
gcc -Wall -I.. -g -O2 -DHAVE_CONFIG_H -DNSCORE -c -o netutils.o netutils.c
```

Figure 5.2.9.5 Compile Nagios Core main program

Step 6: Create dedicated Nagios user and group

```
debian@WorkshopII:/tmp/nagios-4.4.6$ sudo make install-groups-users  
[sudo] password for debian:  
groupadd -r nagios  
useradd -g nagios nagios
```

Figure 5.2.9.6 Create Nagios user and group

Step 7: Next, add the web server user and www-data to Nagios group just created

```
debian@WorkshopII:/tmp/nagios-4.4.6$ sudo usermod -aG nagios www-data
```

Figure 5.2.9.7 Add web server user and www-data

Step 8: Run the make install command to install Nagios main program, CGIs and HTML files

```
debian@WorkshopII:/tmp/nagios-4.4.6$ sudo make install
cd ./base && make install
make[1]: Entering directory '/tmp/nagios-4.4.6/base'
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/bin
/usr/bin/install -c -s -m 774 -o nagios -g nagios nagios /usr/local/nagios/bin
/usr/bin/install -c -s -m 774 -o nagios -g nagios nagiosstats /usr/local/nagios/bin
make[1]: Leaving directory '/tmp/nagios-4.4.6/base'
cd ./cgi && make install
make[1]: Entering directory '/tmp/nagios-4.4.6/cgi'
make install-basic
make[2]: Entering directory '/tmp/nagios-4.4.6/cgi'
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/sbin
for file in *.cgi; do \
    /usr/bin/install -c -s -m 775 -o nagios -g nagios $file /usr/local/nagios/sbin; \
done
make[2]: Leaving directory '/tmp/nagios-4.4.6/cgi'
make[1]: Leaving directory '/tmp/nagios-4.4.6/cgi'
cd ./html && make install
make[1]: Entering directory '/tmp/nagios-4.4.6/html'
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/share
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/share/media
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/share/stylesheets
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/share/contexthelp
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/share/docs
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/share/docs/images
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/share/js
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/share/images
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/share/images/logos
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/share/includes
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/share/ssi
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/share/angularjs
```

Figure 5.2.9.8 Install Nagios main program, CGIs and HTML files

Step 9: To install Nagios service configuration files and enable them to run on system boot

```
debian@WorkshopII:/tmp/nagios-4.4.6$ sudo make install-daemoninit
/usr/bin/install -c -m 755 -d -o root -g root /lib/systemd/system
/usr/bin/install -c -m 755 -o root -g root startup/default-service /lib/systemd/system/nagios.service
Created symlink /etc/systemd/system/multi-user.target.wants/nagios.service → /lib/systemd/system/nagios.service.

*** Init script installed ***
```

Figure 5.2.9.9 Install Nagios service configuration files and enable run on system boot

Step 10: Run the command below install and configure permissions on the directory for holding external command file

```
debian@WorkshopII:/tmp/nagios-4.4.6$ sudo make install-commandmode
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/var/rw
chmod g+s /usr/local/nagios/var/rw

*** External command directory configured ***
```

Figure 5.2.9.10 Install and configure permissions on the directory

Step 11: To setup Nagios configuration files, run the make command with install-config option. This installs sample config files in -usr-local-nagios-etc.

```
debian@WorkshopII:/tmp/nagios-4.4.6$ sudo make install-config
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/etc
/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/etc/objects
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/nagios.cfg /usr/local/nagios/etc/nagios.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/cgi.cgi /usr/local/nagios/etc/cgi.cgi
/usr/bin/install -c -b -m 660 -o nagios -g nagios sample-config/resource.cfg /usr/local/nagios/etc/resource.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/templates.cfg /usr/local/nagios/etc/objects/templates.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/commands.cfg /usr/local/nagios/etc/objects/commands.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/contacts.cfg /usr/local/nagios/etc/objects/contacts.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/timeperiods.cfg /usr/local/nagios/etc/objects/timeperiods.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/localhost.cfg /usr/local/nagios/etc/objects/localhost.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/windows.cfg /usr/local/nagios/etc/objects/windows.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/printer.cfg /usr/local/nagios/etc/objects/printer.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/switchover.cfg /usr/local/nagios/etc/objects/switchover.cfg

*** Config files installed ***

Remember, these are *SAMPLE* config files. You'll need to read
the documentation for more information on how to actually define
services, hosts, etc. to fit your particular needs.
```

Figure 5.2.9.11 Run make command with install-config option

Step 12: To install Apache configuration files for Nagios web interface and execute

```
debian@WorkshopII:/tmp/nagios-4.4.6$ sudo make install-webconf
/usr/bin/install -c -m 644 sample-config/httpd.conf /etc/apache2/sites-enabled/nagios.conf
if [ 0 -eq 1 ]; then \
    ln -s /etc/apache2/sites-enabled/nagios.conf /etc/apache2/sites-enabled/nagios.conf; \
fi

*** Nagios/Apache conf file installed ***
```

Figure 5.2.9.12 Install apache configuration file for nagios

Step 13: Enable Apache rewrite and CGI modules

```
debian@WorkshopII:/tmp/nagios-4.4.6$ sudo a2enmod rewrite cgi
Enabling module rewrite.
Enabling module cgi.
To activate the new configuration, you need to run:
    systemctl restart apache2
```

Figure 5.2.9.13 Install apache configuration file for nagios

Step 14: To setup Nagios Web authentication, you need to create an Apache user for authentication. This can be done using the htpasswd command.

```
debian@WorkshopII:/tmp/nagios-4.4.6$ sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
New password:
Re-type new password:
Adding password for user nagiosadmin
```

Figure 5.2.9.14 Create apache user for authentication

Step 15: Set the ownership of the Nagios Apache authentication configuration file to web-server user, www-data

```
debian@WorkshopII:/tmp/nagios-4.4.6$ sudo chown www-data.www-data /usr/local/nagios/etc/htpasswd.users
```

Figure 5.2.9.15 Set the ownership of the nagios Apache configuration

Step 16: Adjust the file permissions appropriately such that the owner (www-data) has read write access, the group has read access.

```
|debian@WorkshopII:/tmp/nagios-4.4.6$ sudo chmod 640 /usr/local/nagios/etc/htpasswd.users
```

Figure 5.2.9.16 Set the ownership of the nagios Apache configuration

Step 17: Once you are done with configuration, restart Apache

```
|debian@WorkshopII:/tmp/nagios-4.4.6$ systemctl restart apache2
```

Figure 5.2.9.17 Set the ownership of the nagios Apache configuration

Step 18: Start Nagios Core service by running the command below

```
|debian@WorkshopII:/tmp/nagios-4.4.6$ systemctl start nagios.service
```

Figure 5.2.9.18 Start nagios core service

Step 19: Check nagios service status

```
|debian@WorkshopII:/tmp/nagios-4.4.6$ systemctl status nagios.service
● nagios.service - Nagios Core 4.4.6
   Loaded: loaded (/lib/systemd/system/nagios.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2020-12-22 11:54:31 +08; 13s ago
     Docs: https://www.nagios.org/documentation
 Process: 15734 ExecStartPre=/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
 Process: 15735 ExecStart=/usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
 Main PID: 15736 (nagios)
   Tasks: 5 (limit: 2347)
  Memory: 1.7M
 CGroup: /system.slice/nagios.service
         └─15736 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
             ├─15737 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─15738 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─15739 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             └─15740 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
```

Figure 5.2.9.19 Check nagios service status

Step 20: Access to nagios website

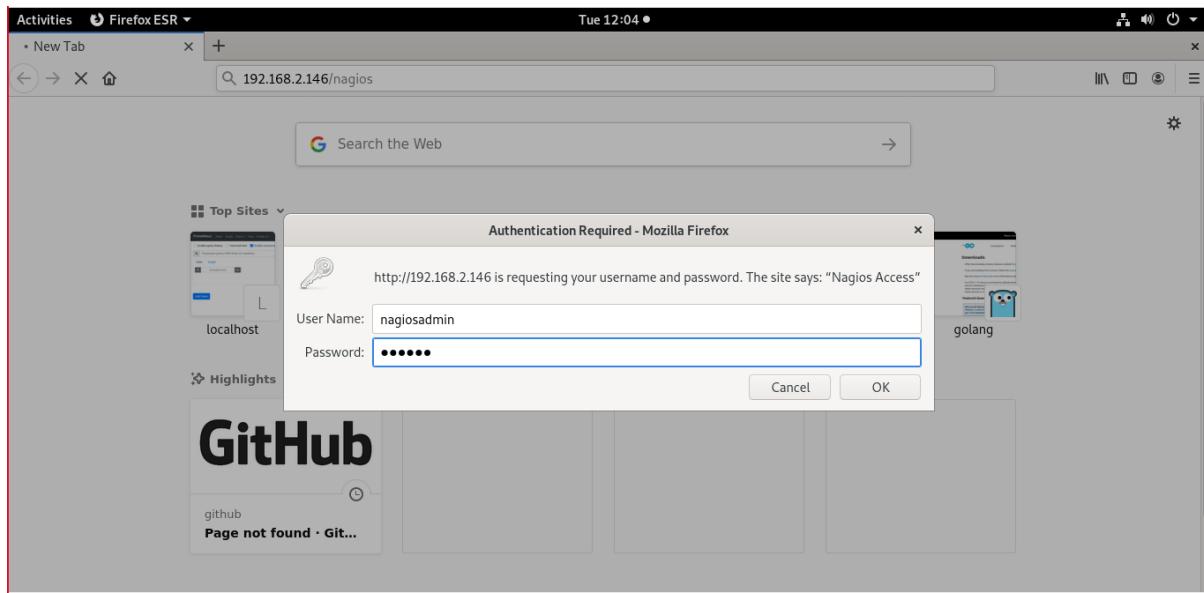


Figure 5.2.9.20 Access to nagios website

Step 21: Web interface of nagios core

A screenshot of the Nagios Core web interface. The title bar says 'Activities Firefox ESR' and the address bar shows 'Nagios: 192.168.2.146'. The main content area features the Nagios Core logo and the text 'Daemon running with PID 15736'. It displays the version information 'Nagios® Core™ Version 4.4.6 April 28, 2020' and a 'Check for updates' button. On the left, there is a navigation sidebar with sections like 'General', 'Current Status', 'Problems', and 'Reports'. The 'Current Status' section is currently selected. The 'Problems' section lists 'Services (Unhandled)', 'Hosts (Unhandled)', and 'Network Outages'. The 'Reports' section lists 'Availability', 'Trends (Legacy)', 'Alerts', 'History', and 'Summary'. A progress bar at the bottom left indicates 'Transferring data from 192.168.2.146...'.

Figure 5.2.9.21 Web interface of nagios core

Install Nagios Core Plugins

Step 22: To monitor your local system (Nagios server), just install the plugins as shown below

```

debian@WorkshopII:~$ wget https://nagios-plugins.org/download/nagios-plugins-2.3.3.tar.gz -P /tmp
--2020-12-22 12:17:14-- https://nagios-plugins.org/download/nagios-plugins-2.3.3.tar.gz
Resolving nagios-plugins.org (nagios-plugins.org)... 72.14.186.43
Connecting to nagios-plugins.org (nagios-plugins.org)|72.14.186.43|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2782610 (2.7M) [application/x-gzip]
Saving to: '/tmp/nagios-plugins-2.3.3.tar.gz'

nagios-plugins-2.3. 100%[=====] 2.65M 1.21MB/s in 2.2s

2020-12-22 12:17:17 (1.21 MB/s) - '/tmp/nagios-plugins-2.3.3.tar.gz' saved [2782610/2782610]

```

Figure 5.2.9.22 Install nagios plugins

Step 23: Extract the plugin

```

debian@WorkshopII:~$ cd /tmp
debian@WorkshopII:/tmp$ tar xzf nagios-plugins-2.3.3.tar.gz

```

Figure 5.2.9.23 Extract the plugins

Step 24: Compile and install the plugins

```

debian@WorkshopII:/tmp$ cd nagios-plugins-2.3.3/
debian@WorkshopII:/tmp/nagios-plugins-2.3.3$ ./configure --with-nagios-user=nagios --with-nagios-group=nagios
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
checking whether make sets $(MAKE)... yes
checking whether to disable maintainer-specific portions of Makefiles... yes
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking for gcc... gcc
checking for C compiler default output file name... a.out
checking whether the C compiler works... yes
checking whether we are cross compiling... no
checking for suffix of executables...
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 for style of include used by make... GNU
checking dependency style of gcc... gcc3
checking how to run the C preprocessor... gcc -E

```

Figure 5.2.9.24 Compile and install plugins

Step 25: Run make and make install for the plugins

```
debian@WorkshopII:/tmp/nagios-plugins-2.3.3$ make && make install
make  all-rerecursive
make[1]: Entering directory '/tmp/nagios-plugins-2.3.3'
Making all in gl
make[2]: Entering directory '/tmp/nagios-plugins-2.3.3/gl'
rm -f alloca.h-t alloca.h && \
{ echo '/* DO NOT EDIT! GENERATED AUTOMATICALLY! */'; \
  cat ./alloca.in.h; \
} > alloca.h-t && \
mv -f alloca.h-t alloca.h
rm -f c++defs.h-t c++defs.h && \
sed -n -e '/_GL_CXXDEFS/, $p' \
< ../build-aux/snippet/c++defs.h \
> c++defs.h-t && \
mv c++defs.h-t c++defs.h
rm -f warn-on-use.h-t warn-on-use.h && \
sed -n -e '/^ .ifndef/, $p' \
< ../build-aux/snippet/warn-on-use.h \
> warn-on-use.h-t && \
mv warn-on-use.h-t warn-on-use.h
rm -f arg-nonnull.h-t arg-nonnull.h && \
sed -n -e '/_GL_ARG_NONNULL/, $p' \
< ../build-aux/snippet/arg-nonnull.h \
> arg-nonnull.h-t && \
    . . .
```

Figure 5.2.9.25 Run make and make install for plugins

Step 26: Restart Nagios

```
debian@WorkshopII:/tmp/nagios-plugins-2.3.3$ systemctl restart nagios
```

Figure 5.2.9.26 Restart nagios

Step 27: Open web interface Nagios. All localhost services are up.

Activities Firefox ESR ▾

Fri 18:17 ●

N Nagios: 192.168.2.146 × +

192.168.2.146/nagios/

Nagios®

General

- Home Documentation

Current Status

- Tactical Overview
- Map (Legacy)
- Hosts
- Services
- Host Groups
 - Summary
 - Grid
- Service Groups
 - Summary
 - Grid
- Problems
 - Services (Unhandled)
 - Hosts (Unhandled)
 - Network Outages
- Quick Search:

Reports

- Availability
- Trends (Legacy)

HTTP OK 12-25-2020 18:08:38 0d 1h 52m 24s 1/4 HTTP/1.1 200 OK - 10975 bytes in 0.001 second response time

PING OK 12-25-2020 18:14:59 0d 1h 51m 7s 1/4 PING OK - Packet loss = 0%, RTA = 0.05 ms

Root Partition OK 12-25-2020 18:14:53 0d 1h 51m 9s 1/4 DISK OK - free space: / 21096 MiB (80.42% inode=90%)

SSH OK 12-25-2020 18:15:31 0d 1h 45m 31s 1/4 SSH OK - OpenSSH_7.9p1 Debian-10+deb10u2 (protocol 2.0)

Swap Usage OK 12-25-2020 18:11:08 0d 0h 9m 54s 1/4 SWAP OK - 100% free (2045 MB out of 2045 MB)

Total Processes OK 12-25-2020 18:11:46 0d 1h 54m 16s 1/4 PROCS OK: 4 processes with STATE = RSZDT

Results 1 - 8 of 8 Matching Services

Page Tour

Figure 5.2.9.27 Localhost service status is OK

Install iReasoning MIB Browser

Step 28: Download iReasoning MIB Browser from the webpage

```
debian@WorkshopII:~$ wget http://www.ireasoning.com/download/mibfree/mibbrowser.zip
--2021-01-05 04:11:23--  http://www.ireasoning.com/download/mibfree/mibbrowser.zip
Resolving www.ireasoning.com (www.ireasoning.com)... 149.28.57.150
Connecting to www.ireasoning.com (www.ireasoning.com)|149.28.57.150|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10622507 (10M) [application/zip]
Saving to: 'mibbrowser.zip'

mibbrowser.zip      34%[=====>]  3.48M  1.79MB/s   in 1.9s

2021-01-05 04:11:26 (1.79 MB/s) - Read error at byte 3653052/10622507 (Connection reset by peer). Retrying.

--2021-01-05 04:11:27-- (try: 2)  http://www.ireasoning.com/download/mibfree/mibbrowser.zip
Connecting to www.ireasoning.com (www.ireasoning.com)|149.28.57.150|:80... connected.
HTTP request sent, awaiting response... 206 Partial Content
Length: 10622507 (10M), 6969455 (6.6M) remaining [application/zip]
Saving to: 'mibbrowser.zip'
```

Figure 5.2.9.28 Download MIB Browser

Step 29: Run sudo apt update before installing java

```
debian@WorkshopII:~$ sudo apt update
[sudo] password for debian:
Hit:1 http://security.debian.org/debian-security buster/updates InRelease
Hit:2 http://deb.debian.org/debian buster InRelease
Reading package lists...
Building dependency tree
Reading state information...
2 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

Figure 5.2.9.29 Run sudo apt update before installing java

Step 30: Install Java

```
debian@WorkshopII:~$ sudo apt install default-jre
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  linux-image-4.19.0-11-amd64
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  ca-certificates-java default-jre-headless java-common libatk-wrapper-java
  libatk-wrapper-java-jni openjdk-11-jre openjdk-11-jre-headless
Suggested packages:
  fonts-ipafont-gothic fonts-ipafont-mincho fonts-wqy-microhei
  | fonts-wqy-zenhei fonts-indic
The following NEW packages will be installed:
  ca-certificates-java default-jre default-jre-headless java-common
  libatk-wrapper-java libatk-wrapper-java-jni openjdk-11-jre
  openjdk-11-jre-headless
0 upgraded, 8 newly installed, 0 to remove and 2 not upgraded.
Need to get 37.9 MB of archives.
After this operation, 172 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://deb.debian.org/debian buster/main amd64 java-common all 0.71 [14.4 kB]
Get:2 http://deb.debian.org/debian buster/main amd64 openjdk-11-jre-headless amd64 1
```

Figure 5.2.9.30 Install Java

Step 31: Confirm installation and check the latest java version

```
debian@WorkshopII:~$ java -version
openjdk version "11.0.9.1" 2020-11-04
OpenJDK Runtime Environment (build 11.0.9.1+1-post-Debian-1deb10u2)
OpenJDK 64-Bit Server VM (build 11.0.9.1+1-post-Debian-1deb10u2, mixed mode, sharing)
```

Figure 5.2.9.31 Latest java version

Step 32: Go to the directory of browser.sh in mib browser folder and run browser.sh

```
debian@WorkshopII:~/Downloads/mibbrowser/ireasoning/mibbrowser$ ./browser.sh
/usr/bin/java
Log file: /home/debian/.imibrowser/log/log.txt
```

Figure 5.2.9.32 Run browser.sh

Step 33: iReasoning MIB Browser is automatically runs in GUI

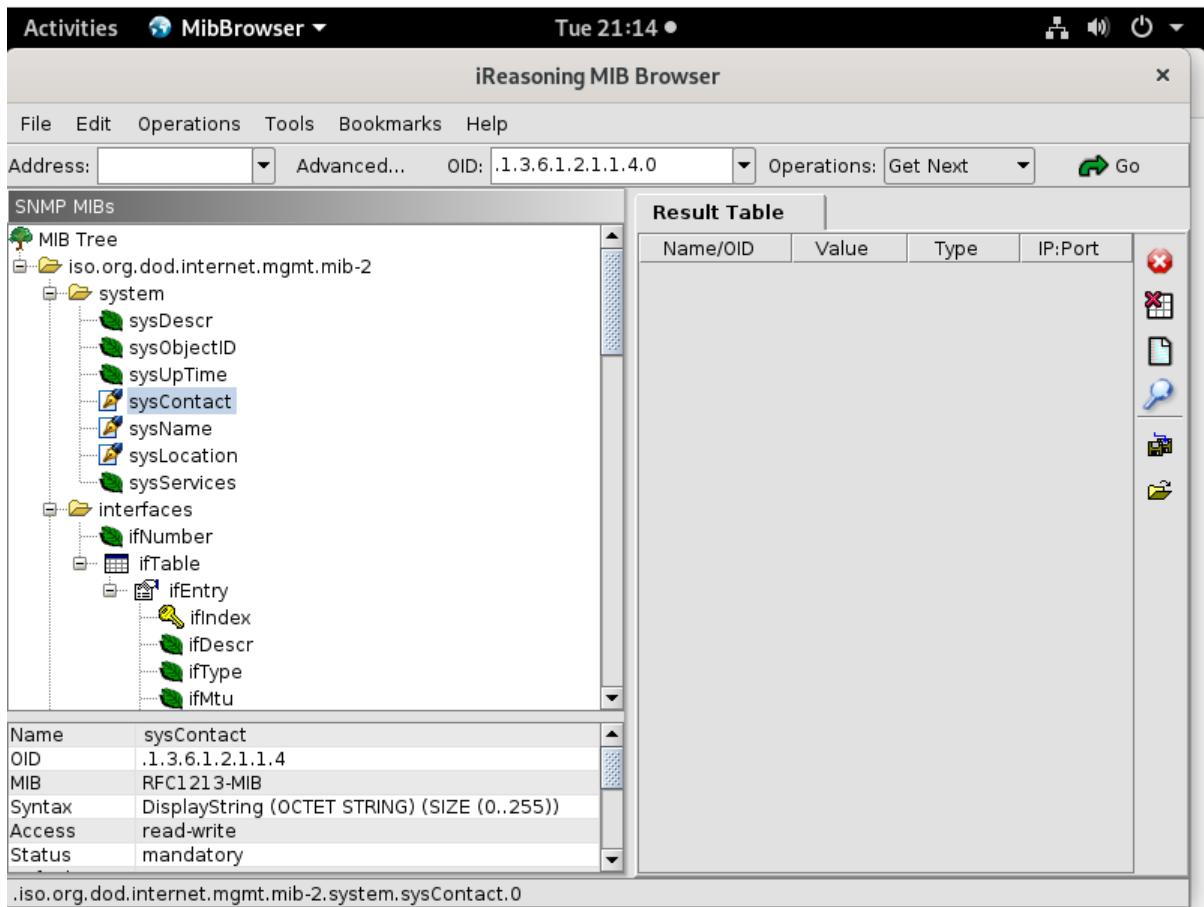


Figure 5.2.9.33 Interface of MIB Browser

Install and configure Net-SNMP

Step 34: Install SNMP and its library

```
debian@WorkshopII:~$ sudo apt-get install -y snmpd snmp
[sudo] password for debian:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  linux-image-4.19.0-11-amd64
Use 'sudo apt autoremove' to remove it.
Suggested packages:
  snmptrapd
The following NEW packages will be installed:
  snmp snmpd
0 upgraded, 2 newly installed, 0 to remove and 2 not upgraded.
Need to get 211 kB of archives.
After this operation, 746 kB of additional disk space will be used.
Get:1 http://security.debian.org/debian-security buster/updates/main amd64 snmp amd64
5.7.3+dfsg-5+deb10u1 [155 kB]
Get:2 http://security.debian.org/debian-security buster/updates/main amd64 snmpd amd64
5.7.3+dfsg-5+deb10u1 [56.1 kB]
Fetched 211 kB in 1s (219 kB/s)
Preconfiguring packages ...
Selecting previously unselected package snmp.
(Reading database ... 169728 files and directories currently installed.)
Preparing to unpack .../snmp_5.7.3+dfsg-5+deb10u1_amd64.deb ...
```

Figure 5.2.9.34 Install SNMP and libraries

Step 35: Before modifying the file, make a copy of the file by the following command

```
debian@WorkshopII:~$ sudo cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.bak
```

Figure 5.2.9.35 Make a copy of the file

Step 36: Command to modify the file

```
debian@WorkshopII:/etc/snmp$ sudo nano snmpd.conf
```

Figure 5.2.9.36 Command to modify the file

Step 37: Edit the file configuration

```

GNU nano 3.2                                     snmpd.conf

# AGENT BEHAVIOUR
#
# Listen for connections from the local system only
#agentAddress udp:127.0.0.1:161
# Listen for connections on all interfaces (both IPv4 *and* IPv6)
agentAddress udp:161,udp6:[::1]:161

# view      systemonly included .1.3.6.1.2.1.1
# view      systemonly included .1.3.6.1.2.1.25.1

view all included .1.3.6.1.2.1.1
view all included .1.3.6.1.2.1.25.1

#rocommunity public localhost
# rocommunity public default -V systemonly
rocommunity public default -V all

# rocommunity6 public default -V systemonly
rocommunity6 public default -V all
#####
#
# SYSTEM INFORMATION
#
# Note that setting these values here, results in the corresponding MIB objects being
# See snmpd.conf(5) for more details
sysLocation    FTMK
sysContact     Afifah
sysServices     72

# Application + End-to-End layers

#####
#
# ACTIVE MONITORING
#
#
trapsink      localhost public          # send SNMPv1 traps
trap2sink      localhost public          # send SNMPv2c traps
#informsink    localhost public          # send SNMPv2c INFORMS

```

Figure 5.2.9.37 Edit the configuration file

Step 38: The following will restart service on Linux, make sure to run with sudo access

```
debian@WorkshopII:/etc/snmp$ sudo service snmpd restart
```

Figure 5.2.9.38 Restart service on Linux

Step 39: On systemd systems, run the following command

```
debian@WorkshopII:/etc/snmp$ sudo systemctl restart snmpd.service
```

Figure 5.2.9.39 Restart service snmp on systemd system

Step 40: Test whether SNMP can read the system and interface MIB's using the snmpwalk command

```
debian@WorkshopII:/etc/snmp$ sudo snmpwalk -c public -v2c -O e 127.0.0.1
iso.3.6.1.2.1.1.1.0 = STRING: "Linux WorkshopII 4.19.0-13-amd64 #1 SMP Debian 4.19.160
-2 (2020-11-28) x86_64"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (4530) 0:00:45.30
iso.3.6.1.2.1.1.4.0 = STRING: "Afifah"
iso.3.6.1.2.1.1.5.0 = STRING: "WorkshopII"
iso.3.6.1.2.1.1.6.0 = STRING: "FTMK"
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.8.0 = Timeticks: (12) 0:00:00.12
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.49
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.2.1.4
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.2.1.50
iso.3.6.1.2.1.1.9.1.2.9 = OID: iso.3.6.1.6.3.13.3.1.3
iso.3.6.1.2.1.1.9.1.2.10 = OID: iso.3.6.1.2.1.92
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The MIB for Message Processing and Dispatching."
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "The management information definitions for the SNMP
User-based Security Model."
iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The SNMP Management Architecture MIB."
```

Figure 5.2.9.40 Test snmpwalk in command line

Step 41: Run iReasoning MIB Browser to test snmp in GUI. Inout the community string for read and write.

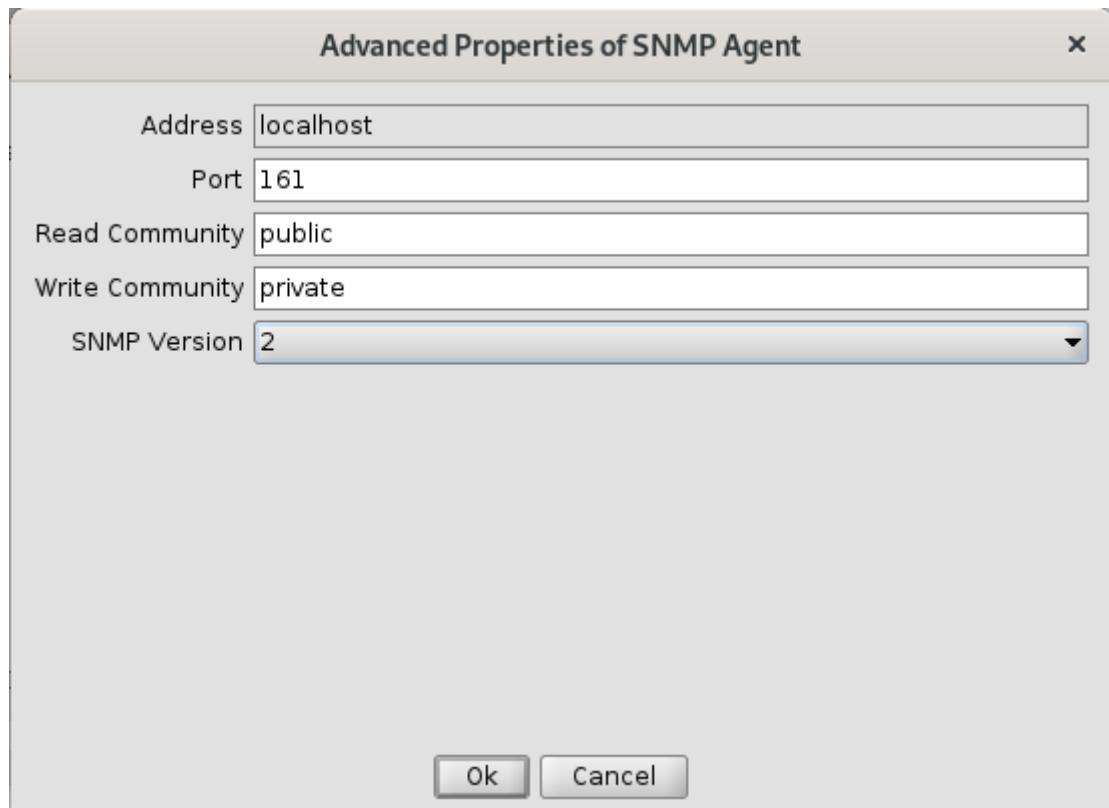


Figure 5.2.9.41 Input the community string for read and write

Step 42: Check whether mib browser get the same information same as the configuration in snmpd.conf

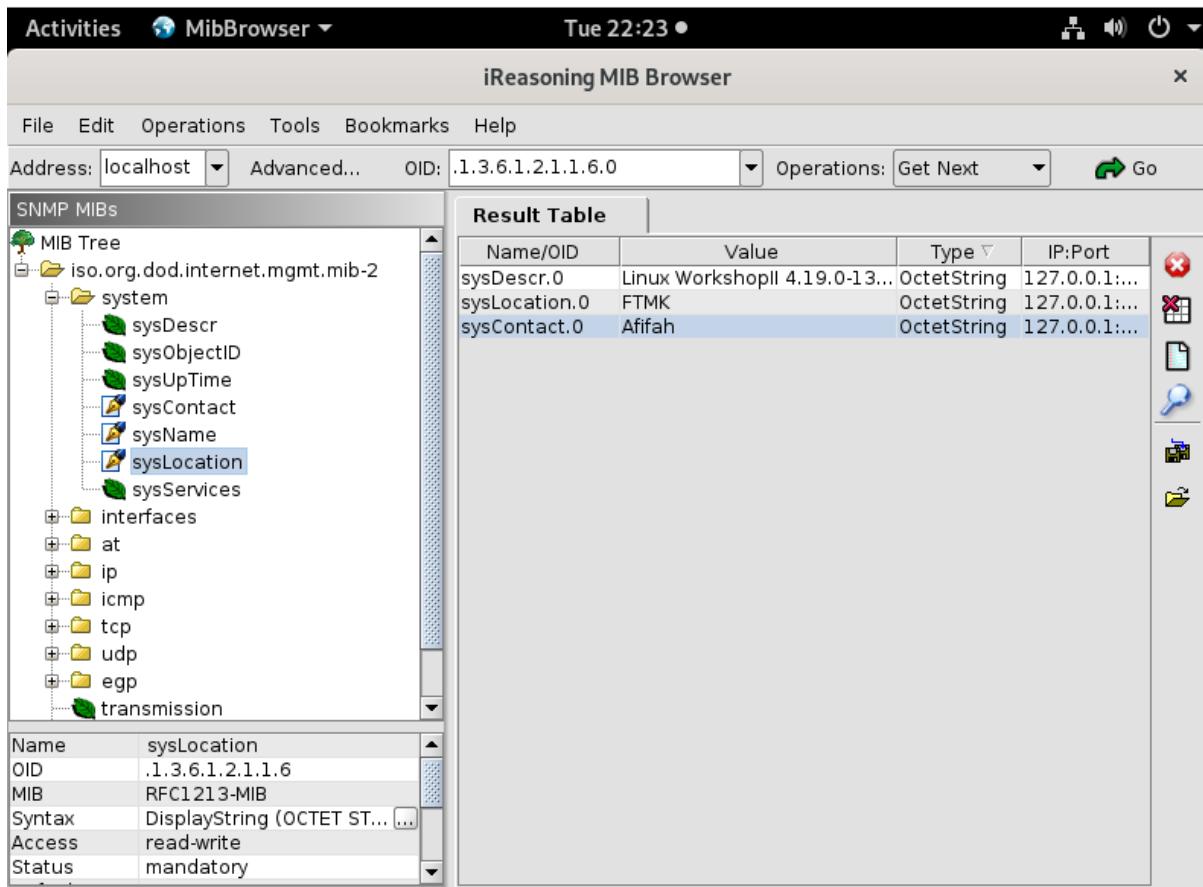


Figure 5.2.9.42 Verify information is same with the one configured n snmpd.conf

Recompile Nagios Plugin

Step 43: Go to the directory of nagios plugin and reconfigure the plugin

```
debian@WorkshopII:~$ cd nagios*/
debian@WorkshopII:~/nagios-plugins-2.3.3$ sudo ./configure
```

Figure 5.2.9.43 Reconfigure nagios plugins

Step 44: Enter root and make install the nagios plugin

```
debian@WorkshopII:~/nagios-plugins-2.3.3$ sudo -i
root@WorkshopII:~# cd /home/debian/nagios*/
root@WorkshopII:/home/debian/nagios-plugins-2.3.3# make $$ make install
```

Figure 5.2.9.44 Enter root and make install nagios plugin

Step 45: Go to the directory to see the available plugin. There you can see check_snmp plugin is available.

```

debian@WorkshopII:/usr/local/nagios/libexec$ ls
check_apt          check_icmp          check_ntp          check_ssh
check_breeze        check_ide_smart     check_ntp_peer    check_ssl_validity
check_by_ssh        check_ifoperstatus check_ntp_time    check_ssntp
check_clamd         check_ifstatus      check_nwstat      check_swap
check_cluster       check_imap          check_oracle      check_tcp
check_dhcp          check_ircd          check_overcr     check_time
check_dig           check_jabber        check_ping        check_udp
check_disk          check_load          check_pop         check_ups
check_disk_smb      check_log           check_procs      check_uptime
check_dns           check_mailq         check_real        check_users
check_dummy         check_mrtg          check_rpc         check_wave
check_file_age      check_mrtgtraf     check_sensors    negate
check_flexlm        check_nagios        check_simap      remove_perfdata
check_ftp           check_nttp          check_smtp       urlize
check_hpjd          check_nttps         check_snmp       utils.pm
check_http          check_nt            check_spop       utils.sh

```

Figure 5.2.9.45 check_snmp plugin is available

Configure SNMP on Switch and Router

Step 46: Configure SNMP on Router HQ. Configure community string.

```

HQ(config)#snmp-server community public ro
HQ(config)#snmp-server community private rw
HQ(config)#snmp-server contact Afifah
HQ(config)#snmp-server location FTMK

```

Figure 5.2.9.46 Configure SNMP on router HQ

Step 47: Configure SNMP on Router Branch. Configure community string.

```

Branch(config)#snmp-server community public ro
Branch(config)#snmp-server community private rw
Branch(config)#snmp-server contact Afifah
Branch(config)#snmp-server location FTMK

```

Figure 5.2.9.47 Configure SNMP on router Branch

Step 48: Configure management ip vlan for SwitchHQ

```
SwitchHQ(config)#int vlan 20
SwitchHQ(config-if)#ip address 192.168.2.3 255.255.255.128
SwitchHQ(config-if)#no shut
SwitchHQ(config-if)#int vlan 30
SwitchHQ(config-if)#ip address 192.168.2.131 255.255.255.240
SwitchHQ(config-if)#no shut
SwitchHQ(config-if)#int vlan 40
SwitchHQ(config-if)#ip address 192.168.2.147 255.255.255.248
SwitchHQ(config-if)#no shut
```

Figure 5.2.9.48 Configure management ip for vlan SwitchHQ

Step 49: Configure community string for SwitchHQ

```
SwitchHQ(config)#snmp-server community public ro
SwitchHQ(config)#snmp-server community private rw
SwitchHQ(config)#snmp-server contact Afifah
SwitchHQ(config)#snmp-server location FTMK
```

Figure 5.2.9.49 Configure community string for vlan SwitchHQ

Step 50: Configure management ip vlan for SwitchBranch

```
SwitchBranch(config)#int vlan 10
SwitchBranch(config-if)#ip address 192.168.1.3 255.255.255.0
```

Figure 5.2.9.50 Configure community string for vlan SwitchBranch

Step 51: Configure community string for SwitchBranch

```
SwitchBranch(config)#snmp-server community public ro
SwitchBranch(config)#snmp-server community private rw
SwitchBranch(config)#snmp-server contact Afifah
SwitchBranch(config)#snmp-server location FTMK
```

Figure 5.2.9.51 Configure community string for vlan SwitchBranch

Monitoring Router and Switch for HQ and Branch

Step 52: Edit configuration file. Uncomment cfg_file=/usr/local/nagios/etc/objects/switch.cfg

```

GNU nano 3.2          /usr/local/nagios/etc/nagios.cfg      Modified

cfg_file=/usr/local/nagios/etc/objects/timeperiods.cfg
cfg_file=/usr/local/nagios/etc/objects/templates.cfg

# Definitions for monitoring the local (Linux) host
cfg_file=/usr/local/nagios/etc/objects/localhost.cfg

# Definitions for monitoring a Windows machine
#cfg_file=/usr/local/nagios/etc/objects/windows.cfg

# Definitions for monitoring a router/switch
cfg_file=/usr/local/nagios/etc/objects/switch.cfg

```

Figure 5.2.9.52 Uncomment a line for switch.cfg

Step 53: Edit file switch.cfg and configure monitoring for router and switch

```

#####
#
# HOST DEFINITIONS
#
#####

# Define the switch that we'll be monitoring

define host {

    use           generic-switch          ; Inherit defau$ 
    host_name     RouterHQ               ; The name we're givin$ 
    alias         RouterHQ               ; A longer name associated wi$ 
    address       192.168.2.1           ; IP address of t$ 
    hostgroups   Devices                ; Host groups th$ 
}

define host {

    use           generic-switch          ; Inherit defau$ 
    host_name     RouterISP              ; The name we're givi$ 
    alias         RouterISP              ; A longer name associated w$ 
    address       200.200.201.2          ; IP address of$ 
    hostgroups   Devices                ; Host groups t$ 
}

define host {

    use           generic-switch          ; Inherit defau$ 
    host_name     SwitchHQ              ; The name we're givin$ 
    alias         SwitchHQ              ; A longer name associated wi$ 
    address       192.168.2.3           ; IP address of t$ 
    hostgroups   Devices                ; Host groups t$ 
}

```

```

define host {
    use generic-switch ; Inherit defau$;
    host_name SwitchBranch ; The name we're g$;
    alias SwitchBranch ; A longer name associate$;
    address 200.200.200.1 ; IP address of$;
    hostgroups Devices ; Host groups t$;
}

#####
#
# HOST GROUP DEFINITIONS
#
#####

# Create a new hostgroup for switches

define hostgroup {
    hostgroup_name Devices ; The name of th$;
    alias Network Environment ; Long name of t$;
}

#
# Create a service to PING to switch/router

define service {
    use generic-service ; Inherit value$;
    host_name RouterHQ ; The name of the host$;
    service_description PING ; The service d$;
    check_command check_ping!200.0,20%!600.0,60% ; The command u$;
    check_interval 5 ; Check the ser$;
    retry_interval 1 ; Re-check the $;
}

define service {
    use generic-service ; Inherit value$;
    host_name RouterISP ; The name of the hoss$;
    service_description PING ; The service d$;
    check_command check_ping!200.0,20%!600.0,60% ; The command u$;
    check_interval 5 ; Check the ser$;
    retry_interval 1 ; Re-check the $;
}

define service {
    use generic-service ; Inherit value$;
    host_name SwitchBranch ; The name of the $;
    service_description PING ; The service d$;
    check_command check_ping!200.0,20%!600.0,60% ; The command u$;
    check_interval 5 ; Check the ser$;
    retry_interval 1 ; Re-check the $;
}

```

```

define service {

    use          generic-service      ; Inherit value$
    host_name    SwitchHQ            ; The name of the host
    service_description PING           ; The service d$ 
    check_command   check_ping!200.0,20%!600.0,60% ; The command u$ 
    check_interval 5                ; Check the ser$ 
    retry_interval 1                ; Re-check the $ 

}

define service {

    use          generic-service      ; Inherit value$
    host_name    RouterHQ            ; The name of the host
    service_description Uptime         ; The service d$ 
    check_command   check_snmp!-C public -o sysUpTime.0
}

define service {

    use          generic-service      ; Inherit value$
    host_name    RouterISP           ; The name of the host
    service_description Uptime         ; The service d$ 
    check_command   check_snmp!-C public -o sysUpTime.0
}

define service {

    use          generic-service      ; Inherit value$
    host_name    SwitchBranch         ; The name of the host
    service_description Uptime         ; The service d$ 
    check_command   check_snmp!-C public -o .1.3.6.1.2.1.1.3.0
}

define service {

    use          generic-service      ; Inherit value$
    host_name    SwitchHQ            ; The name of the host
    service_description Uptime         ; The service d$ 
    check_command   check_snmp!-C public -o sysUpTime.0
}

#Router HQ - Inbound and Outbound

#Below this is inbound
define service {

    use          generic-service      ; Inherit value$
    host_name    RouterHQ            ; The name of the host
    service_description Port f0/0.20 In ; The service d$ 
    check_command   check_snmp!-C public -o .1.3.6.1.2.1.2.2.1.10.11
}

define service {

    use          generic-service      ; Inherit value$
    host_name    RouterHQ            ; The name of the host
    service_description Port f0/0.30 In ; The service d$ 
    check_command   check_snmp!-C public -o .1.3.6.1.2.1.2.2.1.10.12
}

```

```

define service {
    use generic-service ; Inherit value$
    host_name RouterHQ
    service_description Port f0/0.40 In
    check_command check_snmp!-C public -o .1.3.6.1.2.1.2.2.1.10.13
}

define service {
    use generic-service ; Inherit value$
    host_name RouterHQ
    service_description Port s0/0 In
    check_command check_snmp!-C public -o .1.3.6.1.2.1.2.2.1.10.2
}

#Router HQ - Inbound and Outbound

#Below this is outbound

define service {
    use generic-service ; Inherit value$
    host_name RouterHQ
    service_description Port f0/0.20 Out
    check_command check_snmp!-C public -o .1.3.6.1.2.1.2.2.1.16.11
}

define service {
    use generic-service ; Inherit value$
    host_name RouterHQ
    service_description Port f0/0.30 Out
    check_command check_snmp!-C public -o .1.3.6.1.2.1.2.2.1.16.12
}

define service {
    use generic-service ; Inherit value$
    host_name RouterHQ
    service_description Port f0/0.40 Out
    check_command check_snmp!-C public -o .1.3.6.1.2.1.2.2.1.16.13
}

define service {
    use generic-service ; Inherit value$
    host_name RouterHQ
    service_description Port s0/0 Out
    check_command check_snmp!-C public -o .1.3.6.1.2.1.2.2.1.16.2
}

```

```

#Below this is inbound

define service {

    use          generic-service           ; Inherit value$
    host_name    RouterBranch
    service_description Port f0/0.10 In
    check_command   check_snmp!-C public -o .1.3.6.1.2.1.2.2.1.10.11
}

define service {

    use          generic-service           ; Inherit value$
    host_name    RouterBranch
    service_description Port s0/1 In
    check_command   check_snmp!-C public -o .1.3.6.1.2.1.2.2.1.10.4
}

#Router Branch - Inbound and Outbound

#Below this is outbound

define service {

    use          generic-service           ; Inherit value$
    host_name    RouterBranch
    service_description Port f0/0.10 Out
    check_command  check_snmp!-C public -o .1.3.6.1.2.1.2.2.1.16.11
}

define service {

    use          generic-service           ; Inherit value$
    host_name    RouterBranch
    service_description Port s0/1 Out
    check_command  check_snmp!-C public -o .1.3.6.1.2.1.2.2.1.16.4
}

#Switch HQ - Inbound and Outbound

#Below this is inbound

define service {

    use          generic-service           ; Inherit value$
    host_name    SwitchHQ
    service_description Port g0/0 In
    check_command  check_snmp!-C public -o .1.3.6.1.2.1.2.2.1.10.1
}

```

```

define service {
    use generic-service ; Inherit value$  

    host_name SwitchHQ  

    service_description Port g0/0 In  

    check_command check_snmp!-C public -o .1.3.6.1.2.1.2.2.1.10.1
}

define service {
    use generic-service ; Inherit value$  

    host_name SwitchHQ  

    service_description Port g0/1 In  

    check_command check_snmp!-C public -o .1.3.6.1.2.1.2.2.1.10.2
}

define service {
    use generic-service ; Inherit value$  

    host_name SwitchHQ  

    service_description Port g0/2 In  

    check_command check_snmp!-C public -o .1.3.6.1.2.1.2.2.1.10.3
}

define service {
    use generic-service ; Inherit value$  

    host_name SwitchHQ  

    service_description Port g0/3 In  

    check_command check_snmp!-C public -o .1.3.6.1.2.1.2.2.1.10.4
}

#Below this is outbound

define service {
    use generic-service ; Inherit value$  

    host_name SwitchHQ  

    service_description Port g0/0 Out  

    check_command check_snmp!-C public -o .1.3.6.1.2.1.2.2.1.16.1
}

define service {
    use generic-service ; Inherit value$  

    host_name SwitchHQ  

    service_description Port g0/1 Out  

    check_command check_snmp!-C public -o .1.3.6.1.2.1.2.2.1.16.2
}

```

```

define service {
    use generic-service ; Inherit value$  

    host_name SwitchHQ  

    service_description Port g0/2 Out  

    check_command check_snmp!-C public -o .1.3.6.1.2.1.2.2.1.16.3
}

define service {
    use generic-service ; Inherit value$  

    host_name SwitchHQ  

    service_description Port g0/3 Out  

    check_command check_snmp!-C public -o .1.3.6.1.2.1.2.2.1.16.4
}

#Switch Branch - Inbound and Outbound

#Below this is inbound

define service {
    use generic-service ; Inherit value$  

    host_name SwitchBranch  

    service_description Port g0/0 In  

    check_command check_snmp!-C public -o .1.3.6.1.2.1.2.2.1.10.1
}

define service {
    use generic-service ; Inherit value$  

    host_name SwitchBranch  

    service_description Port g0/1 Out  

    check_command check_snmp!-C public -o .1.3.6.1.2.1.2.2.1.10.2
}

```

```

#Switch Branch - Inbound and Outbound

#Below this is outbound

define service {

    use          generic-service           ; Inherit value$
    host_name    SwitchBranch
    service_description  Port g0/0 Out
    check_command   check_snmp!-C public -o .1.3.6.1.2.1.2.2.1.16.1
}

#Switch Branch - Inbound and Outbound

#Below this is outbound

define service {

    use          generic-service           ; Inherit value$
    host_name    SwitchBranch
    service_description  Port g0/0 Out
    check_command   check_snmp!-C public -o .1.3.6.1.2.1.2.2.1.16.1
}

define service {

    use          generic-service           ; Inherit value$
    host_name    SwitchBranch
    service_description  Port g0/1 Out
    check_command   check_snmp!-C public -o .1.3.6.1.2.1.2.2.1.16.2
}

```

Figure 5.2.9.53 Edit configuration for file switch.cfg

Install Performance Graph for Nagios Core using PNP4Nagios

Step 54: Get update for installing PNP4Nagios

```

root@WorkshopII:~# apt-get update
Hit:1 http://deb.debian.org/debian buster InRelease
Hit:2 http://security.debian.org/debian-security buster/updates InRelease
Reading package lists... Done

```

Figure 5.2.9.54 Get update before install PNP4Nagios

Step 55: Perform all this command of installation

```
root@WorkshopII:~# apt-get install -y rrdtool librrds-perl php-gd php-xml
Reading package lists... Done
Building dependency tree
Reading state information... Done
php-gd is already the newest version (2:7.3+69).
php-xml is already the newest version (2:7.3+69).
The following packages were automatically installed and are no longer required:
  courier-authdaemon courier-authlib courier-authlib-userdb courier-base
  expect libcourier-unicode4 libfam0 linux-image-4.19.0-11-amd64 tcl-expect
Use 'apt autoremove' to remove them.
The following NEW packages will be installed:
  libdbi1 librrd8 librrds-perl rrdtool
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
root@WorkshopII:~# cd /tmp
root@WorkshopII:/tmp# wget -O pnp4nagios.tar.gz https://github.com/lingej/pnp4nagios/archive/0.6.26.tar.gz
--2021-01-02 18:58:58--  https://github.com/lingej/pnp4nagios/archive/0.6.26.tar.gz
Resolving github.com (github.com)... 13.250.177.223
Connecting to github.com (github.com)|13.250.177.223|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/lingej/pnp4nagios/tar.gz/0.6.26 [following]
--2021-01-02 18:58:58--  https://codeload.github.com/lingej/pnp4nagios/tar.gz/0.6.26
Resolving codeload.github.com (codeload.github.com)... 13.250.162.133
Connecting to codeload.github.com (codeload.github.com)|13.250.162.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/x-gzip]
Saving to: 'pnp4nagios.tar.gz'

pnp4nagios.tar.gz      [ =>          ]  2.89M  3.50MB/s   in 0.8s

2021-01-02 18:59:00 (3.50 MB/s) - 'pnp4nagios.tar.gz' saved [3026672]
root@WorkshopII:/tmp# cd pnp4nagios-0.6.26
root@WorkshopII:/tmp/pnp4nagios-0.6.26# ./configure --with-httpd-conf=/etc/apache2/sites-enabled
root@WorkshopII:/tmp/pnp4nagios-0.6.26# make all
```

```

root@WorkshopII:/tmp/pnp4nagios-0.6.26# echo '' >> /usr/local/nagios/etc/objects/commands.cfg
root@WorkshopII:/tmp/pnp4nagios-0.6.26# echo 'define command {' >> /usr/local/nagios/etc/objects/commands.cfg
root@WorkshopII:/tmp/pnp4nagios-0.6.26# echo '      command_name      process-host-perfdata-file-bulk-npcd' >> /usr/local/nagios/etc/objects/commands.cfg
root@WorkshopII:/tmp/pnp4nagios-0.6.26# echo '      command_line      /bin/mv /usr/local/pnp4nagios/var/host-perfdata /usr/local/pnp4nagios/var/spool/host-perfdata.$TIMET$' >> /usr/local/nagios/etc/objects/commands.cfg
root@WorkshopII:/tmp/pnp4nagios-0.6.26# echo '}' >> /usr/local/nagios/etc/objects/commands.cfg
root@WorkshopII:/tmp/pnp4nagios-0.6.26# echo '' >> /usr/local/nagios/etc/objects/commands.cfg
root@WorkshopII:/tmp/pnp4nagios-0.6.26# echo 'define command {' >> /usr/local/nagios/etc/objects/commands.cfg
root@WorkshopII:/tmp/pnp4nagios-0.6.26# echo '      command_name      process-service-perfdata-file-bulk-npcd' >> /usr/local/nagios/etc/objects/commands.cfg
root@WorkshopII:/tmp/pnp4nagios-0.6.26# echo '      command_line      /bin/mv /usr/local/pnp4nagios/var/service-perfdata /usr/local/pnp4nagios/var/spool/service-perfdata.$TIMET$' >> /usr/local/nagios/etc/objects/commands.cfg
root@WorkshopII:/tmp/pnp4nagios-0.6.26# echo '}' >> /usr/local/nagios/etc/objects/commands.cfg
root@WorkshopII:/tmp/pnp4nagios-0.6.26# echo '' >> /usr/local/nagios/etc/objects/commands.cfg


---


root@WorkshopII:/tmp/pnp4nagios-0.6.26# make install


---


root@WorkshopII:/tmp/pnp4nagios-0.6.26# make install-webconf


---


root@WorkshopII:/tmp/pnp4nagios-0.6.26# make install-config


---


root@WorkshopII:/tmp/pnp4nagios-0.6.26# make install-init


---


root@WorkshopII:/tmp/pnp4nagios-0.6.26# systemctl daemon-reload
root@WorkshopII:/tmp/pnp4nagios-0.6.26# systemctl enable npcd.service
npcd.service is not a native service, redirecting to systemd-sysv-install.
root@WorkshopII:/tmp/pnp4nagios-0.6.26# systemctl start npcd.service


---


root@WorkshopII:/tmp/pnp4nagios-0.6.26# systemctl restart apache2.service
root@WorkshopII:/tmp/pnp4nagios-0.6.26# sed -i 's/process_performance_data=0/process_performance_data=1/g' /usr/local/nagios/etc/nagios.cfg


---


root@WorkshopII:/tmp/pnp4nagios-0.6.26# sed -i 's/#host_perfd_file=/host_perfd_file=/g' /usr/local/nagios/etc/nagios.cfg
root@WorkshopII:/tmp/pnp4nagios-0.6.26# sed -i 's/^host_perfd_file=.*$/host_perfd_file=\\usr\\local\\pnp4nagios\\var\\service-perfdata/g' /usr/local/nagios/etc/nagios.cfg


---


root@WorkshopII:/tmp/pnp4nagios-0.6.26# sed -i 's/^#host_perfd_file_template=.*$/host_perfd_file_template=DATATYPE::HOSTPERFDATA\\tTIMET::$TIMET$\\tHOSTNAME::$HOSTNAME$\\tHOSTPERFDATA::$HOSTPERFDATA$\\tHOSTCHECKCOMMAND::$HOSTCHECKCOMMAND$\\tHOSTSTATE::$HOSTSTATE$\\tHOSTSTATETYPE::$HOSTSTATETYPE$/g' /usr/local/nagios/etc/nagios.cfg
root@WorkshopII:/tmp/pnp4nagios-0.6.26# sed -i 's/#host_perfd_file_mode=/host_perfd_file_mode=/g' /usr/local/nagios/etc/nagios.cfg


---


root@WorkshopII:/tmp/pnp4nagios-0.6.26# sed -i 's/^#host_perfd_file_processing_interval=.*$/host_perfd_file_processing_interval=15/g' /usr/local/nagios/etc/nagios.cfg
root@WorkshopII:/tmp/pnp4nagios-0.6.26# sed -i 's/^#host_perfd_file_processing_command=.*$/host_perfd_file_processing_command=process-host-perfdata-file-bulk-npcd/g' /usr/local/nagios/etc/nagios.cfg


---


root@WorkshopII:/tmp/pnp4nagios-0.6.26# sed -i 's/#service_perfdata_file=/service_perfdata_file=/g' /usr/local/nagios/etc/nagios.cfg
root@WorkshopII:/tmp/pnp4nagios-0.6.26# sed -i 's/^service_perfdata_file=.*$/service_perfdata_file=\\usr\\local\\pnp4nagios\\var\\service-perfdata/g' /usr/local/nagios/etc/nagios.cfg

```

```
root@WorkshopII:/tmp/pnp4nagios-0.6.26# echo '' >> /usr/local/nagios/etc/objects/commands.cfg
root@WorkshopII:/tmp/pnp4nagios-0.6.26# echo 'define command {' >> /usr/local/nagios/etc/objects/commands.cfg
root@WorkshopII:/tmp/pnp4nagios-0.6.26# echo '    command_name    process-host-perfdata-file-bulk-npcd' >> /usr/local/nagios/etc/objects/commands.cfg
root@WorkshopII:/tmp/pnp4nagios-0.6.26# echo '    command_line    /bin/mv /usr/local/pnp4nagios/var/host-perfdata /usr/local/pnp4nagios/var/spool/host-perfdata.$TIMET$' >> /usr/local/nagios/etc/objects/commands.cfg
root@WorkshopII:/tmp/pnp4nagios-0.6.26# echo '}' >> /usr/local/nagios/etc/objects/commands.cfg
root@WorkshopII:/tmp/pnp4nagios-0.6.26# echo '' >> /usr/local/nagios/etc/objects/commands.cfg
root@WorkshopII:/tmp/pnp4nagios-0.6.26# echo 'define command {' >> /usr/local/nagios/etc/objects/commands.cfg
root@WorkshopII:/tmp/pnp4nagios-0.6.26# echo '    command_name    process-service-perfdata-file-bulk-npcd' >> /usr/local/nagios/etc/objects/commands.cfg
root@WorkshopII:/tmp/pnp4nagios-0.6.26# echo '    command_line    /bin/mv /usr/local/pnp4nagios/var/service-perfdata /usr/local/pnp4nagios/var/spool/service-perfdata.$TIMET$' >> /usr/local/nagios/etc/objects/commands.cfg
root@WorkshopII:/tmp/pnp4nagios-0.6.26# echo '}' >> /usr/local/nagios/etc/objects/commands.cfg
root@WorkshopII:/tmp/pnp4nagios-0.6.26# echo '' >> /usr/local/nagios/etc/objects
root@WorkshopII:/tmp/pnp4nagios-0.6.26# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

Figure 5.2.9.55 Perform all the command for installation

Install NSClient++ and monitor Server Windows

Step 56: Installation of SNMP Agent NSClient++ on server windows and configure monitoring server windows at sudo nano /usr/local/nagios/etc/windows.cfg.

```
#####
#
# HOST DEFINITIONS
#
#####

# Define a host for the Windows machine we'll be monitoring
# Change the host_name, alias, and address to fit your situation

define host {

    use          windows-server      ; Inherit default values fro$ 
    host_name    WIN-A90KB5EE034    ; The name we're giving$ 
    alias        WIN-A90KB5EE034    ; A longer name associated wit$ 
    address      192.168.2.130     ; IP address of the host
}

#
# HOST GROUP DEFINITIONS
#
#####

# Define a hostgroup for Windows machines
# All hosts that use the windows-server template will automatically be a member $ 

define hostgroup {

    hostgroup_name   windows-servers      ; The name of the hostgroup
    alias           Windows Servers       ; Long name of the group
}

#####
#
# SERVICE DEFINITIONS
#
#####

# Create a service for monitoring the version of NSClient++ that is installed
# Change the host_name to match the name of the host you defined above

define service {

    use          generic-service
    host_name    WIN-A90KB5EE034
    service_description  NSClient++ Version
    check_command   check_nt!CLIENTVERSION
}
```

```

# Create a service for monitoring the uptime of the server
# Change the host_name to match the name of the host you defined above

define service {

    use                  generic-service
    host_name           WIN-A90KB5EE034
    service_description Uptime
    check_command       check_nt!UPTIME
}

# Create a service for monitoring CPU load
# Change the host_name to match the name of the host you defined above

define service {

    use                  generic-service
    host_name           WIN-A90KB5EE034
    service_description CPU Load
    check_command       check_nt!CPULOAD!-l 5,80,90
}

# Create a service for monitoring memory usage
# Change the host_name to match the name of the host you defined above

define service {

    use                  generic-service
    host_name           WIN-A90KB5EE034
    service_description Memory Usage
    check_command       check_nt!MEMUSE!-w 80 -c 90
}

# Create a service for monitoring C:\ disk usage
# Change the host_name to match the name of the host you defined above

define service {

    use                  generic-service
    host_name           WIN-A90KB5EE034
    service_description C:\ Drive Space
    check_command       check_nt!USEDISKSPACE!-l c -w 80 -c 90
}

```

```

# Change the host_name to match the name of the host you defined above
#For IIS Service
define service {

    use          generic-service
    host_name    WIN-A90KB5EE034
    service_description  World Wide Web Publishing Service
    check_command   check_nt!SERVICESTATE!-d SHOWALL -l W3SVC
    check_interval  0.08
    retry_interval  0.08
    check_period    24x7
}

# Create a service for monitoring the DHCP Server service
# Change the host_name to match the name of the host you defined above

define service {

    use          generic-service
    host_name    WIN-A90KB5EE034
    service_description  DHCP Server
    check_command   check_nt!SERVICESTATE!-d SHOWALL -l DHCPServer
    check_interval  0.08
    retry_interval  0.08
    check_period    24x7
}

# Create a service for monitoring the DNS Server service
# Change the host_name to match the name of the host you defined above

define service {

    use          generic-service
    host_name    WIN-A90KB5EE034
    service_description  DNS Server
    check_command   check_nt!SERVICESTATE!-d SHOWALL -l DNS
    check_interval  0.08
    retry_interval  0.08
    check_period    24x7
}

# Create a service for monitoring the AD Domain service
# Change the host_name to match the name of the host you defined above
define service {
    use          generic-service
    host_name    WIN-A90KB5EE034
    service_description  Active Directory Domain Services
    check_command   check_nt!SERVICESTATE!-d SHOWALL -l NTDS
    check_interval  0.08
    retry_interval  0.08
    check_period    24x7
}

```

Figure 5.2.9.56 Edit configuration file for windows.cfg

Install NRPE plugin and monitor Server Debian

Step 57: Installation of SNMP Agent NRPE Plugin on server debian and configure monitoring server debian at sudo nano /usr/local/nagios/etc/servers/WorkshopII.cfg.

```
GNU nano 3.2      /usr/local/nagios/etc/servers/WorkshopII.cfg

define host{
    use          linux-server
    host_name   WorkshopII
    alias       WorkshopII
    address     192.168.2.146
}

define hostgroup{
    hostgroup_name  linux-server
    alias           Linux Servers
    members         WorkshopII
}

define service{
    use          local-service
    host_name   WorkshopII
    service_description Current Load
    check_command  check_nrpe!check_load
}

define service{
    use          local-service
    host_name   WorkshopII
    service_description FTP
    check_command  check_ftp
}

define service{
    use          local-service
    host_name   WorkshopII
    service_description Linux Email
    check_command  check_smtp
}
```

Figure 5.2.9.57 Edit configuration file for WorkshopII.cfg

5.2.10. AAA (Authentication, Authorization and Accounting) using Radius

Installation and setup the Radius

Step 1: Add roles and features Wizard > Select Role based or feature-based installation > Click button Next. To installation new roles and feature.

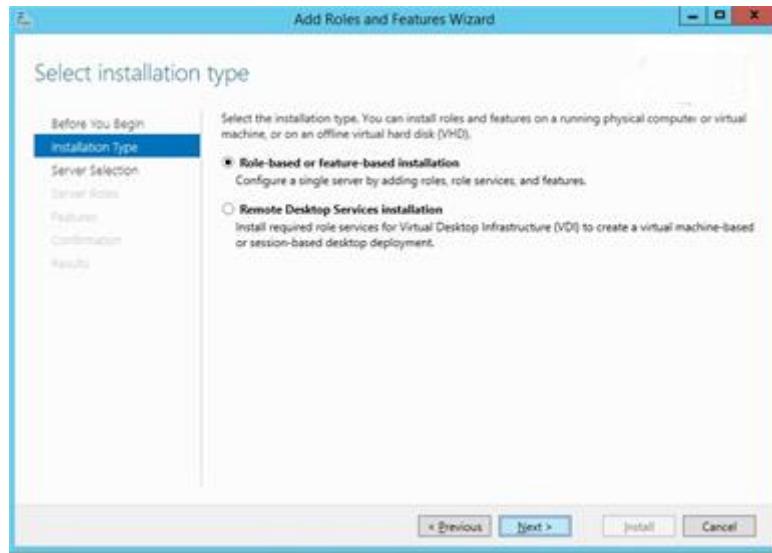


Figure 5.2.10.1 Add roles

Step 2: After select a server from the server pool > Select Network Policy and Access Services

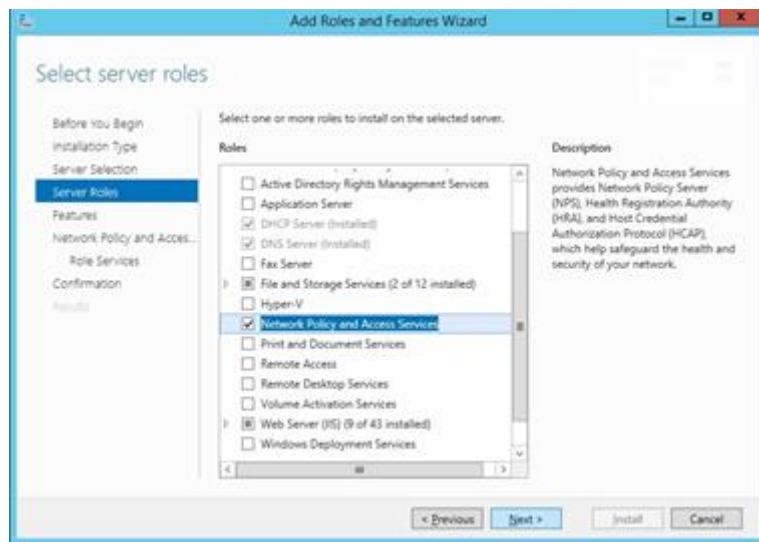


Figure 5.2.10.2 Server pool

Step 3: Then, click Add Feature. To add new tools is Network Policy and Access Services Tools.

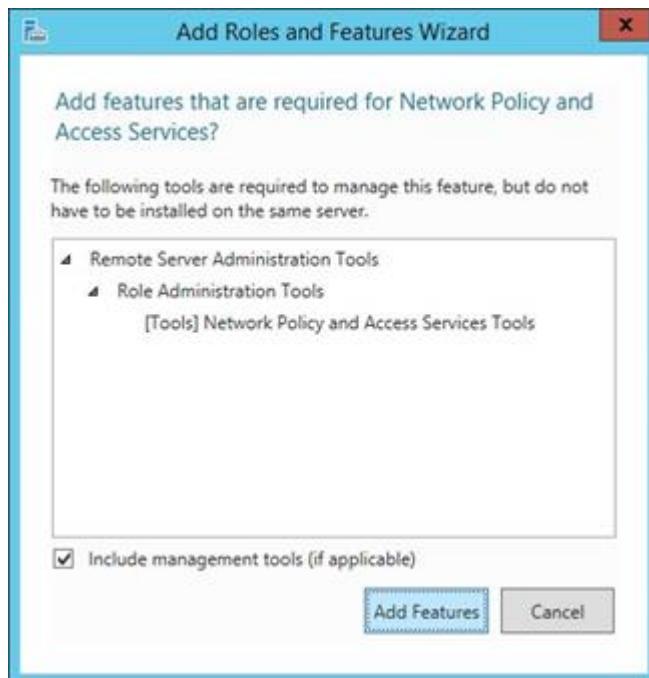


Figure 5.2.10.3 Add features

Step 4: After finish click Network Policy and Access Services > Click Next > Network Policy Server > Click Next and Click button Install to install new tools is Network Policy Server and Network Policy and Access Services.

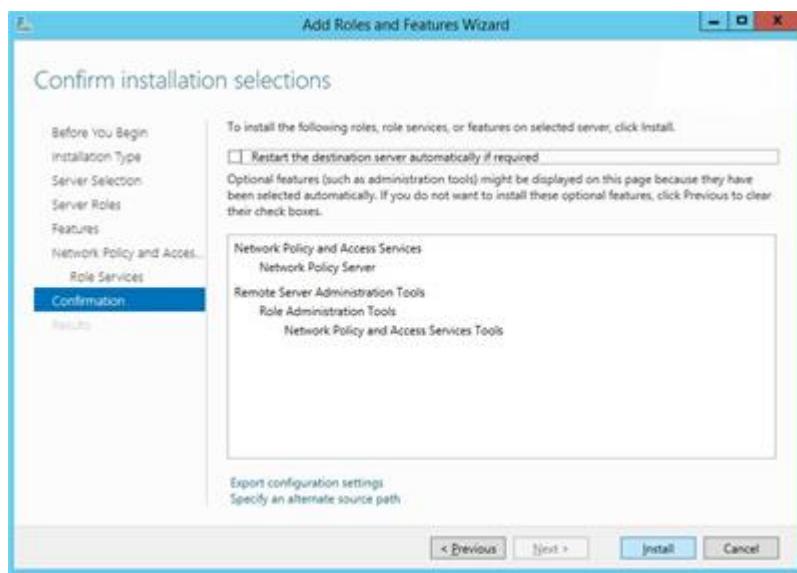


Figure 5.2.10.4 Install Roles and Features

Step 5: Integrate with user that already create by Active Directory (AD) this users for privilege level 15

The screenshot shows the Windows Active Directory Users and Computers management console. The left pane displays a tree view of the directory structure under 'group1.com'. The right pane is a table listing users with columns for Name, Type, and Description. The users listed are Afifahh, Aishah, Amirahh, Ariq, Faris, Group1, Hazim, and Yongg, all categorized as 'User' type.

Name	Type
Afifahh	User
Aishah	User
Amirahh	User
Ariq	User
Faris	User
Group1	User
Hazim	User
Yongg	User

Figure 5.2.10.5 group1IntegrateAD user

Step 6: Create new user and group for privilege level 1

The screenshot shows the Windows Active Directory Users and Computers management console. The left pane displays a tree view of the directory structure under 'group1.com'. The right pane is a table showing a single user entry for 'Samad' with 'User' type. The 'Radius' folder under 'ITDepartment' is highlighted in the tree view.

Name	Type	Description
Samad	User	

Figure 5.2.10.6 Radius group

Step 7: Click user name and click right then select add to group **group1IntegrateAD**

Step 8: After finish select add to group. Now select group is **group1IntegrateAD** and click Check Names to confirm the group will be selected. Then, click OK.

Step 9: Select a group name is **group1IntegrateAD** and click right. Select a properties to check have a user will done be group members

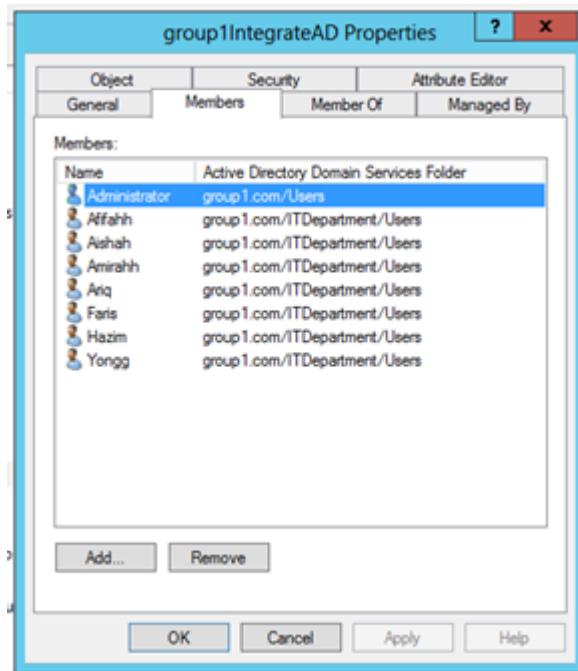


Figure 5.2.10.7 Group member

Step 10: First go to tools at Service manager and select a Network Policy Server. After that, click NPS (Local) > Click RADIUS Clients and Servers > Click RADIUS Clients.

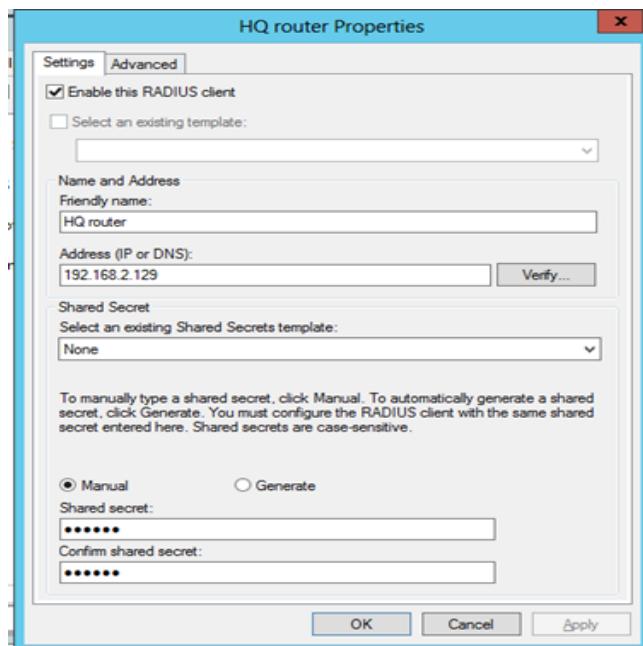


Figure 5.2.10.8 HQ router properties

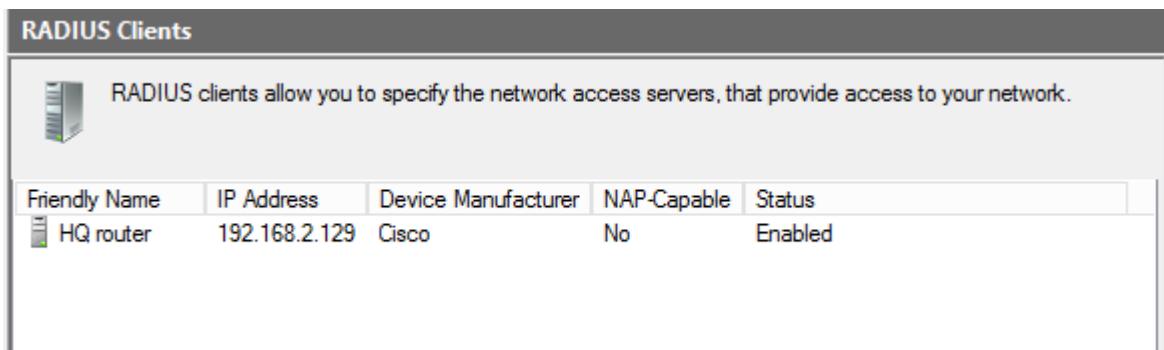


Figure 5.2.10.9 Radius Clients

Step 11: Select a Policies. After that, click Network Policy. The Network Policy is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy. It is the successor of Internet Authentication Service (IAS).

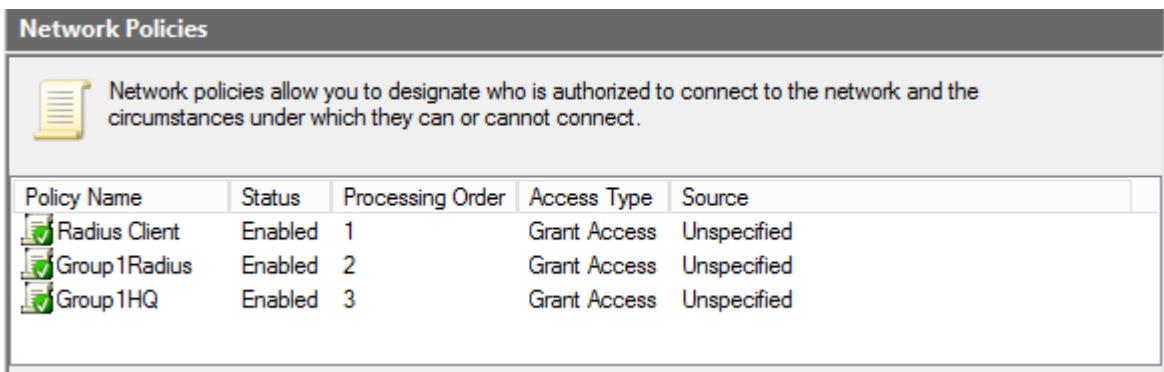


Figure 5.2.10.10 Network policies

Step 12: Select a Network Policy then click right and select New Network Policy. Create a new policy name

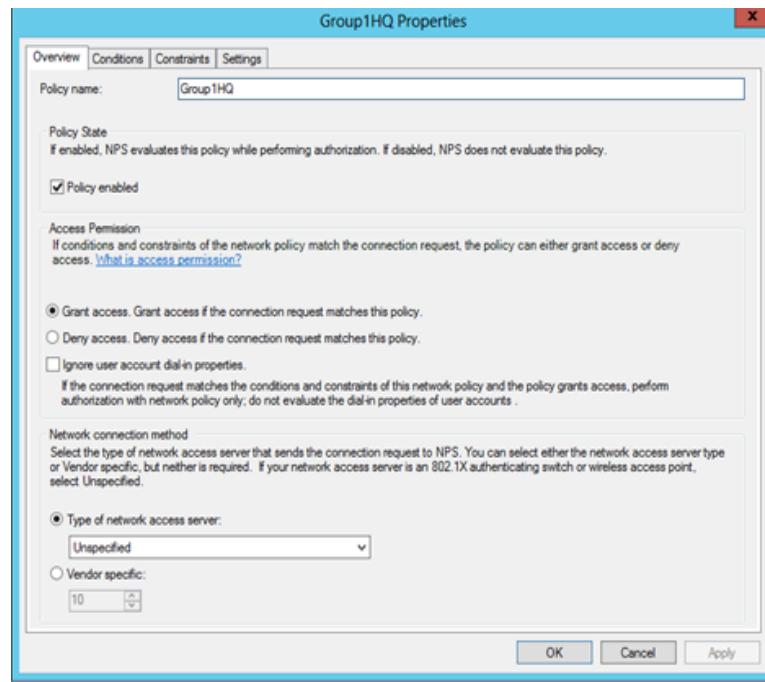


Figure 5.2.10.11 Group HQ overview

Step 13: After click Select condition go to Windows Groups and click button Add.

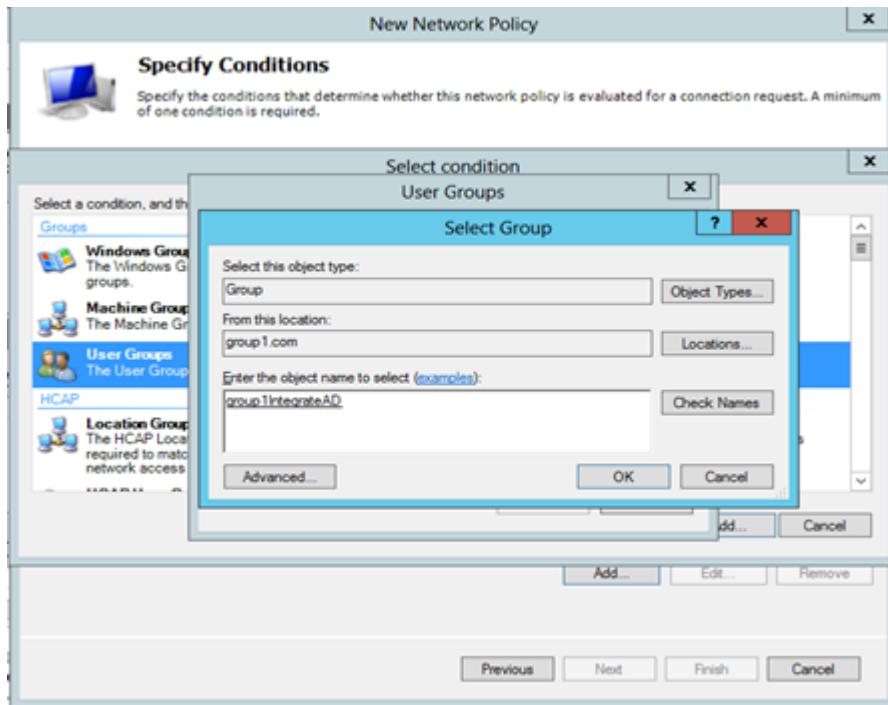


Figure 5.2.10.12 Group select

Step 14: After finish set up the specify condition for Windows Groups. Then, go to page Configure Settings > Select a Standard at Radius Attributes > Click Framed Protocol (PPP) > Click button Remove. After that, done removed the Click Framed Protocol (PPP). After finish that, go to Vendor Specific.

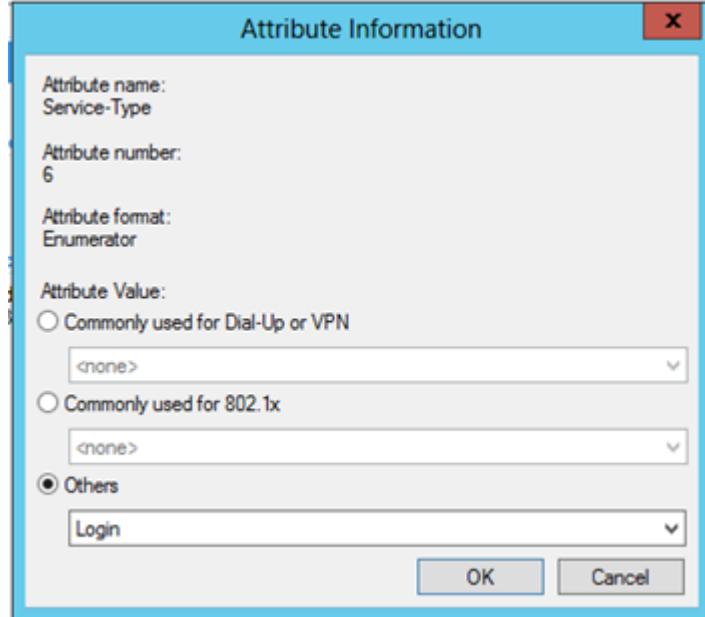


Figure 5.2.10.13 Attribute information

Step 15: After click Vendor Specific, go to Add Vendor Specific Attribute and Select the CiscoAV-Pair with Vendor is Cisco. Then click button Add.

Step 16: After click button add for Cisco-AV-Pair with Vendor is Cisco. Enter the new attribute value is “shell-priv-lvl-15”. Then click the button OK.

Step 17: After finish set up the Cisco-AV-Pair with Vendor is Cisco and it has value “shell-privlvl-15”. Then, the output of result Vendor Specific.

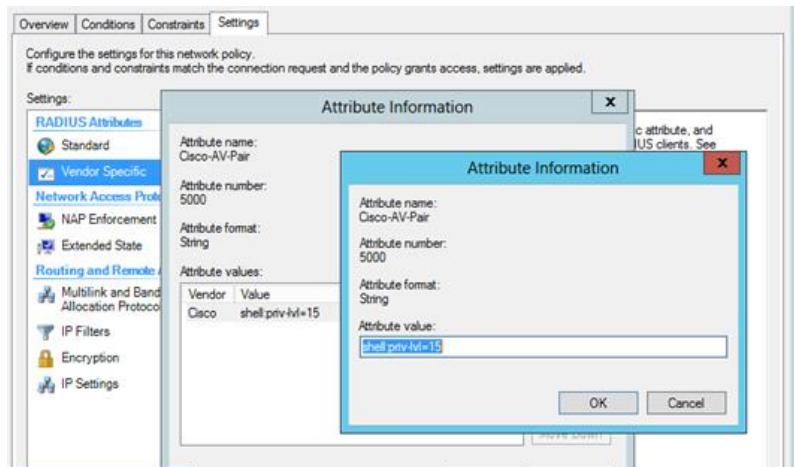


Figure 5.2.10.14 Vendor specific information

Step 18: After that, Select an Accounting. After that, click Change Log Properties. Accounting is atomically configure a local or remote SQL server with a database for NPS accounting.

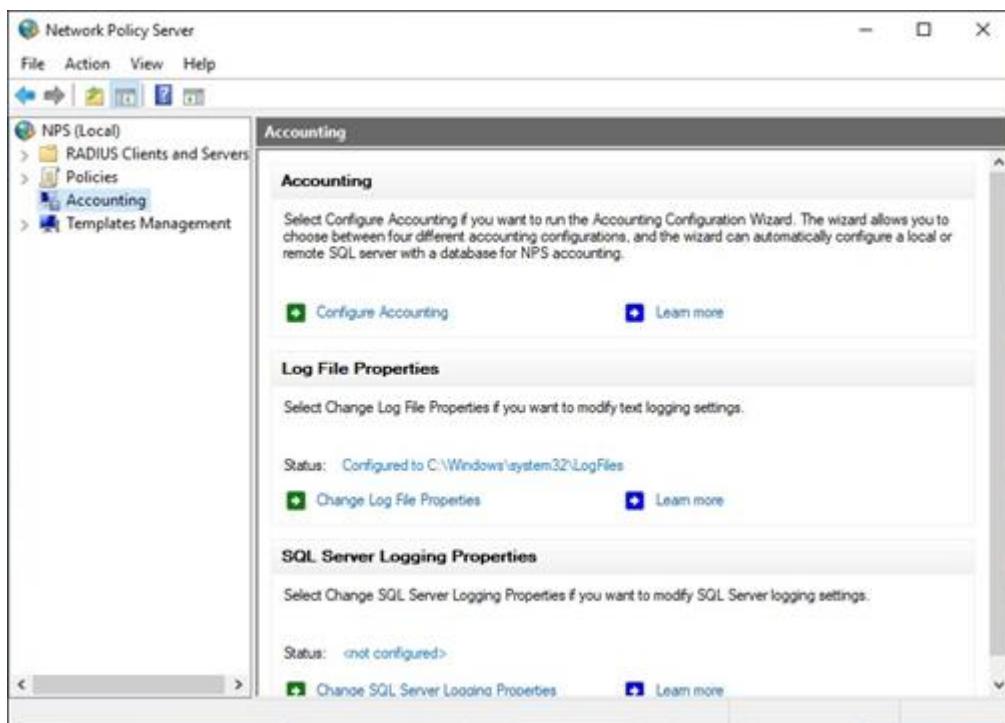


Figure 5.2.10.15 Accounting

Step 19: Log File Properties, it can setting and

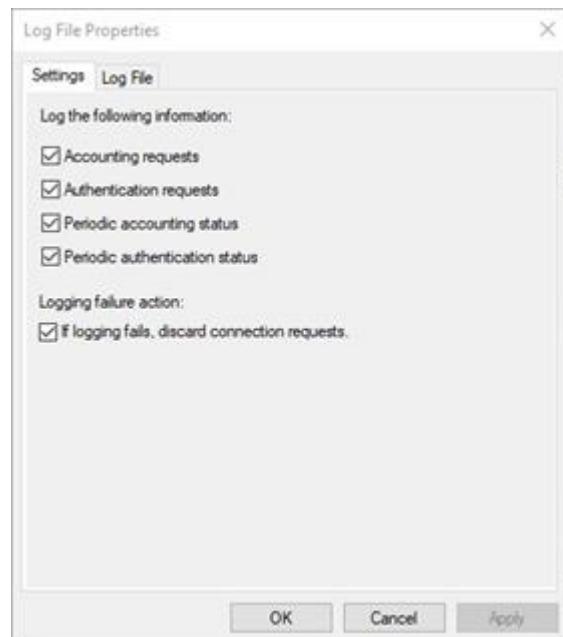


Figure 5.2.10.16 Settings log file

Step 20: Log File Properties can create new log file likely Daily, Weekly, Monthly, Never and When log file reached that size. Then click OK.

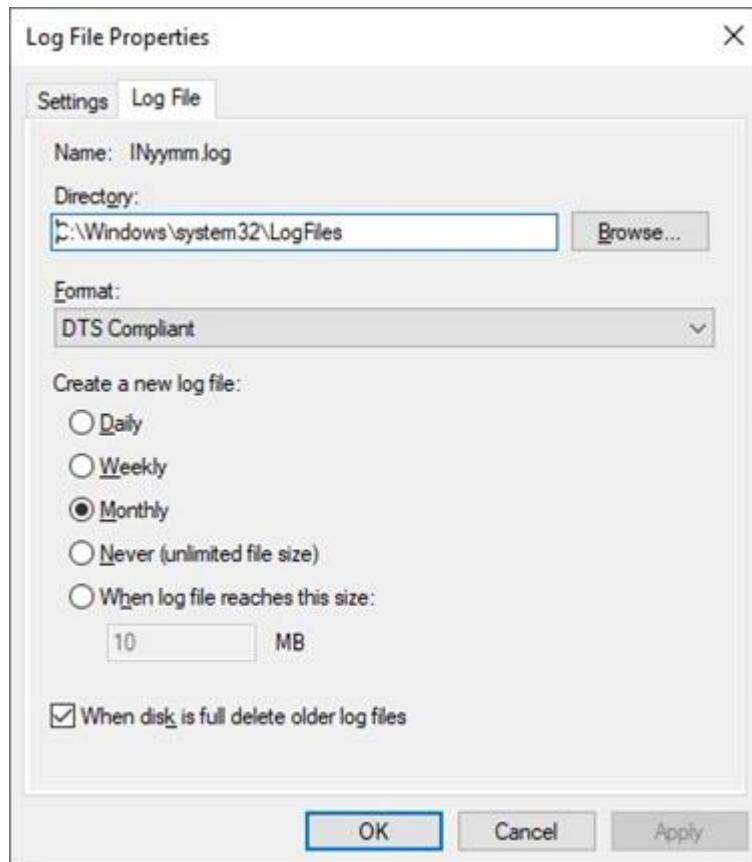


Figure 5.2.10.17 Log file

AAA Configuration

Step 1: Create aaa authentication login, create aaa group server radius. Then, create aaa authorization exec default group. Lastly, write debug radius.

```
HQ(config)#aaa new-model
HQ(config)#aaa new-model
HQ(config)#aaa group server radius RADIUS-SERVER
HQ(config-sg-radius)#server-pr
HQ(config-sg-radius)#server-private 192.168.1.130 auth
HQ(config-sg-radius)#server-private 192.168.1.130 auth-port 1812 acc
HQ(config-sg-radius)##$8.1.130 auth-port 1812 acct-port 1813 key group7
HQ(config-sg-radius)#exit
HQ(config)#aaa au
HQ(config)#aaa authentication login defa
HQ(config)#aaa authentication login default group RADIUS-SERVER local
HQ(config)#aaa autho
HQ(config)#aaa authorization exec def
HQ(config)#aaa authorization exec default group RADIUS-SERVER local if
HQ(config)#$zation exec default group RADIUS-SERVER local if-authenticated
HQ(config)#aaa auth
HQ(config)#aaa author
HQ(config)#aaa authorization console
HQ(config)#[
```

Figure 5.2.10.18 AAA configure

Step 2: Lastly, debug AAA Authentication

```
HQ#debug aaa authen
HQ#debug aaa authentication
AAA Authentication debugging is on
HQ#debug autho
HQ#debug authori
HQ#debug aaa authori
HQ#debug aaa authorization
AAA Authorization debugging is on
HQ#debug ra
HQ#debug rad
HQ#debug radius
Radius protocol debugging is on
Radius protocol brief debugging is off
Radius protocol verbose debugging is off
Radius packet hex dump debugging is off
Radius packet protocol debugging is on
Radius elog debugging debugging is off
Radius packet retransmission debugging is off
Radius server fail-over debugging is off
Radius elog debugging debugging is off
HQ#[
```

Figure 5.2.10.19 AAA debug

5.2.11. Layer 2 Security - VLAN and Port Security

Port Security

Step 1: Configure port security for windows server with interface GigabitEthernet0/2

```
Enter configuration commands, one per line. End with CNTL/Z.
SwitchHQ(config)#int gi0/2
SwitchHQ(config-if)#switchport mode access
SwitchHQ(config-if)#switchport port-security
SwitchHQ(config-if)#switchport port-security maximum 2
SwitchHQ(config-if)#switchport port-security violation restrict
SwitchHQ(config-if)#switchport port-security mac-address sticky
SwitchHQ(config-if)#switchport port-security aging time 120
SwitchHQ(config-if)#end
```

Figure 5.2.11.1 Configure Port for Windows Server

Step 2: Configure port security for Debian server with interface GigabitEthernet0/3

```
SwitchHQ(config)#int gi0/3
SwitchHQ(config-if)#switchport mode access
SwitchHQ(config-if)#switchport port-security
SwitchHQ(config-if)#switchport port-security maximum 2
SwitchHQ(config-if)#switchport port-security violation restrict
SwitchHQ(config-if)#switchport port-security mac-address sticky
SwitchHQ(config-if)#switchport port-security aging time 120
SwitchHQ(config-if)#end
```

Figure 5.2.11.2 Configure Port for Debian Server

Step 3: Configure port security for ITDepartment with interface GigabitEthernet0/1

```
Enter configuration commands, one per line. End with CNTL/Z.
SwitchHQ(config)#int gi0/1
SwitchHQ(config-if)#switchport mode access
SwitchHQ(config-if)#switchport port-security
SwitchHQ(config-if)#switchport port-security maximum 2
SwitchHQ(config-if)#switchport port-security violation restrict
SwitchHQ(config-if)#switchport port-security mac-address sticky
SwitchHQ(config-if)#switchport port-security aging time 120
SwitchHQ(config-if)#end
```

Figure 5.2.11.3 Configure Port for ITDepartment

Step 4: Configure port security for RemoteAccess with interface GigabitEthernet0/1

```
Enter configuration commands, one per line. End with CNTL/Z.
SwitchBranch(config)#int gi0/1
SwitchBranch(config-if)#switchport mode access
SwitchBranch(config-if)#switchport port-security
SwitchBranch(config-if)#switchport port-security maximum 2
SwitchBranch(config-if)#switchport port-security violation restrict
SwitchBranch(config-if)#switchport port-security mac-address sticky
SwitchBranch(config-if)#switchport port-security aging time 120
SwitchBranch(config-if)#end
```

Figure 5.2.11.4 Configure Port for Remote Access

Step 5: Disable unused ports

Unused ports for SwitchHQ

```
SwitchHQ(config)#int range gil/0-2
SwitchHQ(config-if-range)#shutdown
SwitchHQ(config-if-range)#end
```

Figure 5.2.11.5 disable unused ports for SwitchHQ

Unused ports for SwitchBranch

```
Enter configuration commands, one per line. End with CNTL/Z.
SwitchBranch(config)#int range gi0/2-3, gil/0-2
SwitchBranch(config-if-range)#shutdown
```

Figure 5.2.11.6 disable unused ports for SwitchBranch

VLAN Security

The VLAN security purpose is to separate network based on its priority. Besides that, decreasing the chances of confidential information breaches.

Step 1: Create new VLAN name as “unusedport” and assign all the unused port in the new VLAN.

```
SwitchHQ(config)#vlan 110
SwitchHQ(config-vlan)#name unusedport
SwitchHQ(config-vlan)#end
```

Figure 5.2.11.7 create new VLAN for unusedports

Step 2: Assign unused port to a new VLAN

```
SwitchHQ(config)#int range gil/0-2
SwitchHQ(config-if-range)#switchport access vlan 110
SwitchHQ(config-if-range)#end
```

Figure 5.2.11.8 Assign unused port to new VLAN for SwitchHQ

```
SwitchBranch(config)#int range gi0/2-3, gil/0-2
SwitchBranch(config-if-range)#switchport access vlan 110
SwitchBranch(config-if-range)#end
SwitchBranch#
```

Figure 5.2.11.9 Assign unused port to new VLAN for SwitchBranch

Step 3: Change the VLAN status from active to suspend. Any access to suspend VLAN would be automatically blocked essentially. While the traffic will be blackhole. This is to protect unused ports from talking to each other.

```
SwitchHQ(config)#vlan 110
SwitchHQ(config-vlan)#state suspend
SwitchHQ(config-vlan)#end
```

Figure 5.2.11.10 Change VLAN status

Step 4: Secure trunk port

```

SwitchHQ(config)#vlan 100
SwitchHQ(config-vlan)#name Native
SwitchHQ(config-vlan)#int gi0/0
SwitchHQ(config-if)#switchport trunk native vlan 100
SwitchHQ(config-if)#end

```

Figure 5.2.11.11 Securing trunk port

5.2.12. Samba and Samba security

This service is installed in Linux Debian Server. All configurations are done in root mode (superuser).

```

$ su -
# //Entered superuser mode

```

Installing and configuring Samba:

Step 1: Check any update.

```

#sudo apt-get update
#sudo apt-get upgrade

```

Step 2: Install samba and its package.

```

#sudo apt-get install samba
debian@WorkshopII:~$ sudo apt-get install samba
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  attr ibverbs-providers libboost-regex1.67.0 libcephfs2 libgfapi0 libgfrpc0
  libgfrpc0 libglusterfs0 libibverbs1 librados2 libtirpc-common libtirpc3
  python-crypto python-dnspython python-gpg python-ldb python-samba python-tdb
  samba-common samba-common-bin samba-dsdb-modules samba-vfs-modules tdb-tools
Suggested packages:
  python-crypto-doc bind9 bind9utils ctdb ldb-tools ntp | chrony smbdap-tools
  ufw winbind heimdal-clients
The following NEW packages will be installed:
  attr ibverbs-providers libboost-regex1.67.0 libcephfs2 libgfapi0 libgfrpc0
  libgfrpc0 libglusterfs0 libibverbs1 librados2 libtirpc-common libtirpc3
  python-crypto python-dnspython python-gpg python-ldb python-samba python-tdb
  samba samba-common samba-common-bin samba-dsdb-modules samba-vfs-modules
  tdb-tools
0 upgraded, 24 newly installed, 0 to remove and 0 not upgraded.
Need to get 19.9 MB of archives.
After this operation, 70.8 MB of additional disk space will be used.
Do you want to continue? [Y/n] y

```

Figure 5.2.12.1 Installing Samba

Step 3: Install Samba client

```
debian@WorkshopII:~$ sudo apt-get install samba-client
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'smbclient' instead of 'samba-client'
Suggested packages:
  cifs-utils heimdal-clients
The following NEW packages will be installed:
  smbclient
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 463 kB of archives.
After this operation, 1,841 kB of additional disk space will be used.
Get:1 http://security.debian.org/debian-security buster/updates/main amd64 smbclient amd64 2:4.9.5+dfsg-5+deb10u1 [463 kB]
Fetched 463 kB in 1s (581 kB/s)
Selecting previously unselected package smbclient.
(Reading database ... 144978 files and directories currently installed.)
Preparing to unpack .../smbclient_2%3a4.9.5+dfsg-5+deb10u1_amd64.deb ...
Unpacking smbclient (2:4.9.5+dfsg-5+deb10u1) ...
Setting up smbclient (2:4.9.5+dfsg-5+deb10u1) ...
Processing triggers for man-db (2.8.5-2) ...
```

Figure 5.2.12.2 Installing Samba client

Step 4: Enable the Samba service

```
#systemctl enable smbd
```

Step 5: Check the Samba running status

```
# systemctl status smbd
```

Step 6: Add user into samba.

Add user into Samba:

```
#smbpasswd -a debian
```

Step 7: Restart Samba every time after adding a new user.

```
#systemctl restart smbd
```

Step 8: Modify the Samba's configuration file.

This file is located at **/etc/samba/smb.conf**

```
#nano /etc/samba/smb.conf
```

File access permission

Step 1: In smb.conf, add “valid user = debian” in the Tester folder in Samba share. This line will make the Samba will only permit the user tester to access the file. Save.

Step 2: Restart Samba every time after the configuration changed.

```
#systemctl restart smbd.
```

File restriction

Step 1: In terminal, enter root and change the folder permission using chmod command.

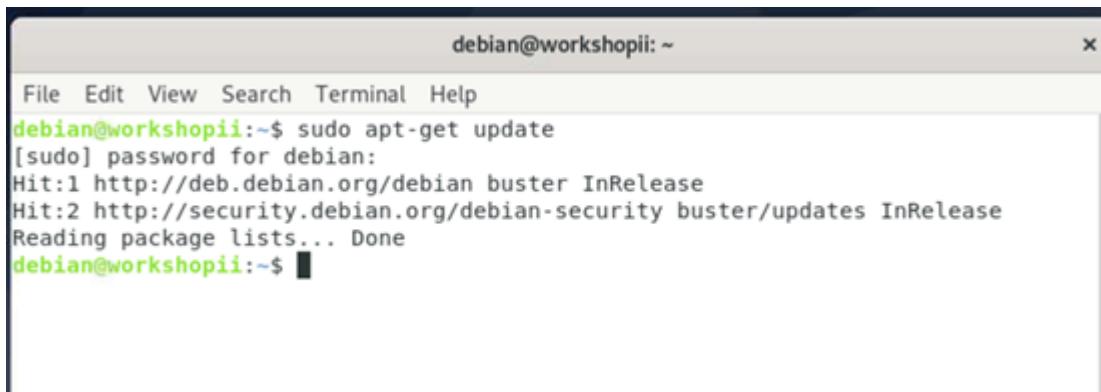
The command will configure the folder to be only can be modify (read, write, execute) by the folder owner which is debian

```
#sudo chmod -R 0700 /samba/debian/
```

5.2.13. User authentication user by integrating AD with linux

Debian Server

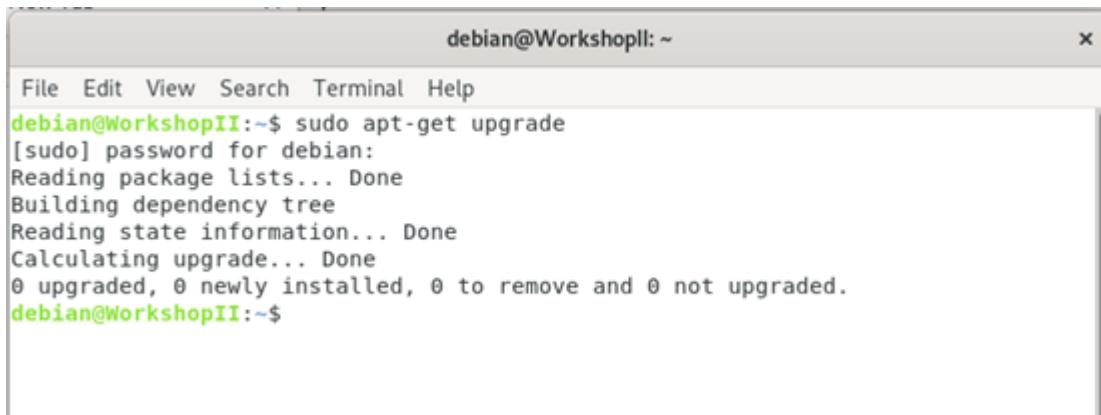
Step 1 : Update and upgrade for the system to get the latest package database.



A screenshot of a terminal window titled "debian@workshopii: ~". The window shows the command "sudo apt-get update" being run. The output indicates that the system is checking for updates from two sources: "deb.debian.org" and "security.debian.org". It shows "Hit" for both sources and "Reading package lists... Done". The command prompt "debian@workshopii:~\$" is visible at the end.

```
File Edit View Search Terminal Help
debian@workshopii:~$ sudo apt-get update
[sudo] password for debian:
Hit:1 http://deb.debian.org/debian buster InRelease
Hit:2 http://security.debian.org/debian-security buster/updates InRelease
Reading package lists... Done
debian@workshopii:~$
```

Figure 5.2.13.1 Update for the system



A screenshot of a terminal window titled "debian@WorkshopII: ~". The window shows the command "sudo apt-get upgrade" being run. The output shows the system reading package lists, building a dependency tree, and calculating an upgrade. It concludes with a message stating "0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded." The command prompt "debian@WorkshopII:~\$" is visible at the end.

```
File Edit View Search Terminal Help
debian@WorkshopII:~$ sudo apt-get upgrade
[sudo] password for debian:
Reading package lists...
Building dependency tree...
Reading state information...
Calculating upgrade...
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
debian@WorkshopII:~$
```

Figure 5.2.13.2 Upgrade for the system

Step 2: Download the PowerBroker Identify Services (PBIS) repository package from Github.

Assets 16	
pbis-open-9.1.0.551.aix.powerpc.lpp.sh	13.4 MB
pbis-open-9.1.0.551.dmg	11.6 MB
pbis-open-9.1.0.551.hpux.ia64.depot.sh	11.3 MB
pbis-open-9.1.0.551.linux.powerpc.ppc64.rpm.sh	16.8 MB
pbis-open-9.1.0.551.linux.powerpc.ppc64le.rpm.sh	15 MB
pbis-open-9.1.0.551.linux.s390x.rpm.sh	16.9 MB
pbis-open-9.1.0.551.linux.x86.deb.sh	6.81 MB
pbis-open-9.1.0.551.linux.x86.rpm.sh	12.6 MB
pbis-open-9.1.0.551.linux.x86_64.deb.sh	7.94 MB
pbis-open-9.1.0.551.linux.x86_64.rpm.sh	14.5 MB
pbis-open-9.1.0.551.solaris.sparcv9.pkg.sh	18.1 MB
pbis-open-9.1.0.551.solaris.x86.pkg.sh	17.8 MB
pbis-open-9.1.0.551.solaris11.sparcv9.pkg.sh	18.6 MB

Figure 5.2.13.3 Download PBIS package

Step 3: Change the execute permission for the downloaded package.

```
debian@WorkshopII:~/Downloads
File Edit View Search Terminal Help
debian@WorkshopII:~/Downloads$ chmod 777 pbis-open-9.1.0.551.linux.x86_64.deb.sh
debian@WorkshopII:~/Downloads$
```

Figure 5.2.13.4 Change Execute Permission

Step 4: Install the PBIS Open Edition by using the following commands.

```

debian@WorkshopII: ~/Downloads
File Edit View Search Terminal Help
debian@WorkshopII:~/Downloads$ sudo sh pbis-open-9.1.0.551.linux.x86_64.deb.sh
[sudo] password for debian:
Creating directory pbis-open-9.1.0.551.linux.x86_64.deb
Verifying archive integrity... All good.
Uncompressing pbis-open-9.1.0.551.linux.x86_64.deb.....
Installing packages and old packages will be removed
Selecting previously unselected package pbis-open-upgrade.
(Reading database ... 145007 files and directories currently installed.)
Preparing to unpack .../pbis-open-upgrade_9.1.0.551_amd64.deb ...
Unpacking pbis-open-upgrade (9.1.0.551) ...
Setting up pbis-open-upgrade (9.1.0.551) ...
Selecting previously unselected package pbis-open.
(Reading database ... 145009 files and directories currently installed.)
Preparing to unpack .../pbis-open_9.1.0.551_amd64.deb ...
Unpacking pbis-open (9.1.0.551) ...
Setting up pbis-open (9.1.0.551) ...
Importing registry...

Processing triggers for man-db (2.8.5-2) ...

Installing Packages was successful

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

```

Figure 5.2.13.5 Installation of PBIS Open Edition

Step 5: Create an Active Directory group which include AD users

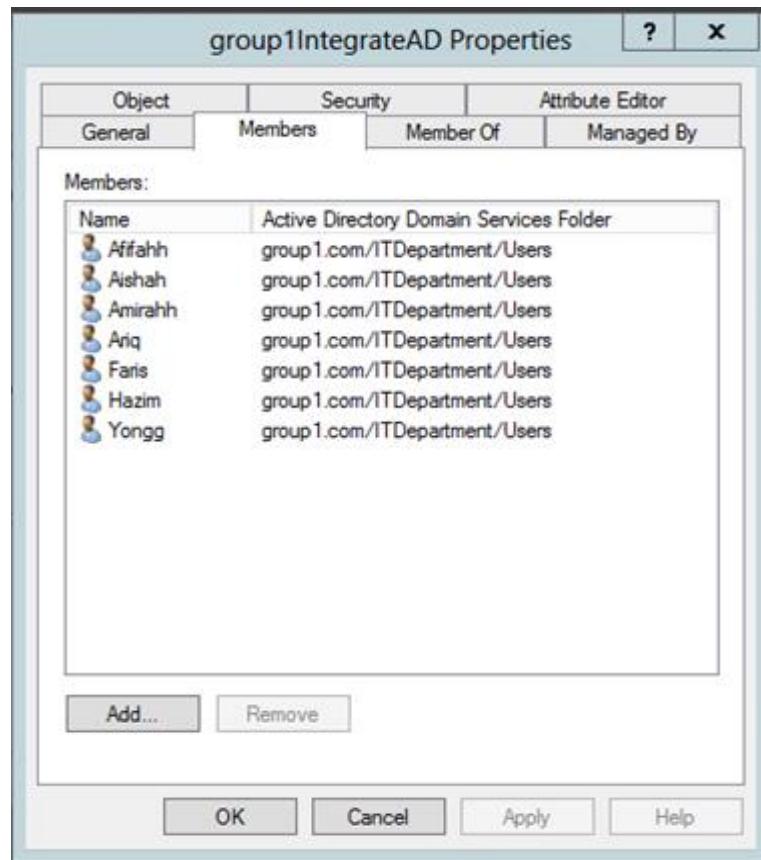
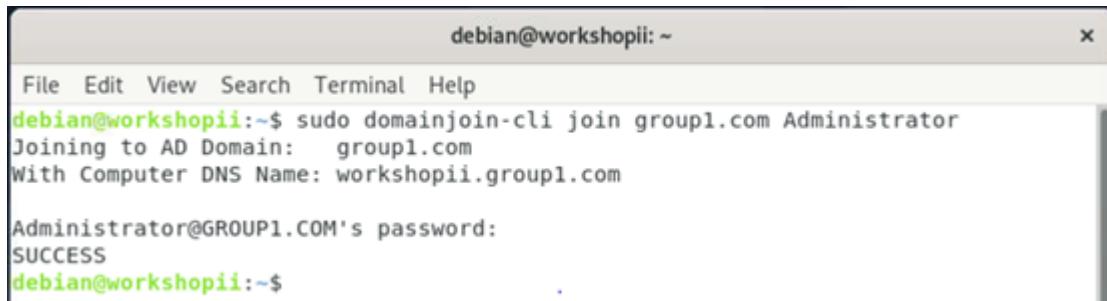


Figure 5.2.13.6 Create AD group with users

Step 6 : Next join the Debian system to integrate with Windows Active Directory with a user created on Active Directory by using following commands. After successfully joining Debian client to the Windows Active Directory will show a “SUCCESS” message.

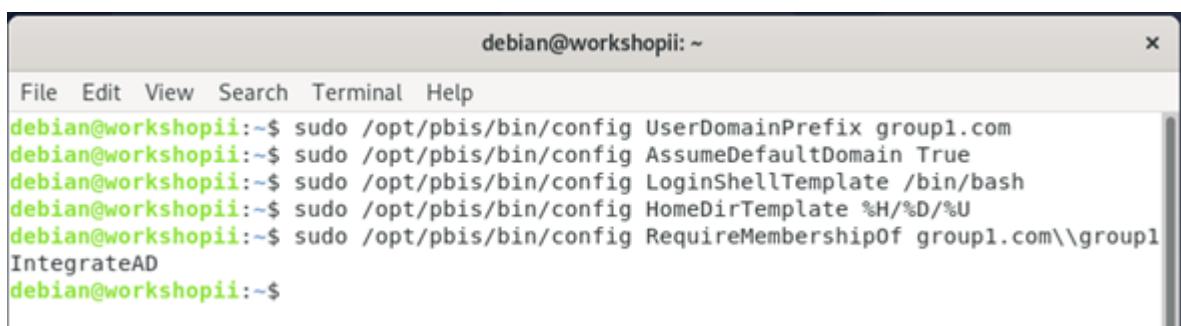


```
debian@workshopii:~$ sudo domainjoin-cli join group1.com Administrator
Joining to AD Domain: group1.com
With Computer DNS Name: workshopii.group1.com

Administrator@GROUP1.COM's password:
SUCCESS
debian@workshopii:~$
```

Figure 5.2.13.7 Joining system to Active Directory

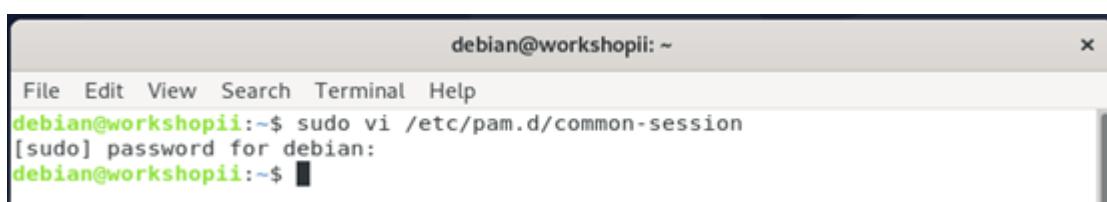
Step 7: Setup Active Directory login settings.



```
debian@workshopii:~$ sudo /opt/pbis/bin/config UserDomainPrefix group1.com
debian@workshopii:~$ sudo /opt/pbis/bin/config AssumeDefaultDomain True
debian@workshopii:~$ sudo /opt/pbis/bin/config LoginShellTemplate /bin/bash
debian@workshopii:~$ sudo /opt/pbis/bin/config HomeDirTemplate %H/%D/%U
debian@workshopii:~$ sudo /opt/pbis/bin/config RequireMembershipOf group1.com\group1
IntegrateAD
debian@workshopii:~$
```

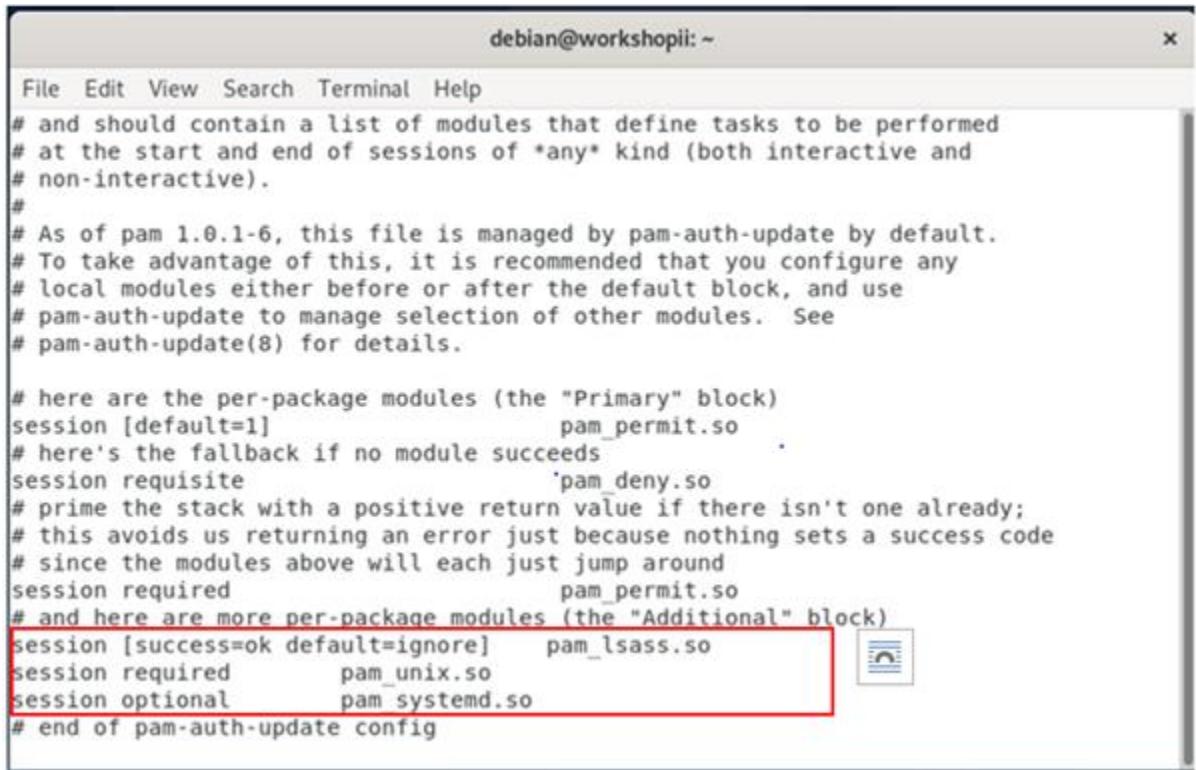
Figure 5.2.13.8 Configure login settings

Step 8 : Change to pam.d directory and open the pam.d common session file.pam(Pluggable Authentication Modules): provide dynamic authentication support for applications and services in a Linux system.



```
debian@workshopii:~$ sudo vi /etc/pam.d/common-session
[sudo] password for debian:
debian@workshopii:~$
```

Figure 5.2.13.9 Change directory and Open common session file



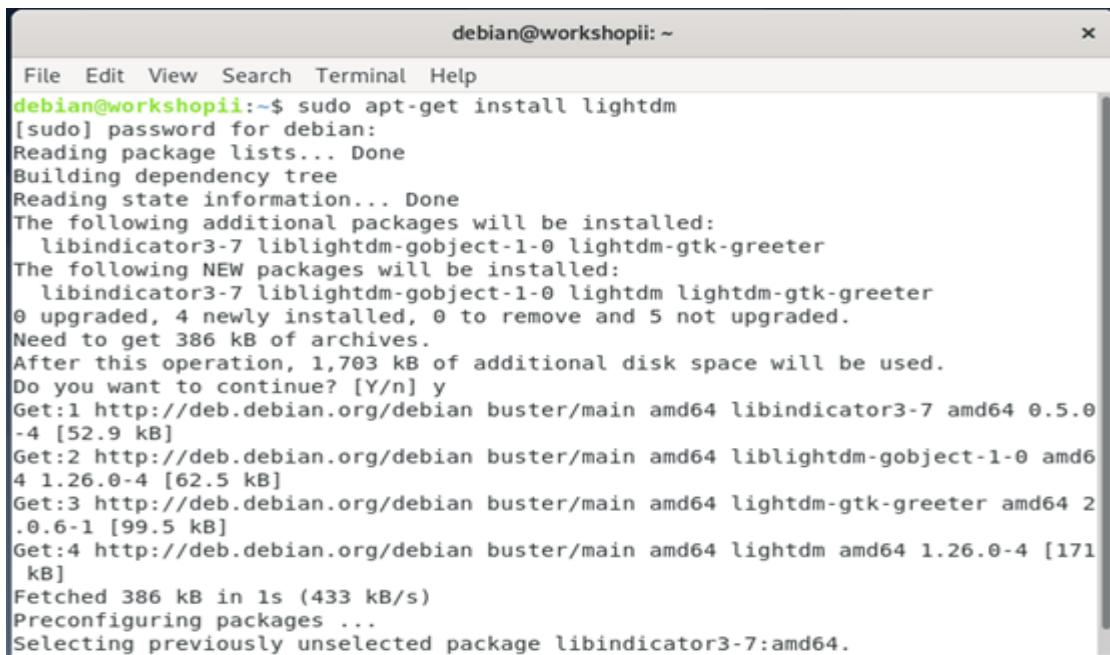
```
debian@workshopii: ~
File Edit View Search Terminal Help
# and should contain a list of modules that define tasks to be performed
# at the start and end of sessions of *any* kind (both interactive and
# non-interactive).
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# 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)
session [default=1]          pam_permit.so
# here's the fallback if no module succeeds
session requisite           pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
session required             pam_permit.so
# and here are more per-package modules (the "Additional" block)
session [success=ok default=ignore]    pam_lsass.so
session required               pam_unix.so
session optional              pam_systemd.so
# end of pam-auth-update config
```

Step 9: Editing the configuration for the common session file. pam_lsass.so : local security authority subsystem service in pam.

Figure 5.2.13.10 Editing common session file

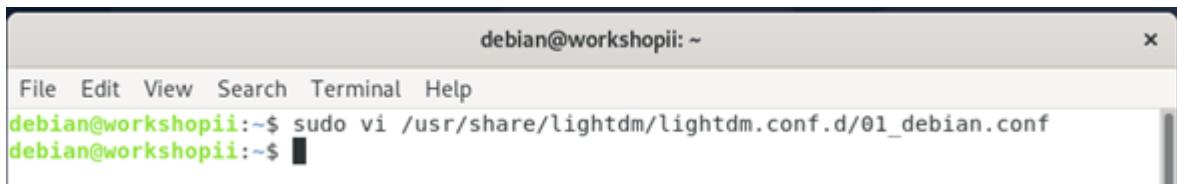
Step 10: Install the lightdm that are not considered in Debian by using the following commands.



```
debian@workshopii:~$ sudo apt-get install lightdm
[sudo] password for debian:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libindicator3-7 liblightdm-gobject-1-0 lightdm-gtk-greeter
The following NEW packages will be installed:
  libindicator3-7 liblightdm-gobject-1-0 lightdm lightdm-gtk-greeter
0 upgraded, 4 newly installed, 0 to remove and 5 not upgraded.
Need to get 386 kB of archives.
After this operation, 1,703 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://deb.debian.org/debian buster/main amd64 libindicator3-7 amd64 0.5.0-4 [52.9 kB]
Get:2 http://deb.debian.org/debian buster/main amd64 liblightdm-gobject-1-0 amd64 1.26.0-4 [62.5 kB]
Get:3 http://deb.debian.org/debian buster/main amd64 lightdm-gtk-greeter amd64 2.0.6-1 [99.5 kB]
Get:4 http://deb.debian.org/debian buster/main amd64 lightdm amd64 1.26.0-4 [171 kB]
Fetched 386 kB in 1s (433 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libindicator3-7:amd64.
```

Figure 5.2.13.11 Installation of lightdm

Step 11: Change to lightdm.conf.d directory and open the configuration (01_debian.conf) file which the lightdm is used for display manager running in Debian.

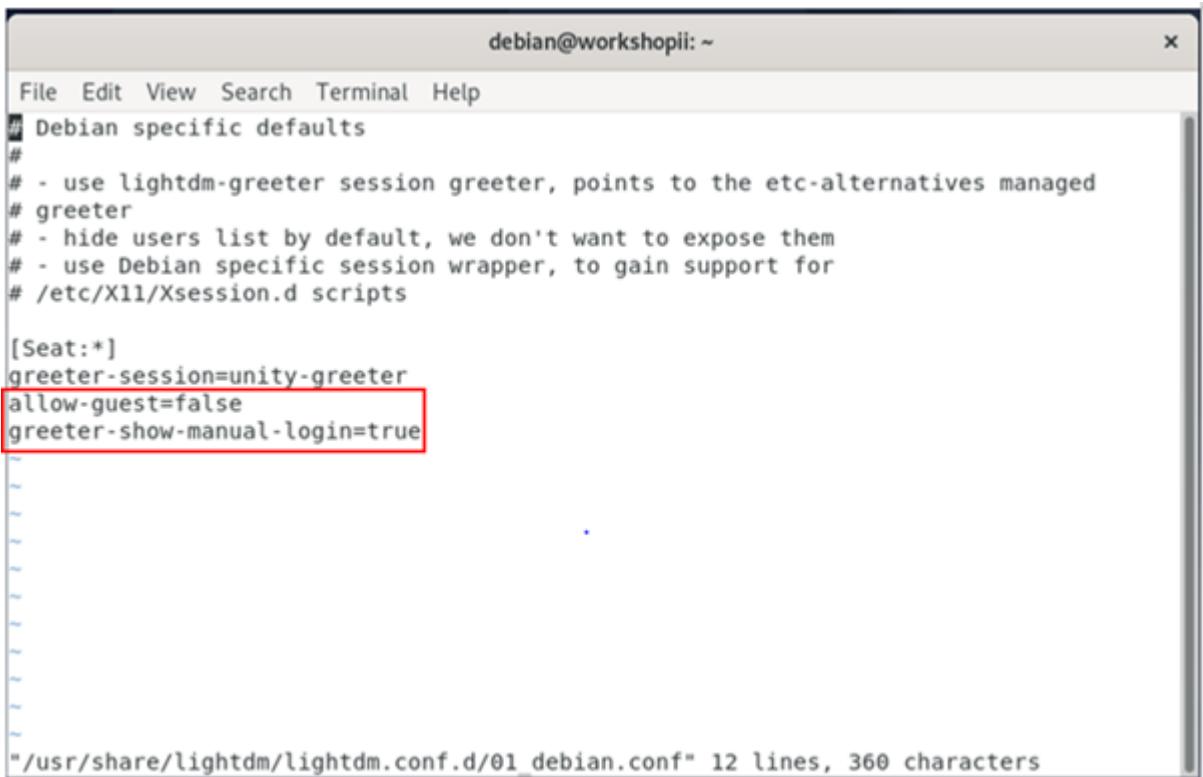


```
debian@workshopii:~$ sudo vi /usr/share/lightdm/lightdm.conf.d/01_debian.conf
debian@workshopii:~$
```

Figure 5.2.13.12 Change directory and Open configuration file

Step 12: Editing for the configuration (01_debian.conf) file.

allow-guest=false: to disable guest login
greeter-show-manual-greeter-show-manual-login=true : to allow manual login



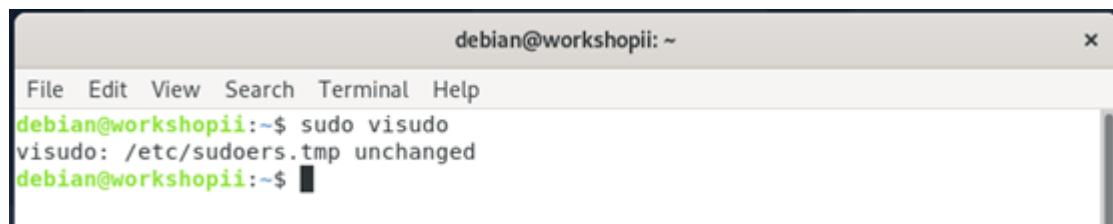
```
debian@workshopii: ~
File Edit View Search Terminal Help
# Debian specific defaults
#
# - use lightdm-greeter session greeter, points to the etc-alternatives managed
# greeter
# - hide users list by default, we don't want to expose them
# - use Debian specific session wrapper, to gain support for
# /etc/X11/Xsession.d scripts

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

"/usr/share/lightdm/lightdm.conf.d/01_debian.conf" 12 lines, 360 characters
```

Figure 5.2.13.13 Editing configuration file

Step 13: Open and update sudoers file to enable AD users to use sudo permission. After updating the sudoers file and saving the file. **MUST USE root USER and visudo to edit the /etc/sudoers file.**



```
debian@workshopii: ~
File Edit View Search Terminal Help
debian@workshopii:~$ sudo visudo
visudo: /etc/sudoers.tmp unchanged
debian@workshopii:~$
```

Figure 5.2.13.14 Open sudoers file

```
debian@workshopii: ~
File Edit View Search Terminal Help
GNU nano 3.2          /etc/sudoers.tmp

Defaults      mail_badpass
Defaults      secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:$

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

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

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
%GROUP1\\group1integratead  ALL=(ALL:ALL)  ALL
# See sudoers(5) for more information on "#include" directives:

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

Figure 5.2.13.15 Update sudoers file on Debian

Step 14: Logout for the current user and sign in for the integrated active directory accounts.

5.2.14. Intrusion Detection System (IDS) and Port Mirroring

INSTALLATION

Step 1: Install all the latest updated packages.

- a) Installation of updated package.

```
debian@WorkshopII:~$ sudo su
[sudo] password for debian:
root@WorkshopII:/home/debian# apt-get install -y build-essential
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

Figure 5.2.14.1: Install build-essential

```
root@WorkshopII:/home/debian# apt-get install -y libpcap-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

Figure 5.2.14.2: Install libpcap-dev

```
root@WorkshopII:/home/debian# apt-get install -y libpcre3-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

Figure 5.2.14.3: Install libpcre3-dev

```
root@WorkshopII:/home/debian# apt-get install -y libdumbnet-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

Figure 5.2.14.4: Install libdumbnet-dev

```
root@WorkshopII:/home/debian# apt-get install -y bison flex
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

Figure 5.2.14.5: Install bison flex

- b) Create ~snort_src folder.

```
root@WorkshopII:/home/debian# mkdir ~snort_src
```

Figure 5.2.14.6: Create ~snort_src folder

```
root@WorkshopII:/home/debian# cd ~snort_src  
root@WorkshopII:/home/debian/~snort_src# █
```

Figure 5.2.14.7: Go to the ~snort_src folder

Step 2: Install the latest daq-2.0.7.

- a) Download, build and install the latest DAQ (Data Acquisition Library) 2.0.7.

```
root@WorkshopII:/home/debian/~snort_src# wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz
```

Figure 5.2.14.8: Download DAQ 2.0.7

```
root@WorkshopII:/home/debian/~snort_src# tar zxvf daq-2.0.7.tar.gz
```

Figure 5.2.14.9: Extract daq-2.0.7.tar.gz

```
root@WorkshopII:/home/debian/~snort_src# cd daq-2.0.7  
root@WorkshopII:/home/debian/~snort_src/daq-2.0.7# █
```

Figure 5.2.14.10: Go to the daq-2.0.6 folder

Step 3: Configure daq-2.0.7.

```
root@WorkshopII:/home/debian/~snort_src# cd daq-2.0.7  
root@WorkshopII:/home/debian/~snort_src/daq-2.0.7# ./configure
```

Figure 5.2.14.11: Unpack and configure daq-2.0.7

```
root@WorkshopII:/home/debian/~snort_src/daq-2.0.7# make
make all-recursive
make[1]: Entering directory '/home/debian/~snort_src/daq-2.0.7'
Making all in api
```

Figure 5.2.14.12: Make the daq-2.0.7

```
root@WorkshopII:/home/debian/~snort_src/daq-2.0.7# make install
```

Figure 5.2.14.13: Install the daq-2.0.7

```
root@WorkshopII:/home/debian/~snort_src/daq-2.0.7# apt-get install -y zlib1g-dev
Reading package lists... Done
```

Figure 5.2.14.14: Install zlib1g-dev

Step 4: Install the latest snort-2.9.17.

- Download, build and install the latest Snort 2.9.17

```
root@WorkshopII:/home/debian/~snort_src# wget https://www.snort.org/downloads/snort/snort-2.9.17.tar.gz
--2020-11-26 17:36:30-- https://www.snort.org/downloads/snort/snort-2.9.17.tar.gz
Resolving www.snort.org (www.snort.org)... 104.18.139.9, 104.18.138.9, 2606:4700
```

Figure 5.2.14.15: Download snort-2.9.17

```
root@WorkshopII:/home/debian/~snort_src# tar xvzf snort-2.9.17.tar.gz
```

Figure 5.2.14.16: Extract snort-2.9.17.tar.gz

```
root@WorkshopII:/home/debian/~snort_src/snort-2.9.17# ./configure --enable-sourcefire --disable-open-appid
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
```

Figure 5.12.14.17: Go to snort-2.9.17 and configure the snort

```
root@WorkshopII:/home/debian/~snort_src/snort-2.9.17# make
```

Figure 5.2.14.18: Make the snort-2.9.17

```
root@WorkshopII:/home/debian/~/snort_src/snort-2.9.17# make install
```

Figure 5.2.14.19: Install the snort-2.9.17

Step 5: Configure snort-2.9.17

- a) Create an unprivileged Snort account and required initial files.
- b) Update the shared libraries to avoid any error when trying to run snort.

```
root@WorkshopII:/home/debian/~/snort_src# sudo ldconfig
```

Figure 5.2.14.20: Command to update the shared library

- c) Create a symlink to the snort library.

```
root@WorkshopII:/home/debian/~/snort_src# ln -s /usr/local/bin/snort /usr/sbin/snort
```

Figure 5.2.14.21: Create a symlink

- d) Create a regular user and a group to run snort daemon.

```
root@WorkshopII:/home/debian/~/snort_src# sudo groupadd snort
```

Figure 5.2.14.22: Group add snort

```
root@WorkshopII:/home/debian/~/snort_src# sudo useradd snort -r -s /sbin/nologin -c SNORT_IDS -g snort
```

Figure 5.2.14.22: Create user

e) Create file.

```
mkdir /etc/snort/rules
```

Figure 5.2.14.23: Create rules file

```
root@WorkshopII:/home/debian/~/snort_src# mkdir /usr/local/lib/snort_dynamicrul
```

Figure 5.2.14.24: Create dynamic rules file

```
root@WorkshopII:/home/debian/~/snort_src# mkdir /var/log/snort
```

Figure 5.2.14.25: Create a log file

f) Change permission.

```
root@WorkshopII:/home/debian/~/snort_src/snort-2.9.17/etc# chmod -R 5775 snort
```

Figure 5.2.14.26: Change permission for snort file

```
root@WorkshopII:/home/debian/~/snort_src# chmod -R 5775 /var/log/snort/
```

Figure 5.2.14.27: Set permission for log file

```
root@WorkshopII:/home/debian/~/snort_src# chmod -R 5775 /usr/local/lib/snort_dynamicrul
```

Figure 5.2.14.28: Set permission for dynamic rules file

g) Change ownership.

```
root@WorkshopII:/home/debian/~/snort_src/snort-2.9.17/etc# chown -R snort:snort snort
```

Figure 5.2.14.29: Change ownership for snort file

```
root@WorkshopII:/home/debian/~/snort_src# chown -R snort:snort /var/log/snort
```

Figure 5.2.14.30: Change ownership for log file

```
root@WorkshopII:/home/debian/~/snort_src# chown -R snort:snort /usr/local/lib/snort_dynarmicrul
```

Figure 5.2.14.31: Change ownership for dynamic rules file

- h) Create new files for white and blacklists as well as the local rules.

```
root@WorkshopII:/home/debian/~/snort_src# touch /usr/local/lib/snort/rules/white_list.rules /usr/local/lib/snort/rules/black_list.rules /usr/local/lib/snort/rules/local.rules
```

Figure 5.2.14.32: Create a white and black file in rules

- i) Copy configuration files.

```
root@WorkshopII:/home/debian/~/snort_src/snort-2.9.17/etc# cp *.conf* snort  
root@WorkshopII:/home/debian/~/snort_src/snort-2.9.17/etc# cp *.map* snort
```

Figure 5.2.14.33: Command to copy the configuration

- j) Check completion of installing snort-2.9.17.

```
root@WorkshopII:/home/debian/~snort_src# snort -V

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

root@WorkshopII:/home/debian/~snort_src#
```

Figure 5.2.14.34: Installation complete

Step 6: Update snort.conf

- With the configuration and rule files in place, edit the snort.conf to modify a few parameters. Open the configuration file to edit.

```
root@WorkshopII:/home/debian/~snort_src/snort-2.9.17/etc/snort# nano snort.conf
```

Figure 5.2.14.35: Open the configuration file

- Find the following sections in the configuration file and change the parameters.

```
# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.2.146
```

Figure 5.2.14.36: Insert the Debian IP address

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

Figure 5.2.14.37: Insert external network address with !\$HOME_NET

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

Figure 5.2.14.38: Change the path to the rules files

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

Figure 5.2.14.39: Set the absolute path appropriately

- c) Lastly, scroll down to the bottom of the file to find the list of included rule sets. We need to uncomment the locals rules include a line to allow Snort to load any custom rules. We also need to comment the others include line.

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

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

Figure 5.2.14.40: Comment all the include line except local.rules

Step 7: Testing snort.conf

Once we are done with the configuration file, save the changes and exit the editor. Our snort should now be ready to run and test the configuration using T to enable test mode.

```
root@WorkshopII:/home/debian/~snort_src/snort-2.9.17/etc/snort# snort -T -c snort.conf
```

Figure 5.2.14.41: Command for testing configuration

```
Using libpcap version 1.8.1
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11

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

Snort successfully validated the configuration!
Snort exiting
root@WorkshopII:/home/debian/~snort_src/snort-2.9.17/etc/snort#
```

Figure 5.2.14.42: Result for configuration

Step 8: Creating a custom snort rule to test Snort.

- To test if Snort is logging alerts as intended, add a custom detection rule alert on incoming ICMP connections to the local rules file.

```
root@workshopii:/home/debian/~snort_src# nano ../local.rules
```

Figure 5.2.14.43: Open our local rules

- Add the line with rule consist of the following parts:
 - Action for traffic matching the rule, alert in this case.
 - Traffic protocol of ICMP information.
 - The source address and port marked as any to include all addresses and ports.

4. Destination address and port \$HOME_NET as declared in the configuration and any for the port

5. Some additional bits:

- Log message.
- Unique rule identifier (sid) which for local rules needs to be 10000001 or higher.
- Rule version number.

```
GNU nano 3.2                               /etc/snort/local.rules

alert icmp 192.168.2.4 any -> $HOME_NET any (msg:"ITDepartment ping Debian"; GID:1; sid:20000001; rev:001;)
alert icmp 192.168.2.130 any -> $HOME_NET any (msg:"Windows ping Debian"; GID:1; sid:20000002; rev:002;)
#alert icmp 192.168.1.2 any -> $HOME_NET any (msg:"RemoteAccess ping Debian"; GID:1; sid:20000003; rev:003;)

alert icmp 192.168.2.130 any -> 192.168.2.4 any (msg:"Windows ping ITDepartment"; GID:1; sid:20000004; rev:004;)
alert icmp 192.168.2.4 any -> 192.168.2.130 any (msg:"ITDepartment ping Windows"; GID:1; sid:20000005; rev:005;)

alert icmp 192.168.2.130 any -> 192.168.1.2 any (msg:"Windows ping RemoteAccess"; GID:1; sid:20000006; rev:006;)
#alert icmp 192.168.1.2 any -> 192.168.2.130 any (msg:"RemoteAccess ping Windows"; GID:1; sid:20000007; rev:007;)

#alert icmp 192.168.2.4 any -> 192.168.1.2 any (msg:"ITDepartment ping RemoteAccess"; GID:1; sid:20000008; rev:008;)
#alert icmp 192.168.1.2 any -> 192.168.2.4 any (msg:"RemoteAccess ping ITDepartment"; GID:1; sid:20000009; rev:009;)
```

Figure 5.2.14.44: Custom snort rules

PORT MIRRORING

Step 1: Setup interface gi0/0 as source port and gi1/0 as the destination port.

```
SwitchHQ(config)#no monitor session 1 source interface gi0/0
SwitchHQ(config)#no monitor session 1 destination interface gi1/0
```

Figure 5.2.14.45: Setup source port

```
monitor session 1 source interface Gi0/0
monitor session 1 destination interface Gi1/0
!
end
```

Figure 5.2.14.46: Result after setup source and destination port

5.2.15. IPSec VPN server for remote employees

SoftEther VPN Server Installation - Windows Server 2012

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

The screenshot shows the SoftEther VPN Project website. The navigation bar includes links for Top, Why SoftEther VPN, Documents, Download, Support, and About Project. A search bar is also present. On the left, a sidebar menu lists options like SoftEther VPN Project, Why SoftEther VPN, Screenshots, Specification, Documents, Download (which is highlighted), Version History (ChangeLog), Source Code, Support & Forum, About SoftEther VPN Project, and Japanese (日本語). Below this is a 'Table of contents' section with links to Primary Download Server (Windows Azure), Download from CNET Download.com, Download from Softpedia.com, and See also. The main content area is titled 'Download' and contains text about the open-source nature of SoftEther VPN and its availability on Windows Azure. It lists download links for CNET Download.com and Softpedia.com, along with supported languages (English, Japanese, Simplified Chinese) and operating systems (Windows, Linux, Mac OS X, FreeBSD, Solaris).

Figure 5.2.15.1 : Go to website and click download

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

This screenshot shows the 'Download' page of the SoftEther VPN website. The main title is 'Download'. Below it is a paragraph about the open-source nature of SoftEther VPN. The 'Primary Download Server (hosted by Windows Azure)' section is shown, with the 'Download SoftEther VPN' link circled in red. This link leads to the download page for Windows Azure. The page also lists download links for CNET Download.com and Softpedia.com, along with supported languages and operating systems.

Figure 5.2.15.2 : Download SoftEther VPN

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



Figure 5.2.15.3 : Choose requirement

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



Figure 5.2.15. 4 : Download section

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

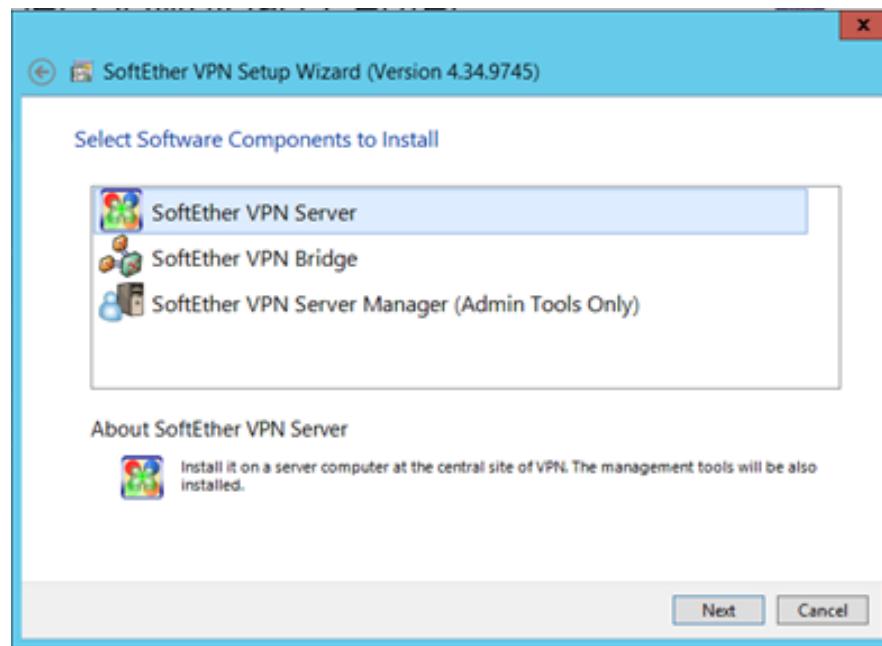


Figure 5.2.15.5: Choose software component to install

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

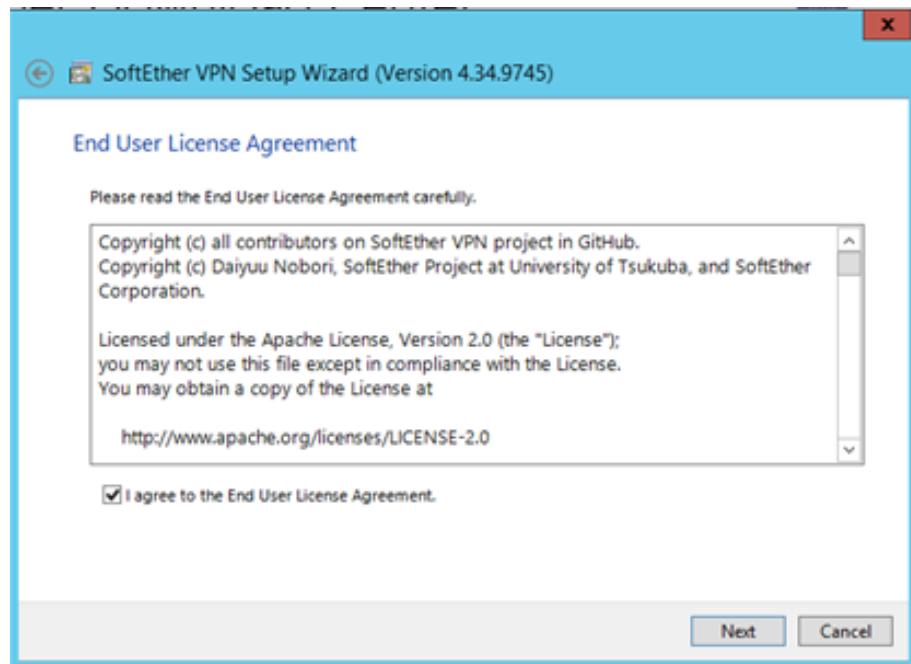


Figure 5.2.15.6 : Agree to End user Agreement

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

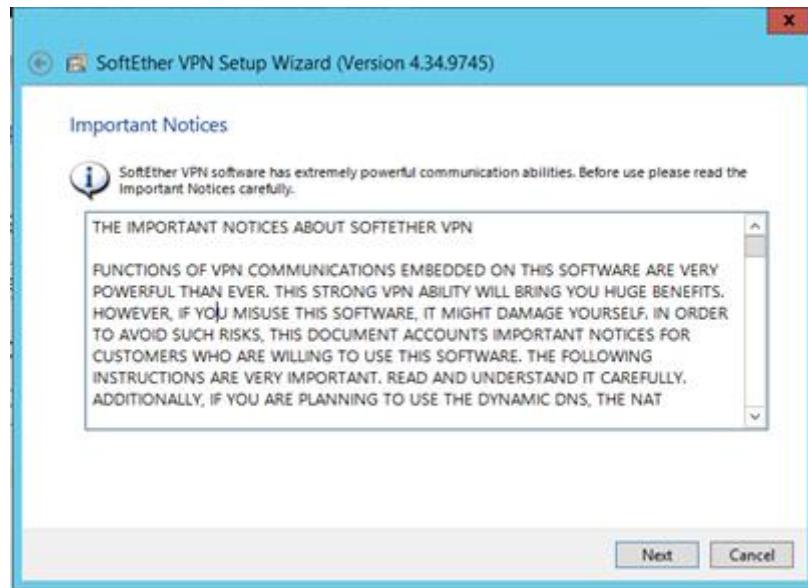


Figure 5.2.15.7 : Important Notice

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

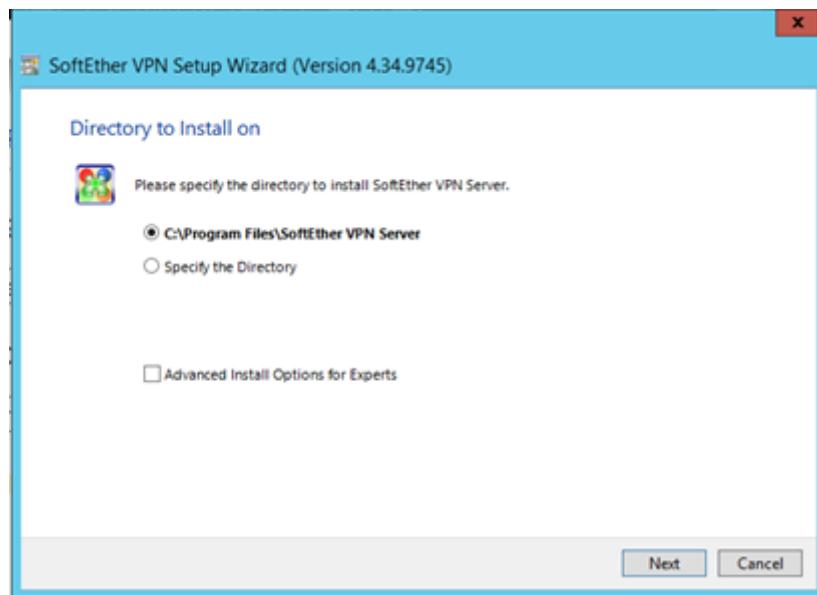


Figure 5.2.15.8 : Path Selection

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

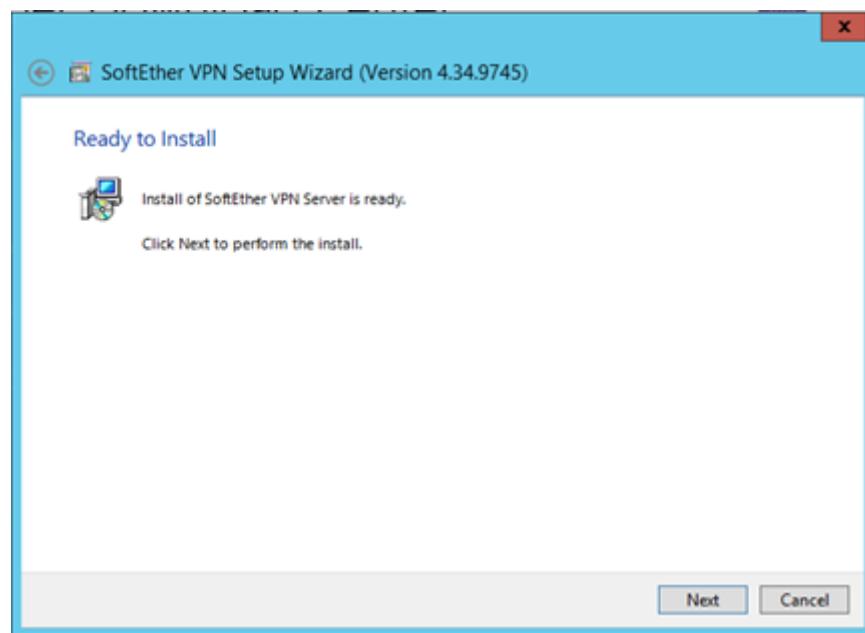


Figure 5.2.15.9 : Wait for installation

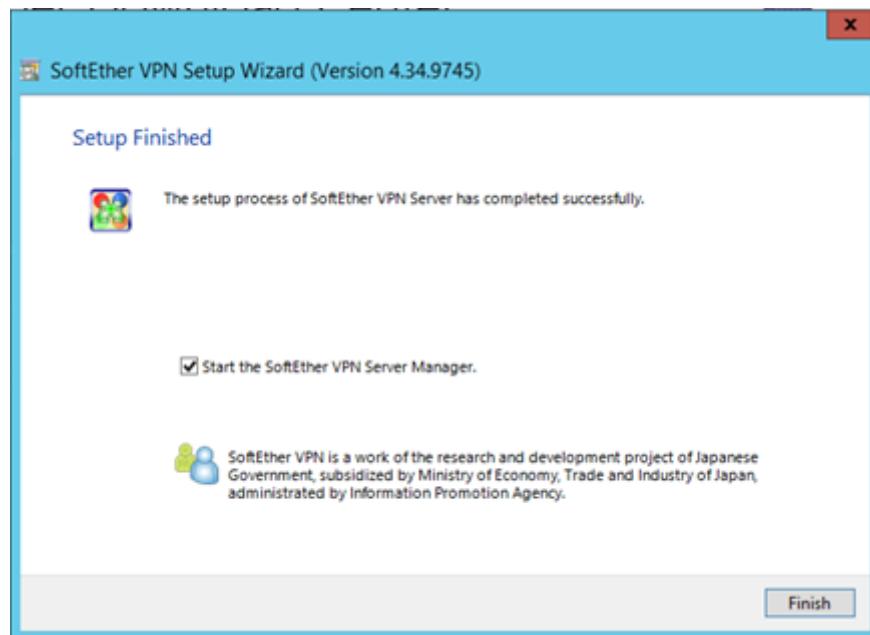


Figure 5.2.15.10 : Finish installation

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



Figure 5.2.15.11 SoftEther VPN Server Manager Interface

Configuration of SoftEther VPN Server



Figure 5.2.15.12 : Select local host

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

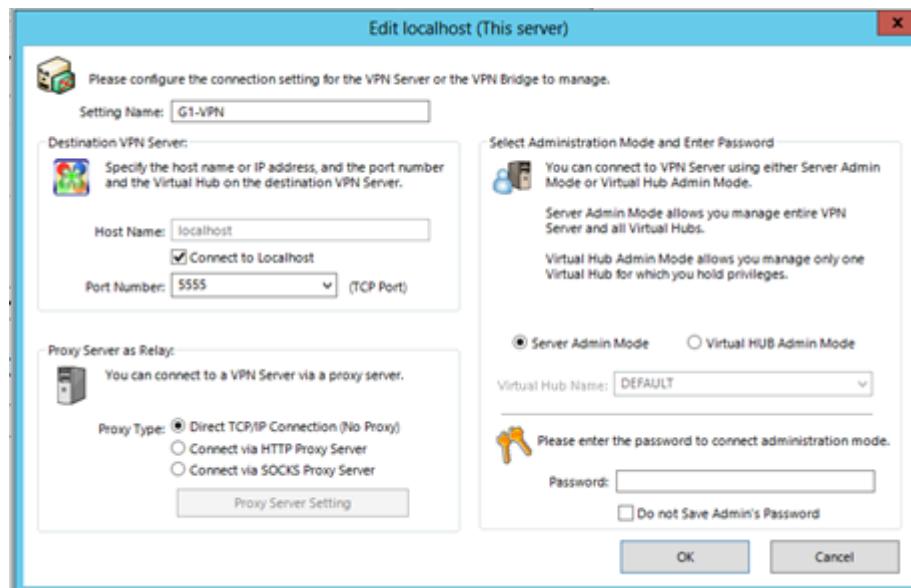


Figure 5.2.15.13 : Set up local host

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



Figure 5.2.15.14 : Set administrator password

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

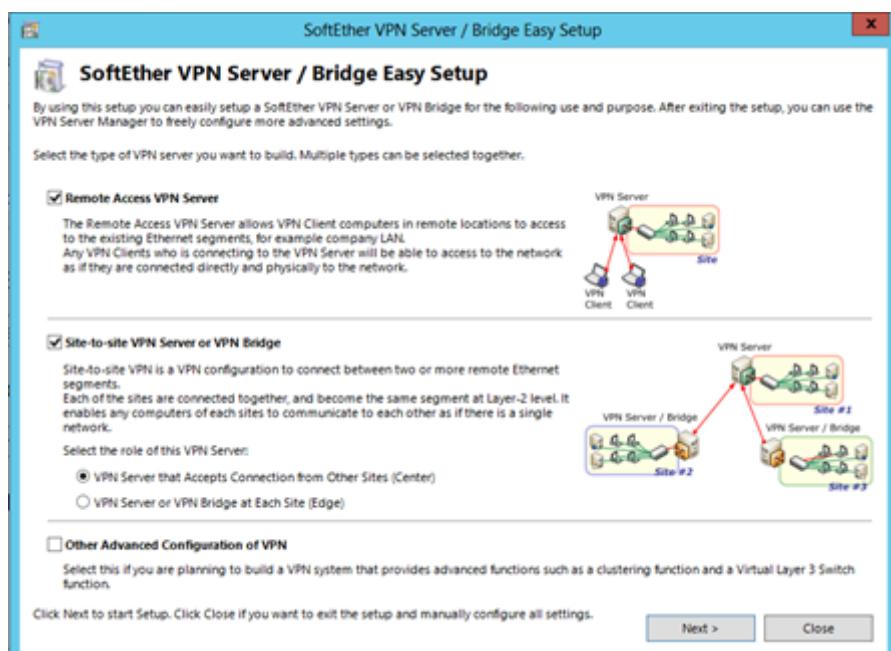


Figure 5.2.15.15 : Set up bridge



Figure 5.2.15.16 : Set up confirmation notice

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

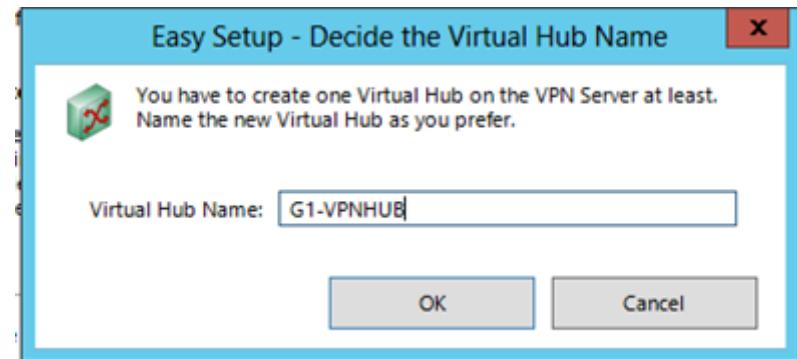


Figure 5.2.15.17 : Set up Virtual Hub Name

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

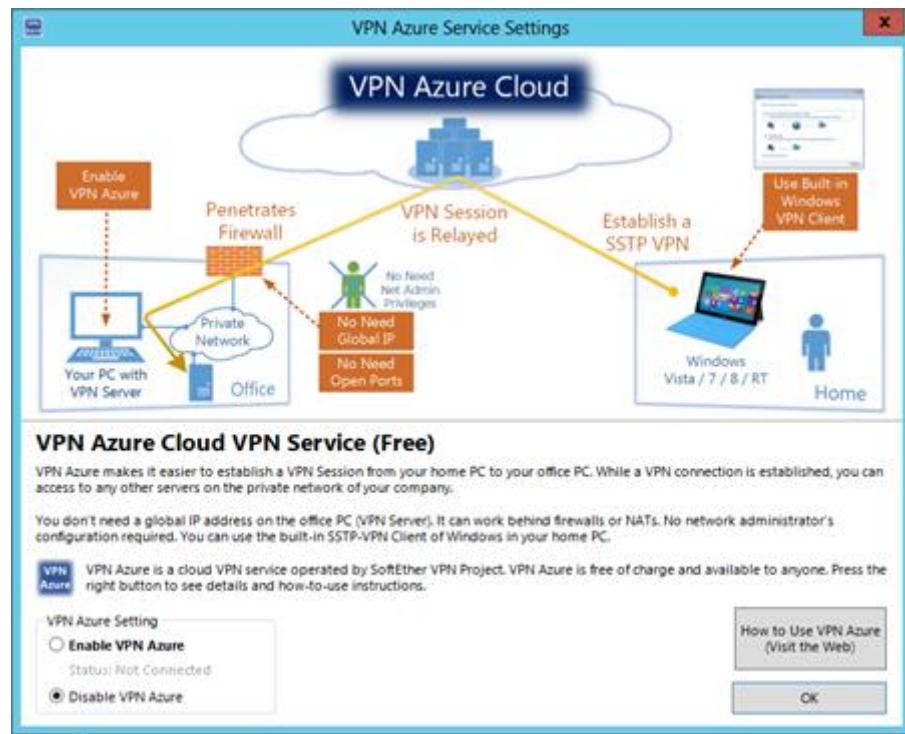


Figure 5.2.15.18 : Disable VPN Azure Services

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

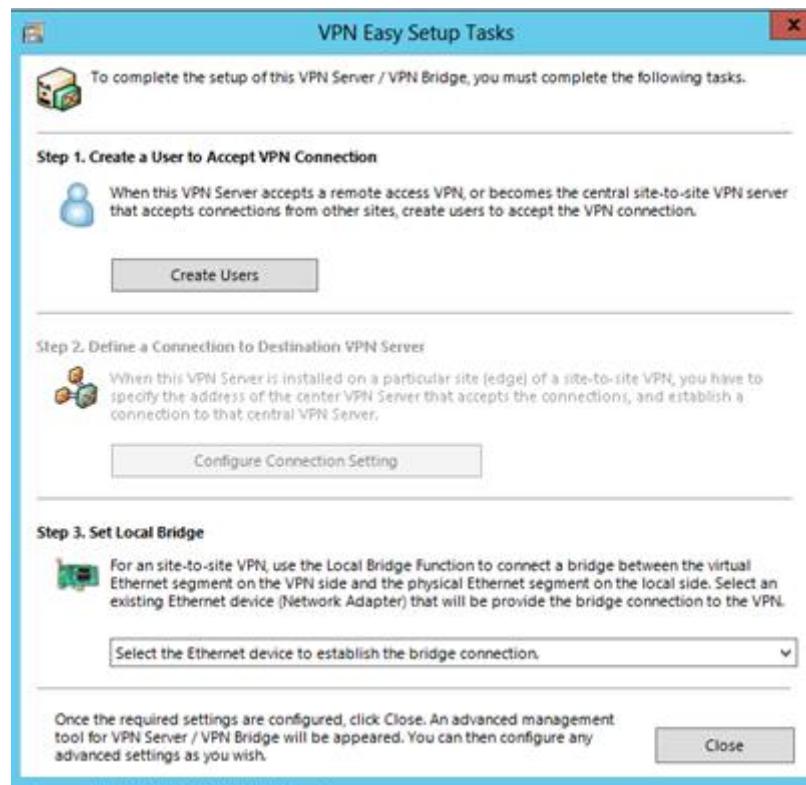


Figure 5.2.15.19 : Create a new user

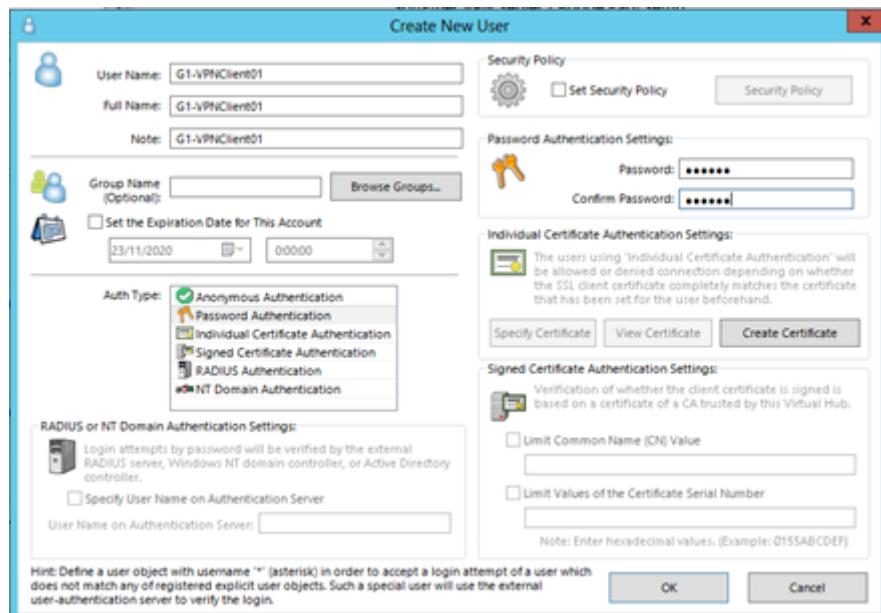


Figure 5.2.15.20 : Set up new user

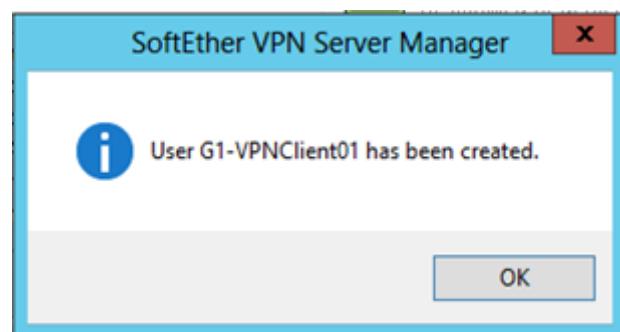


Figure 5.2.15.21 : Confirmation alert of user created

A screenshot of the "Manage Users" window from the SoftEther VPN Server Manager. The title bar says "Manage Users". The main area shows a table with one row of data. The table has columns: User Name, Full Name, Group Name, Description, Auth Method, Num Logins, and Last Login. The data row is:

User Name	Full Name	Group Name	Description	Auth Method	Num Logins	Last Login
G1-VPNClient01	G1-VPNClient01	-	G1-VPNClient01	Password Authe...	0	(None)

At the bottom are buttons for New, Edit, View User Info, Remove, Refresh, and Exit.

Figure 5.2.15.22 : Manage user

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



Figure 5.2.15.23 : Set up local bridge

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

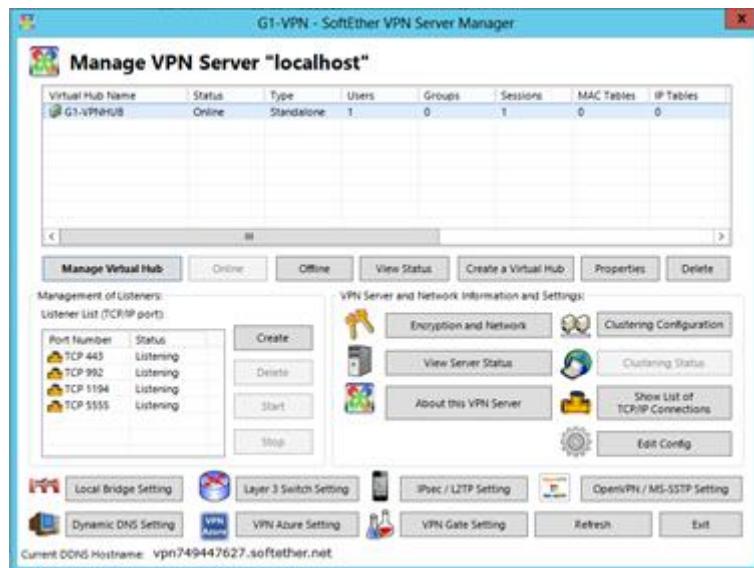


Figure 5.2.16.24: Manage Virtual Hub

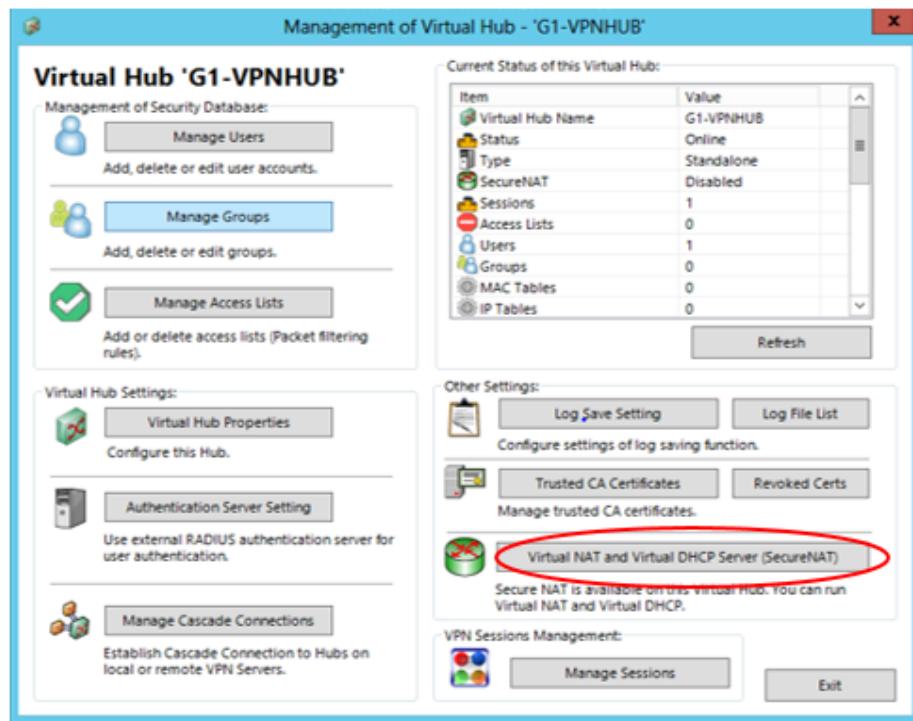


Figure 5.2.15.25: Choose Virtual NAT and Virtual DHCP Server (SecureNAT).

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

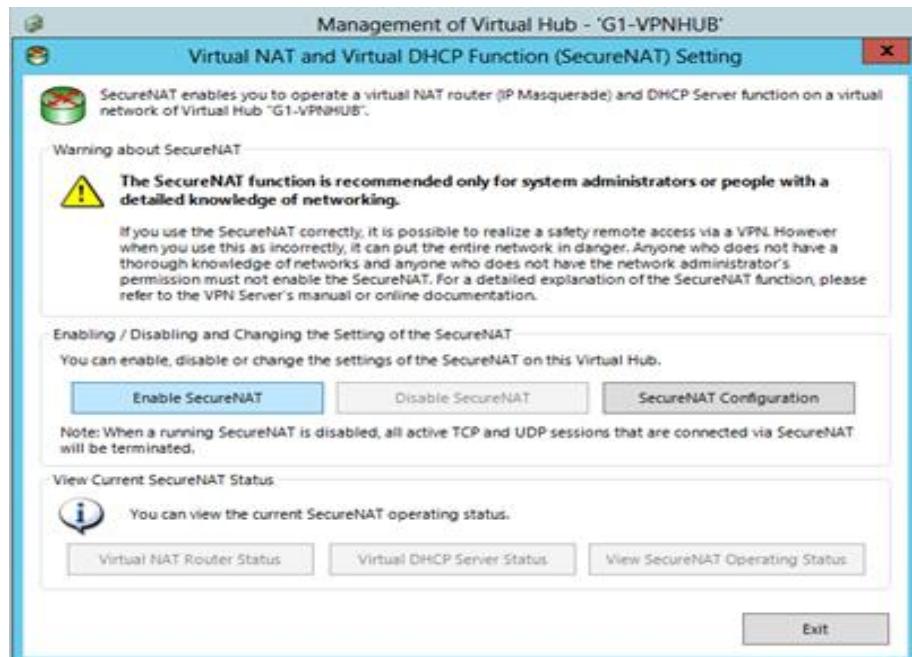


Figure 5.2.15.26: Enable SecueNAT

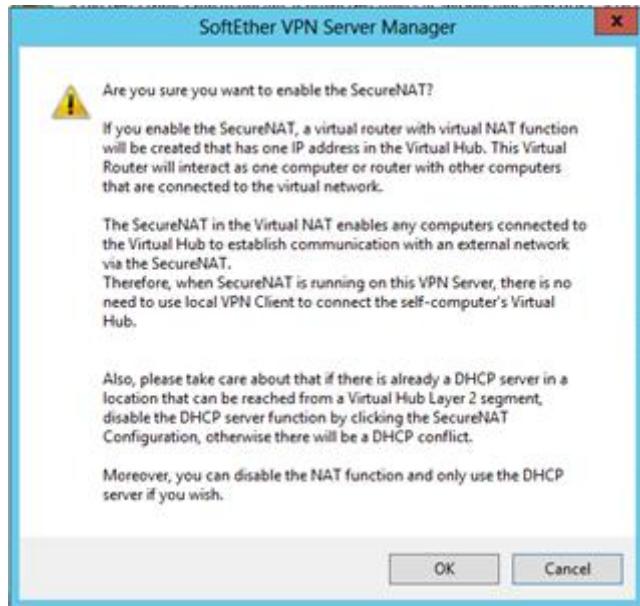


Figure 5.2.15.27: Enable SecureNAT alert

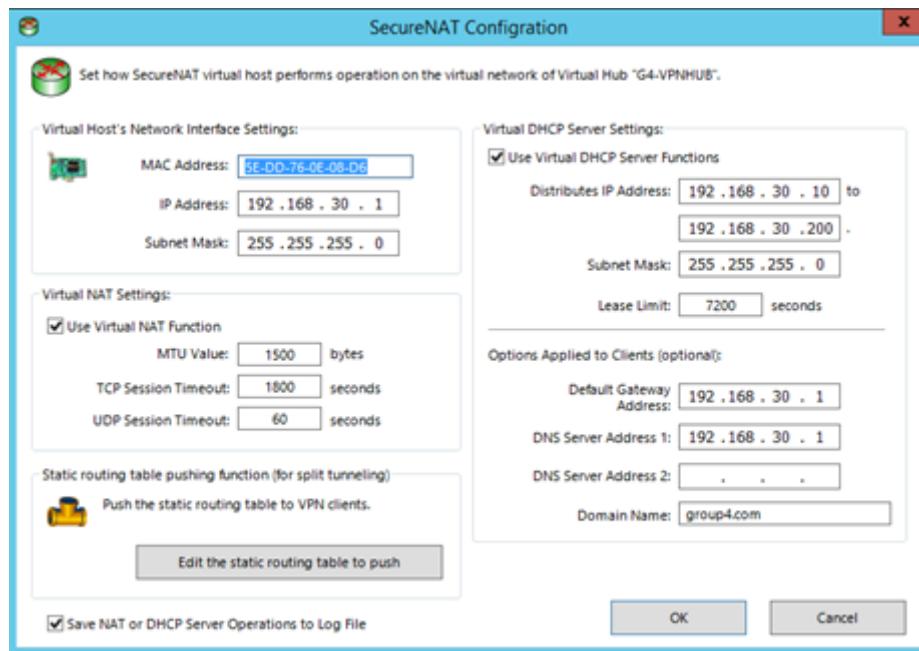


Figure 5.2.15.28: IP address provided by SecureNAT

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

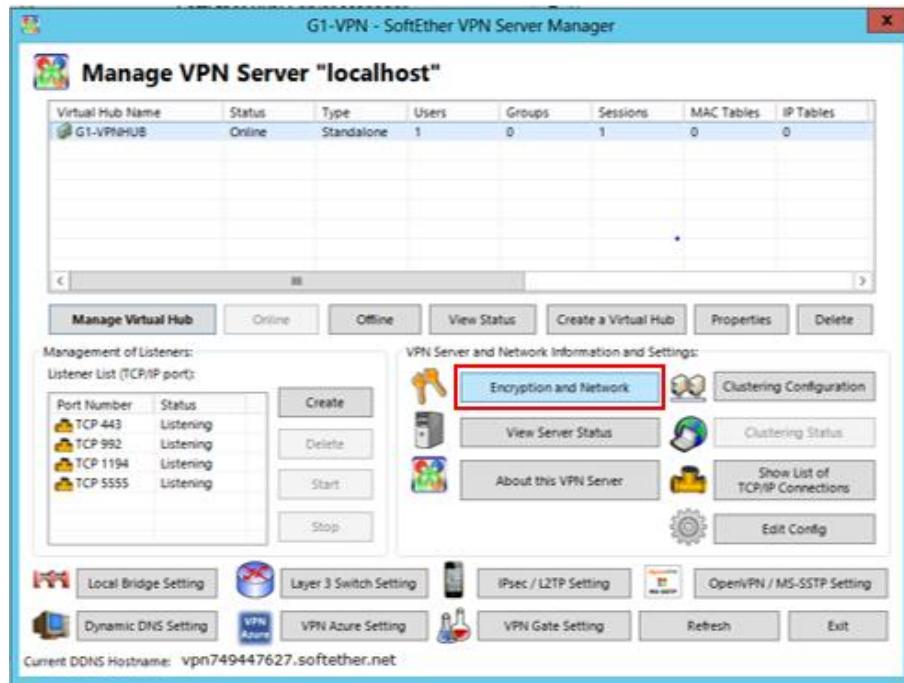


Figure 5.2.15.29 : Select Encryption and Network

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

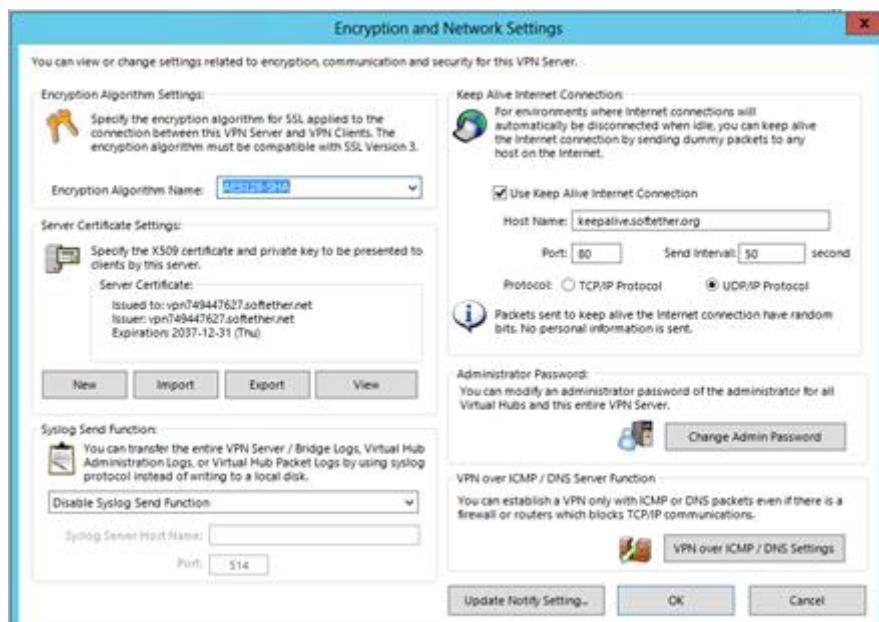


Figure 5.2.15.30 : Modify encryption algorithm name

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



Figure 5.2.15.31 : Select IPsec / L2TP Setting

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

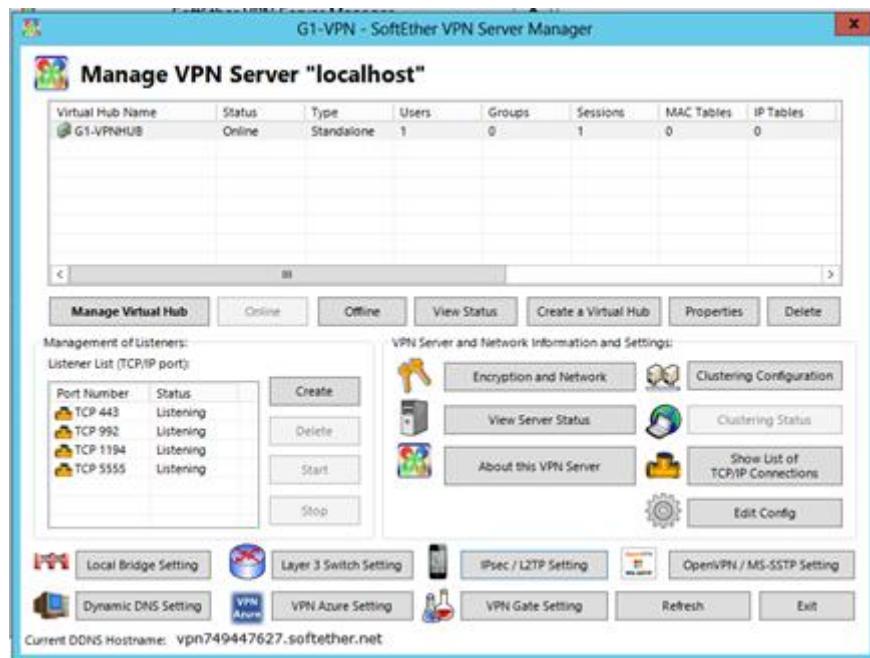


Figure 5.2.15.32 : Virtual Hub is created

SoftEther VPN Client Installation- (It Department and Remote Branch)

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

The screenshot shows the SoftEther VPN Project website. The left sidebar has a 'Download' section highlighted. The main content area is titled 'Download' and contains information about the open-source nature of the software and download links for Windows Azure, CNET Download.com, and Softpedia.com.

University of Tsukuba, Japan.

SoftEther VPN

Top Why SoftEther VPN Documents Download Support About Project

University of Tsukuba, Japan.

SoftEther VPN Project > Download

Download

SoftEther VPN is [open-source free software](#). You may use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of SoftEther VPN.

Primary Download Server (hosted by Windows Azure):

- [Download SoftEther VPN](#)

Language: English, Japanese and Simplified Chinese.
OS: Windows, Linux, Mac OS X, FreeBSD and Solaris.

Download from CNET Download.com:

- [Download SoftEther VPN from CNET Download.com](#)

Download from Softpedia.com:

- [Download SoftEther VPN from Softpedia.com](#)

Figure 5.2.15.33: Go to website and click download

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

The screenshot shows the 'Download' page on the SoftEther VPN website. It features the same layout as the previous screenshot, with sections for Windows Azure download, CNET Download.com, and Softpedia.com.

Download

SoftEther VPN is [open-source free software](#). You may use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of SoftEther VPN.

Primary Download Server (hosted by Windows Azure):

- [Download SoftEther VPN](#)

Language: English, Japanese and Simplified Chinese.
OS: Windows, Linux, Mac OS X, FreeBSD and Solaris.

Download from CNET Download.com:

- [Download SoftEther VPN from CNET Download.com](#)

Download from Softpedia.com:

- [Download SoftEther VPN from Softpedia.com](#)

Figure 5.2.15.34 : Download SoftEther VPN

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

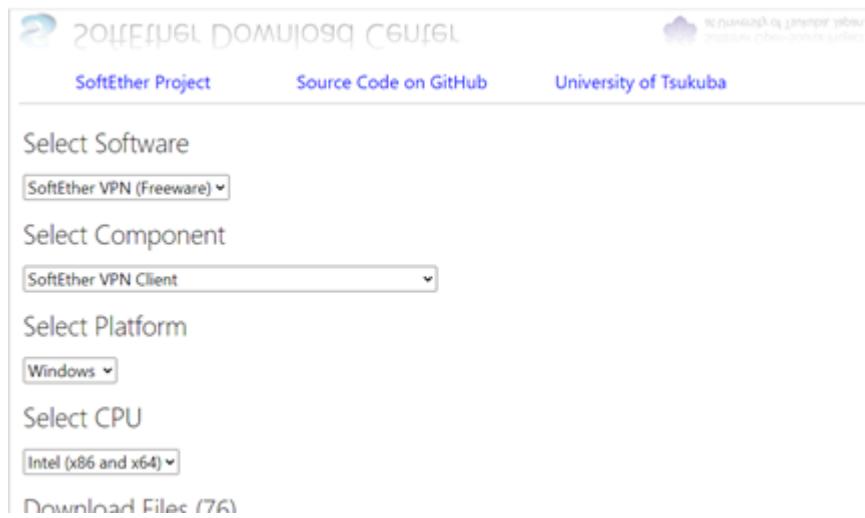


Figure 5.2.15.35 : Choose requirement

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

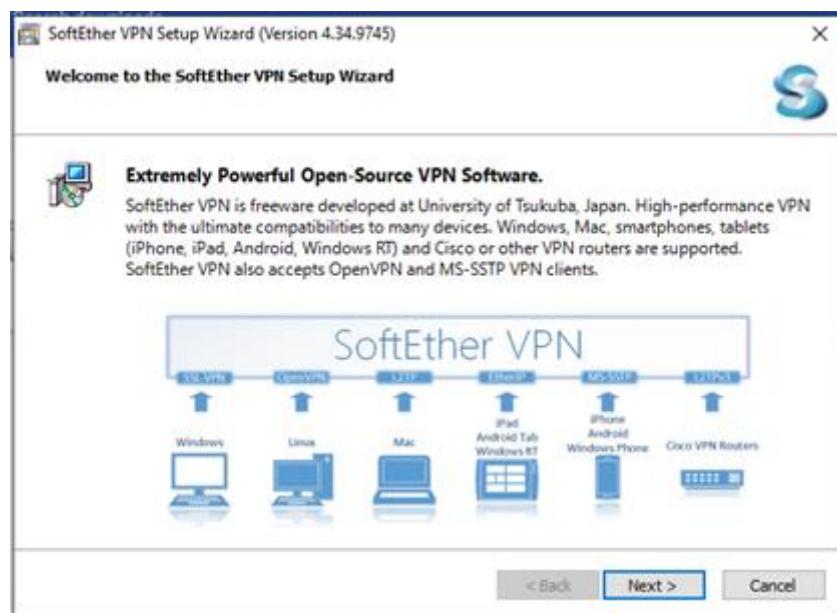


Figure 5.2.15.36 : Download section

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

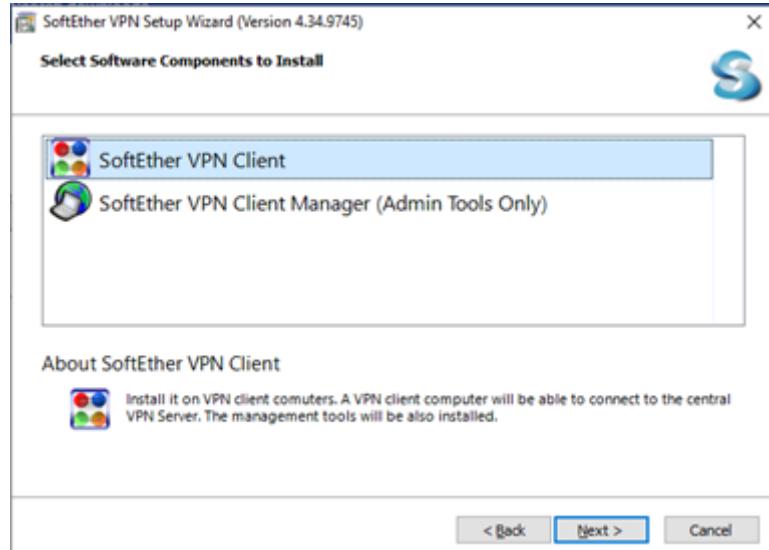


Figure 5.2.15.37 : Choose software component to install

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

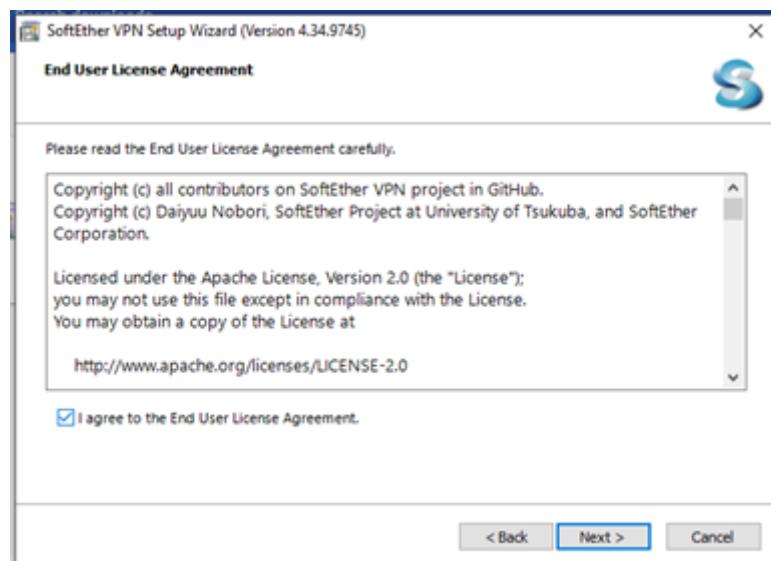


Figure 5.2.15.38 : Agree to End User Agreement

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

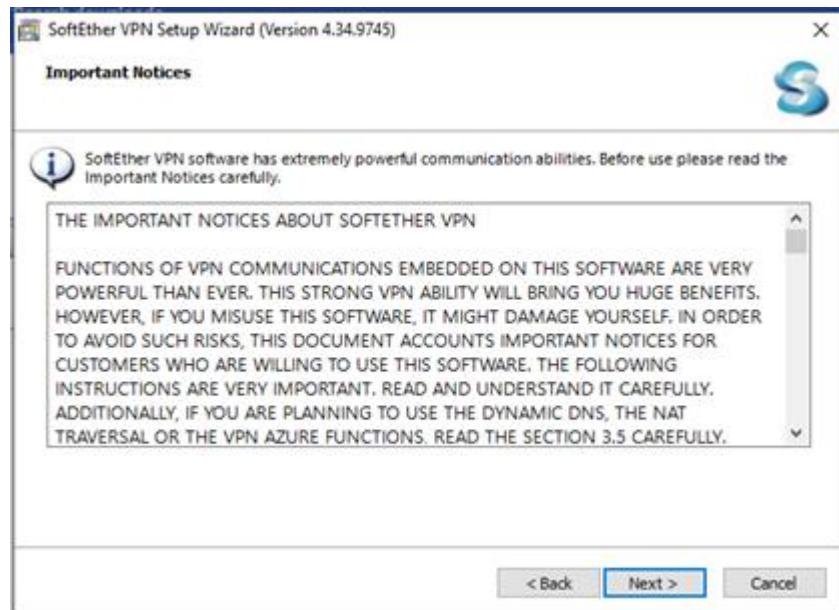


Figure 5.2.15.39 : Important Notice

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

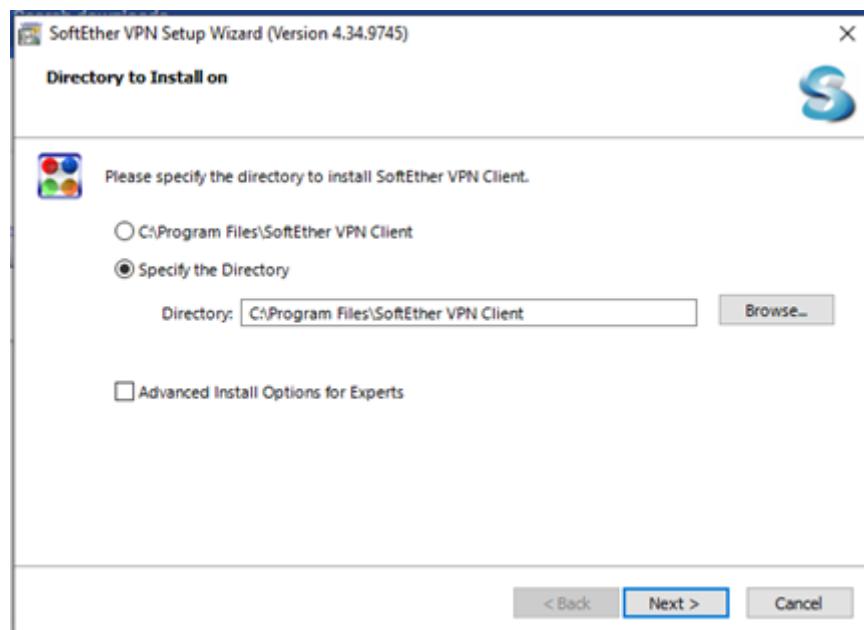


Figure 5.2.15.40 : Path Selection

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

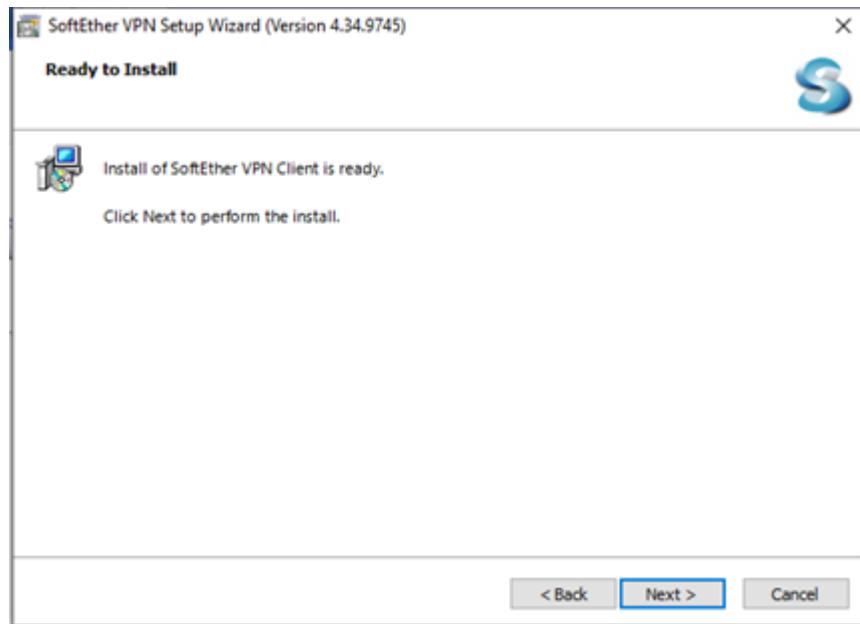


Figure 5.2.15.41 : Wait for installation

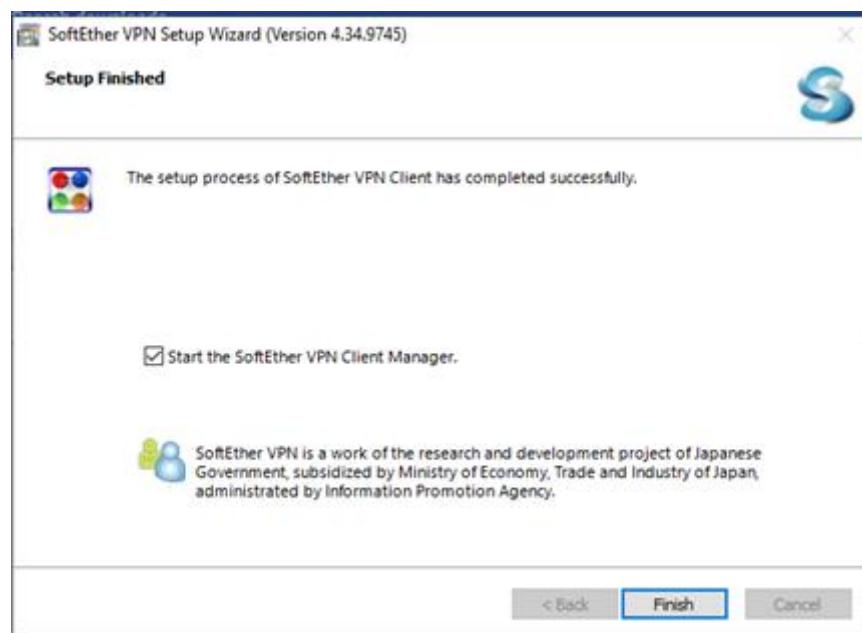


Figure 5.2.15.42 : Finish installation

Configuration of SoftEther VPN Client (IT Department)

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

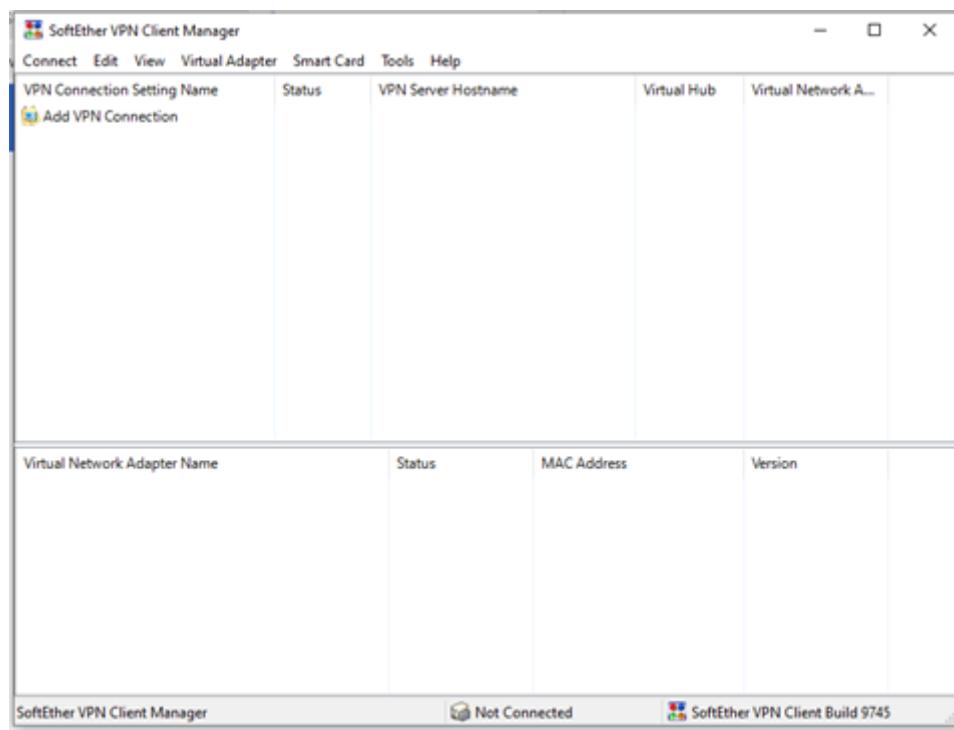


Figure 5.2.15.43 : GUI of SoftEther VPN Client Manager



Figure 5.2.15.44 : Create new Virtual Network Adapter

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



Figure 5.2.15.45 : Set up Virtual Network Adapter name

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

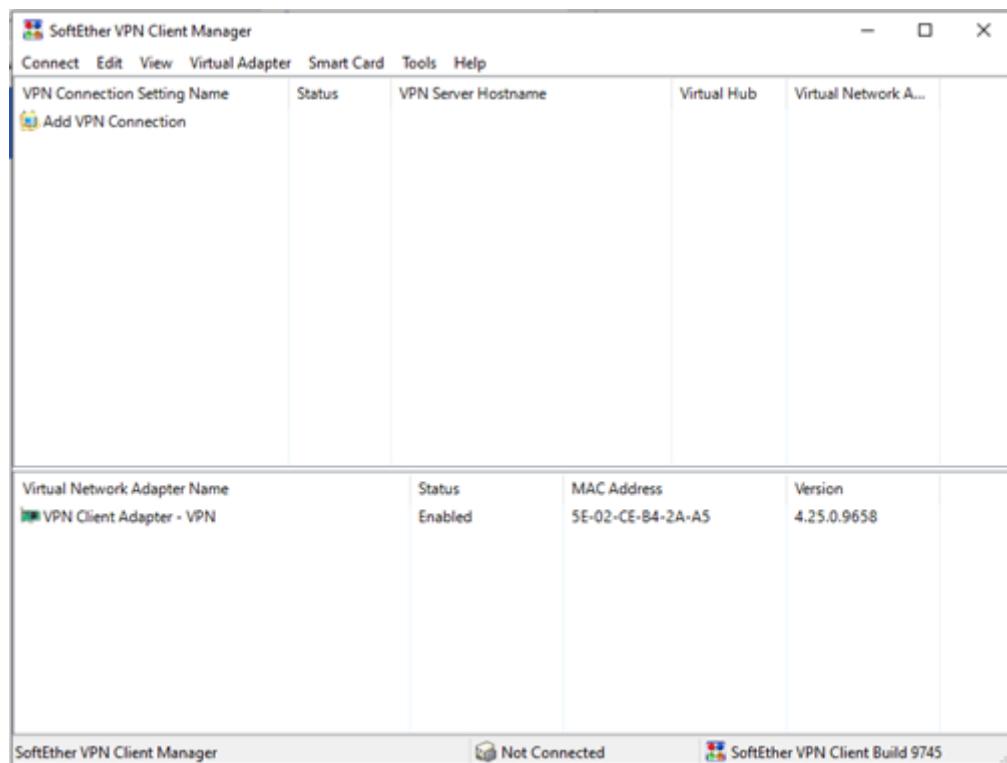


Figure 5.2.15.46 : New virtual network adapter

Step 4: Next, select Add VPN Connection again, a New VPN Connection Setting Properties window will pop out. Change the Setting Name as (G1-VPNConnect), Host Name as < SoftEther VPN Server IP Address >, Port 5555 and Virtual Hub name as (G1-VPNHUB). On User Authentication Settings, change Auth Type to Standard Password Authentication and insert the username (G1-VPNCClient01) and password (Windows12345) that want to be login. Lastly, click the OK button.

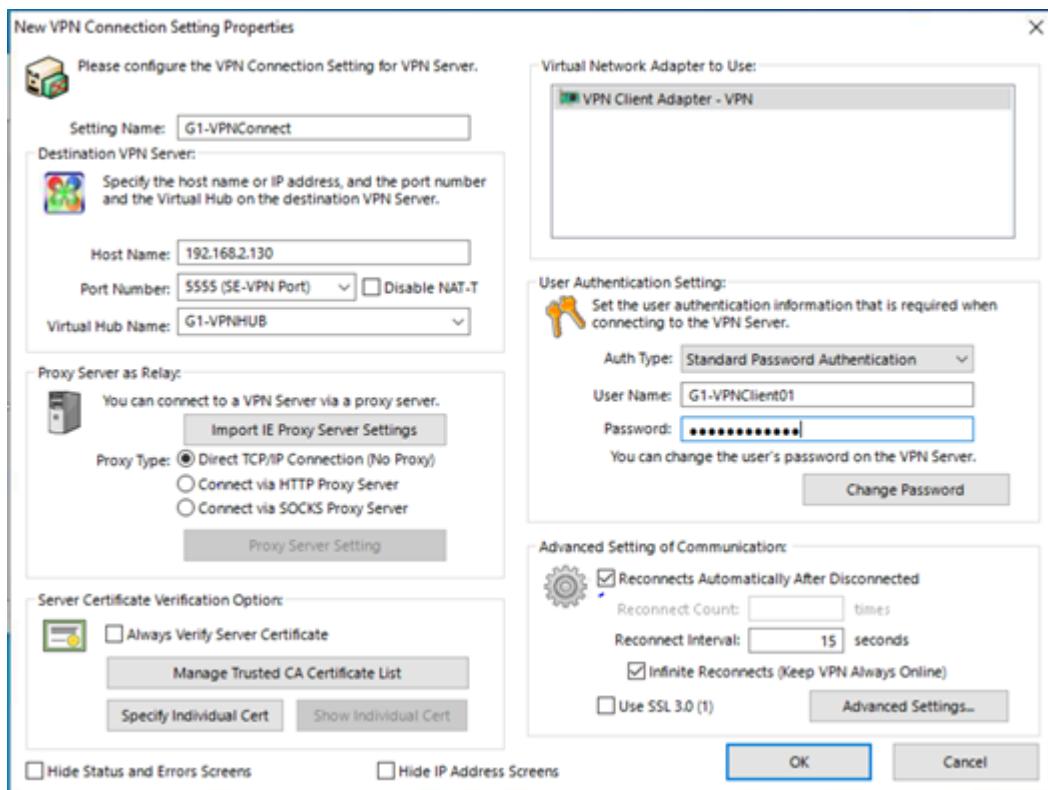


Figure 5.2.15.47 : Set up VPN Connection

Step 5 : Success to create a New VPN Connection.

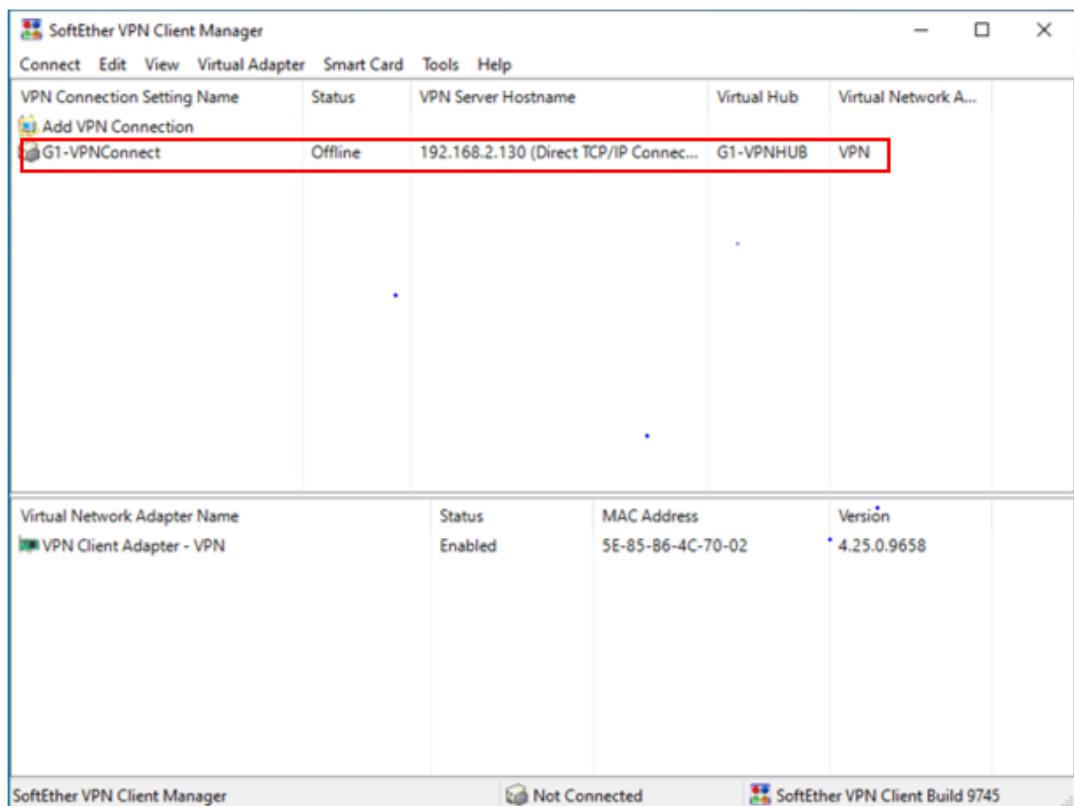


Figure 5.2.15.48 : VPN Connection created

Configuration of SoftEther VPN Client (Remote Access)

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

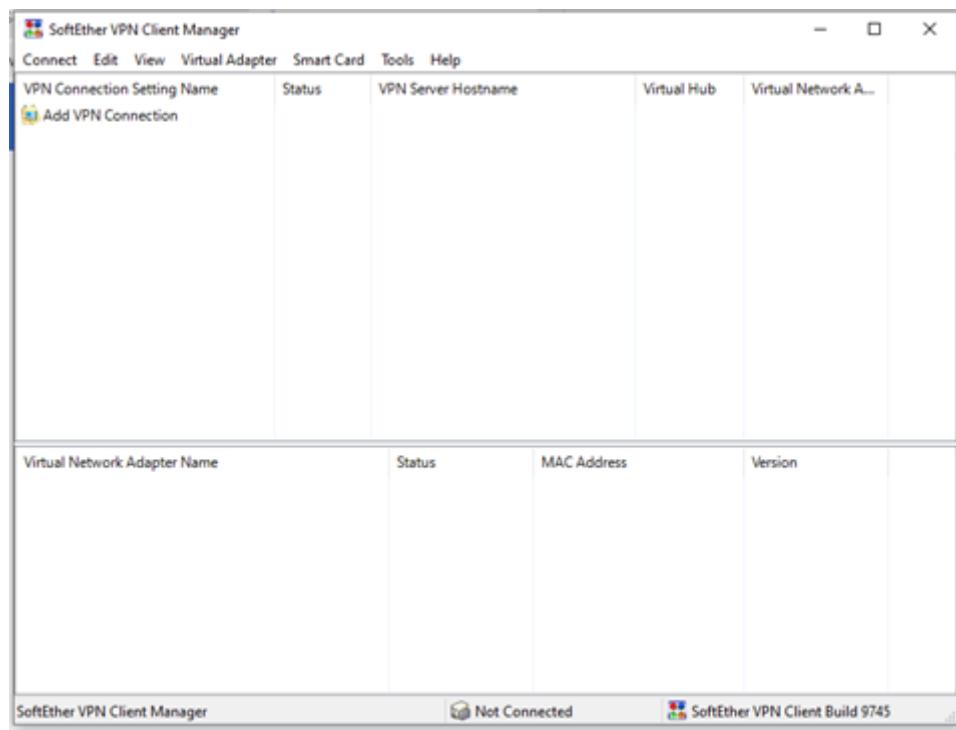


Figure 5.2.15.49 : GUI of SoftEther VPN Client Manager

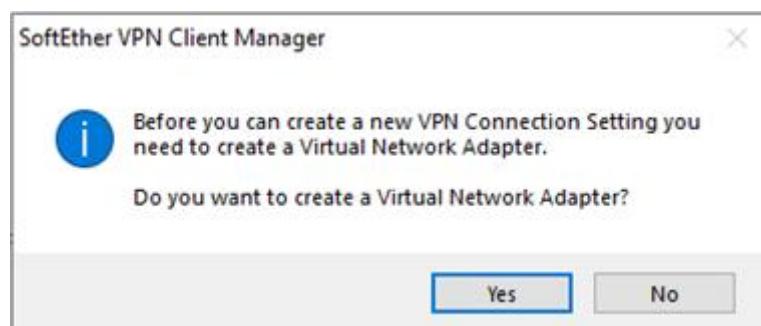


Figure 5.2.15.52 : Create new Virtual Network Adapter

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



Figure 5.2.15.50 : Set up Virtual Network Adapter name

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

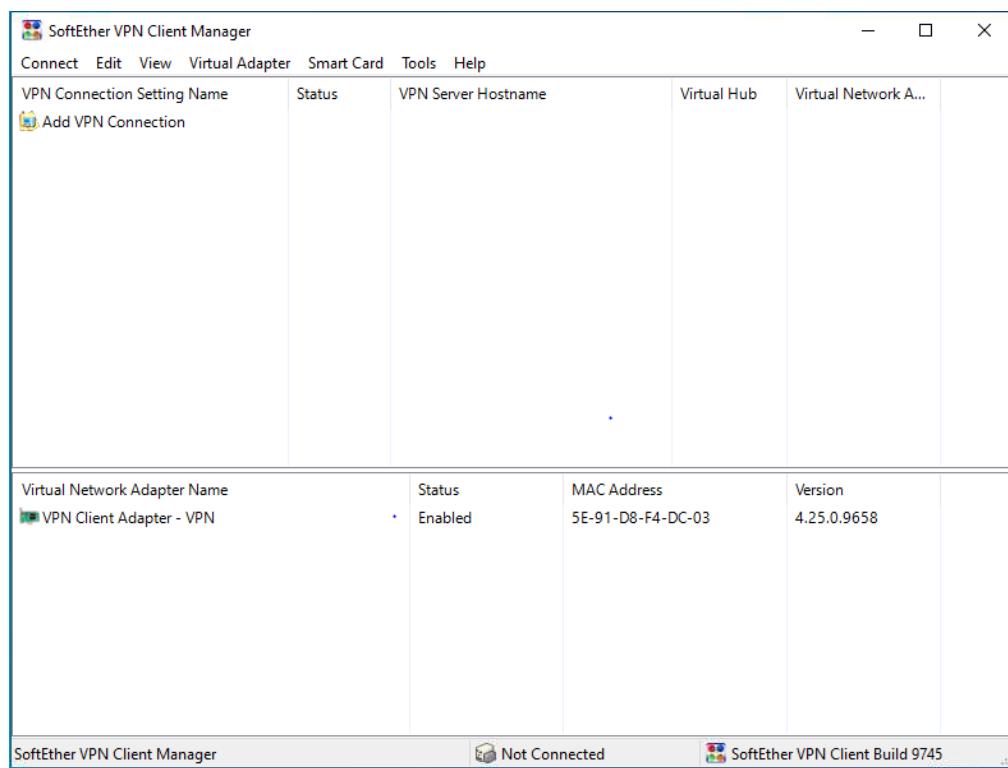


Figure 5.2.15.51 : New virtual network adapter

Step 4: Next, select Add VPN Connection again, a New VPN Connection Setting Properties window will pop out. Change the Setting Name as (G1-VPNConnect), Host Name as < SoftEther VPN Server IP Address >, Port 5555 and Virtual Hub name as (G1-VPNHUB). On User Authentication Settings, change Auth Type to Standard Password Authentication and insert the username (G1-VPNClient01) and password (Windows12345) that want to be login. Lastly, click the OK button.

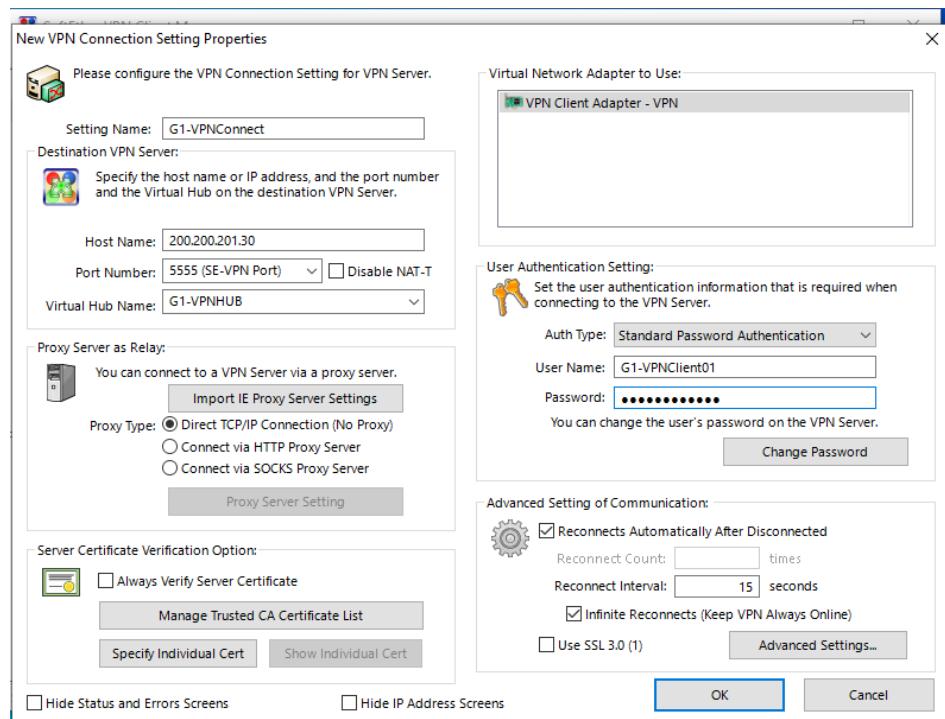


Figure 5.2.15.52 : Set up VPN Connection

Step 5 : Success to create a New VPN Connection.

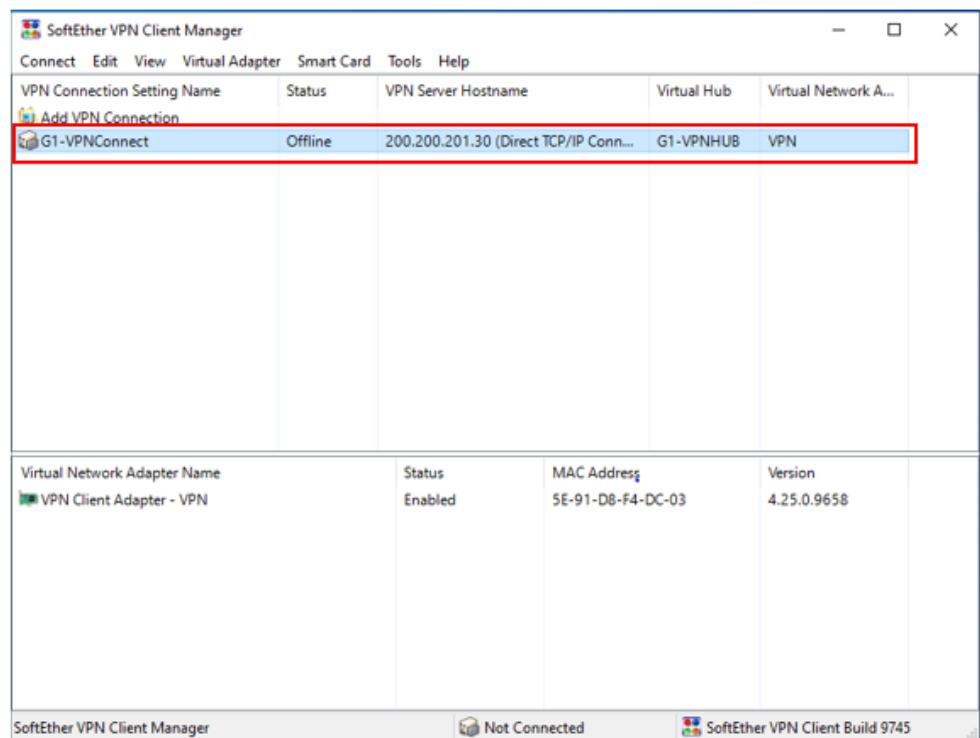


Figure 5.2.15.53 : VPN Connection created

5.2.16. Windows Server Hardening and Vulnerability Report

1. Configure Audit Policy

Step1 : Open Local Security Policy

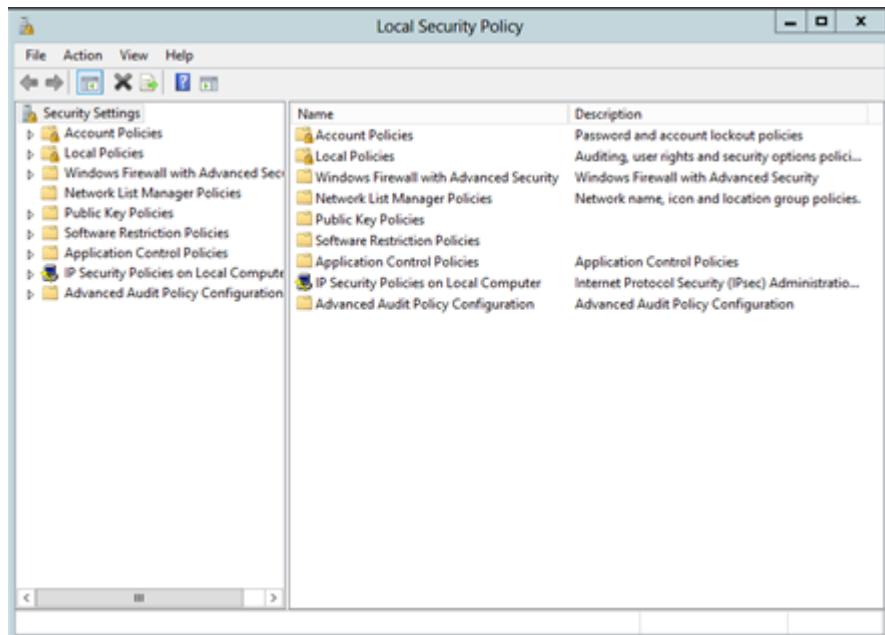


Figure 5.2.16.1 Local Security Policy

Step 2 : Check if the “Audit privilege use” has changed or not. If not, double-click

on the policy and change the setting.

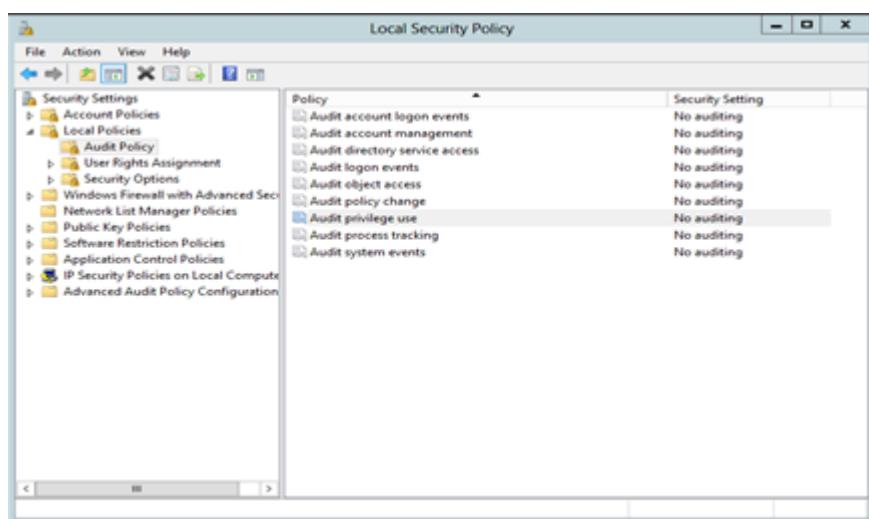


Figure 5.2.16.2 Audit privilege use

Step 3 : Tick on both **Success** and **Failure**. Then, click **Apply** and **OK**.

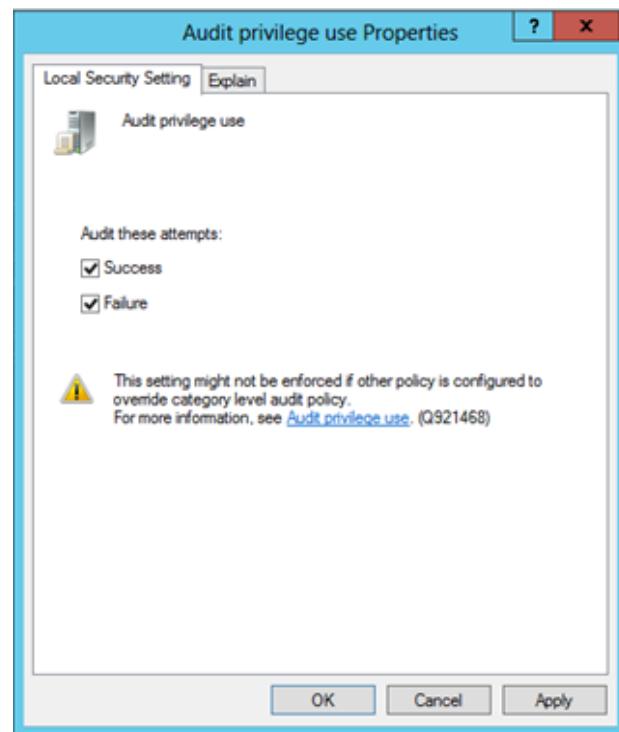


Figure 5.2.16.3 Audit privilege use Properties

Step 4 : All necessary security setting have been configured.

The screenshot shows the 'Local Security Policy' snap-in. The left pane displays a tree view of security settings, including 'Security Settings', 'Account Policies', 'Local Policies' (with 'Audit Policy' selected), 'Use Rights Assignment', 'Security Options', 'Windows Firewall with Advanced Sec...', 'Network List Manager Policies', 'Public Key Policies', 'Software Restriction Policies', 'Application Control Policies', 'IP Security Policies on Local Computer', and 'Advanced Audit Policy Configuration'. The right pane lists audit policies with their current security settings:

Policy	Security Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	Success, Failure
Audit process tracking	No auditing
Audit system events	No auditing

Figure 5.2.16.4 Audit Policy use - Success, Failure

2. Configure BitLocker Drive Encryption

Step 1 : Open **Server Manager**. Click **Features** and **Add Features**. Then, **Add Roles and Features Wizard** will appear. After that, click **Next** button.

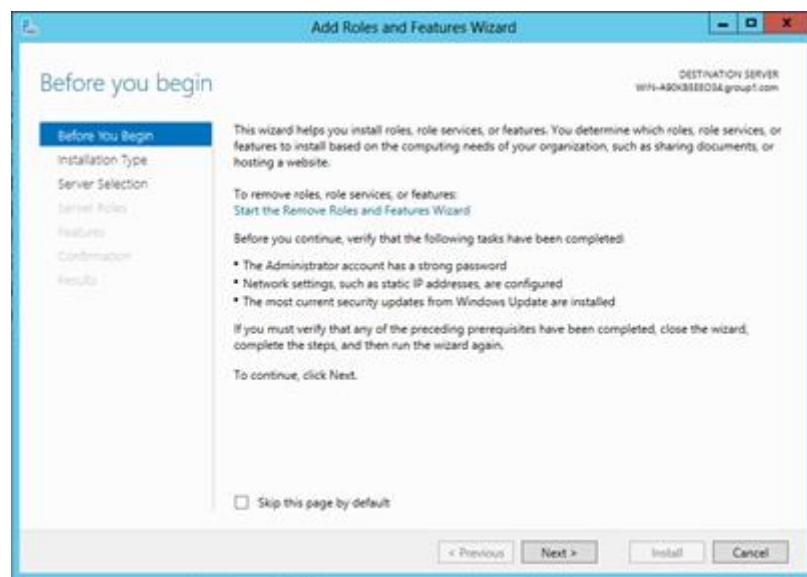


Figure 5.2.16.5 Add Roles and Features Wizard

Step 2: Then, install **BitLocker Drive Encryption** by click **Install** button.



Figure 5.2.16.6 Confirm installation selections

Step 4 : Finish installation and restart the server.

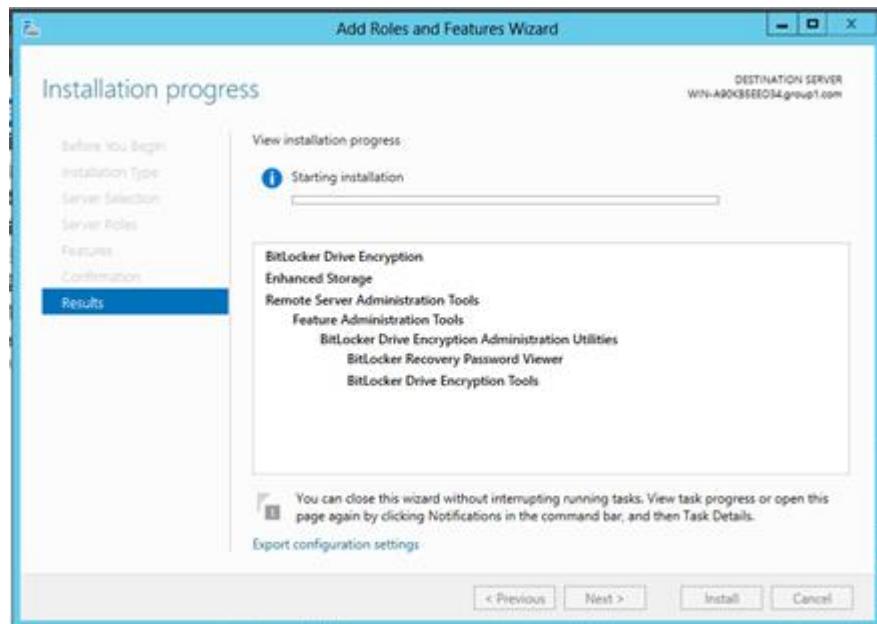


Figure 5.2.16.7 Installation progress

3. Configure Windows Firewall

Step 1 : Open Windows Firewall with Advanced Security.

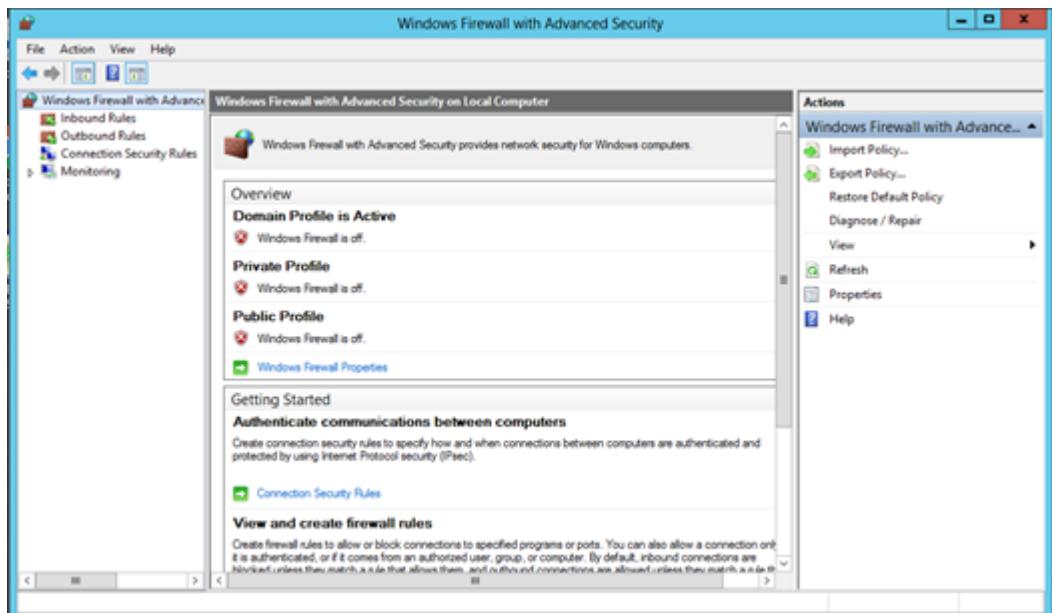


Figure 5.2.16.8 Windows Firewall with Advanced Security

Step 2 : On **Firewall state**, block **Inbound connections** and allow **Outbound connection**.

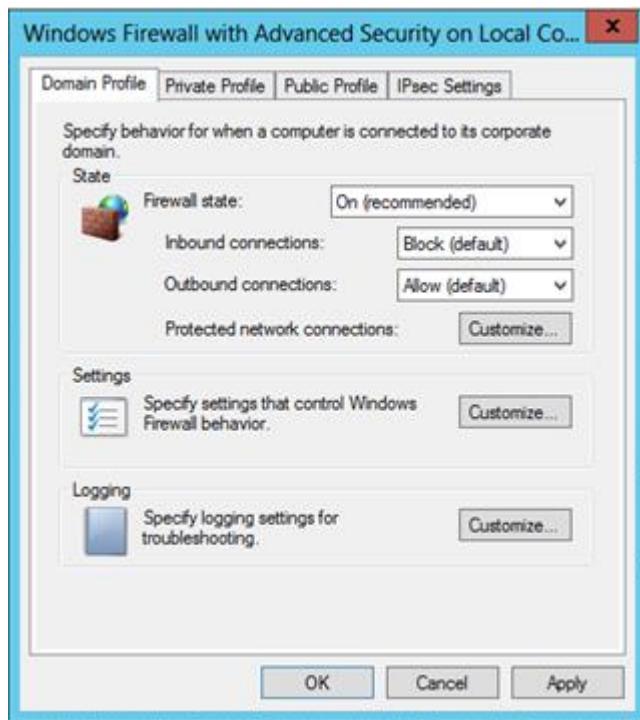


Figure 5.2.16.9 Domain Profile

Step 3 : Firewall overview after enabling.



Figure 5.2.16.10 Windows Firewall with Advanced Security after enabling

4. Disable Automatic

Step 1 : Press the *Win + R* keys on your keyboard, to open the Run window. Then, type “*services.msc*” and hit Enter or press *OK*.

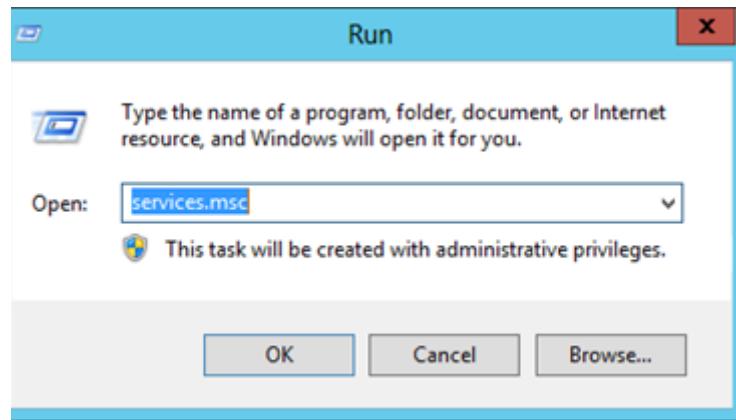


Figure 5.2.16.11 services.msc

Step 2 : Inspect the list of services available and double-click on unnecessary services. Firstly, double click on **Print Spooler** services. Then, change the Startup type from “Automatic” to “Disabled”.

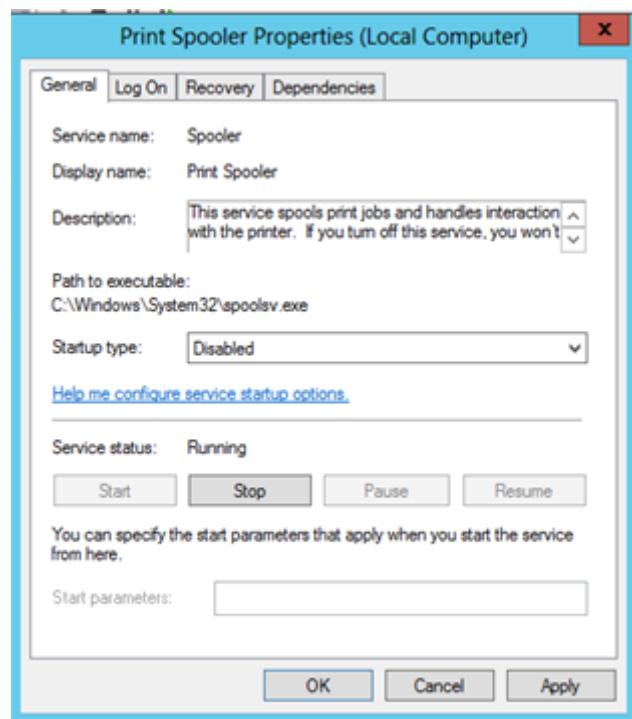


Figure 5.2.16.12 Print Spooler Properties

Step 3 : Next, double click on **Distributed Transaction Coordinator**. Change **Startup type** from “Automatic” to “Disabled”.

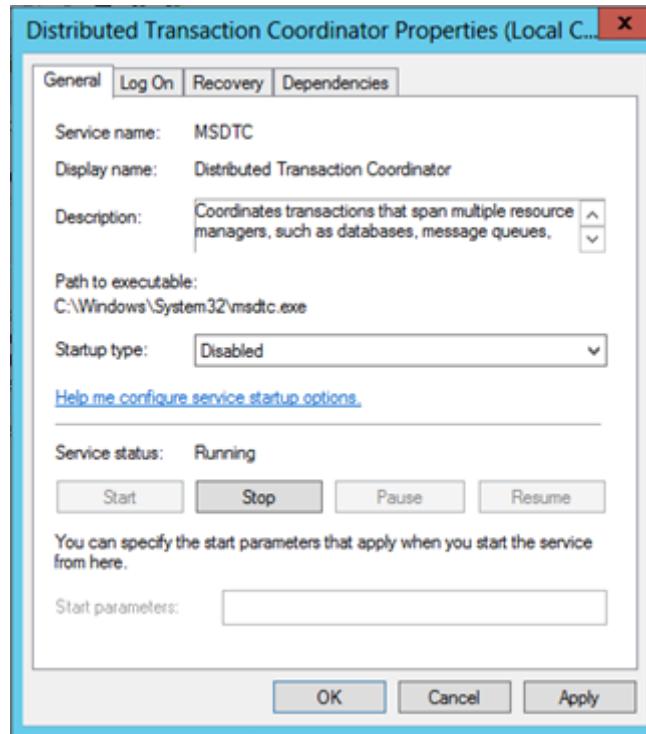


Figure 5.2.16.13 Distributed Transaction Coordinator

5. Windows Error Reporting

Step 1 : Press the *Win + R* keys on your keyboard, to open the Run window. Then, type “*services.msc*” and hit Enter or press *OK*.

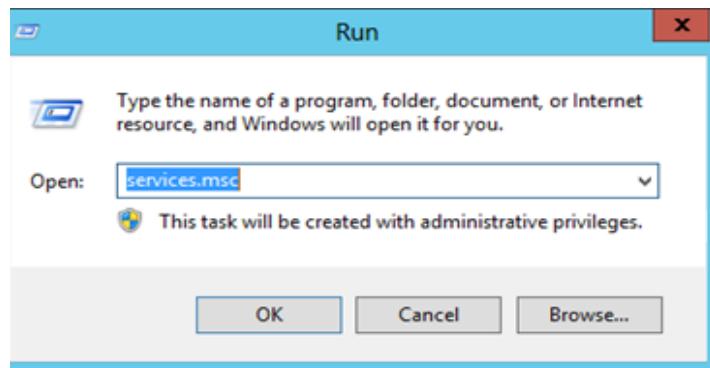


Figure 5.2.16.14 services.msc

Step 2 : Change the **Windows Error Reporting Service** for **Startup type** to “**Automatic**”.

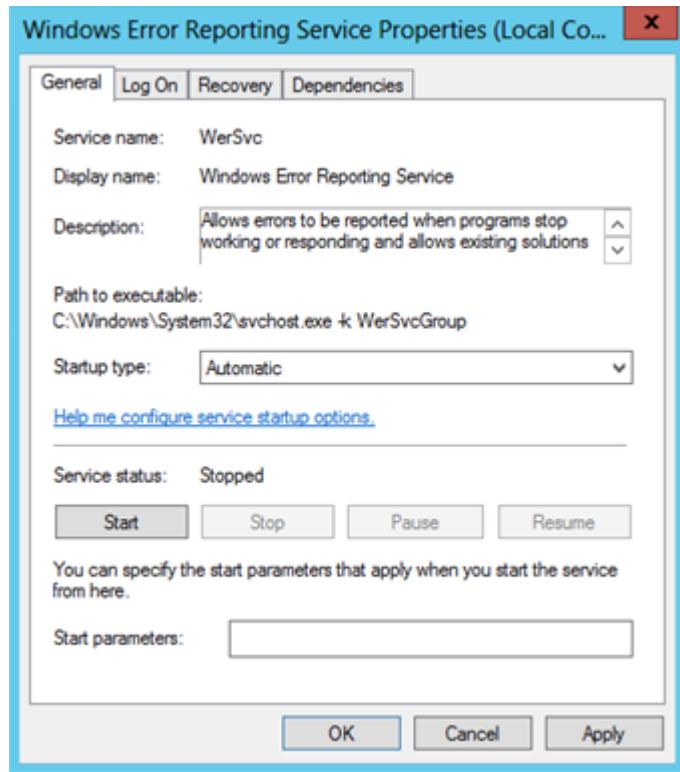


Figure 5.2.16.15 Windows Error Reporting Service

6. Secure Socket Tunneling Protocol

Step 1 : Press the *Win + R* keys on your keyboard, to open the Run window. Then, type “*services.msc*” and hit Enter or press *OK*.

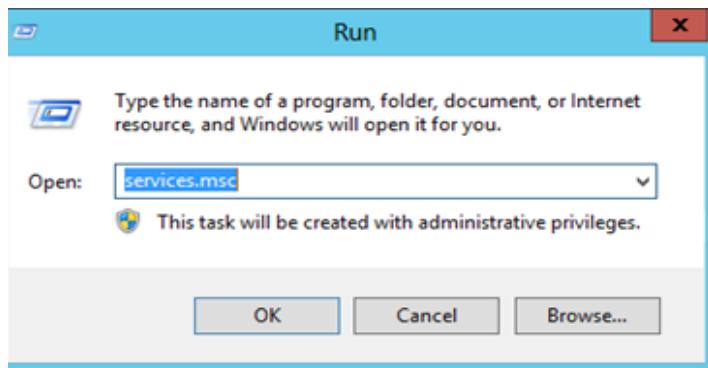


Figure 5.2.16.16 services.msc

Step 2 : Change the **Startup type** from “**Manual**” to “**Automatic**” for **Secure Socket Tunneling Protocol Service**.

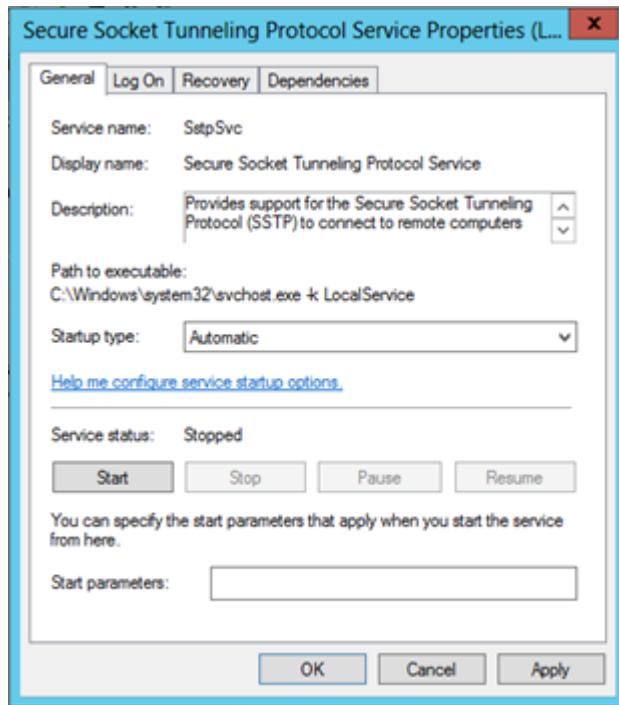


Figure 5.2.16.17 Secure Socket Tunneling Protocol Service

7. NetLogon Service

Step 1 : Press the *Win + R* keys on your keyboard, to open the Run window. Then, type “*services.msc*” and hit Enter or press *OK*.

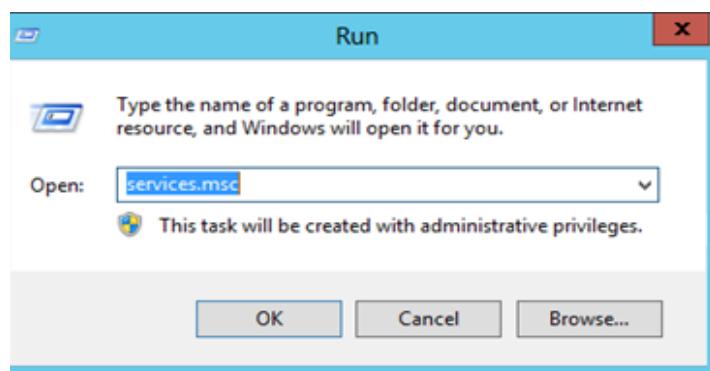


Figure 5.2.16.18 services.msc

Step 2 : Ensure NetLogon startup type is Automatic and started.

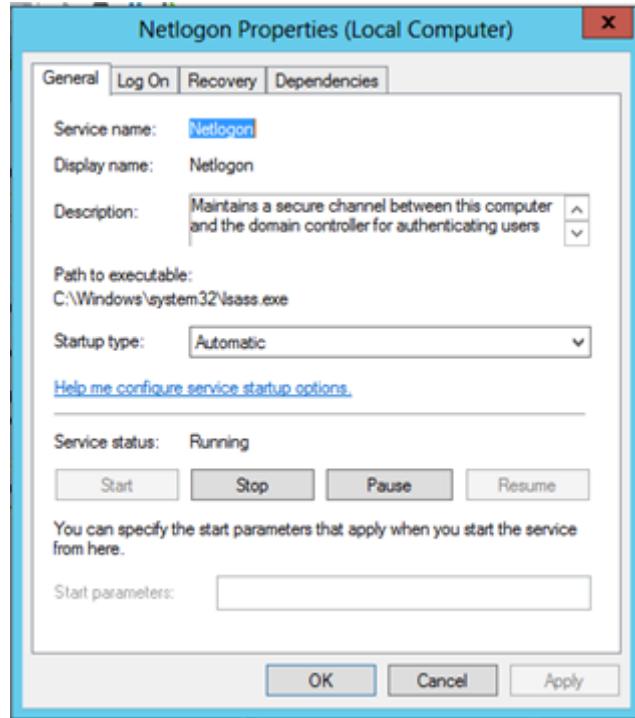


Figure 5.2.16.19 NetLogon Properties

8. Configure Security Configuration Wizard

Step 1: Configure a security policy. First search Security Configuration Wizard in the search box and click on it. Then, the **Security Configuration Wizard** will be appeared as below. To continue, click **Next**.



Figure 5.2.16.20 Welcome to the Security Configuration Wizard

Step 2 : Next, choose “Create a new security policy” and click Next.



Figure 5.2.16.21 Configuration Action

Step 3 : Enter server name and click **Next**



Figure 5.2.16.22 Select Server

Step 4 : Wait for processing to complete and click **Next**. Then, start for **Role-Based Service Configuration**.



Figure 5.2.16.23 Processing Security Configuration Database

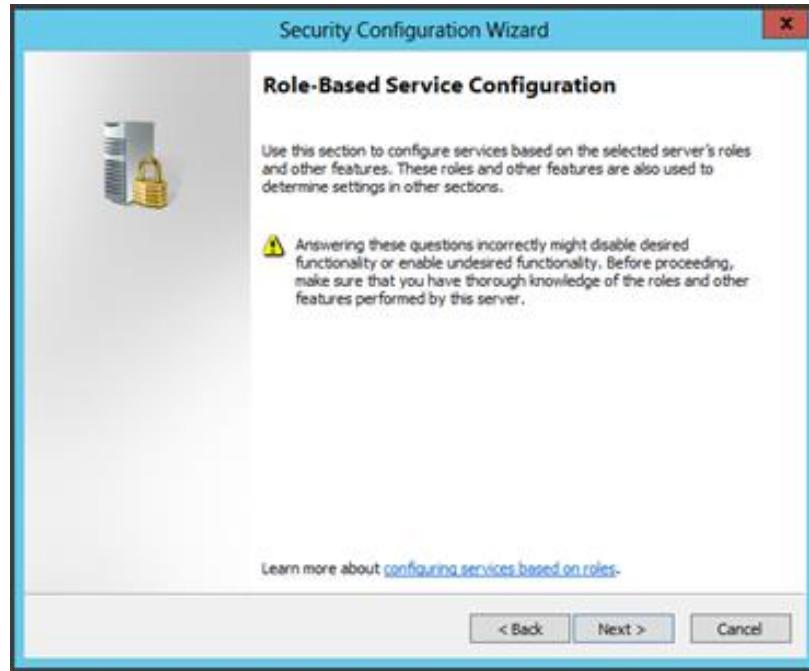


Figure 5.2.16.24 Role-Based Service Configuration

Step 5 : After that, for **Select Server Roles**, we select the necessary server roles that the selected server performs and click **Next**.

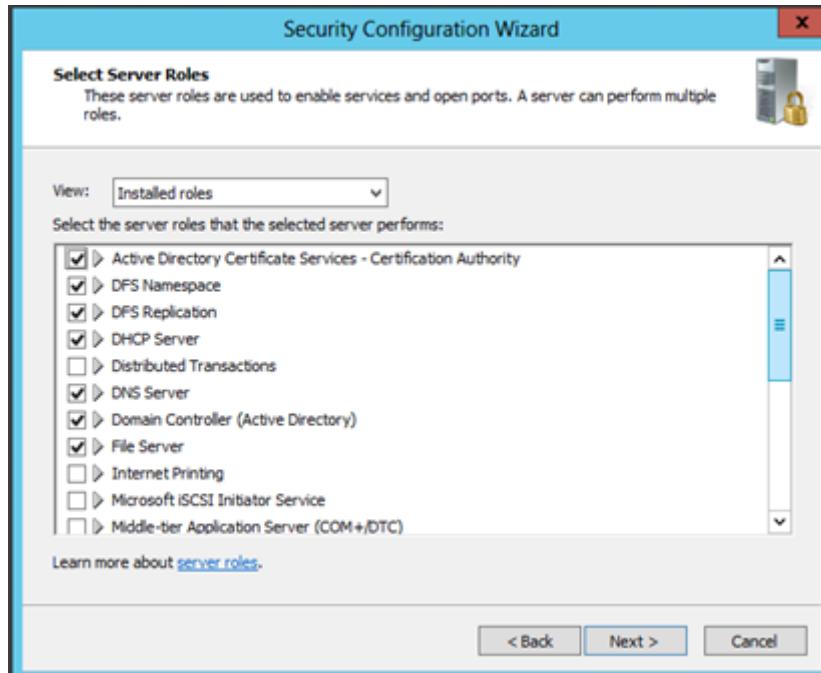


Figure 5.2.16.25 Select Server Roles

Step 6 : For **Select Client Features**, we select the necessary client features that the selected server performs and click **Next**.

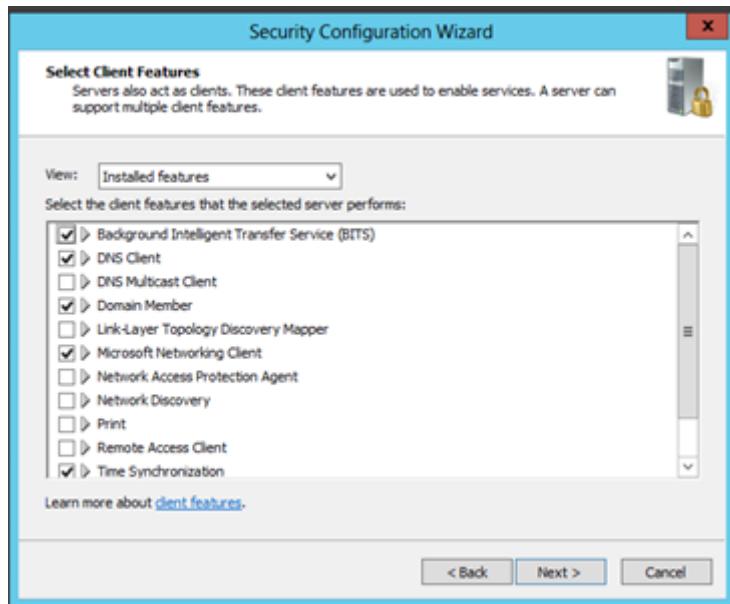


Figure 5.2.16.26 Select Client Features

Step 7 : Next, for **Select Administration and Other Options**, we select the necessary options used to administrate the selected server and click **Next**.

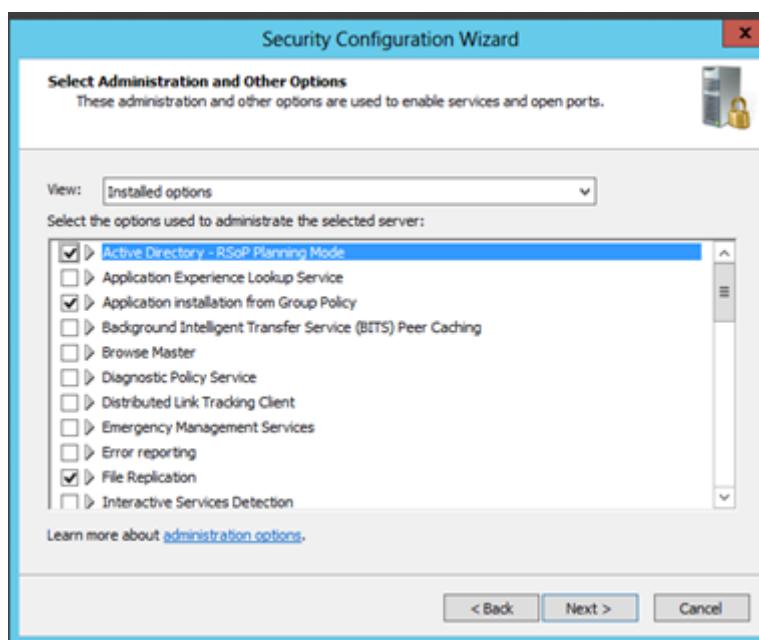


Figure 5.2.16.27 Select Administration and Other Options

Step 8 : Then, tick on “**Do not change the startup mode of the service**” and click **Next**.



Figure 5.2.16.28 Handling Unspecified Services

Step 9 : Confirm the service changes and click **Next**.

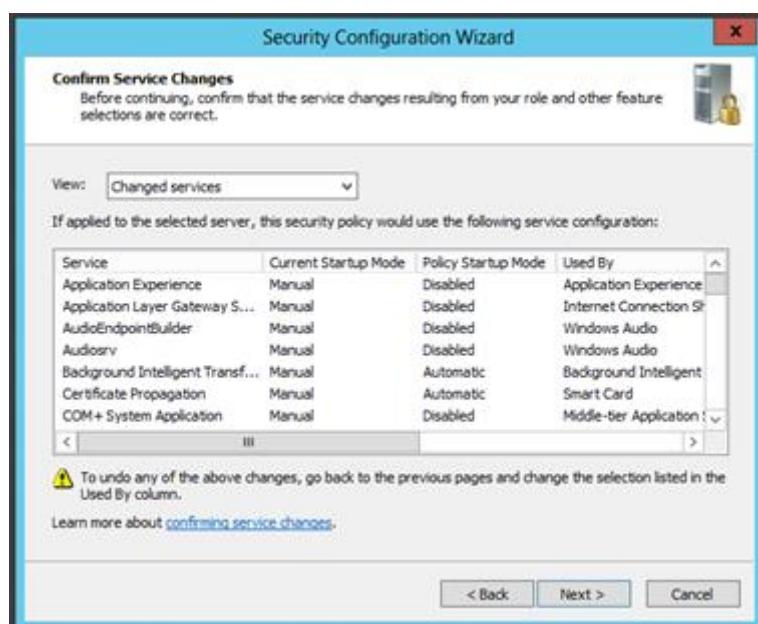


Figure 5.2.16.29 Confirm Service Changes

Step 10 : Next, to configure **Network Security**, click **Next** button.



Figure 5.2.16.30 Network Security

Step 11 : Select necessary network security rules and click **Next**.

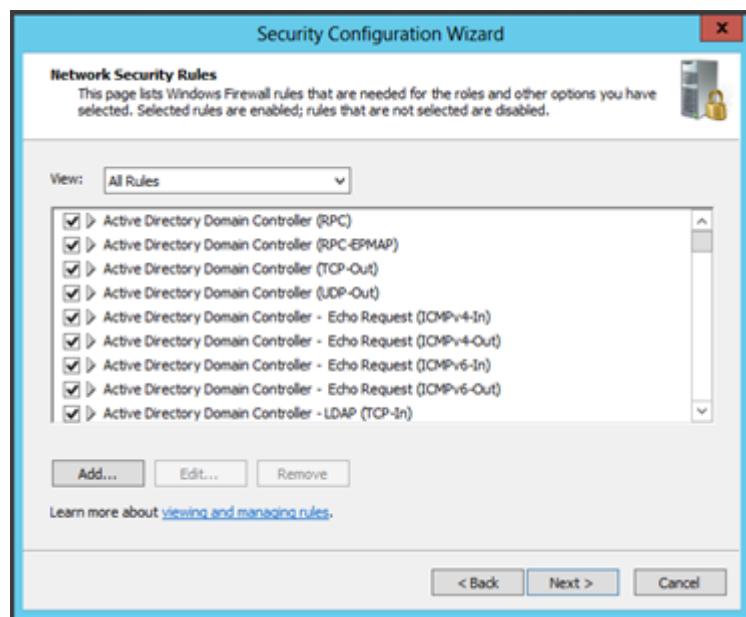


Figure 5.2.16.31 Network Security Rules

Step 12 : Then, to configure **Registry Setting**, click **Next** button.



Figure 5.2.16.32 Registry Settings

Step 13 : For **Require SMB Security Signatures**, the following information determines whether Server Message Block (SMB) security signatures are enabled or required. Then, click **Next**.



Figure 5.2.16.33 Require SMB Security Signatures

Step 14 : For **Outbound Authentication Method**, choose “**Domain Account**” and click Next.



Figure 5.2.16.34 Outbound Authentication Methods

Step 15 : For **Outbound Authentication using Domain Accounts**, choose “**Windows NT 4.0 Service Pack 6a or later operating systems**” and click Next.

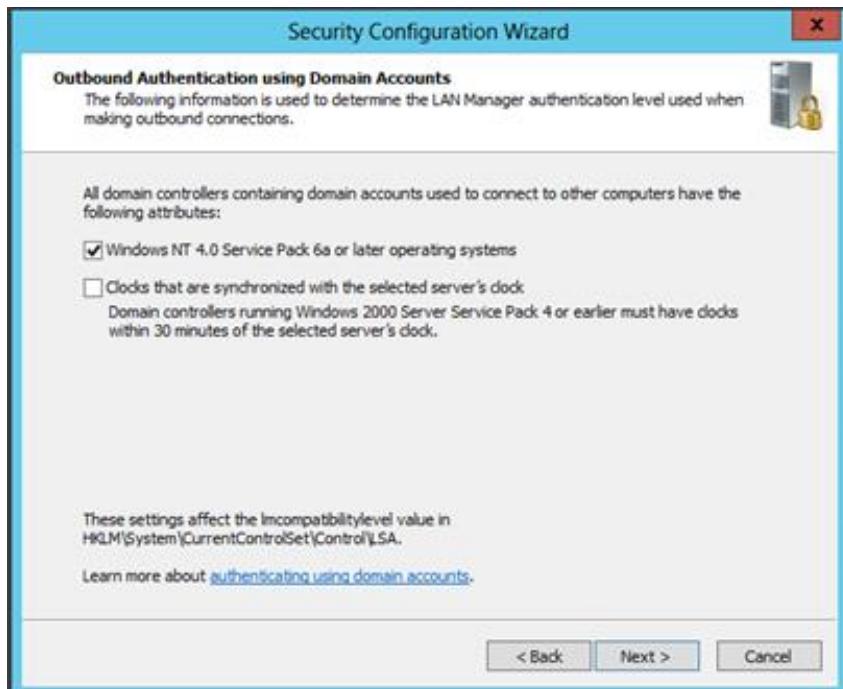


Figure 5.2.16.35 Outbound Authentication using Domain Accounts

Step 16 : After that, confirm the **Registry Settings Summary**.

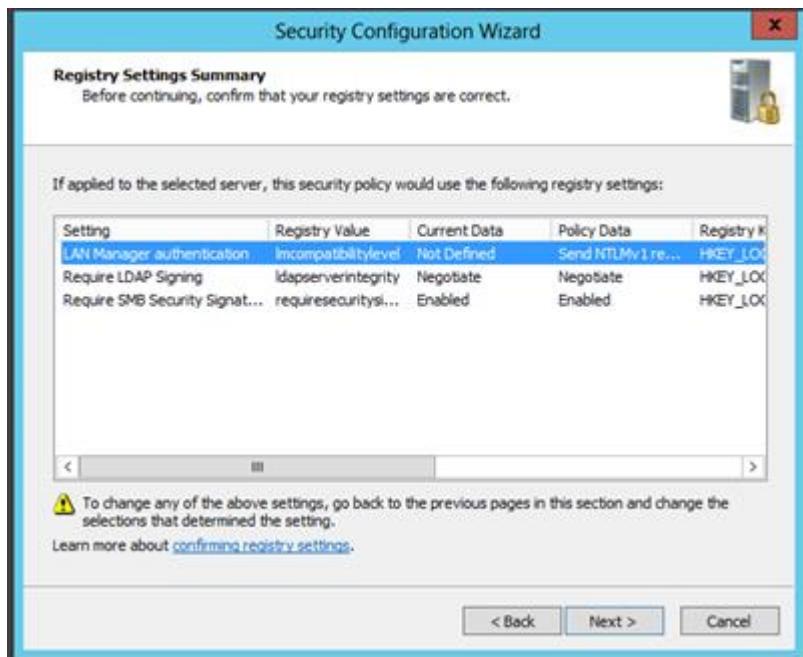


Figure 5.2.16.36 Registry Settings Summary

Step 17 : To configure **Audit Policy**, click **Next**.



Figure 5.2.16.37 Audit Policy

Step 18 : For **System Audit Policy**, select “**Audit successful and unsuccessful activities**” and click **Next**.



Figure 5.2.16.38 System Audit Policy

Step 19 : After that, check the **Audit Policy Summary** and click **Next**.



Figure 5.2.16.39 Audit Policy Summary

Step 20 : To save security policy, click **Next**.

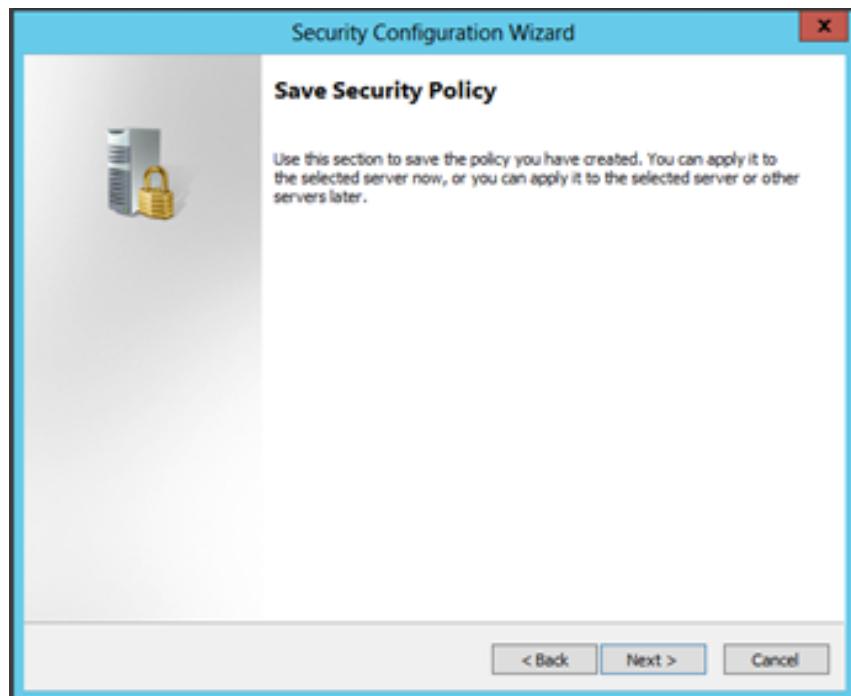


Figure 5.2.16.40 Save Security Policy

Step 21 : For **Security Policy File Name**, rename the security policy file name and then, click **Next**.

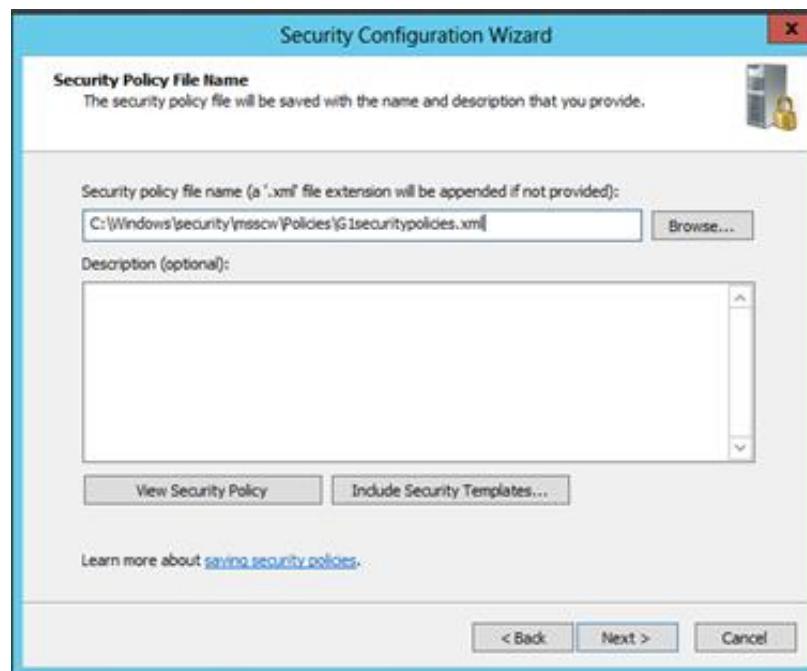


Figure 5.2.16.41 Security Policy File Name

Step 22 : For **Apply Security Policy**, choose “**Apply now**” and click Next button.



Figure 5.2.16.42 Apply Security Policy

Step 23 : After successfully completed the **Security Configuration Wizard**, click **Finish** to close this wizard.

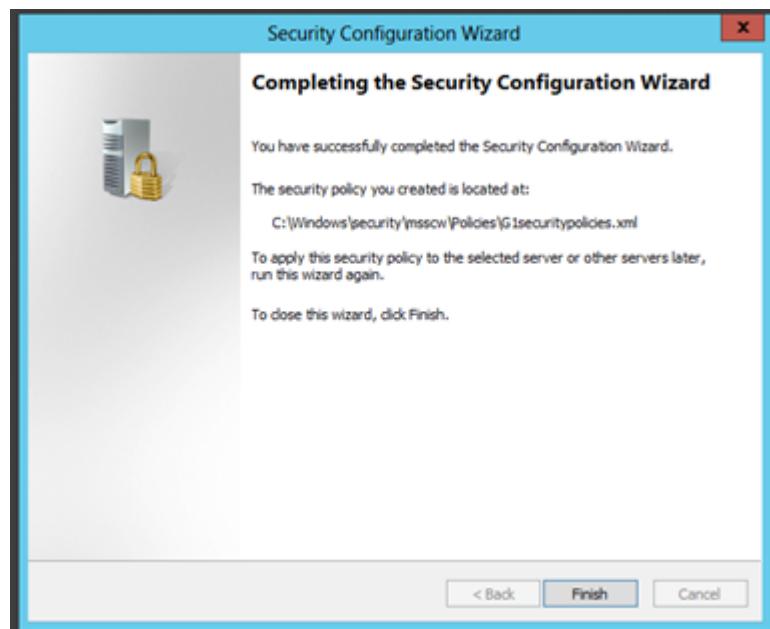


Figure 5.2.16.43 Completing the Security Configuration Wizard

5.2.17. Linux Server Hardening and Vulnerability Report

DEBIAN SERVER HARDENING

1. System Update

Keeping the system up to date is necessary after installing any operating system. It reduces known vulnerabilities that are in your system.

Step 1: Install the system update by type command *apt update*

```
root@workshopii:/home/debian# apt update
Hit:1 http://deb.debian.org/debian buster InRelease
Get:2 http://security.debian.org/debian-security buster/updates InRelease [65.4
kB]
Get:3 http://security.debian.org/debian-security buster/updates/main Sources [16
8 kB]
Get:4 http://security.debian.org/debian-security buster/updates/main amd64 Packa
ges [260 kB]
Get:5 http://security.debian.org/debian-security buster/updates/main Translation
-en [142 kB]
Fetched 635 kB in 22s (28.9 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
10 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

Figure 5.2.17.1: *apt update*

Step 2: Install updates (if any) by using command *apt upgrade*.

```
root@workshopii:/home/debian# apt upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following NEW packages will be installed:
  linux-image-4.19.0-13-amd64
The following packages will be upgraded:
  gir1.2-javascriptcoregtk-4.0 gir1.2-webkit2-4.0 libjavascriptcoregtk-4.0-18
  libp11-kit0 libwebkit2gtk-4.0-37 linux-image-amd64 p11-kit p11-kit-modules
  python-apt-common python3-apt
10 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 20.0 MB/68.6 MB of archives.
After this operation, 270 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

Figure 5.2.17.2: apt upgrade

Step 3: Reboot your server by using command *reboot*.

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

Figure 5.2.17.3: Reboot

Step 4: To set a daily update, go to Software and Updates. Then click Updates bar then choose “daily”.

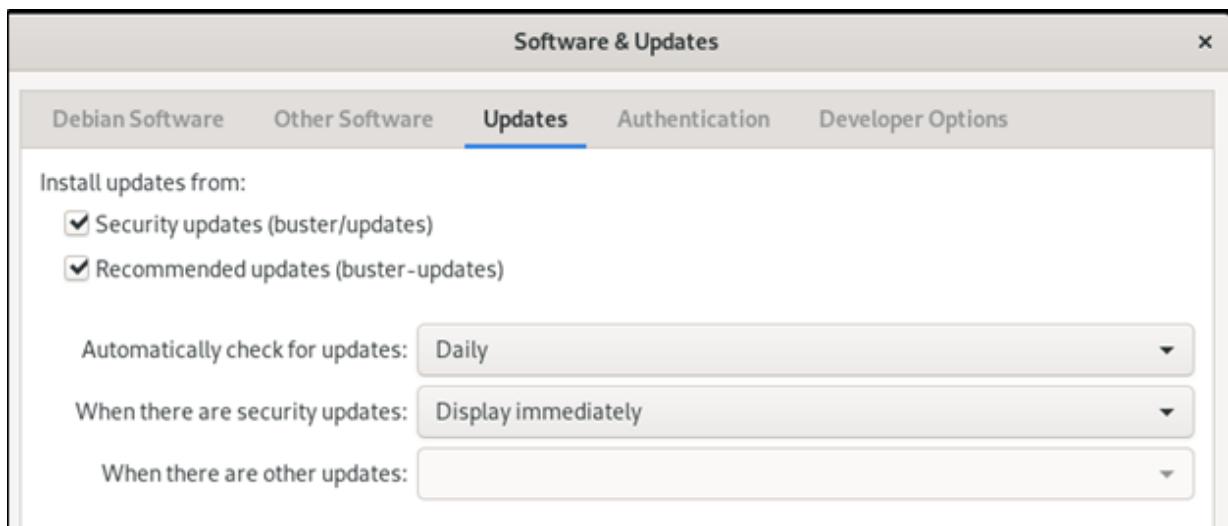


Figure 5.2.17.4: Daily update

2. Uncomplicated Firewall (ufw)

Step 1: Install uncomplicated firewall by using command *apt install ufw*.

```
root@workshopii:/home/debian# apt install ufw
Reading package lists... Done
Building dependency tree
Reading state information... Done
ufw is already the newest version (0.36-1).
```

Figure 5.2.17.5: apt install ufw

Step 2: Check the status of ufw by using command *ufw status*.

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

Figure 5.2.17.6: ufw status

Step 3: Modify the default rules using command *ufw default deny incoming* and *ufw default allow outgoing*.

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

Figure 5.2.17.7: ufw default deny incoming

Step 4: Enable access to the port used by SSH, port 22, using command *ufw allow ssh*.

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

Figure 5.2.17.8: ufw allow ssh

Step 5: Start and enable ufw by using command *ufw enable*.

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

Figure 5.2.17.9: ufw enable

3. Password Expiration

Step 1: When creating user accounts, we make the policy where it has a minimum and maximum password age to force the user to change password.

```
root@WorkshopII:~# chage -M 180 -I 30 -W 14 debian
```

Figure 5.2.17.10: Set password expiration

```
root@WorkshopII:/home/debian# chage -l debian
Last password change : Jan 23, 2021
Password expires      : Jul 22, 2021
Password inactive     : Aug 21, 2021
Account expires        : never
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
```

Figure 5.2.17.11: Password expiration

(-M) = Maximum password age by days

-M	Set the maximum password age of x days
-I	Set the inactivity period of x days after password expiration
-W	Set the warning period of x days before password expiration

4. Set the minimum number of password

Step 1: We set the minimum password to avoid the password easy to crack.

```

root@workshopii:/home/debian# apt-get install libpam-cracklib --force-yes -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  linux-image-4.19.0-11-amd64
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  libpam-cracklib
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 88.2 kB of archives.
After this operation, 119 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian buster/main amd64 libpam-cracklib amd64 1.3.1-5 [88.2 kB]
Fetched 88.2 kB in 0s (273 kB/s)
Selecting previously unselected package libpam-cracklib:amd64.
(Reading database ... 153251 files and directories currently installed.)
Preparing to unpack .../libpam-cracklib_1.3.1-5_amd64.deb ...
Unpacking libpam-cracklib:amd64 (1.3.1-5) ...
Setting up libpam-cracklib:amd64 (1.3.1-5) ...
Processing triggers for man-db (2.8.5-2) ...
W: --force-yes is deprecated, use one of the options starting with --allow instead.

```

Figure 5.2.17.12: Install libpam-cracklib

Step 2: Edit the password configuration file, as shown in the figure.

```

GNU nano 3.2                               /etc/pam.d/common-password

# 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=1 default=ignore]    pam_unix.so obscure use_authtok 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 5.2.17.13: Password configuration file

5. Port Scanning

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

Step 1: Installing Nmap

```
root@workshopii:/home/debian# apt-get install nmap
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  linux-image-4.19.0-11-amd64
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  liblinear3 nmap-common
Suggested packages:
  liblinear-tools liblinear-dev ncat ndiff zenmap
The following NEW packages will be installed:
  liblinear3 nmap nmap-common
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 5,834 kB of archives.
After this operation, 25.8 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://deb.debian.org/debian buster/main amd64 liblinear3 amd64 2.1.0+dfsg-4 [41.2 kB]
Get:2 http://deb.debian.org/debian buster/main amd64 nmap-common all 7.70+dfsg1-6+deb10u1 [3,898 kB]
Get:3 http://deb.debian.org/debian buster/main amd64 nmap amd64 7.70+dfsg1-6+deb10u1 [1,895 kB]
Fetched 5,834 kB in 2s (3,503 kB/s)
```

Figure 5.2.17.14: Install nmap

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

```
root@workshopii:/home/debian# nmap -v -sS localhost
Starting Nmap 7.70 ( https://nmap.org ) at 2021-01-02 15:59 +08
Initiating SYN Stealth Scan at 15:59
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 22/tcp on 127.0.0.1
Discovered open port 139/tcp on 127.0.0.1
Discovered open port 445/tcp on 127.0.0.1
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 631/tcp on 127.0.0.1
Completed SYN Stealth Scan at 15:59, 1.58s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000010s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
631/tcp   open  ipp
```

Figure 5.2.17.15: Identify open port

6. Disable CUPS and close port IPP

Common Unix Printing System (CUPS) is a modular printing system for Unix-like computer OS that allows a computer to act as a printing server. Our server does not need these services, and we disable it.

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

```
root@WorkshopII:~# echo "manual">> ../cups.override  
root@WorkshopII:~# service cups stop
```

Figure 5.2.17.16: Disable CUPS

Step 2: List the port using this command

```
root@WorkshopII:/home/debian# nmap -v -sT localhost
```

Figure 5.2.17.17: List the port

7. 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 disable Bluetooth service for security.

Step 1: Open the local Configuration file of Bluetooth

```
debian@WorkshopII:~$ sudo nano /etc/rc.local
```

Figure 5.2.17.18: Bluetooth configuration file

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

GNU nano 3.2	/etc/rc.local	Modified
rfkill block bluetooth exit 0		

Figure 5.2.17.19: Add “rfkill block bluetooth”

Step 3: Save and Exit

Step 4: Open the main configuration file of Bluetooth

```
debian@WorkshopII:~$ sudo nano /etc/bluetooth/main.conf
```

Figure 5.2.17.20: Bluetooth main file

Step 5: Add this command

DiscoverableTimeout=0

InitiallyPowered=false

GNU nano 3.2	/etc/bluetooth/main.conf	Modified
[General]		
# Defaults to 'BlueZ X.YZ', if Name is not set here and plugin 'hostname' is no\$ # The plugin 'hostname' is loaded by default and overrides the Name set here so # consider modifying /etc/machine-info with variable PRETTY_HOSTNAME=<NewName> \$ #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		

Figure 5.2.17.21: Add command

Step 6: Save and exit

Step 7: View the Bluetooth status

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

Jan 24 11:04:42 WorkshopII systemd[1]: Condition check resulted in Bluetoot...ped.
Jan 24 11:06:48 WorkshopII systemd[1]: Condition check resulted in Bluetoot...ped.
Hint: Some lines were ellipsized, use -l to show in full.
```

Figure 5.2.17.22: Bluetooth status

5.2.18. Audit Compliance

Reference	Audit Area, Objective, Question and Description		Status		
Checklist	Section	Audit Question	Findings	Compliance (/)	Non-Compliance (/)
1.0 SECURITY POLICY					

1.1 Security Policy

1.1.1 Security policy document	<p>-Whether the existence of a security policy, which is approved by the supervisor, published and communicated as appropriate to all users.</p> <p>-Whether it states the management commitment and set out the organizational approach to managing information security.</p>	Security policy status done in final report.	/	
1.1.2 Review and evaluation	<p>-Whether the security policy has an owner, who is responsible for its maintenance and review according to a defined review process.</p> <p>-Whether the process ensures that a review takes place in response to</p>		/	

	any changes affecting the basis of the original assessment such as significant security incidents, new vulnerabilities and changes to company.		
--	--	--	--

2.0 ORGANISATIONAL SECURITY

2.1 Information security infrastructure

2.1.1 Management information security forum	Whether there is a management forum to ensure there is a clear direction and visible management support for security initiatives within the organisation.	Briefing about Workshop2 and having group discussion.	/	
2.1.2 Information security coordination	Whether there is a cross-functional forum of management representatives from relevant parts of the organisation to coordinate the implementation of information controls.	Discuss about networking service (IPv4 tunnelling, VPN, VLSM, Routing & NAT).	/	

2.1.3 Allocation of information security responsibilities.	Whether full responsibilities for the protection of individual assets and for carrying out specific security processes were clearly defined.	Advise group members not to leave important information publicly.	/	
2.1.4 Authorisation process for information processing facilities	Whether there is a management authorisation process in place for any new information processing facility. This should include all new facilities such as hardware and software.	Authorisation at all server, switch and router.	/	
2.1.5 Security advise from supervisor	-Whether information security advice is obtained where appropriate. -A specific individual may provide advice in security decision making.	Supervisor provide information about firewall, routing and NAT and ACL.	/	
2.1.6 Independent review of information security	Whether the implementation of security policy is reviewed independently on regular basis. This is provide assurance that organisational practises properly reflect the policy.	Review by group's member.	/	

2.2 Security of third party

2.2.1 Security requirements in third party contracts	Whether there is a formal contract containing, or referring to, all the security requirements to ensure compliance with the organization's security policies and standards.	No contract	/	
2.2.2 Identification of risks from third party	Whether risks from third party access are identified and appropriate security controls implemented.	ACL is implemented	/	

3.0 ASSET CLASSIFICATION AND CONTROL

3.1 Accountability of assets

3.1.1 Inventory of assets	<p>-Whether an inventory or register is maintained with the important assets associated with each information system.</p> <p>-Whether each of asset identifies has an owner, the security classification defined and agreed and the location identified.</p>	Fill asset form for each equipment before use.	/	
---------------------------------	--	--	---	--

3.2 Information classification

3.2.1 Classification guidelines	Whether there is an information classification scheme or guideline in place; which will assist in determining how the information is to be handled and protected.	IP Addressing is saved at google drive to refer.	/	
3.2.2 Information labelling and handling	Whether an appropriate set of procedures are defined for information labelling and handling in accordance with the classification scheme adopted by organization.	Label IP Address of each server and client	/	

4.0 PERSONNEL SECURITY

4.1 Security in job definition and resourcing

4.1.1 Including security in job responsibilities	<p>-Whether security roles and responsibilities as laid in Organisation's information security policy is documented where appropriate.</p> <p>-This should include general responsibilities for implementing and maintaining security policy as well as specific.</p>	Security policy status done in final report.	/	
---	---	--	---	--

4.2 Responding security weakness

4.2.1 Reporting security weakness	Whether a formal reporting procedure or guideline exists for user, to report security weakness in, or threats, to systems or services.	Not provided in reports	/	
4.2.2 Reporting software malfunctions	Whether procedures were established to report any software malfunctions.	Not provided in reports	/	

4.2.3 Reporting hardware malfunctions	Whether procedures were established to report any hardware malfunctions.	Not provided in reports	/	
4.2.4 Disciplinary process	Whether there is a formal disciplinary process in place for employee who have violated organisational security policies and procedures.	Advice group's member to avoid appearance of unethical or compromising practises .	/	

5.0 PHYSICAL AND ENVIRONMENTAL SECURITY

5.1 Secure Area

5.1.1 Physical security Perimeter	<p>-What physical border security facility has been implemented to protect the information processing services.</p> <p>-Some examples of such security facility are alarm, thumbprint.</p>	Students write their names and thumb scans to enter lab.	/	
--	--	--	---	--

5.1.2 Physical entry controls	What entry controls are in place to allow only authorised person should be allowed access to secure areas by using access controlled devices.	Student should thumbprints to enter lab	/	
5.1.3 Securing rooms and facilities	Whether the rooms, which have the Information processing service, are locked or have lockable door or safes.	Have lockable door.	/	
	Whether the information processing service is protected from natural and man-made disaster.	Equipment is protected by password	/	

5.2 Equipment Security

5.2.1 Equipment siting and protection	Whether the equipment was located in appropriate place to minimize unnecessary access into lab areas.	All equipment is located in own group lab	/	
	Whether controls were adopted to minimize risk from potential threats such as theft, fire, and electrical supply interfaces.	Lab provide fire extinguisher and smoke detector.	/	
	Whether there is a policy toward eating, drinking and smoking on in proximity to information processing facilities.	Policy provided	/	
	Whether environmental conditions are monitored which would adversely affect the information processing services.	Monitored by technician	/	
5.2.2 Equipment Maintenance	-Whether the equipment is maintained as per the supplier's recommended service intervals and specifications.	Maintained by technician	/	

5.2.3 Securing equipment off-premises	<p>-Whether any equipment usage outside a organization's premises for information processing has to be authorized by the management.</p>	Username and password are required to access equipment.	/	
	<p>-Whether the security provided for this equipment while outside the premises are on par with or more than the security provided inside the premises.</p>	Equal	/	

5.3 General Controls

5.3.1 Clear Desk and Clear Screen Policy	<p>Whether automatic computer screen locking facility is enabled. This would lock the screen when the computer is left unattended for a period.</p>	Screen lock for each server.	/	
5.3.2 Removal of property	<p>Whether equipment, information or software can be taken offsite without appropriate authorization.</p>	Cannot be taken offsite	/	

6.0 COMMUNICATION AND OPERATIONS MANAGEMENT

6.1 Operational Procedure and responsibilities

6.1.1 Documented Operating System	Whether the Security Policy has identified any operating system procedures such as Back-Up, Equipment maintenance etc.,	Not all back-up are documented	/	
6.1.2 Segregation of duties	Whether duties of responsible are separated in order to reduce opportunities for unauthorized modifications or misuse of information service.	Services are divided to each group's member	/	

6.2 Protection Against Malicious Software

6.2.1 Control against malicious	<p>-Whether there any exist control against malicious software usage.</p> <p>-Whether the security policy does address software licensing issues such as prohibiting usage of unauthorized software.</p>	No control being applied		/
	<p>Whether antivirus software is installed on the computers to checks and isolate or remove any viruses from computer and media.</p>	No antivirus is installed		/

6.3 Housekeeping

6.3.1 Information back-up	<p>Whether Back-up of essential business information such as server, network components, configuration backups etc., were taken regularly.</p>	configuration backup applied	/	
6.3.2 Fault Logging	<p>Whether faults are reported and well managed. This includes correctives action being taken, review of the fault logs and checking the actions taken.</p>	Corrective actions being taken	/	

--	--	--	--

6.4 Network Management

6.4.1 Network Controls	Whether there exist any special controls to safeguard confidentiality and integrity of data processing over the public network and to protect the system. Such as Virtual Private Network and other encryption.	VPN, applied	SSH	/	
-------------------------------	---	--------------	-----	---	--

6.5 Exchange of Information and Software

6.5.1 Security of Media in transit	<p>-Whether security of media while being transported into account.</p> <p>-Whether the media is well secured from unauthorized access, misuse or corruption.</p>	SFTP, security	Samba	/	
---	---	----------------	-------	---	--

7.0 ACCESS CONTROL

7.1 User Access Control

7.1.1 User Registration	Whether there is any formal user registration and guest user procedure for granting access to multi-user information system and services.	Active Directory (AD)	/	
7.1.2 Privilege Management	-Whether the allocation and use of any privileges in multi-user information system environment is restricted and controlled -i.e., Privileges are allocated on need-to-use basis; privileges are allocated only after formal authorisation process.	Network Policy Server (NPS)	/	
7.1.3 User Password Management	The allocation and reallocation of password should be controlled thorough a formal management process.	Password created through formal process	/	

	Whether the users are asked to sign a statement to keep the password confidential.	No statement being applied	/
--	--	----------------------------	---

7.2 User Responsibilities

7.2.1 Password use	Whether there are guidelines in place to guide users in selecting and maintaining secure passwords.	-Password must be 8 or more characters. -Password meet complexity requirements.	/
7.2.2 Unattended User Equipment	Whether the user are made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibility to implement such protection.	Provide to all equipment. (All server, router and switch)	/

7.3 Network Access Control

7.3.1 Segregation in networks	Whether the network (where third party need access to information system) is segregated using perimeter security	-Internal firewall such as proxy server, routing & NAT	/
--------------------------------------	--	--	---

	mechanisms such as firewall.	-External firewall ACL		
7.3.2 Node Authentication	<p>-Whether connects to remote computer systems that are outside organizations security management are authenticated.</p> <p>-Node authentication can serve as an alternate means of authenticating groups of remote users where they are connected to a secure, shared computer facility.</p>	Implemented	/	
7.3.3 Network Connection Protocols	Whether there exists any network connection control for shared networks that extend beyond the organisational boundaries. Example: electronic email, web access, file transfers, etc.,	Not applicable.	/	
7.3.4 Network Routing Control	Whether there exists any network control to ensure computers and information flows do not breach the access control policy of the business applications. This is often essential for networks shared with non-organisations users.	Routing & NAT	/	

	Whether the routing controls are based on the true source and destination identification mechanism. Example: Network Address Translation (NAT).	Routing & NAT	/	
7.3.5 Security of Network Services	Whether the organisation, using public or private network service does ensure that a clear description of security attributes of all services used is provided.	Routing & NAT	/	
7.4 Operating System Access Control				
7.4.1 Automatic terminal identification	Whether automatic identification mechanism is used to authenticate connections.	Not implemented		/

7.4.2 Terminal log-on procedures	<p>Whether access to information system is attainable only via a secure log-on process.</p>	<p>Implemented</p>	<p>/</p>	
	<p>Whether there is a procedure in place for logging in to an information system. This is to minimise the opportunity of unauthorised access.</p>	<p>Implemented</p>	<p>/</p>	
7.4.3 User identification and Authorization	<p>-Whether unique identifier is provided to every user such as operators, system administrators and all other staff including technical.</p>	<p>All group's member have identification and authorization.</p>	<p>/</p>	
	<p>Whether the authentication method used does substantiate the claimed identity of the user; commonly used method: Password that only the user knows.</p>	<p>Users are authenticated.</p>	<p>/</p>	
7.4.4 Use of System Utilities	<p>Whether the system utilities that comes with the computer installations, but may override system and application control is tightly controlled.</p>	<p>Utility not override</p>	<p>/</p>	

7.4.5 Terminal Time-Out	Inactive terminal in public areas should be configured to clear the screen or shut down automatically after a defined period of inactivity.	Router and switch	/
--------------------------------	---	-------------------	---

7.5 Application Access Control

7.5.1 Sensitive System Isolation	Whether there are sensitive systems are provided with isolated computing environment such as running on a dedicated computer, share resources only with trusted application systems, etc.,	No sensitive system are provided.	/
---	--	-----------------------------------	---

7.6 Monitoring System Access and Use

7.6.1 Event Logging	Whether audit logs recording exceptions and other security relevant events are produced and kept for an agreed period to assist in future investigations and access control monitoring.	Accounting in Radius Server	/
----------------------------	---	-----------------------------	---

7.6.2 Monitoring System Use	<p>-Whether procedure are set up for monitoring the use of information processing facility.</p> <p>-The procedure should ensure that the users are performing only the activities that are explicitly authorised.</p>	Monitored by Nagios NMS for Linux, IDS	/	
	Whether the results of monitoring activities are reviewed regularly.	Monitoring activities are reviewed regularly	/	
7.6.3 Message Authentication	<p>-Whether an assessment of security risk was carried out to determine if message authentication is required.</p> <p>-Message authentication is a technique to detect unauthorized changes.</p>	“Access denied” pop-up when unauthorized user trying to access.	/	
7.6.4 Output Data Validation	Whether the data output of application system is validated to ensure that the processing of stored information is correct.	Router and switch can be access by entering correct username and password.	/	

8.0 SYSTEM DEVELOPMENT AND MAINTENANCE

8.1 Security in Application Systems

8.1.1 Input Data Validation	Whether data input to application system is validated to ensure that it is correct and appropriate.	“Access denied” pop-up when unauthorized user trying to access.	/	
8.1.2 Message Authentication	-Whether an assessment of security risk was carried out to determine if message authentication is required. -Message authentication is a technique to detect unauthorized changes.	“Access denied” pop-up when unauthorized user trying to access.	/	
8.1.3 Output Data Validation	Whether the data output of application system is validated to ensure that the processing of stored information is correct.	Access is permitted by entering valid username and password.	/	

8.2 Cryptographic Controls

8.2.1 Encryption	-Whether encryption technique used to protect the data. -Whether assessments were conducted to analyse the sensitivity of the data and the level of protection needed.	SSH, enable secret in router and switch	/	
-------------------------	---	---	---	--

8.2.2 Digital Signatures	Whether Digital signature were used to protect the authenticity and integrity of electronic documents.	No digital signature	/	
8.2.3 Key Management	Whether there is a management system is in place to support the organisation's use of cryptographic techniques such as Secret key technique and Public key technique.	The shared key in Radius Server is same with key authentication using radius server(AAA)	/	
	Whether the Key management system is based on set of standard, procedures and secure methods.	Yes	/	

8.3 Security in development and support process

8.3.1 Change control procedures	<p>-Whether there are any controls in place for the implementation of software on operational systems.</p> <p>-This is to minimize the risk of corruption of operational systems.</p>	Not implemented		/
8.3.2 Technical review of operating system changes	<p>-Whether there are processes in place to ensure application system is reviewed and tested after change in operating system.</p> <p>-Periodically it is necessary to upgrade operating system i.e., to install service, patches etc.,</p>	Yes	/	
8.3.3 Outsourced Software Development	<p>-Whether there are controls in place over outsourcing software.</p> <p>-Testing before installations to detect malware</p>	VPN (SoftEther) SSH	/	
<h2>9.0 COMPLIANCE</h2>				

9.1 Aspects of Services Continuity Management

9.1.1 Testing, maintaining and re-accessing services	Whether services are tested regularly to ensure that they are up-to-date and effective.	Service tested	/	
---	---	----------------	---	--

9.2 Compliance with Legal Requirements

9.2.1 Identification of Applicable legislation	-Whether specific controls and individual responsibilities to meet these requirements were defined and documented.	Documented and defined in final report	/	
9.2.2 Safeguarding of Organisational records	Whether important records of the organisation are protected from loss destruction and false function.	Logbook	/	
9.2.3 Data Protection and Privacy of Personal Information	Whether there is a management structure and control in place to protect data and privacy of personal information.	Password is encrypted and protected	/	

9.2.4 Prevention of misuse of information processing facility	<p>-Whether use of information processing facilities for any unauthorized purpose.</p> <p>-Whether at the log-on a warning message is presented on the computer screen indicating that the system being entered is private and that unauthorized access not permitted.</p>	Unauthorized access cannot access server, router and switch	/	
9.2.5 Collection of Evidence	<p>Whether the process involved in collecting the evidence is in accordance with legal and industry best practise.</p>	Accounting login Radius Server (Log)	/	
<h3>9.3 Review of Security Policy and Technical Compliance</h3>				
9.3.1 Compliance with Security Policy	<p>Whether all areas within the organisation is considered for regular review to ensure compliance with security policy, standards and procedures.</p>	Security policy documented in final report.	/	

9.3.2 Technical compliance checking	Whether information systems were regularly checked for compliance with security implementation standards.	Harden Linux Server, Harden Windows Server, Security Hardening Checklist.	/	
--	---	---	---	--

9.4 System Audit Considerations

9.4.1 System Audit Controls	Whether audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruption to workshop.	Yes	/	
------------------------------------	--	-----	---	--

5.3. Conclusion

Installation and configuration are important procedures to be done before testing the services. Installation of a program is the act of putting the program onto a computer system so that it can be executed. Because the requisite process varies for each program and each computer, many programs come with a general-purpose or dedicated installer (a specialized program which automates most of the work required for their installation). This stage must be done carefully to make sure the service can be run efficiently during the testing part. The installation guide will help get up and running in no time.

6. CHAPTER 6: TESTING

6.1. Introduction

Testing section is to ensure all services are configured and running smoothly.

There are many ways of testing for each service. In this section, we are going to test all the services that have been configured and set up. One of the important things on testing is as it is important to isolate each part and show that the individual parts are correct.

Testing also 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. A good testing service is when we can find errors. Therefore, it is important to find errors and try to modify them for the best performance.

6.2. Services testing

6.2.1. Routing and NAT

Routing

Step 1: sh ip bgp summary for Router HQ

```
HQ#sh ip bgp summary
BGP router identifier 200.200.201.1, local AS number 50001
BGP table version is 4, main routing table version 4
2 network entries using 240 bytes of memory
4 path entries using 208 bytes of memory
4/1 BGP path/bestpath attribute entries using 496 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 1024 total bytes of memory
BGP activity 8/0 prefixes, 11/0 paths, scan interval 60 secs

Neighbor      V   AS MsgRcvd MsgSent    TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:DB8:1:2::2 4  50002     549     547        4     0     0 09:01:15      2
200.200.201.2   4  50002     545     545        4     0     0 09:01:39      2
...
```

Figure 6.2.1.1 sh ip bgp summary on Router HQ

Step 2: sh ip bgp summary for Router ISP

```

ISP#sh ip bgp summary
BGP router identifier 200.200.201.2, local AS number 50002
BGP table version is 3, main routing table version 3
2 network entries using 240 bytes of memory
2 path entries using 104 bytes of memory
4/1 BGP path/bestpath attribute entries using 496 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 920 total bytes of memory
BGP activity 8/0 prefixes, 9/0 paths, scan interval 60 secs

Neighbor      V   AS MsgRcvd MsgSent    TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:DB8:1:2::1 4 50001      547      549        3     0    0 09:01:55      0
2001:DB8:5:6::6 4 50003      547      549        3     0    0 09:01:58      0
200.200.200.6   4 50003      545      545        3     0    0 09:01:58      0
200.200.201.1   4 50001      546      546        3     0    0 09:02:19      0

```

Figure 6.2.1.2 sh ip bgp summary on Router ISP

Step 3: sh ip bgp summary for Router Branch

```

Branch#sh ip bgp summary
BGP router identifier 200.200.200.6, local AS number 50003
BGP table version is 4, main routing table version 4
2 network entries using 240 bytes of memory
4 path entries using 208 bytes of memory
4/1 BGP path/bestpath attribute entries using 496 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 1024 total bytes of memory
BGP activity 8/0 prefixes, 10/0 paths, scan interval 60 secs

Neighbor      V   AS MsgRcvd MsgSent    TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:DB8:5:6::5 4 50002      550      548        4     0    0 09:02:41      2
200.200.200.5   4 50002      546      546        4     0    0 09:02:42      2

```

Figure 6.2.1.3 sh ip bgp summary on Router Branch

NAT

Step 4: sh ip nat translation for Router HQ when Server Windows ping 200.200.200.6 which is Router Branch serial address

```

HQ#sh ip nat trans
Pro Inside global      Inside local      Outside local      Outside global
--- 200.200.201.100    192.168.2.4       ---             ---
icmp 200.200.201.30:1 192.168.2.130:1    200.200.200.6:1    200.200.200.6:1
--- 200.200.201.30    192.168.2.130       ---             ---
udp 200.200.201.40:41266 192.168.2.146:41266 200.200.200.6:161 200.200.200.6:161
udp 200.200.201.40:43071 192.168.2.146:43071 200.200.200.6:161 200.200.200.6:161
udp 200.200.201.40:44497 192.168.2.146:44497 200.200.200.1:161 200.200.200.1:161
udp 200.200.201.40:48589 192.168.2.146:48589 200.200.200.1:161 200.200.200.1:161
--- 200.200.201.40      192.168.2.146       ---             ---

```

Figure 6.2.1.4 sh ip nat translation on Router HQ

Step 5: sh ip nat translation for Router Branch when PC Remote access ping 200.200.201.30 which is external IP address for Windows Server

```
Branch#sh ip nat trans
Pro Inside global      Inside local        Outside local       Outside global
icmp 200.200.200.100:1 192.168.1.2:1    200.200.201.30:1   200.200.201.30:1
--- 200.200.200.100   192.168.1.2        ---                 ---
icmp 200.200.200.1:10732 192.168.1.3:10732 200.200.201.40:10732 200.200.201.40:10732
--- 200.200.200.1     192.168.1.3        ---                 ---
```

. Figure 6.2.1.5 sh ip nat translation on Router Branch

6.2.2. DNS (IPv4 & IPv6)

Step 1: nslookup from client IT Department to windows server

```
C:\Windows\system32\cmd.exe - nslookup

C:\Users\Group1>nslookup
Default Server: win-a90kb5eeo34.group1.com
Address: 2001:3200:1000:3000::2

> remoteaccess.group1.com
Server: win-a90kb5eeo34.group1.com
Address: 2001:3200:1000:3000::2

Name: remoteaccess.group1.com
Addresses: 2001:3200:1000:1000::2
          192.168.1.2

> itdepartment.group1.com
Server: win-a90kb5eeo34.group1.com
Address: 2001:3200:1000:3000::2

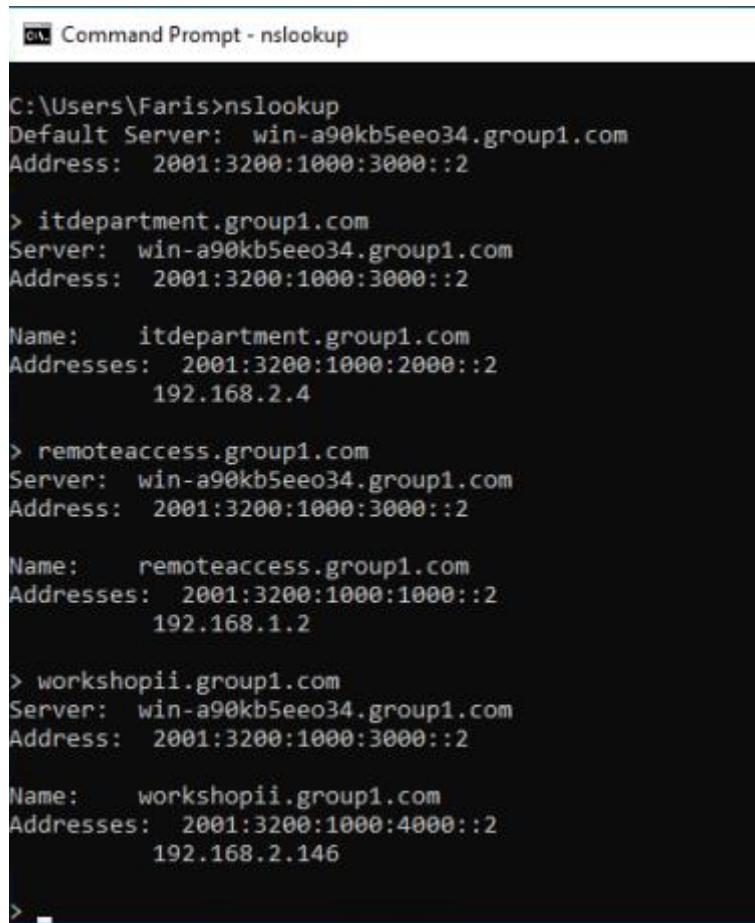
Name: itdepartment.group1.com
Addresses: 2001:3200:1000:2000::2
          192.168.2.4

> workshopii.group1.com
Server: win-a90kb5eeo34.group1.com
Address: 2001:3200:1000:3000::2

Name: workshopii.group1.com
Addresses: 2001:3200:1000:4000::2
          192.168.2.146
```

Figure 6.2.2.1 nslookup from client IT Department

Step 2: nslookup from client Remote Access to windows server



```
Command Prompt - nslookup

C:\Users\Faris>nslookup
Default Server: win-a90kb5eeo34.group1.com
Address: 2001:3200:1000:3000::2

> itdepartment.group1.com
Server: win-a90kb5eeo34.group1.com
Address: 2001:3200:1000:3000::2

Name: itdepartment.group1.com
Addresses: 2001:3200:1000:2000::2
192.168.2.4

> remoteaccess.group1.com
Server: win-a90kb5eeo34.group1.com
Address: 2001:3200:1000:3000::2

Name: remoteaccess.group1.com
Addresses: 2001:3200:1000:1000::2
192.168.1.2

> workshopii.group1.com
Server: win-a90kb5eeo34.group1.com
Address: 2001:3200:1000:3000::2

Name: workshopii.group1.com
Addresses: 2001:3200:1000:4000::2
192.168.2.146

>
```

Figure 6.2.2.2 nslookup from client Remote Access

6.2.3. Active Directory

Step 1: Test the connection by using the ping command from the cmd. The ping should get a reply from the server.

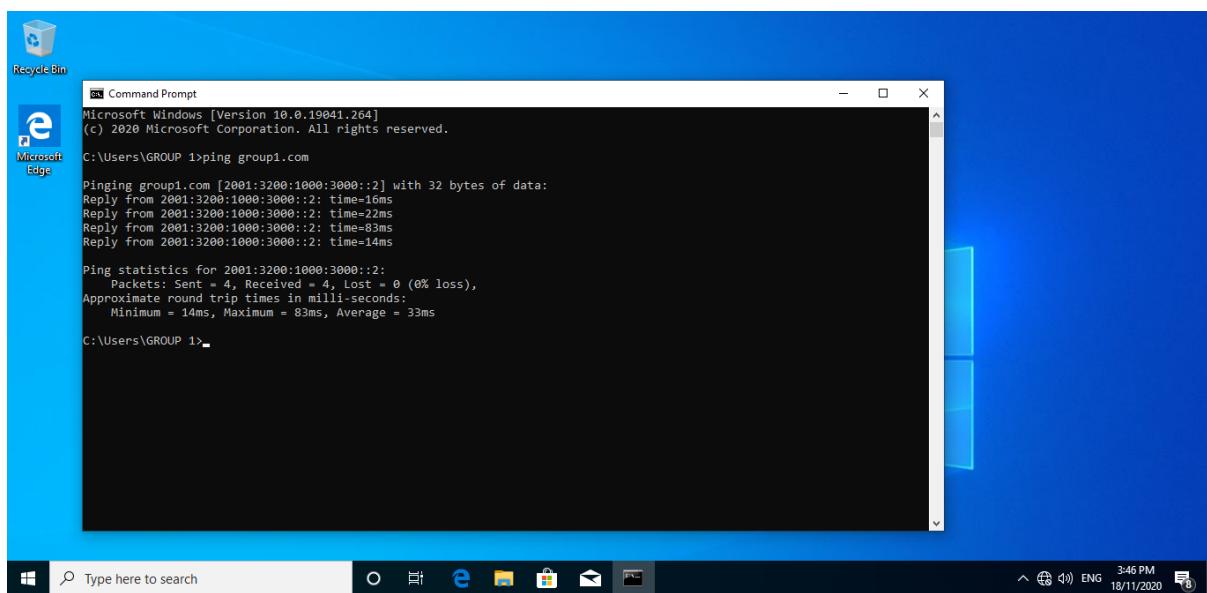


Figure 6.2.3.1 Ping in cmd

Step 2: Navigate to the computer's properties and click change setting at the right side.

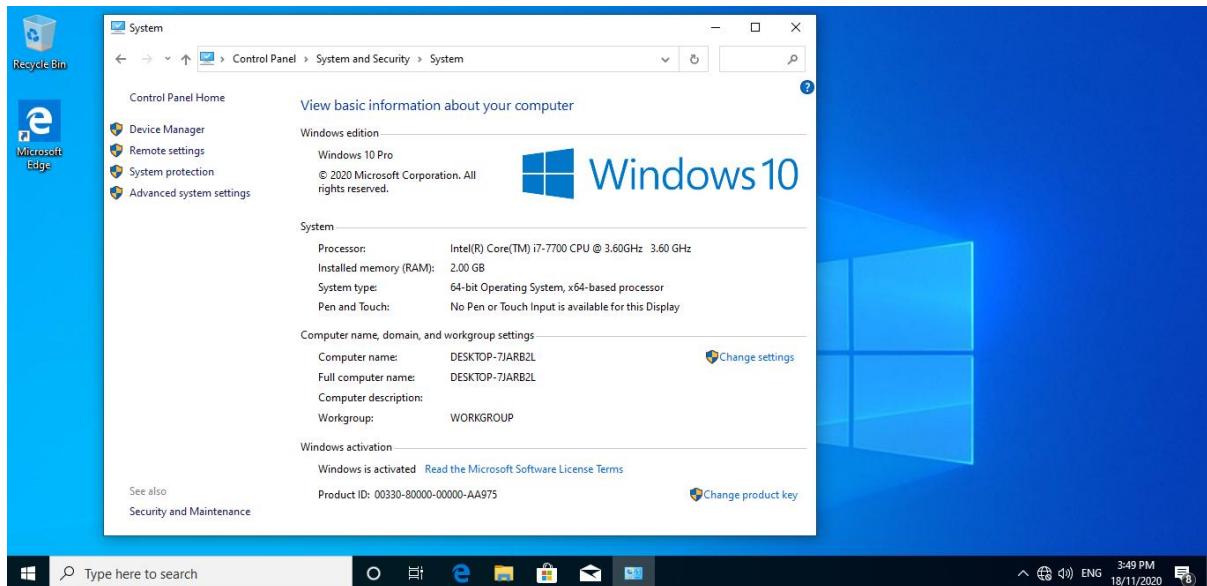


Figure 6.2.3.2 System tab

Step 3: Click Change at the windows to change the domain of the computer.

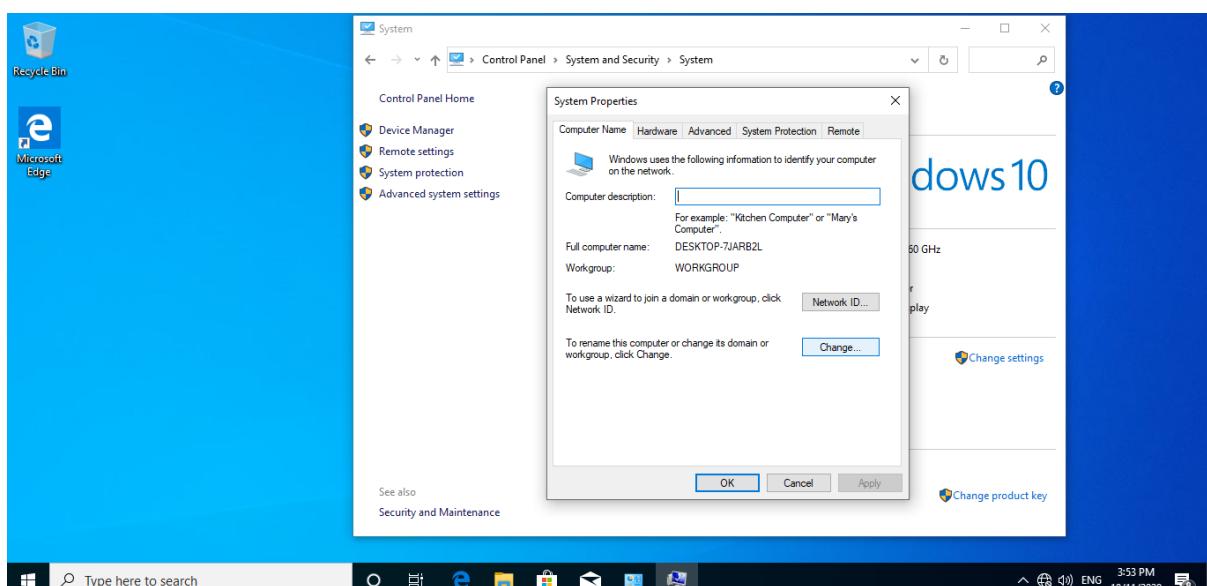


Figure 6.2.3.3 System properties tab

Step 4: The following windows will show up. These windows will allow users to change the domain of the computers.

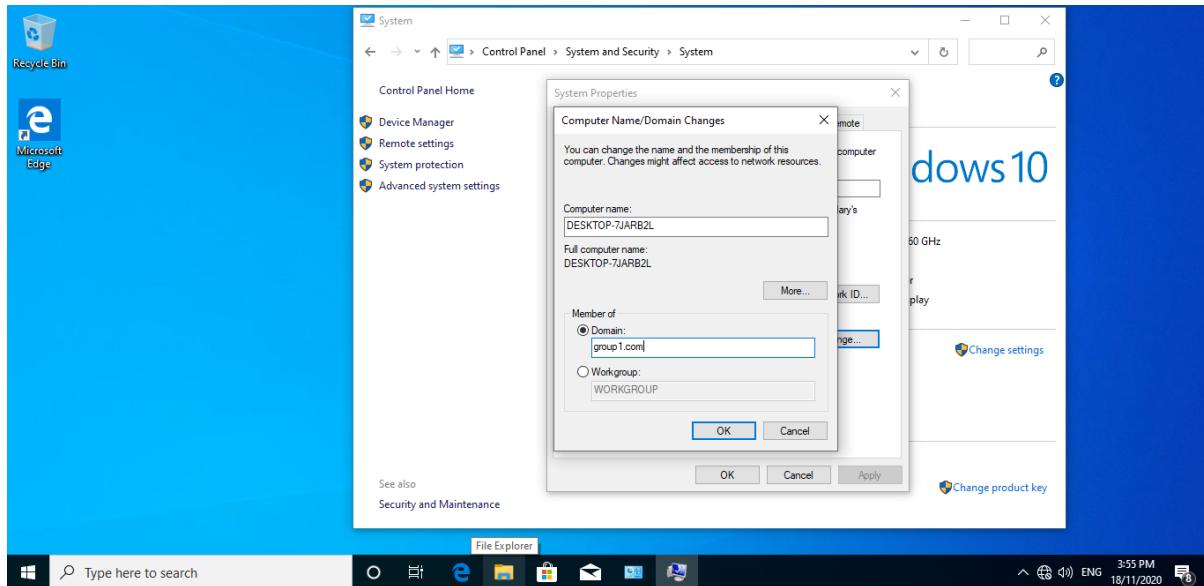


Figure 6.2.3.4 Computer name/domain changes tab

Step 5: Enter one of the users and its password that has already been created in the server.

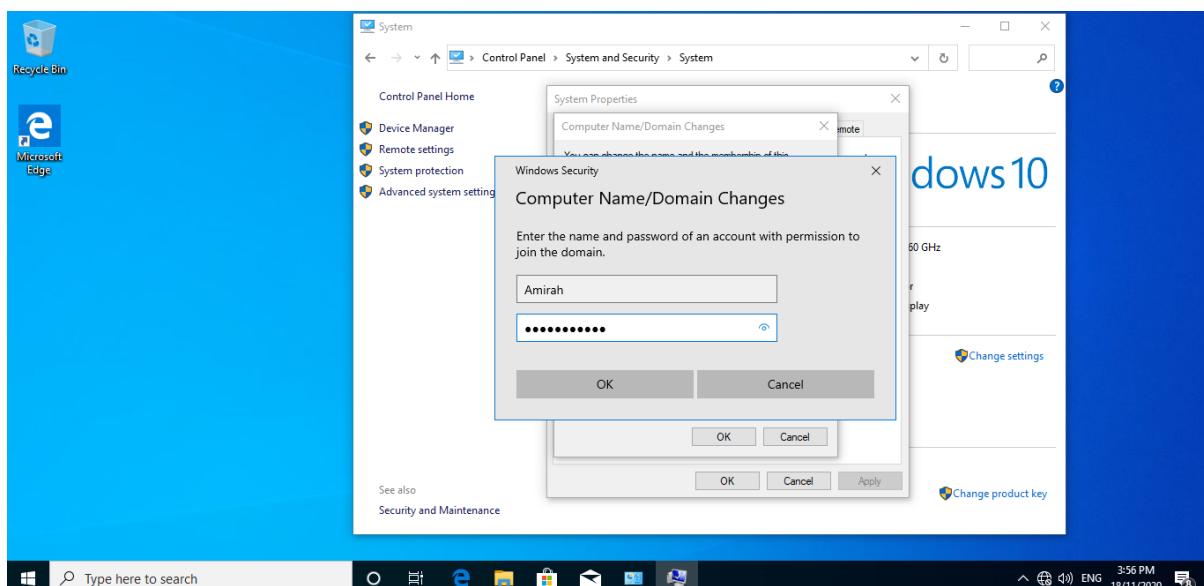


Figure 6.2.3.5 Username and password entered

Step 6: The windows show that the computer has successfully joined the domain controller.

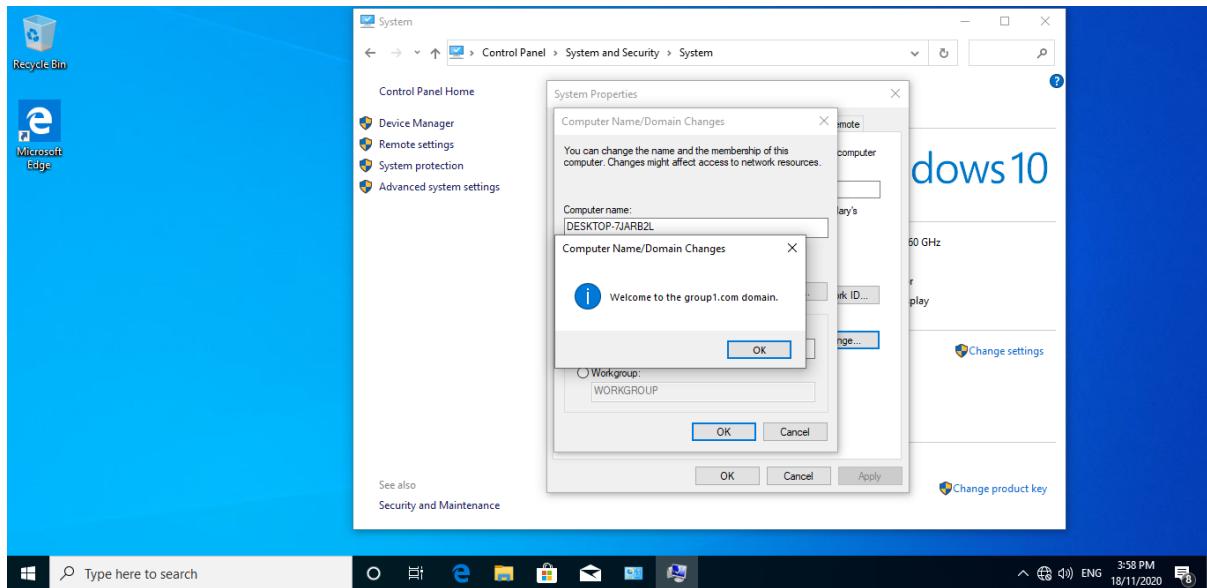


Figure 6.2.3.6 Domain successfully join

Step 7: Type the command below in cmd to apply the GPO in the client.

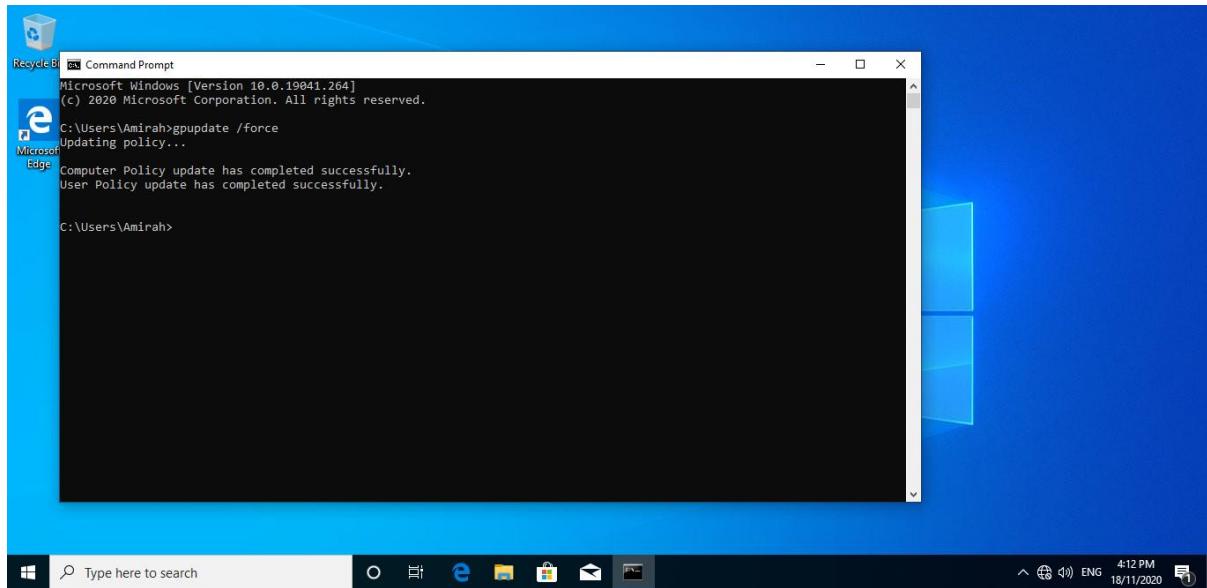


Figure 6.2.3.7 Command to apply GPO

Step 8: Testing the first GPO which is account lockout policy which when a user attempts to log in to the account using the wrong password for the first, second and third time. The screen will show up like this.

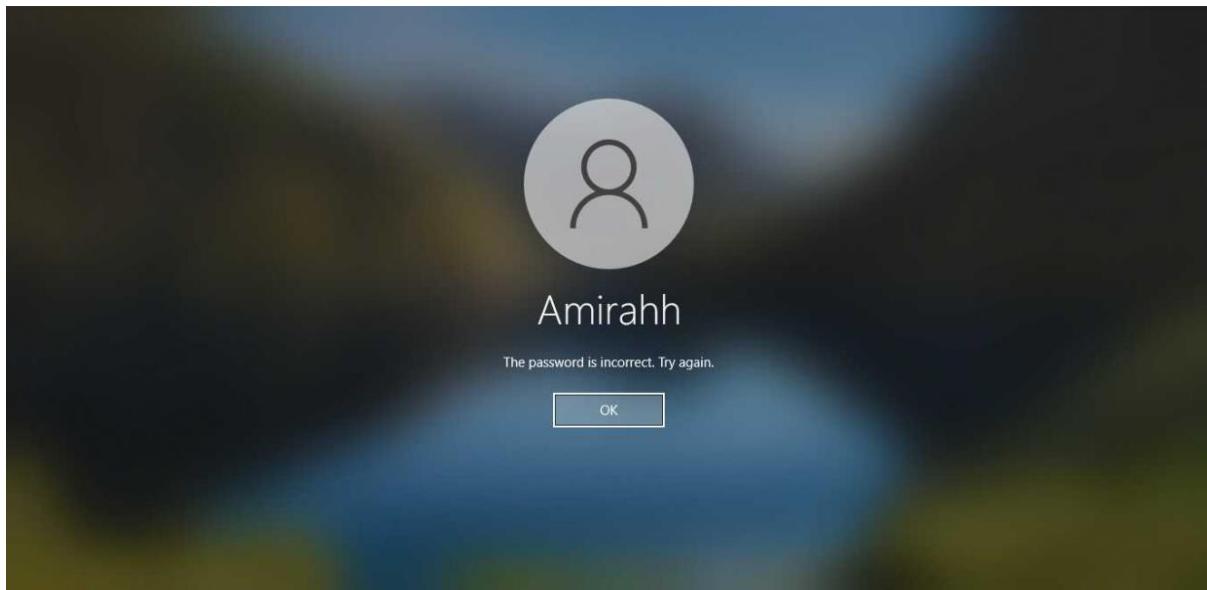


Figure 6.2.3.8 Testing of the first GPO

Step 9: The screen will show up like this when a user tries to log in after the third attempt which shows that the account will be locked for about 2 minutes until it can log in again after 2 minutes.

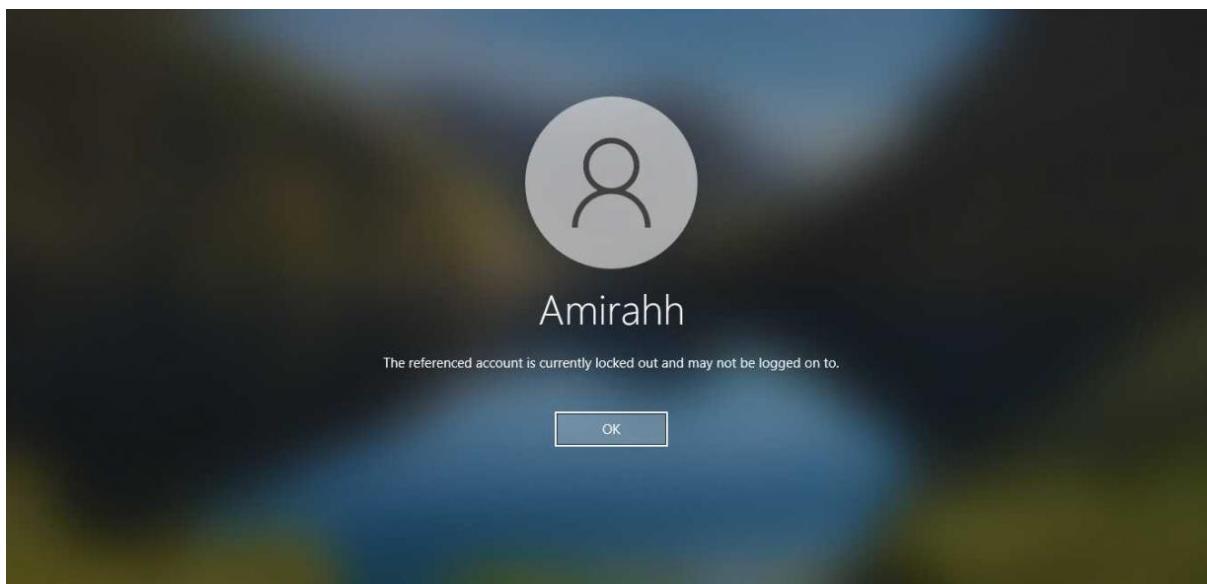


Figure 6.2.3.9 Account is being locked

Step 10: Testing the second GPO which is a banner that will shows before user wants to log into their account

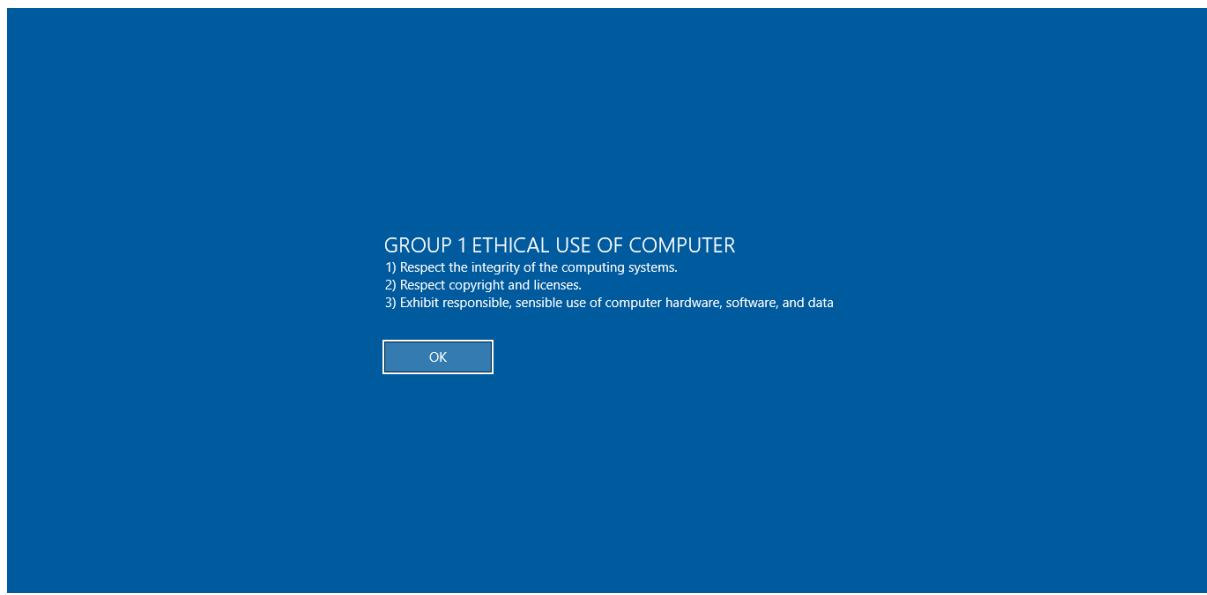


Figure 6.2.3.10 Testing of the second GPO

6.2.4. DHCP (IPv4 & IPv6)

IPv4 Testing

Step 1: Open command prompt at the client and type ipconfig and check for client to either get the ipv4 automatically from the DHCP server.

```
Command Prompt
Microsoft Windows [Version 10.0.19041.264]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\Faris>ipconfig

Windows IP Configuration

Unknown adapter VPN - VPN Client:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
IPv6 Address . . . . . : 2001:3200:1000:1000:0:27:1da3:8a84
IPv6 Address . . . . . : 2001:3200:1000:1000:69fa:b8f3:166e:c64b
Temporary IPv6 Address. . . . . : 2001:3200:1000:1000:71b5:acc:36ea:289e
Link-local IPv6 Address . . . . : fe80::69fa:b8f3:166e:c64b%8
IPv4 Address. . . . . : 192.168.1.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::c002:9dff:fe08:0%8
192.168.1.1
```

Figure 6.2.4 1 ipconfig IPv4 remote

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

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Group1> ipconfig

Windows IP Configuration

Unknown adapter VPN - VPN Client:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
IPv6 Address . . . . . : 2001:3200:1000:2000:54ce:cd64:1db0:7840
Temporary IPv6 Address . . . . . : 2001:3200:1000:2000:5fb:16d2:bb2b:9b4c
Link-local IPv6 Address . . . . . : fe80::54ce:cd64:1db0:7840%10
IPv4 Address . . . . . : 192.168.2.4
Subnet Mask . . . . . : 255.255.255.128
Default Gateway . . . . . : fe80::c001:98ff:fe74:0%10
                           192.168.2.1
```

Figure 6.2.4 2 ipconfig IPv4 ITDepartment

Step 2: Open the Windows Server and open the DHCP services. Find IPv4>Scope>Scope Lease. Check the list for ipv4 match with client ip address.

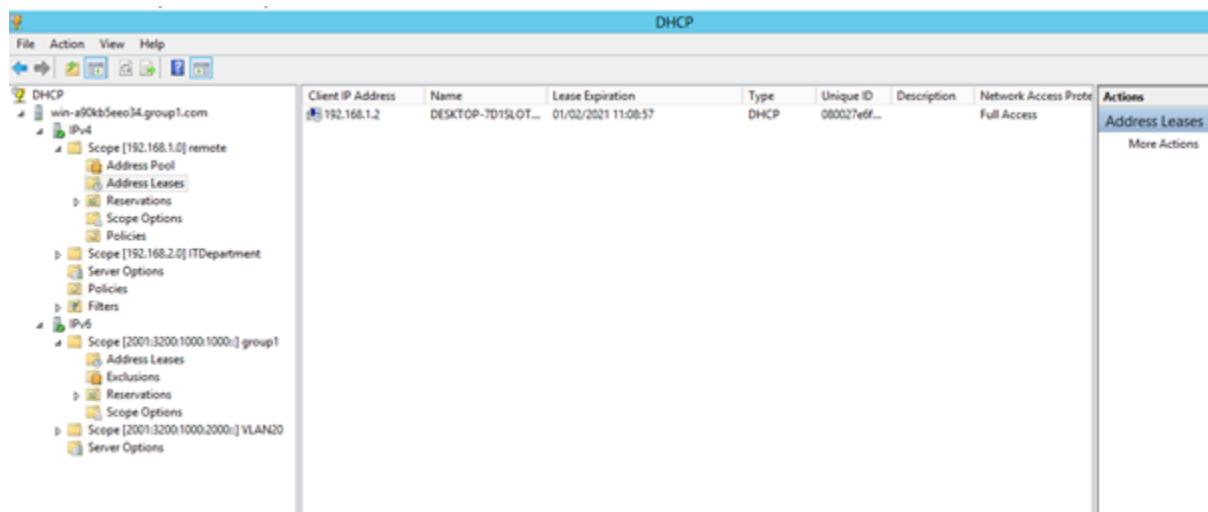


Figure 6.2.4 3 Address Lease IPv4 remote

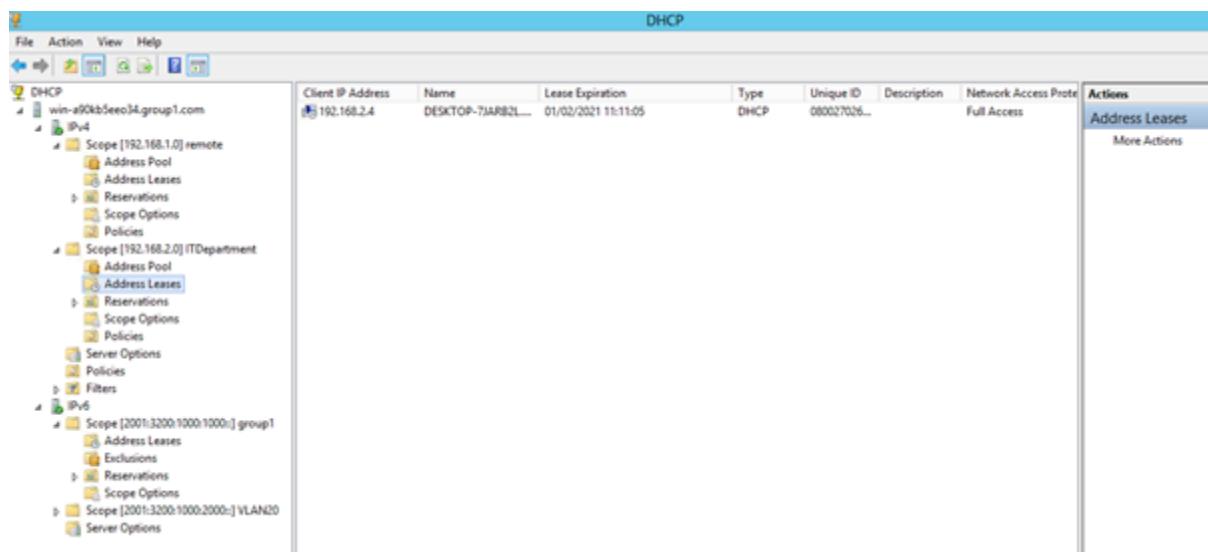


Figure 6.2.4 4 Address Lease IPv4 ITDepartment

IPv6 Testing

Step 1: Open command prompt at the client and type ipconfig and check for client either get the ipv6 automatically from the DHCP server.

```

C:\ Command Prompt
Microsoft Windows [Version 10.0.19041.264]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\Faris>ipconfig

Windows IP Configuration

Unknown adapter VPN - VPN Client:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . .

Ethernet adapter Ethernet:
Connection-specific DNS Suffix . . .
IPv6 Address. . . . . : 2001:3200:1000:1000:0:27:1da3:8a84
IPv6 Address. . . . . : 2001:3200:1000:1000:69fa:b8f3:166e:c64b
Temporary IPv6 Address. . . . . : 2001:3200:1000:1000:71b5:acc:36ea:289e
Link-local IPv6 Address . . . . . : fe80::69fa:b8f3:166e:c64b%8
IPv4 Address. . . . . : 192.168.1.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::c002:9dff:fe08:0%8
192.168.1.1

```

Figure 6.2.4 5 ipconfig IPv6

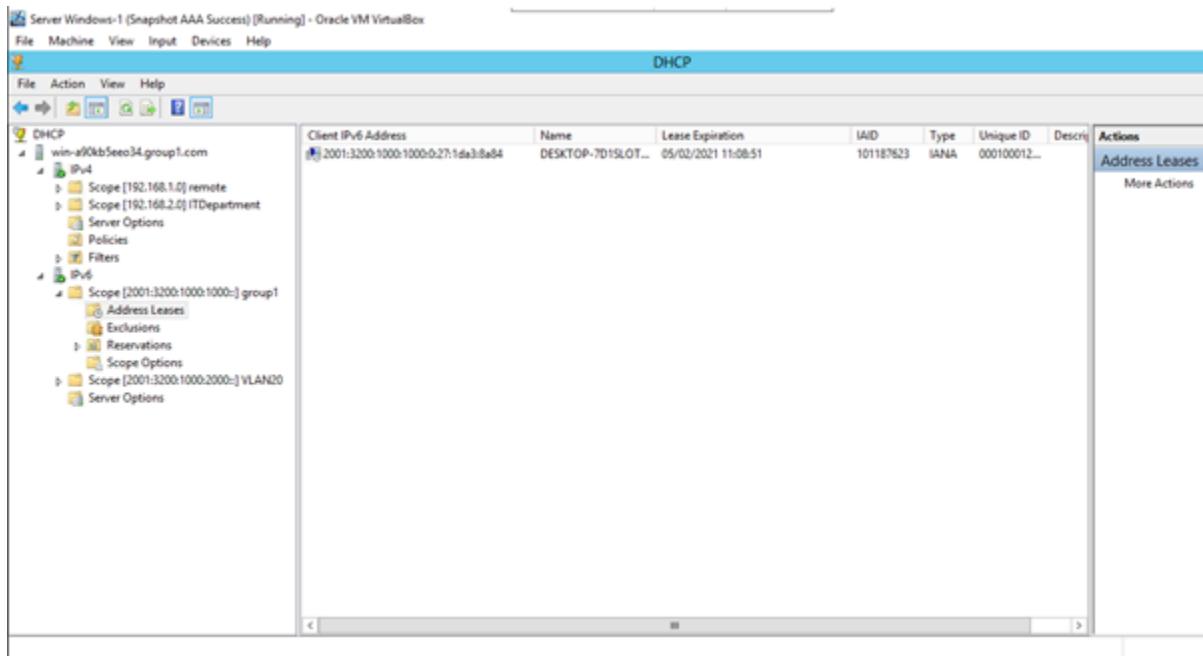


Figure 6.2.4 6 Address Lease IPv6

6.2.5. Web, SSL and Virtual Hosting

Web

Search <http://www.group1.com>

NAME	MATRIC NO.
NURUL AFIFAH BINTI AHMAD MAHIN	B031810378
MUHAMMAD ARIQ BIN ADNAN	B031810393
AHMAD FARIS BIN MAZLAN	B031810253
AMIRAH SYAHIRAH BINTI ARIFFIN	B031810233
AHMAD AKMAL AZIM BIN ZULKIFLI	B031810402
TAN CHUN YONG	B031810217

Figure 6.2.5.1 Web

SSL

Search <https://www.group1.com>

NAME	MATRIC NO.
NURUL AFIFAH BINTI AHMAD MAHIN	B031810378
MUHAMMAD ARIQ BIN ADNAN	B031810393
AHMAD FARIS BIN MAZLAN	B031810253
AMIRAH SYAHIRAH BINTI ARIFFIN	B031810233

Figure 6.2.5.2 SSL

Virtual Host

Search <http://vhgroup1.com>



Figure 6.2.5.3 Virtual Host

6.2.6. Linux Email Server

Receive email from other AD user

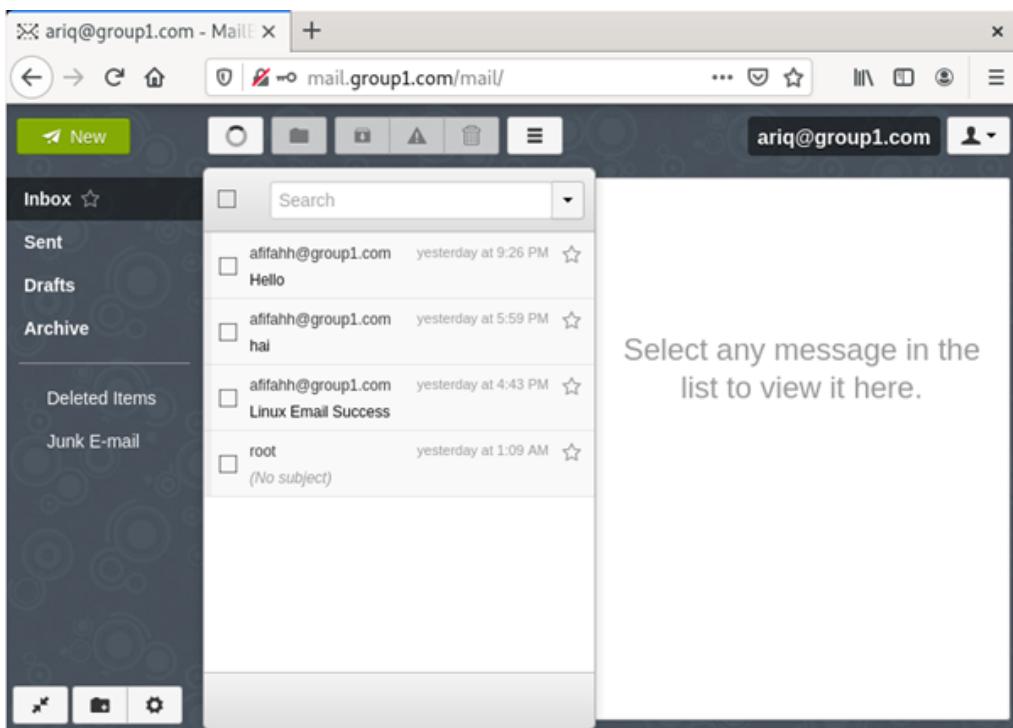


Figure 6.2.6.1 Inbox

Send email success

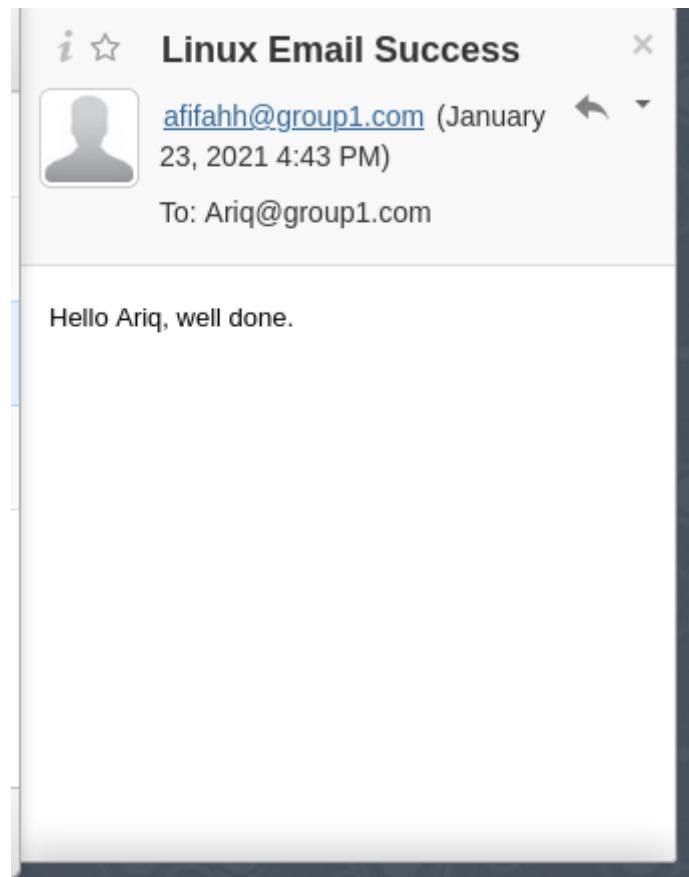


Figure 6.2.6.2 Success send

6.2.7. Access Control List

Step 1: Open nagios in a web browser before applying acl of rule 1 at RemoteAccess client.

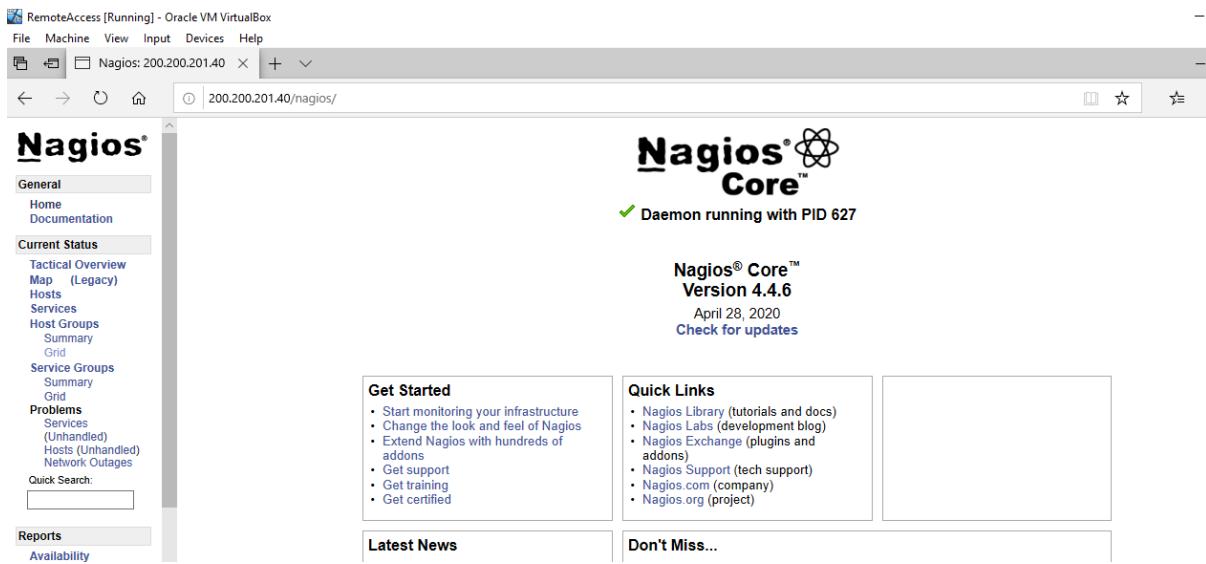


Figure 6.2.7.1 Test nagios before apply acl rule 1

Step 2: Open nagios in a web browser after applying acl of rule 1 at RemoteAccess client.



Figure 6.2.7.2 Test nagios after apply acl rule 1

Step 3: Open linux email in a web browser before applying acl of rule 1 at RemoteAccess client.

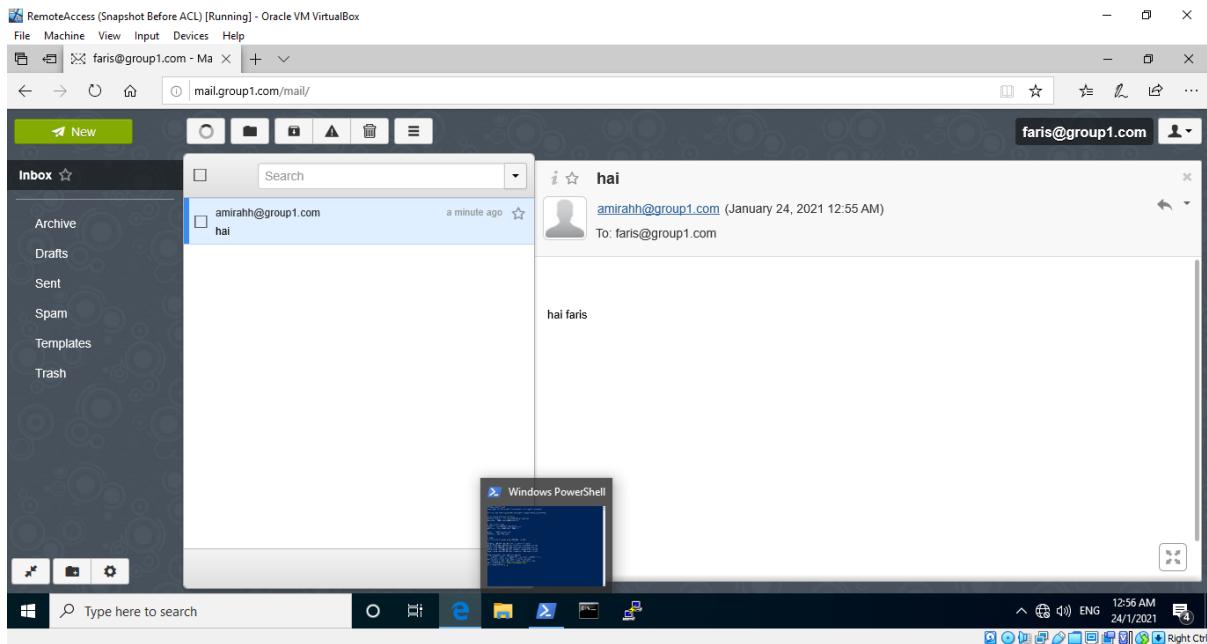


Figure 6.2.7.3 Test linux emails before apply acl rule 1

Step 4: Open linux email in a web browser after applying acl of rule 1 at RemoteAccess client.

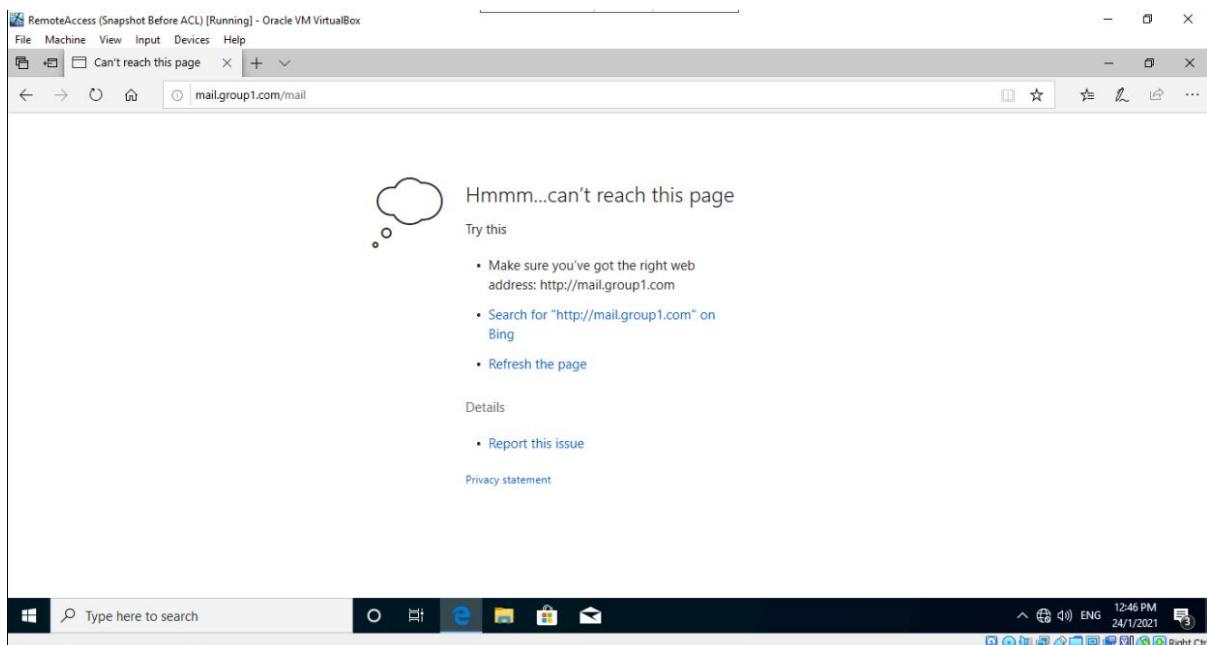


Figure 6.2.7.4 Test linux emails after apply acl rule 1

Step 5: Access ftp user before applying acl of rule 2 at RemoteAccess client.

```
PS C:\Users\Group1> ftp 200.200.201.40
Connected to 200.200.201.40.
220 (vsFTPD 3.0.3)
200 Always in UTF8 mode.
User (200.200.201.40:(none)): ftpuser
331 Please specify the password.
Password:
230 Login successful.
ftp>
```

Figure 6.2.7.5 Test ftp before apply acl rule 2

Step 6: Access ftp user after applying acl of rule 2 at RemoteAccess client.

```
PS C:\Users\Group1> ftp 200.200.201.40
> ftp: connect :Connection timed out
ftp> -
```

Figure 6.2.7.6 Test ftp after apply acl rule 2

Step 7: Open ssh in PuTTY before applying acl of rule 3 at RemoteAccess client.

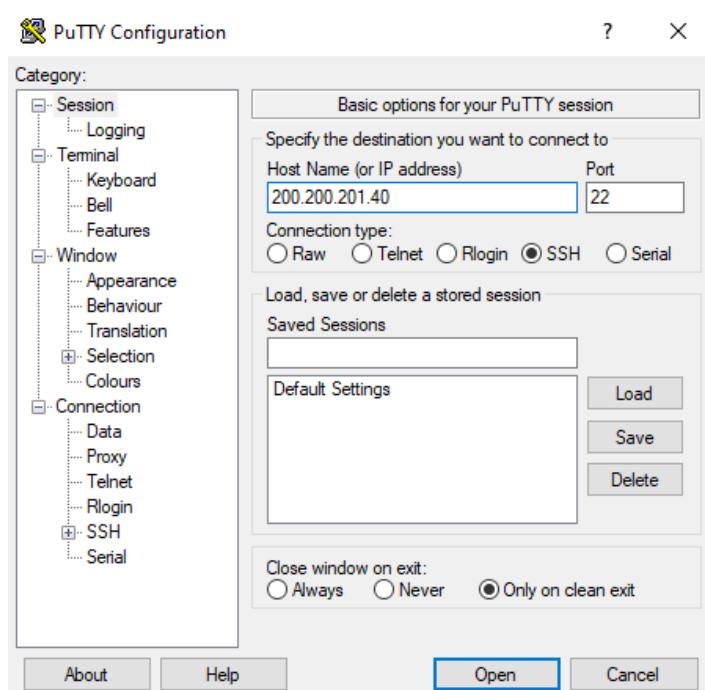
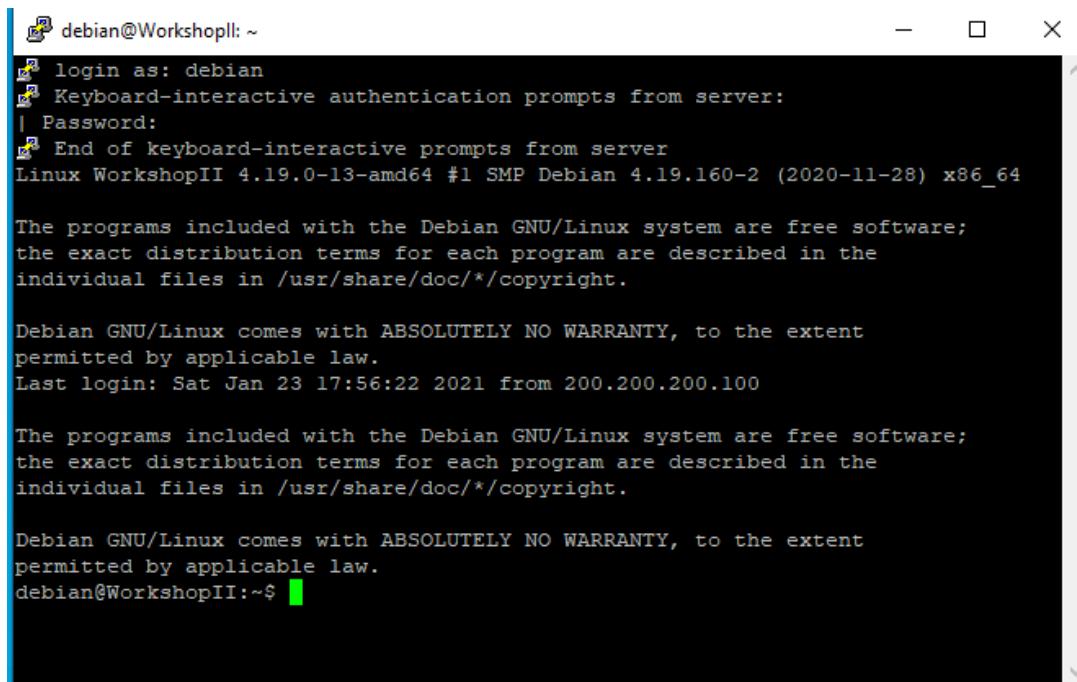


Figure 6.2.7.7 Setup to connect ssh



```
debian@WorkshopII: ~
login as: debian
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
Linux WorkshopII 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Jan 23 17:56:22 2021 from 200.200.200.100

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
debian@WorkshopII:~$
```

Figure 6.2.7.8 Test ssh before apply acl rule 3

Step 8: Open ssh in PuTTY after applying acl of rule 3 at RemoteAccess client.

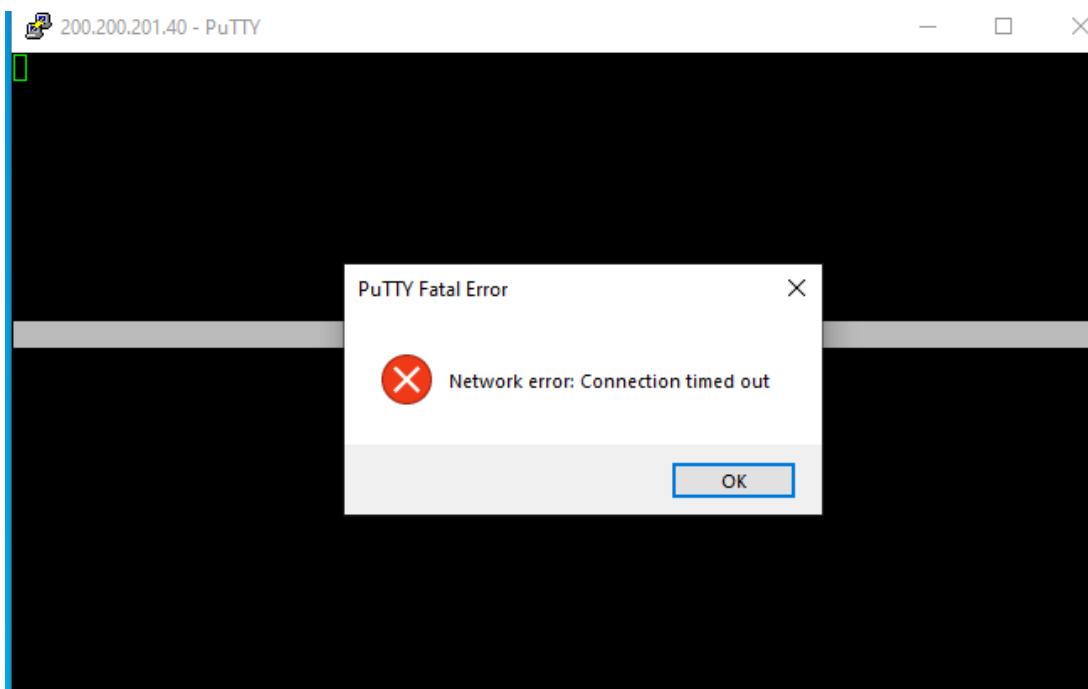


Figure 6.2.7.9 Test ssh after apply acl rule 3

Step 9: Open telnet in PuTTY before applying acl of rule 4 at RemoteAccess client.

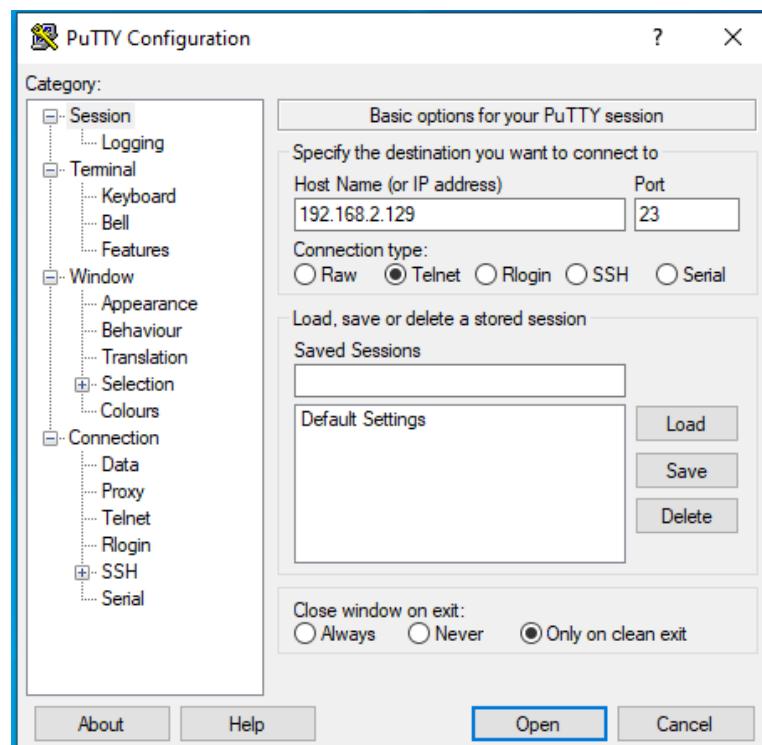


Figure 6.2.7.10 Setup to connect telnet

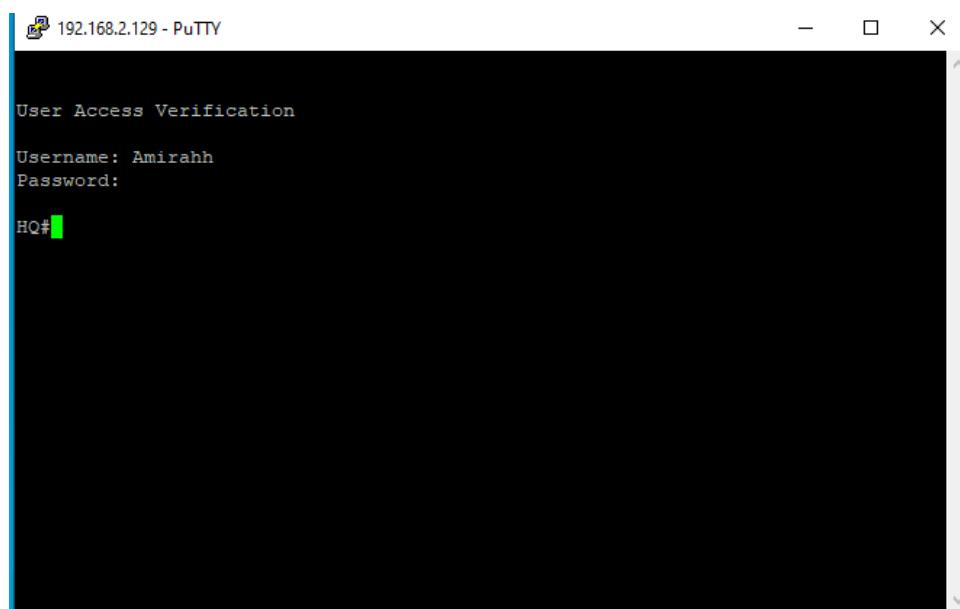


Figure 6.2.7.11 Test telnet before apply acl rule 4

Step 10: Open telnet in PuTTY after applying acl of rule 4 at RemoteAccess client.

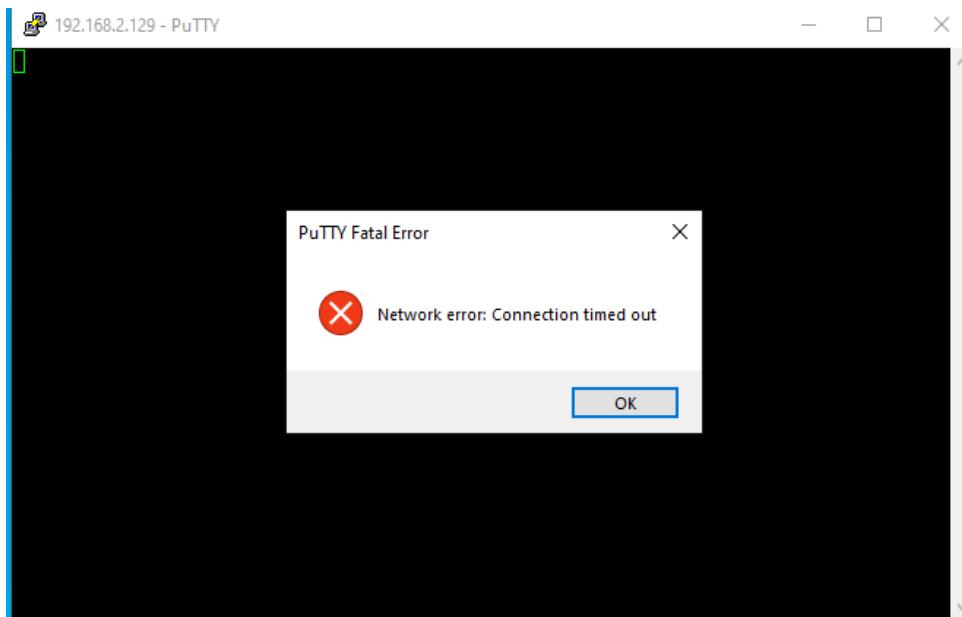


Figure 6.2.7.12 Test telnet after apply acl rule 4

6.2.8. IPSec Site-to-Site Tunneling

Step 1 : show that isakmp is active by using “show crypto isakmp sa” .

```
; Success rate is 0 percent (0/5)
HQ#sh cry isa sa
IPv4 Crypto ISAKMP SA
dst           src           state      conn-id slot status
200.200.200.6 200.200.201.1  QM_IDLE    1001     0 ACTIVE
IPv6 Crypto ISAKMP SA
```

Figure 6.2.8 3 Tunnel is active

Step 2 : Show the ipsec by using command "show crypto ipsec sa" .

```

HQ#sh crypto ipsec sa
interface: Serial0/0
  Crypto map tag: VPN-MAP, local addr 200.200.201.1

  protected vrf: (none)
  local ident (addr/mask/prot/port): (200.200.201.1/255.255.255.255/47/0)
  remote ident (addr/mask/prot/port): (200.200.200.6/255.255.255.255/47/0)
  current_peer 200.200.200.6 port 500
    PERMIT, flags=(origin_is_acl,)
  #pkts encaps: 27, #pkts encrypt: 27, #pkts digest: 27
  #pkts decaps: 110, #pkts decrypt: 110, #pkts verify: 110
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

  local crypto endpt.: 200.200.201.1, remote crypto endpt.: 200.200.200.6
  path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0
  current outbound spi: 0x859592F(140073263)

  inbound esp sas:
    spi: 0x44A96D0A(1151954186)
      transform: esp-aes esp-sha-hmac ,
      in use settings ={Tunnel, }
    conn id: 29, flow_id: SW:29, crypto map: VPN-MAP
    sa timing: remaining key lifetime (k/sec): (4465508/3231)
    IV size: 16 bytes
    replay detection support: Y

```

Figure 6.2.8 2 Current IPSec configuration

Step 3 : Show the ipsec mapping by using command "show crypto session" .

```

HQ#sh crypto sess
Crypto session current status

Interface: Serial0/0
Session status: UP-ACTIVE
Peer: 200.200.200.6 port 500
  IKE SA: local 200.200.201.1/500 remote 200.200.200.6/500 Active
  IPSEC FLOW: permit 47 host 200.200.201.1 host 200.200.200.6
    Active SAs: 2, origin: crypto map

```

Figure 6.2.8 3 Ipsec mapping table

6.2.9. Network Management System

All success monitored services

Linux Servers (linux-servers) -localhost Nagios Core

Step1: Check status monitoring for Localhost Nagios Core

Service Status Details For Host 'localhost'								
Host		Service		Status	Last Check	Duration	Attempt	Status Information
localhost	Current Load		OK	01-24-2021 18:17:43	19d 6h 48m 54s	1/4	OK - load average: 0.02, 0.17, 0.16	
	Current Users		OK	01-24-2021 18:14:31	27d 5h 11m 20s	1/4	USERS OK - 1 users currently logged in	
	HTTP		OK	01-24-2021 18:15:29	1d 2h 46m 7s	1/4	HTTP OK: HTTP/1.1 200 OK - 10975 bytes in 0.000 second response time	
	PING		OK	01-24-2021 18:16:27	8d 8h 50m 49s	1/4	PING OK - Packet loss = 0%, RTA = 0.04 ms	
	Root Partition		OK	01-24-2021 18:17:26	27d 5h 6m 58s	1/4	DISK OK - free space: / 20059 MB (76.50% inode=89%)	
	SSH		OK	01-24-2021 18:17:43	5d 18h 22m 22s	1/4	SSH OK - OpenSSH_7.9p1 Debian-10+deb10u2 (protocol 2.0)	
	Swap Usage		OK	01-24-2021 18:17:43	27d 5h 5m 43s	1/4	SWAP OK - 100% free (2041 MB out of 2046 MB)	
	Total Processes		OK	01-24-2021 18:17:43	27d 5h 5m 5s	1/4	PROCS OK: 53 processes with STATE = RSZDT	

[Page Tour](#)

Figure 6.2.9.1 Status monitoring for localhost

Network Environment (Devices) - Router and switches

Step 2: Check status monitoring for Router HQ

Service Status Details For Host 'RouterHQ'

Host	Service	Status	Last Check	Duration	Attempt	Status Information
RouterHQ	PING		OK	01-05-2021 15:19:43	0d 5h 27m 42s	1/3
	Port fo/0.20 In		OK	01-05-2021 15:17:46	0d 0h 22m 21s	1/3
	Port fo/0.20 Out		OK	01-05-2021 15:13:02	0d 0h 17m 5s	1/3
	Port fo/0.30 In		OK	01-05-2021 15:11:36	0d 0h 18m 31s	1/3
	Port fo/0.30 Out		OK	01-05-2021 15:12:40	0d 0h 17m 27s	1/3
	Port fo/0.40 In		OK	01-05-2021 15:13:43	0d 0h 16m 24s	1/3
	Port fo/0.40 Out		OK	01-05-2021 15:14:47	0d 0h 15m 20s	1/3
	Port s0/0 In		OK	01-05-2021 15:17:30	0d 0h 22m 37s	1/3
	Port s0/0 Out		OK	01-05-2021 15:16:55	0d 0h 23m 12s	1/3
	Uptime		OK	01-05-2021 15:17:58	0d 0h 22m 9s	1/3

Figure 6.2.9.2 Status monitoring for Router HQ

Step 3: Check status monitoring for Router Branch

Service Status Details For Host 'RouterBranch'

Host	Service	Status	Last Check	Duration	Attempt	Status Information
RouterBranch	PING		OK	01-05-2021 15:17:29	0d 0h 21m 33s	1/3
	Port fo/0.10 In		OK	01-05-2021 15:17:03	0d 0h 21m 55s	1/3
	Port fo/0.10 Out		OK	01-05-2021 15:17:54	0d 0h 21m 4s	1/3
	Port s0/1 In		OK	01-05-2021 15:08:58	0d 0h 20m 0s	1/3
	Port s0/1 Out		OK	01-05-2021 15:10:01	0d 0h 18m 57s	1/3
	Uptime		OK	01-05-2021 15:17:03	0d 0h 21m 55s	1/3

Figure 6.2.9.3 Status monitoring for Router Branch

Step 4: Check status monitoring for Switch HQ

Service Status Details For Host 'SwitchHQ'

Limit Results: 100 ▾

Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
SwitchHQ	PING	OK	01-05-2021 15:19:43	0d 4h 8m 16s	1/3	PING OK - Packet loss = 0%, RTA = 20.51 ms
	Port g0/0 In	OK	01-05-2021 15:16:33	0d 0h 14m 35s	1/3	SNMP OK - 32997785
	Port g0/0 Out	OK	01-05-2021 15:15:45	0d 0h 5m 43s+	1/3	SNMP OK - 35728477
	Port g0/1 In	OK	01-05-2021 15:18:34	0d 0h 22m 34s	1/3	SNMP OK - 1874861
	Port g0/1 Out	OK	01-05-2021 15:16:17	0d 0h 5m 1s	1/3	SNMP OK - 2606580
	Port g0/2 In	OK	01-05-2021 15:17:27	0d 0h 23m 41s	1/3	SNMP OK - 18278354
	Port g0/2 Out	OK	01-05-2021 15:16:37	0d 0h 4m 39s	1/3	SNMP OK - 27790840
	Port g0/3 In	OK	01-05-2021 15:16:55	0d 0h 4m 23s	1/3	SNMP OK - 6565338
	Port g0/3 Out	OK	01-05-2021 15:17:03	0d 0h 5m 43s+	1/3	SNMP OK - 4860869
	Uptime	OK	01-05-2021 15:18:24	0d 0h 22m 44s	1/3	SNMP OK - Timeticks: (4130649) 11:28:26.49

age Tour

Figure 6.2.9.4 Status monitoring for Switch HQ

Step 5: Check status monitoring for Switch Branch

Service Status Details For Host 'SwitchBranch'

Limit Results: 100 ▾

Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
SwitchBranch	PING	OK	01-06-2021 21:10:27	0d 0h 31m 46s	1/3	PING OK - Packet loss = 0%, RTA = 52.13 ms
	Port g0/0 In	OK	01-06-2021 21:08:23	0d 0h 13m 42s	1/3	SNMP OK - 1581070
	Port g0/0 Out	OK	01-06-2021 21:08:37	0d 0h 13m 28s	1/3	SNMP OK - 7123227
	Port g0/1 Out	OK	01-06-2021 21:08:50	0d 0h 13m 15s	1/3	SNMP OK - 2233237
	Uptime	OK	01-06-2021 21:10:37	0d 0h 31m 28s	1/3	SNMP OK - Timeticks: (4474287) 12:25:42.87

Figure 6.2.9.5 Status monitoring for Switch Branch

Linux Servers (linux-server) - (hostname: WorkshopII)

Step 6: Check status monitoring for Server Debian

Service Status Details For Host 'WorkshopII'							
Host	Service	Status	Last Check	Duration	Attempt	Status Information	
WorkshopII	Current Load	WARNING	01-24-2021 18:35:23	0d 0h 6m 20s	4/4	WARNING - load average: 0.00, 0.03, 0.08	
	Current Users	OK	01-24-2021 18:36:20	0d 7h 25m 24s	1/4	USERS OK - 1 users currently logged in	
	FTP	OK	01-24-2021 18:32:17	0d 7h 24m 26s	1/4	FTP OK - 0.001 second response time on 192.168.2.146 port 21 [220 (vsFTPD 3.0.3)]	
	Linux Email	OK	01-24-2021 18:32:43	0d 7h 24m 0s	1/4	SMTP OK - 0.042 sec. response time	
	Root / Partition	OK	01-24-2021 18:32:43	0d 7h 24m 0s	1/4	DISK OK - free space: / 20058 MB (76% inode=89%)	
	Total Processes	WARNING	01-24-2021 18:32:44	0d 1h 48m 59s	4/4	PROCS WARNING: 197 processes	

Figure 6.2.9.6 Status monitoring for Server Debian

Windows Servers (windows-servers) - (hostname: WIN-A90KB5EE034)

Step 7: Check status monitoring for Server Windows

Service Status Details For Host 'WIN-A90KB5EE034'							
Host	Service	Status	Last Check	Duration	Attempt	Status Information	
WIN-A90KB5EE034	Active Directory Domain Services	OK	01-06-2021 02:48:20	0d 0h 29m 44s	1/3	NTDS: Started	
	C:\ Drive Space	OK	01-06-2021 02:48:16	0d 0h 40m 16s	1/3	C: - total: 49.66 Gb - used: 10.58 Gb (21%) - free 39.07 Gb (79%)	
	CPU Load	OK	01-06-2021 02:38:42	0d 0h 39m 42s	1/3	CPU Load 0% (5 min average)	
	DHCP Server	OK	01-06-2021 02:48:18	0d 0h 41m 38s	1/3	DHCPServer: Started	
	DNS Server	OK	01-06-2021 02:48:18	0d 0h 28m 58s	1/3	DNS: Started	
	Memory Usage	OK	01-06-2021 02:39:15	0d 0h 39m 18s	1/3	Memory usage: total:2431.57 MB - used: 1021.86 MB (42%) - free: 1409.71 MB (58%)	
	NSClient++ Version	OK	01-06-2021 02:44:43	0d 0h 53m 41s	1/3	NSClient++ 0.5.2.35 2018-01-28	
	Uptime	OK	01-06-2021 02:39:49	0d 0h 38m 44s	1/3	System Uptime - 0 day(s) 1 hour(s) 3 minute(s)	
	World Wide Web Publishing Service	OK	01-06-2021 02:48:20	0d 0h 41m 38s	1/3	W3SVC: Started	

Figure 6.2.9.7 Status monitoring for Server Windows

Testing for status services

- Server Debian

Step 8: Test one of the services (FTP Server) to stop working

```
debian@WorkshopII:~$ sudo service vsftpd stop
debian@WorkshopII:~$ sudo service vsftpd status
● vsftpd.service - vsftpd FTP server
  Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: e
  Active: inactive (dead) since Sun 2021-01-03 14:09:42 +08; 13s ago
    Process: 682 ExecStart=/usr/sbin/vsftpd /etc/vsftpd.conf (code=killed, signal=
  Main PID: 682 (code=killed, signal=TERM)

Jan 03 13:13:51 WorkshopII systemd[1]: Starting vsftpd FTP server...
Jan 03 13:13:51 WorkshopII systemd[1]: Started vsftpd FTP server.
Jan 03 14:09:42 WorkshopII systemd[1]: Stopping vsftpd FTP server...
Jan 03 14:09:42 WorkshopII systemd[1]: vsftpd.service: Main process exited, code
Jan 03 14:09:42 WorkshopII systemd[1]: vsftpd.service: Succeeded.
Jan 03 14:09:42 WorkshopII systemd[1]: Stopped vsftpd FTP server.

[1]+  Stopped                  sudo service vsftpd status
```

Figure 6.2.9.8 Stop service FTP Server

Step 9: Check status monitoring for Server Debian. It shows the start of FTP Service is in critical.

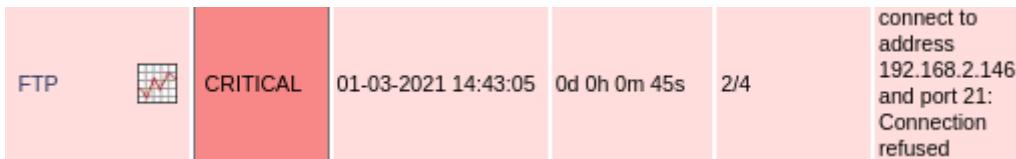


Figure 6.2.9.9 Status FTP is critical

Step 10: Start service FTP Server to start working

```
debian@WorkshopII:~$ sudo systemctl start vsftpd
debian@WorkshopII:~$ sudo service vsftpd status
● vsftpd.service - vsftpd FTP server
  Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: e
  Active: active (running) since Sun 2021-01-03 14:11:08 +08; 9s ago
    Process: 2128 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, s
  Main PID: 2129 (vsftpd)
    Tasks: 1 (limit: 2347)
   Memory: 844.0K
      CGroup: /system.slice/vsftpd.service
              └─2129 /usr/sbin/vsftpd /etc/vsftpd.conf

Jan 03 14:11:08 WorkshopII systemd[1]: Starting vsftpd FTP server...
Jan 03 14:11:08 WorkshopII systemd[1]: Started vsftpd FTP server.

[2]+  Stopped                  sudo service vsftpd status
```

Figure 6.2.9.10 Start service FTP Server

Step 11: Check status monitoring for Server Debian. It shows the start of FTP Service is OK.

FTP		OK	01-03-2021 14:37:34	0d 0h 30m 4s	1/4	FTP OK - 0.004 second response time on 192.168.2.146 port 21 [220 (vsFTPD 3.0.3)]
-----	--	----	---------------------	--------------	-----	---

Figure 6.2.9.11 Status FTP is OK

Testing for status services

- Server Windows

Step 12: Test one of the services to stop working. Stop the process of World Wide Web Publishing Service (Web Server)

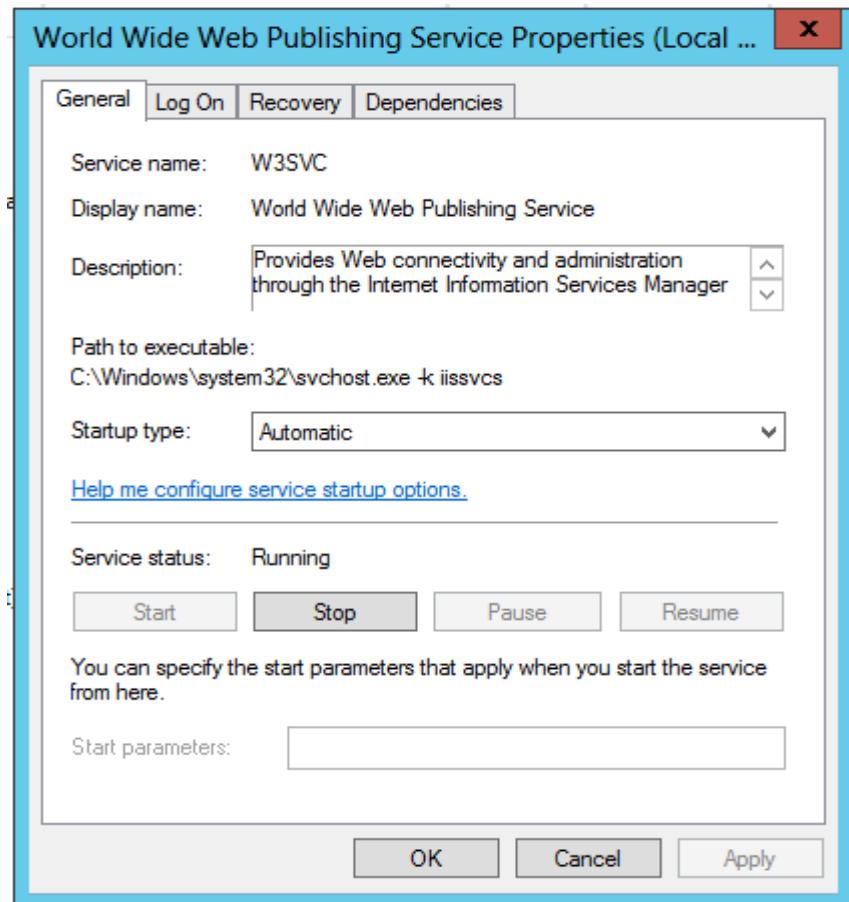


Figure 6.2.9.12 Stop service Web Server

Step 13: Check status monitoring for Server Windows. It shows the start of Web Service is critical.

World Wide Web Publishing Service		CRITICAL	01-03-2021 22:17:01	0d 0h 0m 22s	3/3	W3SVC: Stopped
--	---	----------	---------------------	--------------	-----	-------------------

Figure 6.2.9.13 Status Web service is critical

Step 14: Start service Web Server to start working

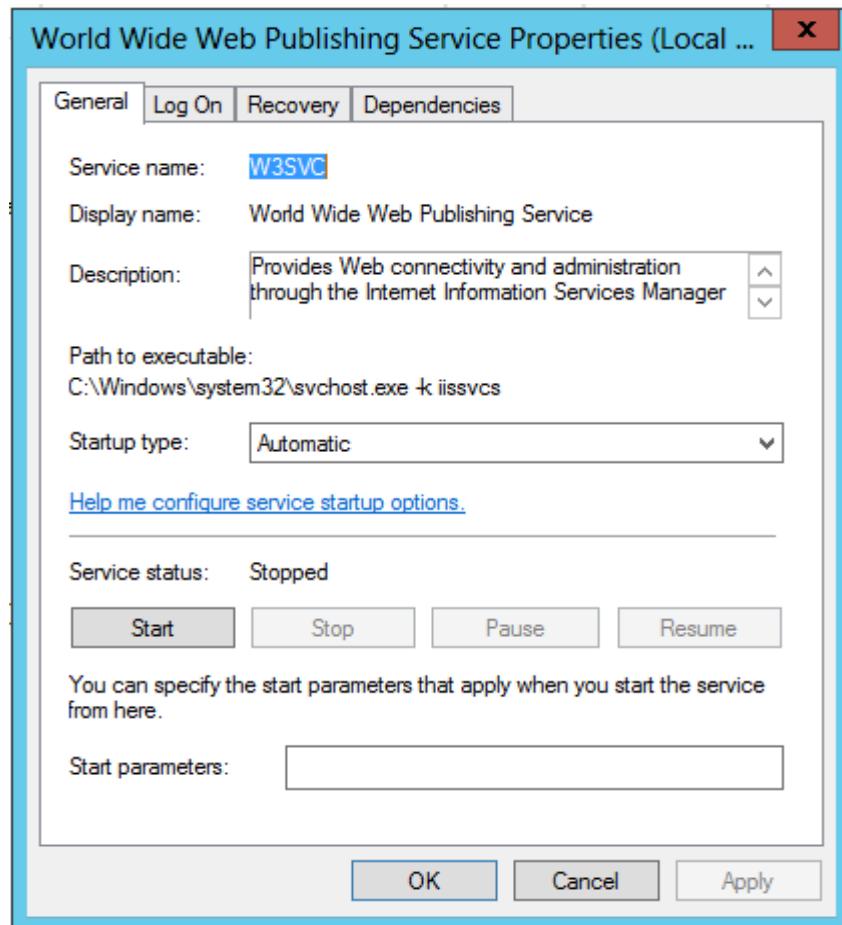


Figure 6.2.9.14 Start service Web Server

Step 15: Check status monitoring for Server Windows. It shows the start of Web Service is OK.

World Wide Web Publishing Service		OK	01-03-2021 22:19:21	0d 0h 0m 29s	1/3	W3SVC: Started
--	---	----	---------------------	--------------	-----	-------------------

Figure 6.2.9.15 Status Web service is OK

6.2.10. AAA (Authentication, Authorization and Accounting) using Radius

Privilege level 15

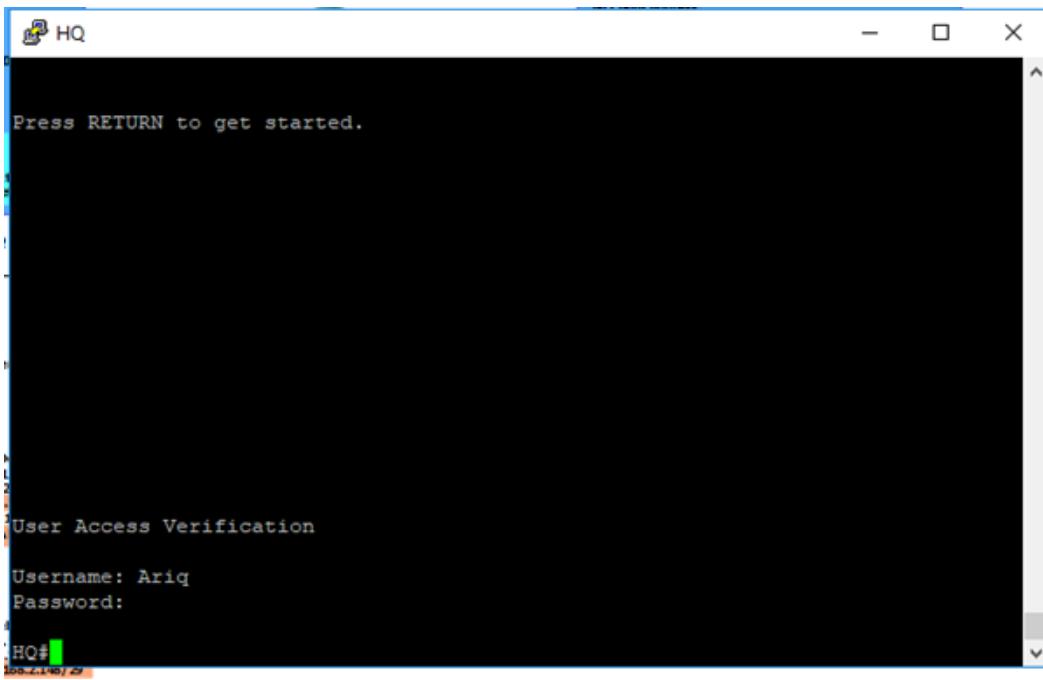


Figure 6.2.10.1 privilege level 15

Privilege level 1

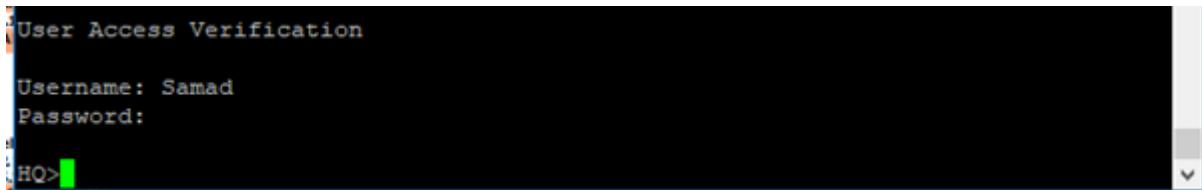


Figure 6.2.10.2 privilege level 1

6.2.11. Layer 2 Security - VLAN and Port Security

Port Security

Step 1 : Display the security action using #sh port-security. From this command, status for unused port are shown.

Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
Gi0/1	2	1	0	Restrict
Gi0/2	2	2	0	Restrict
Gi0/3	2	1	0	Restrict

Figure 6.2.11.1 sh port-security for SwitchHQ

Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
Gi0/1	2	0	0	Restrict

Figure 6.2.11.2 sh port-security for SwitchBranch

Step 2 : Port security details can be seen by mention the port using #sh port-security address.

SwitchHQ#sh port-security address Secure Mac Address Table				
Vlan	Mac Address	Type	Ports	Remaining Age (mins)
20	0800.2702.6005	SecureSticky	Gi0/1	-
30	0800.2714.355d	SecureSticky	Gi0/2	-
30	da9a.6adc.cd6b	SecureSticky	Gi0/2	-
40	0800.2730.5f31	SecureSticky	Gi0/3	-

Figure 6.2.11.3 sh port-security address SwitchHQ

SwitchBranch#sh port-security address Secure Mac Address Table				
Vlan	Mac Address	Type	Ports	Remaining Age (mins)
10	0800.27e6.f800	SecureSticky	Gi0/1	-

Figure 6.2.11.4 sh port-security address SwitchBranch

Step 3 : Trunk port security details can be seen by mention the port using #sh int trunk port.

SwitchHQ#sh int trunk				
Port	Mode	Encapsulation	Status	Native vlan
Gi0/0	on	802.1q	trunking	100
Port		Vlans allowed on trunk		
Gi0/0		1-4094		
Port		Vlans allowed and active in management domain		
Gi0/0		1,20,30,40,100		
Port		Vlans in spanning tree forwarding state and not pruned		
Gi0/0		1,20,30,40,100		

Figure 6.2.11.5 sh int trunk SwitchHQ

```
SwitchBranch#sh int trunk

Port      Mode          Encapsulation  Status        Native vlan
Gi0/0     on           802.1q         trunking    100

Port      Vlans allowed on trunk
Gi0/0     1-4094

Port      Vlans allowed and active in management domain
Gi0/0     1,10,100

Port      Vlans in spanning tree forwarding state and not pruned
Gi0/0     1,10,100
```

Figure 6.2.11.6 sh int trunk SwitchBranch

VLAN Security

Step 1 : By using command ‘show vlan’ on switch

VLAN Name	Status	Ports
1 default	active	
20 ITDepartment	active	Gi0/1
30 Windows	active	Gi0/2
40 Debian	active	Gi0/3
100 Native	active	
110 unusedport	suspended	Gi1/0, Gi1/1, Gi1/2
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

Figure 6.2.11.7 sh vlan for SwitchHQ

VLAN Name	Status	Ports
1 default	active	
10 RemoteAccess	active	Gi0/1
100 Native	active	
110 unusedport	suspended	Gi0/2, Gi0/3, Gi1/0, Gi1/1 Gi1/2
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

Figure 6.2.11.8 sh vlan for SwitchBranch

6.2.12. Samba and Samba security

Client PC

Step 1: Go to client PC, press windows key and R at the same time and type the host IP address of Windows terminal which has installed and configured the samba services

\\\192.168.2.146\samba-share.

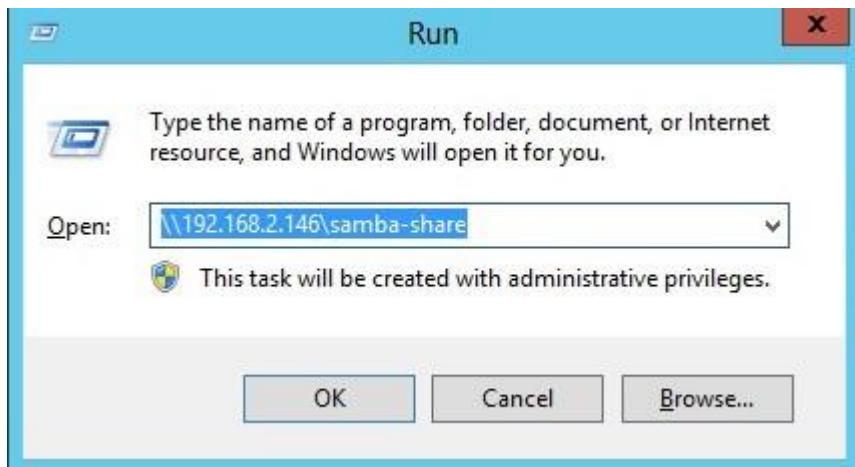


Figure 6.2.12.1 Running IP address

Step 2 : A small window network credentials will pop up requesting for username and password. Enter the username and password of the user that was added into samba group.



Figure 6.2.12.2 Entering username and password to access

Step 3 : The shared folder will be visible and accessible. The user can add, edit, delete and view the file in the samba-share folder.

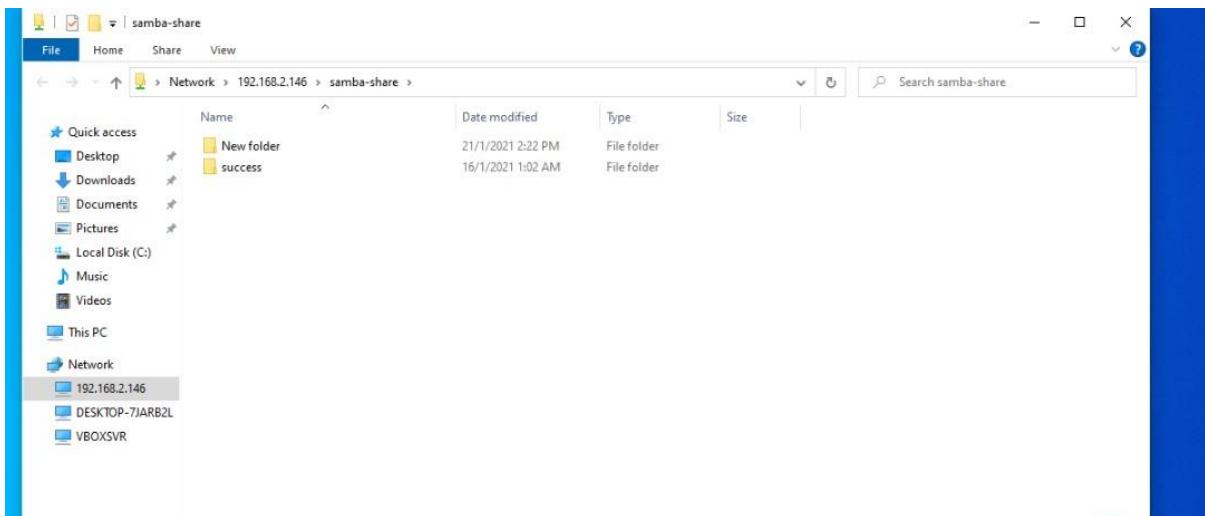


Figure 6.2.12.3 Share files in samba folder

Debian

Step 1: Go to ‘Connect to Server’ in Debian and click on it. Enter ‘smb://samba<server IP address>’ and click “Connect”.



Figure 6.2.12.4 Connect to server

Step 2 : It will pop up a request to log in as an anonymous or registered user. Choose registered user and fill in the username, domain and password then click connect.

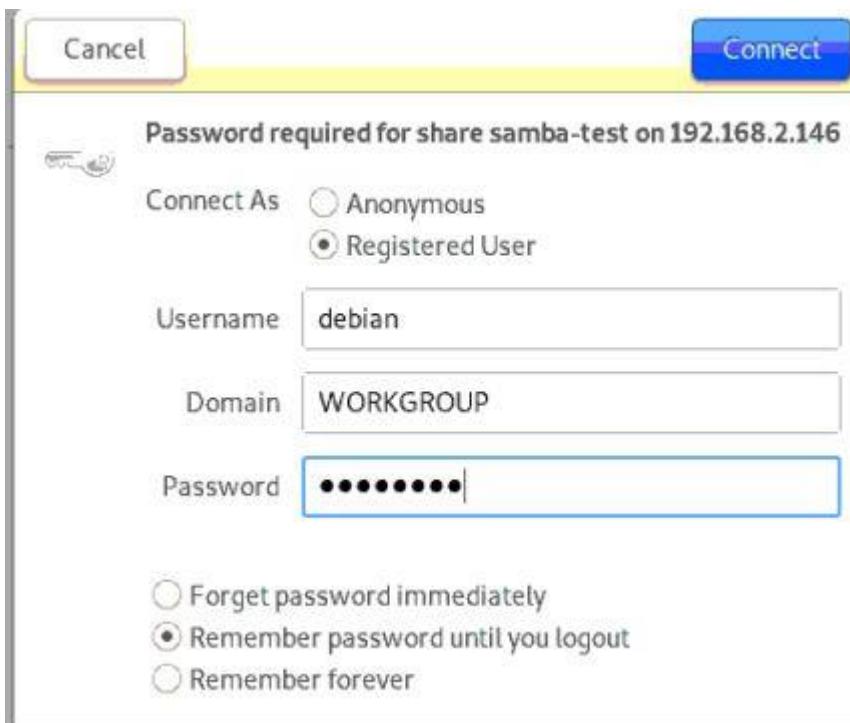


Figure 6.2.12.5 Enter credentials

Step 3 : The shared folder will be shown after that.

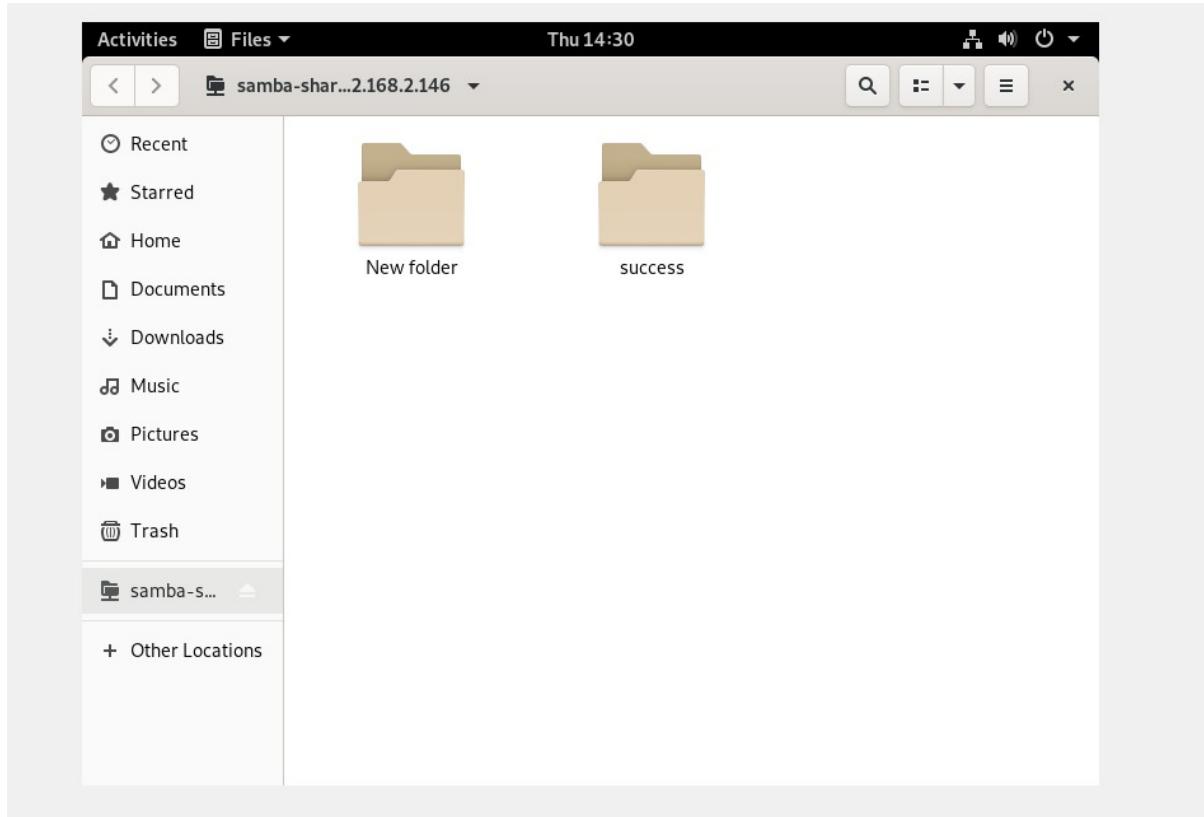


Figure 6.2.12.6 Share folder in Debian

6.2.13. User authentication user by integrating AD with linux

Debian Server

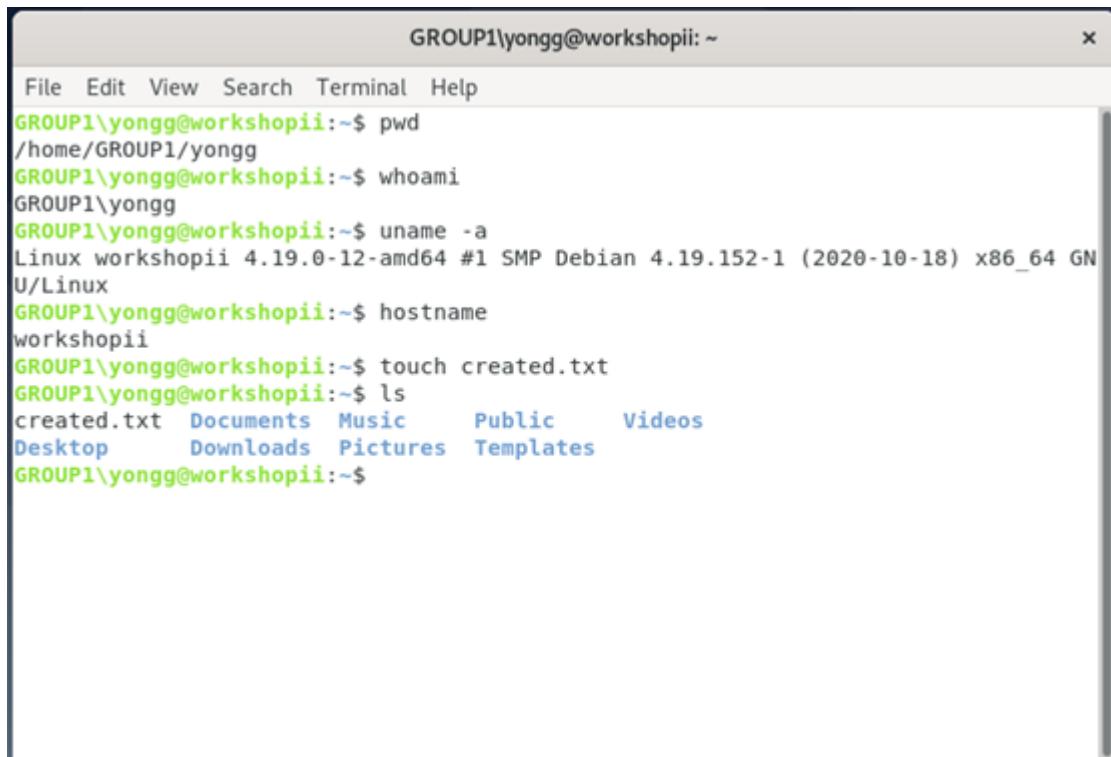
Step 1: Open Terminal and type in the following command to join a domain group. Insert all the credentials that are needed.

```
debian@workshopii: ~
File Edit View Search Terminal Help
debian@workshopii:~$ sudo domainjoin-cli join group1.com
Username: Yong
Joining to AD Domain: group1.com
With Computer DNS Name: workshopii.group1.com

Yong@GROUP1.COM's password:
SUCCESS
debian@workshopii:~$
```

Figure 6.2.13.1 Re-joining AD domain group

Step 2: In the login area, to login for the AD account, type in <USERNAME@DOMAIN_NAME> and password that have been created during the AD service configuration earlier.



The screenshot shows a terminal window titled "GROUP1\yongg@workshopii: ~". The window contains the following command-line session:

```
GROUP1\yongg@workshopii:~$ pwd
/home/GROUP1/yongg
GROUP1\yongg@workshopii:~$ whoami
GROUP1\yongg
GROUP1\yongg@workshopii:~$ uname -a
Linux workshopii 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64 GNU
U/Linux
GROUP1\yongg@workshopii:~$ hostname
workshopii
GROUP1\yongg@workshopii:~$ touch created.txt
GROUP1\yongg@workshopii:~$ ls
created.txt  Documents  Music  Public  Videos
Desktop      Downloads  Pictures  Templates
GROUP1\yongg@workshopii:~$
```

Figure 6.2.13.2 Login successful for AD account

Step 3: Switch to Windows Server workstation and check for the connected Debian system.

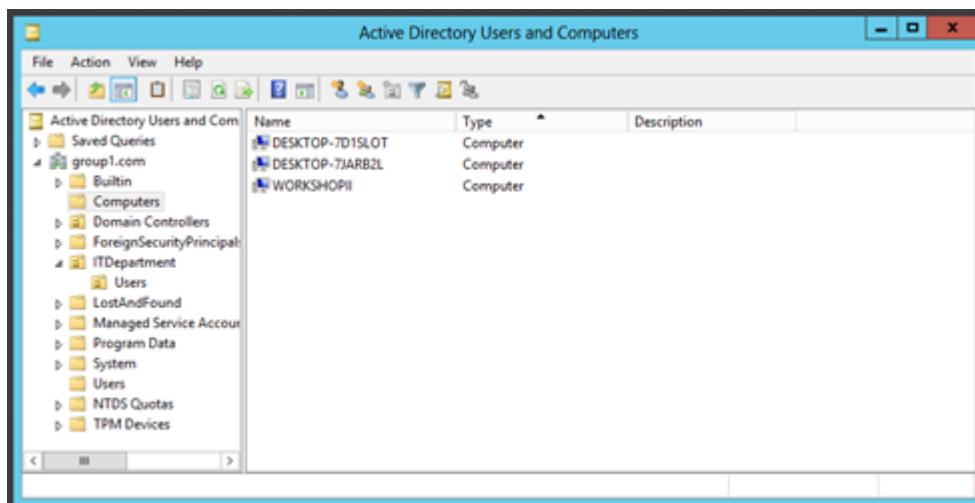
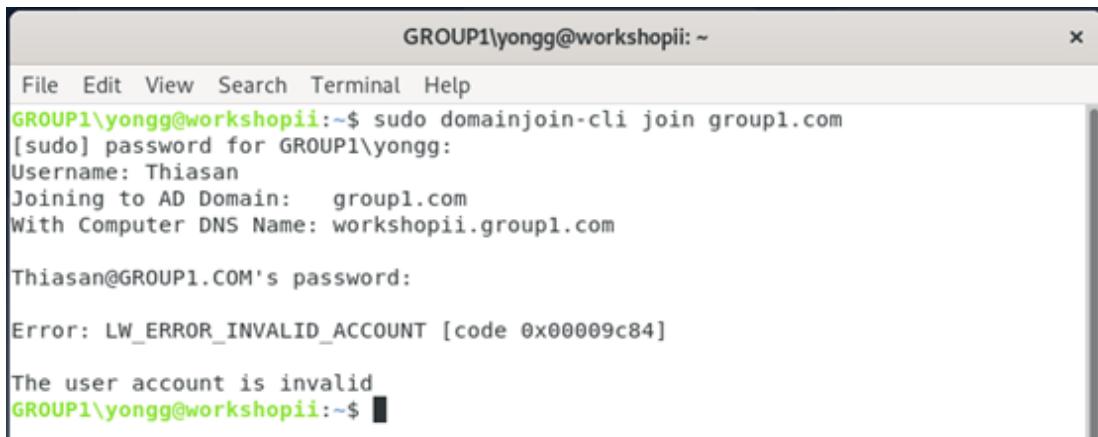


Figure 6.2.13.3 Check connected Debian system

Step 4: Verify for invalid users that does not exist in the Active Directory users.



```
GROUP1\yongg@workshopii: ~
File Edit View Search Terminal Help
GROUP1\yongg@workshopii:~$ sudo domainjoin-cli join group1.com
[sudo] password for GROUP1\yongg:
Username: Thiasan
Joining to AD Domain: group1.com
With Computer DNS Name: workshopii.group1.com

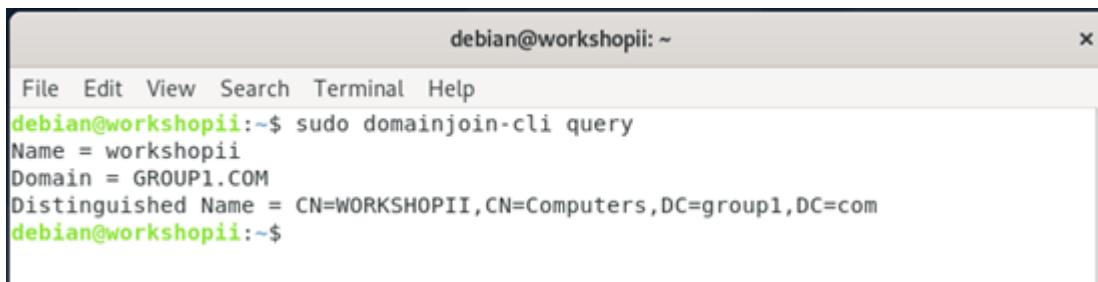
Thiasan@GROUP1.COM's password:

Error: LW_ERROR_INVALID_ACCOUNT [code 0x00009c84]

The user account is invalid
GROUP1\yongg@workshopii:~$
```

Figure 6.2.13.4 Verify invalid account

Step 5: Verify for the joined Active Directory domain with commands.



```
debian@workshopii: ~
File Edit View Search Terminal Help
debian@workshopii:~$ sudo domainjoin-cli query
Name = workshopii
Domain = GROUP1.COM
Distinguished Name = CN=WORKSHOPPII,CN=Computers,DC=group1,DC=com
debian@workshopii:~$
```

Figure 6.2.13.5 Verify AD domain on Debian Server

Step 6: If you want to remove or exit the machine from the domain, use sudo domainjoin-cli leave.



```
debian@workshopii:~$ sudo domainjoin-cli leave
Leaving AD Domain: GROUP1.COM
SUCCESS
debian@workshopii:~$
```

Figure 6.2.13.6 Leave domain on Debian

6.2.14. Intrusion Detection System (IDS) and Port Mirroring

Step 1: Testing IDS on the enp0s9 port

```
debian@WorkshopII:~$ cd /etc/snort
debian@WorkshopII:/etc/snort$ sudo snort -A console -i enp0s9 -u snort -g snort
-c /etc/snort/snort.conf
```

Figure 6.2.14.1: Command to run IDS for port enp0s9

Step 2: Try to ping and the output appeared as below

```
Commencing packet processing (pid=2908)
01/18-01:08:24.091491  [**] [1:10000002:2] ICMP test [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.2.4 -> 192.168.2.145
01/18-01:08:25.110298  [**] [1:10000002:2] ICMP test [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.2.4 -> 192.168.2.145
01/18-01:08:26.128432  [**] [1:10000002:2] ICMP test [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.2.4 -> 192.168.2.145
01/18-01:08:27.159057  [**] [1:10000002:2] ICMP test [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.2.4 -> 192.168.2.145
```

Figure 6.2.14.2: The output of the log that receives the data on port enp0s9

6.2.15. IPSec VPN server for remote employees

Clients Server in Window Server (IT Department)

Testing on Internal Network

Step 1 : Open the SoftEther VPN Client Manager and test for the connection.

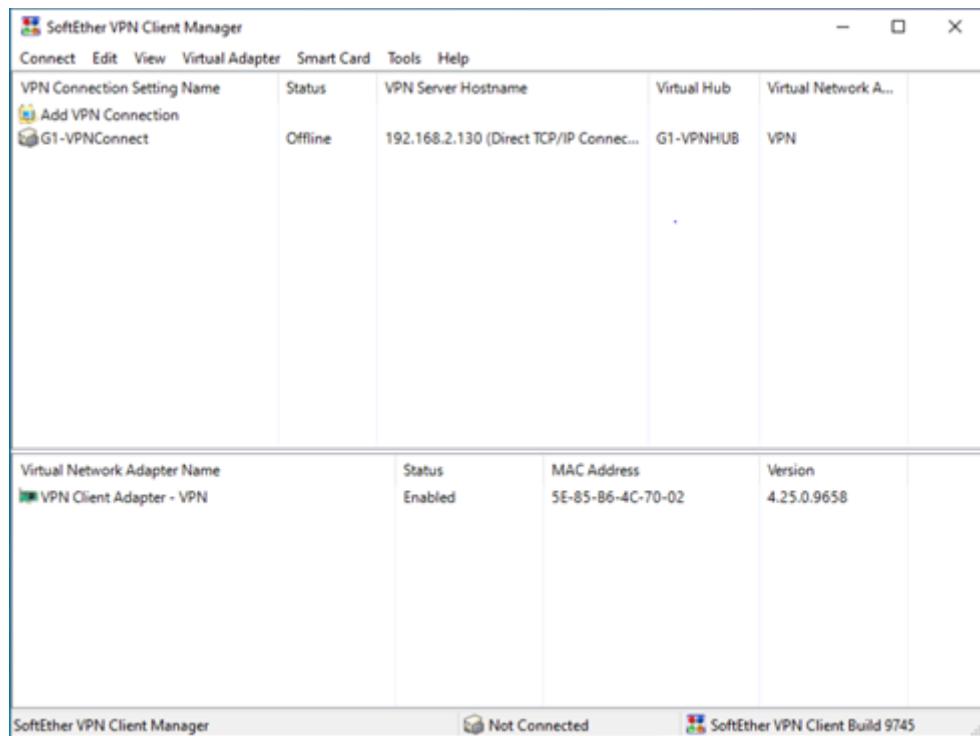


Figure 6.2.15.1 : GUI of SoftEther VPN Client Manager

Step 2 : Select VPN Connection (G1-VPNConnect) and select Connect.

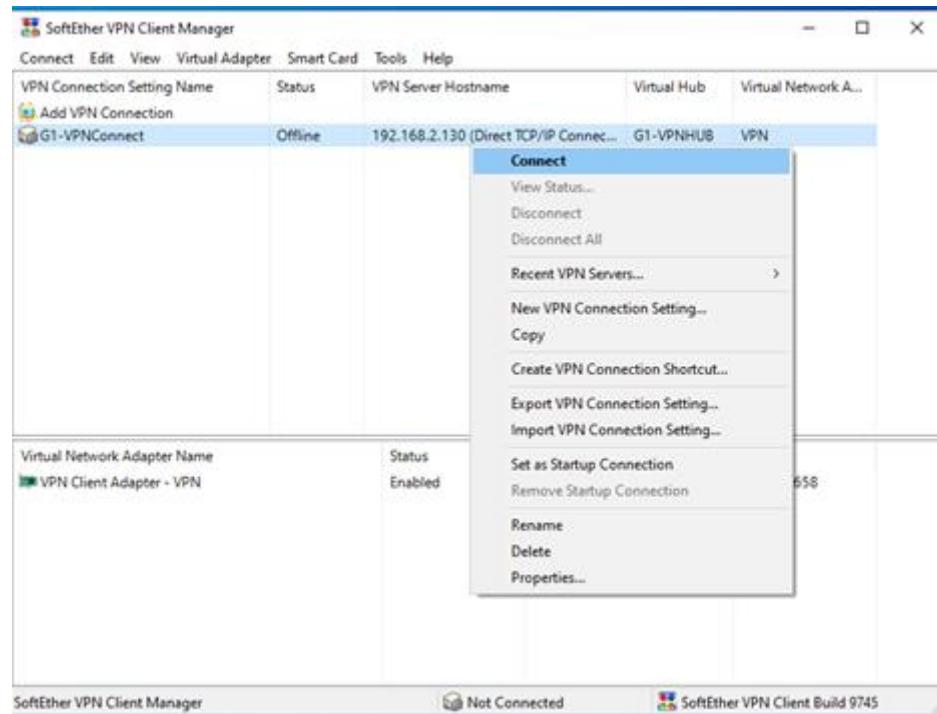


Figure 6.2.15.2 : Connect to VPN

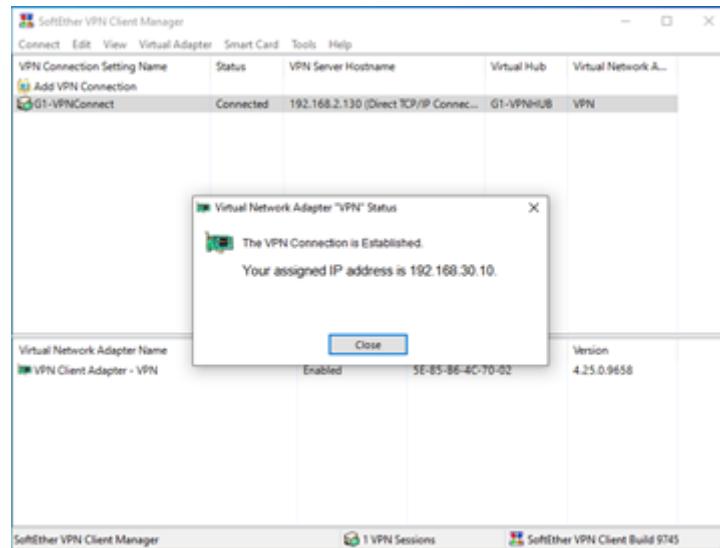


Figure 6.2.15.3 : Connection successful

Step 3 : Go to SoftEther VPN Server Manager machine and verify the VPN connection.

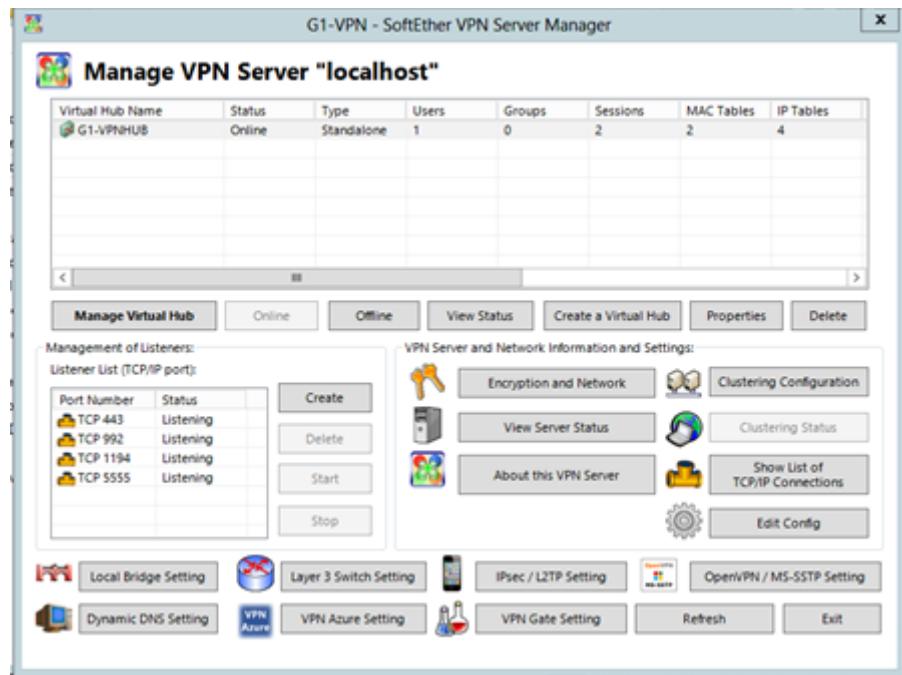


Figure 6.2.15.4 : Verify VPN Connection

Step 4 : Open command prompt and enter command ipconfig /all to verify the ip address assigned by SoftEther VPN.

```
Unknown adapter VPN - VPN Client:

Connection-specific DNS Suffix . : group1.com
Description . . . . . : VPN Client Adapter - VPN
Physical Address . . . . . : 5E-85-B6-4C-70-02
DHCP Enabled . . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::5d8b:4b7b:ab72:9445%15(Preferred)
IPv4 Address. . . . . : 192.168.30.10(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Saturday, 23 January, 2021 10:39:52 AM
Lease Expires . . . . . : Saturday, 23 January, 2021 12:39:52 PM
Default Gateway . . . . . : 192.168.30.1
DHCP Server . . . . . : 192.168.30.1
DHCPv6 IAID . . . . . : 257852854
DHCPv6 Client DUID. . . . . : 00-01-00-01-27-42-00-E5-08-00-27-02-60-05
DNS Servers . . . . . : 192.168.30.1
NetBIOS over Tcpip. . . . . : Enabled
```

Figure 6.2.15.5 : Verify IP address

Clients Server in Window Server (Remote Access)

Testing on External Network

Step 1 : Open the SoftEther VPN Client Manager and test for the connection to Group 1 client network and receive assigned IP address from Group 1 DHCP server.

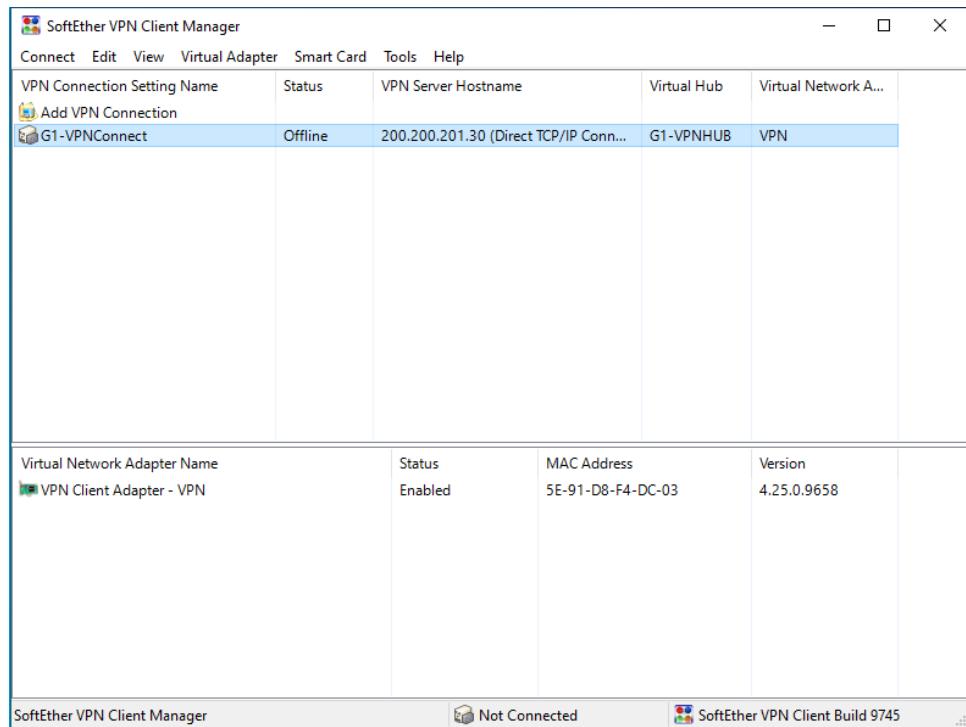


Figure 6.2.15.6 : GUI of SoftEther VPN Client Manager

Step 2 : Right click “G1-VPNConnect” and click properties to view the configuration for Group 1 VPN Connection.

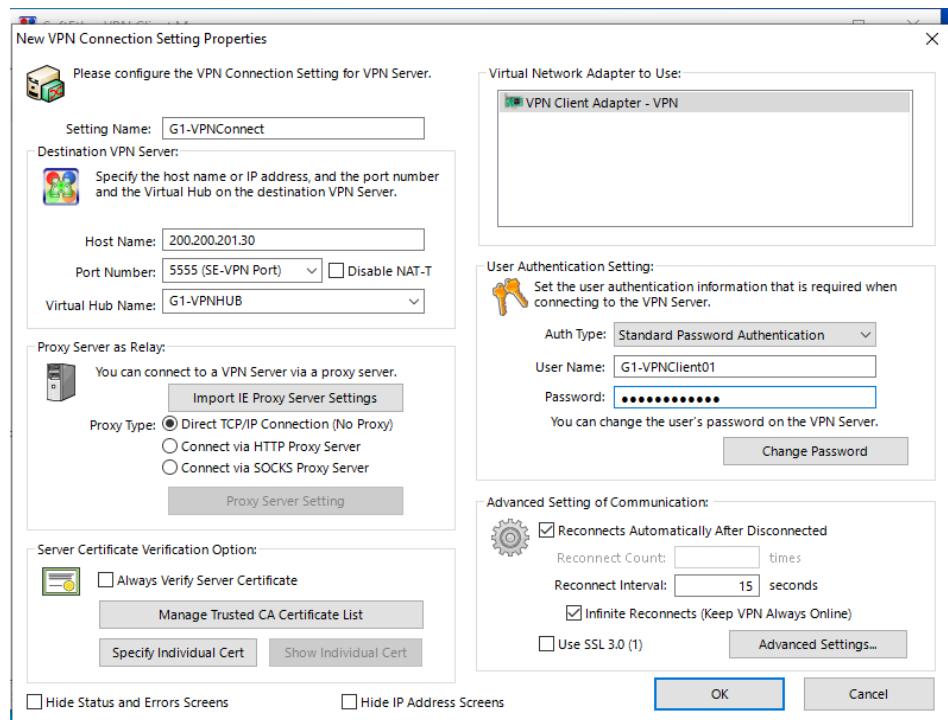


Figure 6.2.15.7 : Properties of G1-OutsideNet

Step 2 : Select VPN Connection (G1-VPNConnect) and select Connect.

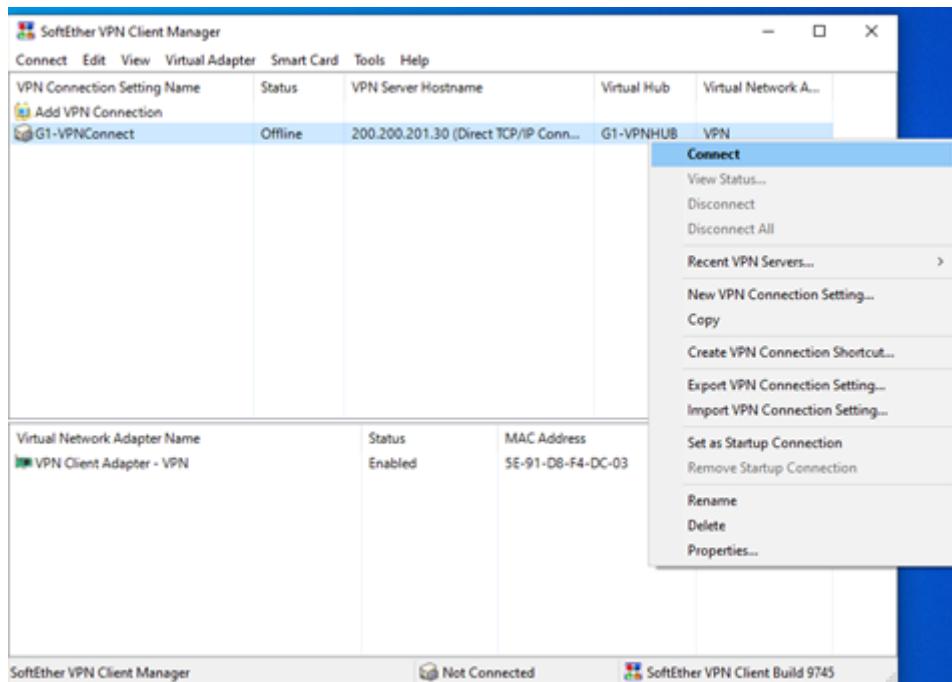


Figure 6.2.15.8 : Connect to VPN

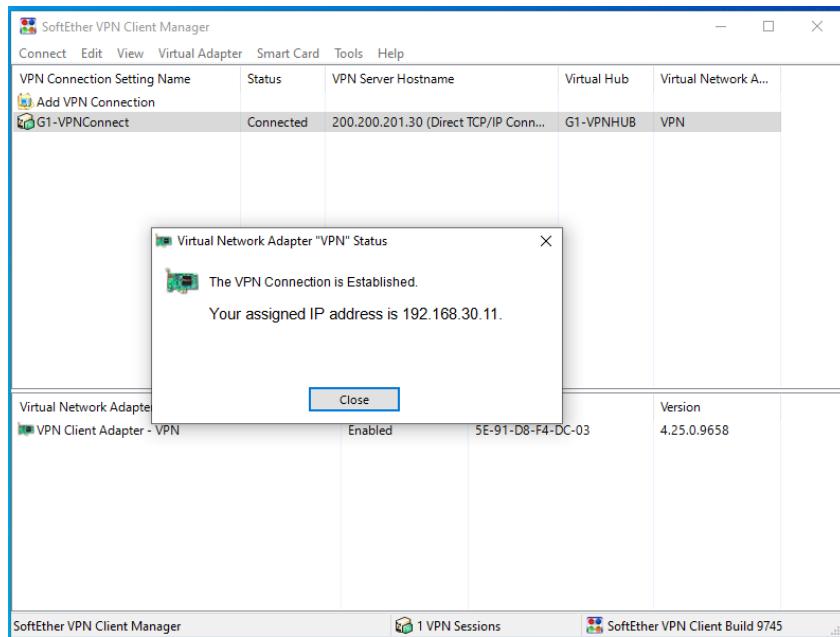


Figure 6.2.15.9 : Connection successful

Step 4 : Open command prompt in client PC Remote Access and enter command ipconfig to verify the ip address assigned by SoftEther VPN

```
Microsoft Windows [Version 10.0.19041.264]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\Group1>ipconfig

Windows IP Configuration

Unknown adapter VPN - VPN Client:
  Connection-specific DNS Suffix . : group1.com
  Link-local IPv6 Address . . . . . : fe80::bd71:e979:7141:c446%16
  IPv4 Address. . . . . : 192.168.30.11
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.30.1

Ethernet adapter Ethernet:
  Connection-specific DNS Suffix . :
  IPv6 Address. . . . . : 2001:3200:1000:1000:69fa:b8f3:166e:c64b
  Temporary IPv6 Address . . . . . : 2001:3200:1000:1000:30f3:30ff:1587:110
  Link-local IPv6 Address . . . . . : fe80::69fa:b8f3:166e:c64b%8
  IPv4 Address. . . . . : 192.168.1.2
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : fe80::c002:9dff:fe88:658

C:\Users\Group1>
```

Figure 6.2.15.10 : Verify ip address in cmd

6.2.16. Windows Server Hardening and Vulnerability Report

Step 1 : Check all necessary security settings.

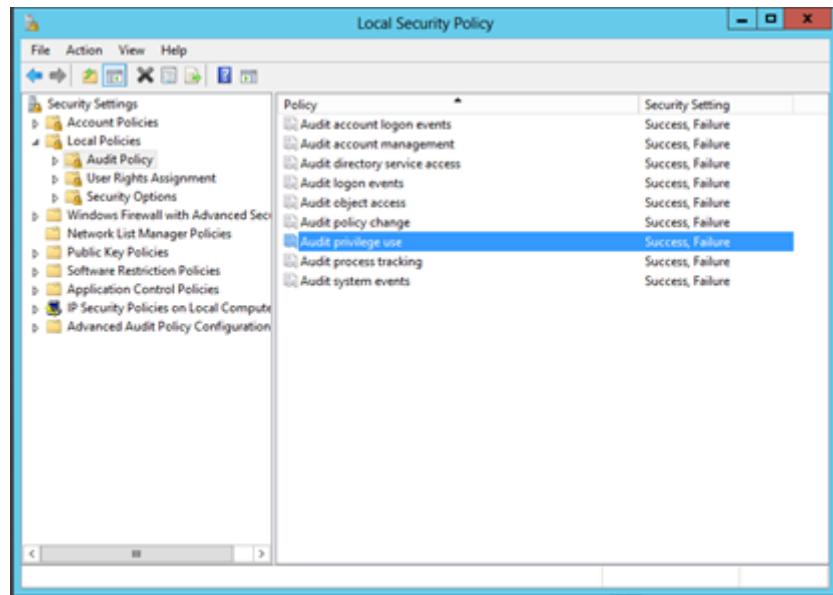


Figure 6.2.16.1 Audit privilege use

Step 2 : Check Firewall overview after enabling.

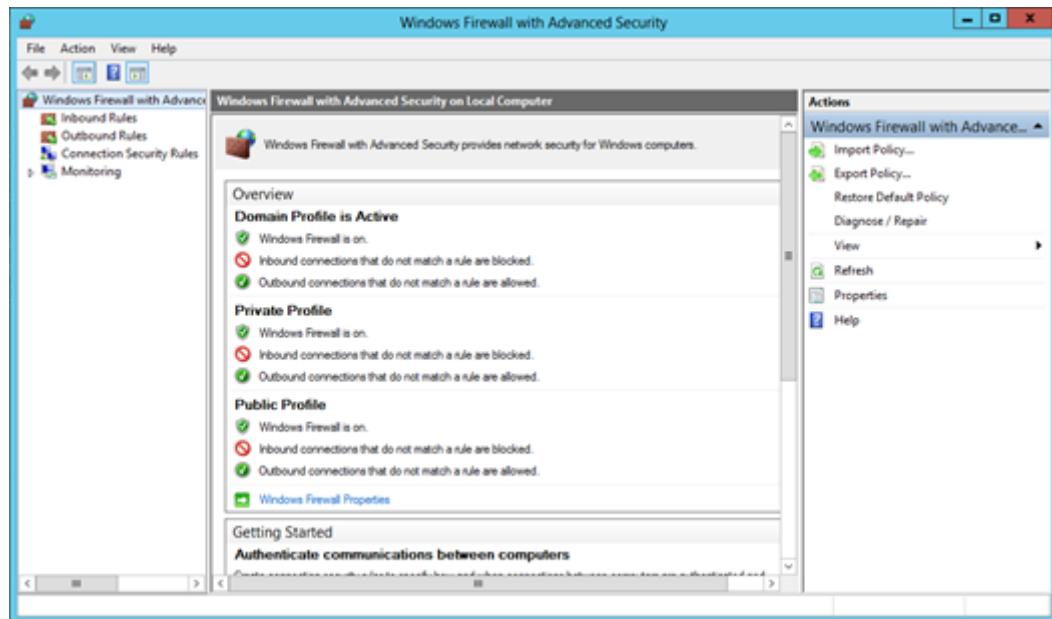


Figure 6.2.16.2 Windows Firewall with Advanced Security

Step 3 : Checking **Password Policy** after enabling the password requirements.

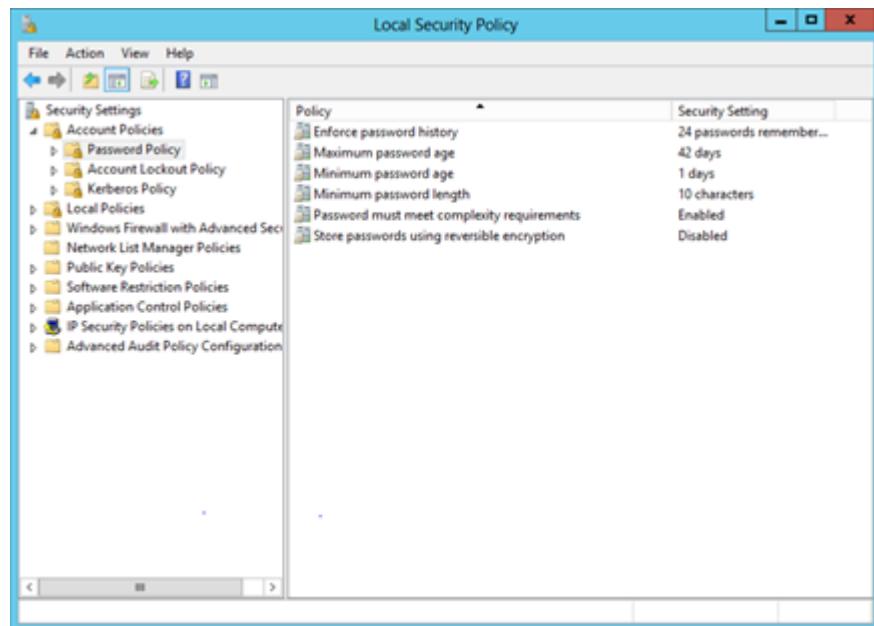


Figure 6.2.16.3 Password Policy

Step 4 : Preview the Account Lockout Policy.

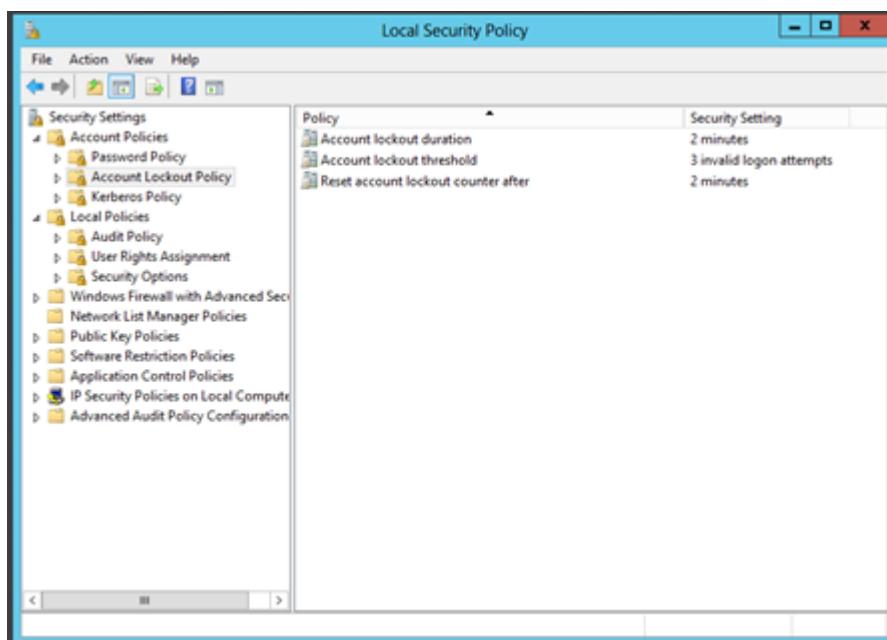


Figure 6.2.16.4 Account Lockout Policy

Step 5 : Preview the Kerberos Policy.

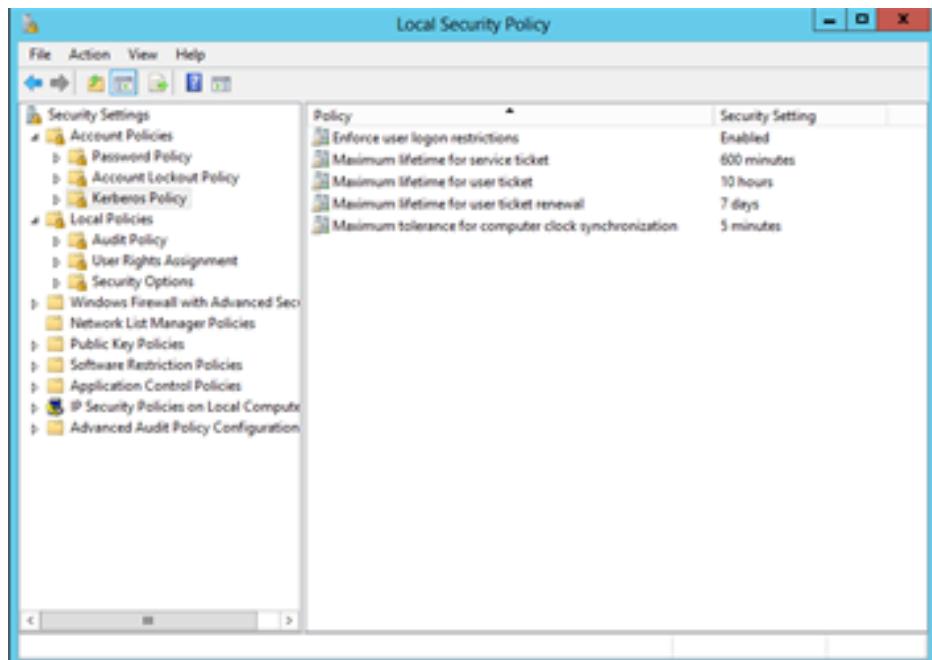


Figure 6.2.16.5 Kerberos Policy

6.2.17. Linux Server Hardening and Vulnerability Report

Step 1: Check on the set up of the password expiration.

```
root@WorkshopII:/home/debian# chage -l debian
Last password change : Jan 23, 2021
Password expires      : Jul 22, 2021
Password inactive     : Aug 21, 2021
Account expires       : never
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
```

Figure 6.2.17.1: Password expiration

Step 2: Check on the set up of the minimum number of password

```
debian@WorkshopII:~$ sudo passwd debian
New password:
BAD PASSWORD: it is WAY too short
BAD PASSWORD: is too simple
Retype new password: █
```

Figure 6.2.17.2: Password length

Step 3: Check on the set up of the firewall ufw

```
debian@WorkshopII:~$ sudo ufw status
Status: active

To                         Action    From
--                         --        --
80                         ALLOW    Anywhere
22/tcp                      ALLOW    Anywhere
22                         ALLOW    192.168.2.146
21                         ALLOW    Anywhere
21/tcp                      ALLOW    Anywhere
443                        ALLOW    Anywhere
143                        ALLOW    Anywhere
25                         ALLOW    Anywhere
80 (v6)                     ALLOW    Anywhere (v6)
22/tcp (v6)                 ALLOW    Anywhere (v6)
21 (v6)                     ALLOW    Anywhere (v6)
21/tcp (v6)                 ALLOW    Anywhere (v6)
443 (v6)                    ALLOW    Anywhere (v6)
143 (v6)                    ALLOW    Anywhere (v6)
25 (v6)                     ALLOW    Anywhere (v6)
```

Figure 6.2.17.3: ufw status

Step 4: Check on the set up of the Bluetooth

```

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

Jan 24 11:04:42 WorkshopII systemd[1]: Condition check resulted in Bluetoot..ped.
Jan 24 11:06:48 WorkshopII systemd[1]: Condition check resulted in Bluetoot..ped.
Hint: Some lines were ellipsized, use -l to show in full.

```

Figure 6.2.17.4: Bluetooth status

Step 5: Check on the set up of the disable CUPS and close port IPP

```

Discovered open port 21/tcp on 127.0.0.1
Discovered open port 5666/tcp on 127.0.0.1
Completed Connect Scan at 03:39, 0.08s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00020s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 989 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds
993/tcp   open  imaps
3306/tcp  open  mysql
5666/tcp  open  nrpe

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
          Raw packets sent: 0 (0B) | Rcvd: 0 (0B)

```

Figure 6.2.17.5: CUPS

Step 6: Check on the open port in the port scanning

```
Discovered open port 631/tcp on 127.0.0.1
Completed SYN Stealth Scan at 03:06, 1.57s elapsed (1000 total ports)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000015s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 988 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds
631/tcp   open  ipp
993/tcp   open  imaps
3306/tcp  open  mysql
5666/tcp  open  nrpe

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.71 seconds
          Raw packets sent: 1061 (46.684KB) | Rcvd: 2134 (89.652KB)
```

Figure 6.2.17.6: Open port

6.2.18. Audit Compliance

Reference	Audit Area, Objective, Question and Description		Status		
Checklist	Section	Audit Question	Findings	Compliance (/)	Non-Compliance (/)
1.0 SECURITY POLICY					

1.1 Security Policy

1.1.1 Security policy document	<p>-Whether the existence of a security policy, which is approved by the supervisor, published and communicated as appropriate to all users.</p> <p>-Whether it states the management commitment and set out the organizational approach to managing information security.</p>	Security policy status done in final report.	/	
1.1.2 Review and evaluation	<p>-Whether the security policy has an owner, who is responsible for its maintenance and review according to a defined review process.</p> <p>-Whether the process ensures that a review takes place in response to</p>		/	

	any changes affecting the basis of the original assessment such as significant security incidents, new vulnerabilities and changes to company.		
--	--	--	--

2.0 ORGANISATIONAL SECURITY

2.1 Information security infrastructure

2.1.1 Management information security forum	Whether there is a management forum to ensure there is a clear direction and visible management support for security initiatives within the organisation.	Briefing about Workshop2 and having group discussion.		
2.1.2 Information security coordination	Whether there is a cross-functional forum of management representatives from relevant parts of the organisation to coordinate the implementation of information controls.	Discuss about networking service (IPv4 tunnelling, VPN, VLSM, Routing & NAT).	/	

2.1.3 Allocation of information security responsibilities.	Whether full responsibilities for the protection of individual assets and for carrying out specific security processes were clearly defined.	Advise group members not to leave important information publicly.	/	

2.1.4 Authorisation process for information processing facilities	Whether there is a management authorisation process in place for any new information processing facility. This should include all new facilities such as hardware and software.	Authorisation at all server, switch and router.	/	
2.1.5 Security advise from supervisor	<ul style="list-style-type: none"> -Whether information security advice is obtained where appropriate. -A specific individual may provide advice in security decision making. 	Supervisor provide information about firewall, routing and NAT and ACL.	/	

2.1.6 Independent review of information security	Whether the implementation of security policy is reviewed independently on regular basis. This is provide assurance that organisational practises properly reflect the policy.	Review by group's member.	/	

2.2 Security of third party

2.2.1 Security requirements in third party contracts	Whether there is a formal contract containing, or referring to, all the security requirements to ensure compliance with the organization's security policies and standards.	No contract	/	
2.2.2 Identification of risks from third party	Whether risks from third party access are identified and appropriate security controls implemented.	ACL is implemented	/	

3.0 ASSET CLASSIFICATION AND CONTROL

3.1 Accountability of assets

3.1.1 Inventory of assets	<p>-Whether an inventory or register is maintained with the important assets associated with each information system.</p> <p>-Whether each of asset identifies has an owner, the security classification defined and agreed and the location identified.</p>	Fill asset form for each equipment before use.	/	
------------------------------	--	--	---	--

3.2 Information classification

3.2.1 Classification guidelines	Whether there is an information classification scheme or guideline in place; which will assist in determining how the information is to be handled and protected.	IP Addressing is saved at google drive to refer.	/	
------------------------------------	---	--	---	--

3.2.2 Information labelling and handling	Whether an appropriate set of procedures are defined for information labelling and handling in accordance with the classification scheme adopted by organization.	Label IP Address of each server and client	/	
---	---	--	---	--

4.0 PERSONNEL SECURITY

4.1 Security in job definition and resourcing

4.1.1 Including security in job responsibilities	<p>-Whether security roles and responsibilities as laid in Organisation's information security policy is documented where appropriate.</p> <p>-This should include general responsibilities for implementing and maintaining security policy as well as specific.</p>	Security policy status done in final report.	/	
--	---	--	---	--

4.2 Responding security weakness

4.2.1 Reporting security weakness	Whether a formal reporting procedure or guideline exists for user, to report security weakness in, or threats, to systems or services.	Not provided in reports	/	
4.2.2 Reporting software malfunctions	Whether procedures were established to report any software malfunctions.	Not provided in reports	/	

4.2.3 Reporting hardware malfunctions	Whether procedures were established to report any hardware malfunctions.	Not provided in reports	/	
4.2.4 Disciplinary process	Whether there is a formal disciplinary process in place for employee who have violated organisational security policies and procedures.	Advice group's member to avoid appearance of unethical or compromising practises .	/	

5.0 PHYSICAL AND ENVIRONMENTAL SECURITY

5.1 Secure Area

5.1.1 Physical security Perimeter	-What physical border security facility has been implemented to protect the information processing services. -Some examples of such security facility are alarm, thumbprint.	Students write their names and thumb scans to enter lab.	/	
--	---	--	---	--

5.1.2 Physical entry controls	What entry controls are in place to allow only authorised person should be allowed access to secure areas by using access controlled devices.	Student should thumbprints to enter lab	/	
5.1.3 Securing rooms and facilities	Whether the rooms, which have the Information processing service, are locked or have lockable door or safes.	Have lockable door.	/	
	Whether the information processing service is protected from natural and man-made disaster.	Equipment is protected by password	/	

5.2 Equipment Security

5.2.1 Equipment siting and protection	Whether the equipment was located in appropriate place to minimize unnecessary access into lab areas.	All equipment is located in own group lab	/	
	Whether controls were adopted to minimize risk from potential threats such as theft, fire, and electrical supply interfaces.	Lab provide fire extinguisher and smoke detector.	/	
	Whether there is a policy toward eating, drinking and smoking on in proximity to information processing facilities.	Policy provided	/	
	Whether environmental conditions are monitored which would adversely affect the information processing services.	Monitored by technician	/	
5.2.2 Equipment Maintenance	-Whether the equipment is maintained as per the supplier's recommended service intervals and specifications.	Maintained by technician	/	

5.2.3 Securing equipment off-premises	<p>-Whether any equipment usage outside a organization's premises for information processing has to be authorized by the management.</p>	Username and password are required to access equipment.	/	
	<p>-Whether the security provided for this equipment while outside the premises are on par with or more than the security provided inside the premises.</p>	Equal	/	

5.3 General Controls

5.3.1 Clear Desk and Clear Screen Policy	<p>Whether automatic computer screen locking facility is enabled. This would lock the screen when the computer is left unattended for a period.</p>	Screen lock for each server.	/	
5.3.2 Removal of property	<p>Whether equipment, information or software can be taken offsite without appropriate authorization.</p>	Cannot be taken offsite	/	

6.0 COMMUNICATION AND OPERATIONS MANAGEMENT

6.1 Operational Procedure and responsibilities

6.1.1 Documented Operating System	Whether the Security Policy has identified any operating system procedures such as Back-Up, Equipment maintenance etc.,	Not all back-up are documented	/	
--	---	--------------------------------	---	--

5.3.2 Removal of property	Whether equipment, information or software can be taken offsite without appropriate authorization.	Cannot be taken offsite	/	
----------------------------------	--	-------------------------	---	--

6.0 COMMUNICATION AND OPERATIONS MANAGEMENT

6.1 Operational Procedure and responsibilities

6.1.1 Documented Operating System	Whether the Security Policy has identified any operating system procedures such as Back-Up, Equipment maintenance etc.,	Not all back-up are documented		
6.1.2 Segregation of duties	Whether duties of responsible are separated in order to reduce opportunities for unauthorized modifications or misuse of information service.	Services are divided to each group's member	/	

6.2 Protection Against Malicious Software

6.2.1 Control against malicious	<p>-Whether there any exist control against malicious software usage.</p> <p>-Whether the security policy does address software licensing issues such as prohibiting usage of unauthorized software.</p>	No control being applied		/
--	--	--------------------------	--	---

	Whether antivirus software is installed on the computers to checks and isolate or remove any viruses from computer and media.	No antivirus is installed	/
--	---	---------------------------	---

6.3 Housekeeping

6.3.1 Information back-up	Whether Back-up of essential business information such as server, network components, configuration backups etc., were taken regularly.	configuration backup applied	/
6.3.2 Fault Logging	Whether faults are reported and well managed. This includes correctives action being taken, review of the fault logs and checking the actions taken.	Corrective actions being taken	/

6.4 Network Management

6.4.1 Network Controls	Whether there exist any special controls to safeguard confidentiality and integrity of data processing over the public network and to protect the system. Such as Virtual Private Network and other encryption.	VPN, applied	SSH	/	
-------------------------------	---	--------------	-----	---	--

6.5 Exchange of Information and Software

6.5.1 Security of Media in transit	-Whether security of media while being transported into account. -Whether the media is well secured from unauthorized access, misuse or corruption.	SFTP, Samba security	/	
---	--	----------------------	---	--

7.0 ACCESS CONTROL

7.1 User Access Control

7.1.1 User Registration	Whether there is any formal user registration and guest user procedure for granting access to multi-user information system and services.	Active Directory (AD)	/	
7.1.2 Privilege Management	<p>-Whether the allocation and use of any privileges in multi-user information system environment is restricted and controlled</p> <p>-i.e., Privileges are allocated on need-to-use basis; privileges are allocated only after formal authorisation process.</p>	Network Policy Server (NPS)	/	
7.1.3 User Password Management	The allocation and reallocation of password should be controlled thorough a formal management process.	Password created through formal process	/	
	Whether the users are asked to sign a statement to keep the password confidential.	No statement being applied		/
<h2>7.2 User Responsibilities</h2>				

7.2.1 Password use	Whether there are guidelines in place to guide users in selecting and maintaining secure passwords.	-Password must be 8 or more characters. -Password meet complexity requirements.	/	
7.2.2 Unattended User Equipment	Whether the user are made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibility to implement such protection.	Provide to all equipment. (All server, router and switch)	/	

7.3 Network Access Control

7.3.1 Segregation in networks	Whether the network (where third party need access to information system) is segregated using perimeter security mechanisms such as firewall.	-Internal firewall such as proxy server, routing & NAT -External firewall ACL	/	
--------------------------------------	---	--	---	--

7.3.2 Node Authentication	<p>-Whether connects to remote computer systems that are outside organizations security management are authenticated.</p> <p>-Node authentication can serve as an alternate means of authenticating groups of remote users where they are connected to a secure, shared computer facility.</p>	Implemented	/	
7.3.3 Network Connection Protocols	<p>Whether there exists any network connection control for shared networks that extend beyond the organisational boundaries. Example: electronic email, web access, file transfers, etc.,</p>	Not applicable.	/	
7.3.4 Network Routing Control	<p>Whether there exists any network control to ensure computers and information flows do not breach the access control policy of the business applications. This is often essential for networks shared with non-organisations users.</p>	Routing & NAT	/	

	Whether the routing controls are based on the true source and destination identification mechanism. Example: Network Address Translation (NAT).	Routing & NAT	/	
7.3.5 Security of Network Services	Whether the organisation, using public or private network service does ensure that a clear description of security attributes of all services used is provided.	Routing & NAT	/	

7.4 Operating System Access Control

7.4.1 Automatic terminal identification	Whether automatic identification mechanism is used to authenticate connections.	Not implemented	/	
7.4.2 Terminal log-on procedures	Whether access to information system is attainable only via a secure log-on process.	Implemented	/	

--	--	--	--

7.4.3 User identification and Authorization	<p>-Whether unique identifier is provided to every user such as operators, system administrators and all other staff including technical.</p>	<p>All group's member have identification and authorization.</p>	/	
	<p>Whether the authentication method used does substantiate the claimed identity of the user; commonly used method: Password that only the user knows.</p>	<p>Users are authenticated.</p>	/	
7.4.4 Use of System Utilities	<p>Whether the system utilities that comes with the computer installations, but may override system and application control is tightly controlled.</p>	<p>Utility not override</p>	/	
7.4.5 Terminal Time-Out	<p>Inactive terminal in public areas should be configured to clear the screen or shut down automatically after a defined period of inactivity.</p>	<p>Router and switch</p>	/	

--	--	--	--

7.5 Application Access Control

7.5.1 Sensitive System Isolation	Whether there are sensitive systems are provided with isolated computing environment such as running on a dedicated computer, share resources only with trusted application systems, etc.,	No sensitive system are provided.	/
---	--	-----------------------------------	---

7.6 Monitoring System Access and Use

7.6.1 Event Logging	Whether audit logs recording exceptions and other security relevant events are produced and kept for an agreed period to assist in future investigations and access control monitoring.	Accounting in Radius Server	/
----------------------------	---	-----------------------------	---

7.6.2 Monitoring System Use	<p>-Whether procedure are set up for monitoring the use of information processing facility.</p> <p>-The procedure should ensure that the users are performing only the activities that are explicitly authorised.</p>	Monitored by Nagios NMS for Linux, IDS	/	
	Whether the results of monitoring activities are reviewed regularly.	Monitoring activities are reviewed regularly	/	
7.6.3 Message Authentication	<p>-Whether an assessment of security risk was carried out to determine if message authentication is required.</p> <p>-Message authentication is a technique to detect unauthorized changes.</p>	“Access denied” pop-up when unauthorized user trying to access.	/	
7.6.4 Output Data Validation	Whether the data output of application system is validated to ensure that the processing of stored information is correct.	Router and switch can be access by entering correct username and password.	/	

8.0 SYSTEM DEVELOPMENT AND MAINTENANCE

8.1 Security in Application Systems

8.1.1 Input Data Validation	Whether data input to application system is validated to ensure that it is correct and appropriate.	“Access denied” pop-up when unauthorized user trying to access.	/	
8.1.2 Message Authentication	-Whether an assessment of security risk was carried out to determine if message authentication is required. -Message authentication is a technique to detect unauthorized changes.	“Access denied” pop-up when unauthorized user trying to access.	/	
8.1.3 Output Data Validation	Whether the data output of application system is validated to ensure that the processing of stored information is correct.	Access is permitted by entering valid username and password.	/	

8.2 Cryptographic Controls

8.2.1 Encryption	<p>-Whether encryption technique used to protect the data.</p> <p>-Whether assessments were conducted to analyse the sensitivity of the data and the level of protection needed.</p>	SSH, enable secret in router and switch	/	
8.2.2 Digital Signatures	Whether Digital signature were used to protect the authenticity and integrity of electronic documents.	No digital signature	/	
8.2.3 Key Management	Whether there is a management system is in place to support the organisation's use of cryptographic techniques such as Secret key technique and Public key technique.	The shared key in Radius Server is same with key authentication using radius server(AAA)	/	
	Whether the Key management system is based on set of standard, procedures and secure methods.	Yes	/	

8.3 Security in development and support process

8.3.1 Change control procedures	<p>-Whether there are any controls in place for the implementation of software on operational systems.</p> <p>-This is to minimize the risk of corruption of operational systems.</p>	Not implemented	/	
8.3.2 Technical review of operating system changes	<p>-Whether there are processes in place to ensure application system is reviewed and tested after change in operating system.</p> <p>-Periodically it is necessary to upgrade operating system i.e., to install service, patches etc.,</p>	Yes	/	
8.3.3 Outsourced Software Development	<p>-Whether there are controls in place over outsourcing software.</p> <p>-Testing before installations to detect malware</p>	VPN (SoftEther) SSH	/	
<h2>9.0 COMPLIANCE</h2>				

9.1 Aspects of Services Continuity Management

9.1.1 Testing, maintaining and re-accessing services	Whether services are tested regularly to ensure that they are up-to-date and effective.	Service tested	/	
---	---	----------------	---	--

9.2 Compliance with Legal Requirements

9.2.1 Identification of Applicable legislation	-Whether specific controls and individual responsibilities to meet these requirements were defined and documented.	Documented and defined in final report	/	
9.2.2 Safeguarding of Organisational records	Whether important records of the organisation are protected from loss destruction and false function.	Logbook	/	
9.2.3 Data Protection and Privacy of Personal Information	Whether there is a management structure and control in place to protect data and privacy of personal information.	Password is encrypted and protected	/	

9.2.4 Prevention of misuse of information processing facility	<p>-Whether use of information processing facilities for any unauthorized purpose.</p> <p>-Whether at the log-on a warning message is presented on the computer screen indicating that the system being entered is private and that unauthorized access not permitted.</p>	Unauthorized access cannot access server, router and switch	/	
9.2.5 Collection of Evidence	<p>Whether the process involved in collecting the evidence is in accordance with legal and industry best practise.</p>	Accounting login Radius Server (Log)	/	
<h3>9.3 Review of Security Policy and Technical Compliance</h3>				
9.3.1 Compliance with Security Policy	<p>Whether all areas within the organisation is considered for regular review to ensure compliance with security policy, standards and procedures.</p>	Security policy documented in final report.	/	

9.3.2 Technical compliance checking	Whether information systems were regularly checked for compliance with security implementation standards.	Harden Linux Server, Harden Windows Server, Security Hardening Checklist.	/	
--	---	---	---	--

9.4 System Audit Considerations

9.4.1 System Audit Controls	Whether audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruption to workshop.	Yes	/	
------------------------------------	--	-----	---	--

6.3. Conclusion

After all the installation of the services in the network and configuration of all the services, we carry out testing to ensure all the services are configured correctly. Although we made the correct configuration step by step, sometimes in the testing phase we might find it unsuccessful. During the testing phase, we found that some services were not working. To troubleshoot it, we check the log file, configuration file and we check on the dependencies and firewall to ensure the required port is open.

Therefore, the testing phase is very important to troubleshoot any problem detected. After all is done, we carry out testing to ensure all the services are running smoothly and the network is up and make it in documentation.

7. CHAPTER 7: CONCLUSION

7.1. Introduction

Through these numerous weeks in Workshop II, there is a lot of networking stuff that has been studied and experienced. With limited knowledge and experience, we successfully managed to set up, configure, maintain, and troubleshoot a complete network infrastructure. We also understood the basic concept of the services in this workshop. All the hard work that has been put into this project is considered as a preparation for us to attend industrial training. The overall performance for this workshop is quite satisfying. Although certain difficulties arose while completing the workshop, we successfully did it before the due date. It is very important in managing every task to prevent any problems and errors from occurring.

We were able to apply the theory that we learnt in the subject of Computer Organization and Architecture, Operating System, Local Area Network, Internet Technology, Network Analysis and Design, Wide Area Network and Network Project Management into this project. Practicing this scenario in either a learning or working environment would help us to solve problems especially in the network communication. Besides that, we will further understand how to implement the IPv6 web, security and network management in this project. Furthermore, we will be able to improve and upgrade our knowledge and skills in developing networks and especially working in a group and implementing our workforce together to solve the problem.

A network infrastructure that we developed is suitable for Small and Medium Enterprise Business since it is in small scale and is easy to manage and implement. Furthermore, it includes all the basic service that needs to run the business. Hopefully, we can achieve our goals or objective that is to make this project a success and able go through the obstacles and challenges faced in completing the task given and to gain all these knowledge and experience. Lastly,

this project as a platform to prepare students before undergoes their Final Year Project and 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

There are lots of disadvantages of the project which are:

- Hard to set up and do the configuration virtually.
- Take lots of time to configure services.
- Require lots of troubleshooting if the network is down.
- Require a strong internet connection to do the configuration of services.

7.4. Project limitation

There are some project limitations that were caused and we had to adapt and work harder to succeed in this project. These limitations are:

1. For students that do not have laptops or gadgets that are suitable for this workshop II, configuring, connecting to VNC and using GNS3 will be very problematic for them.
2. Workshop II deserves more than 3 credit hours. Time spent on Workshop II is definitely more than 3 hours per week. It really takes a lot of effort to get it done well. This is the reason why some students are not willing to

spend hours and hours in this workshop. Because by doing so, it will cost them other subject's grades.

3. Lack of current enterprise technique. Most of the enterprises are implementing switch stacking, load balancing, and server failover. Maybe faculty can introduce this technique into the workshop, as it will be useful for students in their future working environment.

7.5. Conclusion

In conclusion, upon completion of workshop 2, we are expected to be able to install, configure, setup, monitor our own network and services in a virtual environment by using Graphical Network Simulator 3 (GNS3) and virtual machine. Although there are lots of drawbacks when doing it by virtual but we manage to be able to configure all the required services in workshop 2 implementation. By completing the workshop, we can gain knowledge of other services that we are not familiar with.

BIBLIOGRAPHY

APPENDIX

- IPv4 Table Addressing

ROLE	INTERFACE	IP ADDRESS	CI DR	DEFAULT GATEWAY	SUBNET MASK	VLAN ID
Router HQ	Fa0/0.20	192.168.2.1 (IT Department)	/25	N/A	255.255.255.128	20
	Fa0/0.30	192.168.2.129 (Windows)	/28	N/A	255.255.255.240	30
	Fa0/0.40	192.168.2.145 (Debian)	/29	N/A	255.255.255.248	40
	S0/0	200.200.201.1	/24	N/A	255.255.255.0	
Router ISP	S0/0	200.200.201.2	/24	N/A	255.255.255.0	
	S0/1	200.200.200.5	/24	N/A	255.255.255.0	
Router Branch	Fa0/0.10	192.168.1.1 (Remote Access)	/24	N/A	255.255.255.0	
	S0/1	200.200.200.6	/24	N/A	255.255.255.0	
Remote Access (PC)	NIC	192.168.1.10 (Static before DHCP)	/24	192.168.1.1	255.255.255.0	10
IT Department (PC)	NIC	192.168.2.10 (Static before DHCP)	/25	192.168.2.1	255.255.255.128	20

Server Windows	NIC	192.168.2.130	/28	192.168.2.129	255.255.255.240	30
Server Debian	NIC	192.168.2.146	/29	192.168.2.145	255.255.255.248	40

- **VLSM IPv4**

SUBNET NAME	HOST NEEDED	NETWORK ADDRESS	CI DR	SUBNET MASK	USABLE IP ADDRESS	BROADCAST ADDRESS
Remote Access	150	192.168.1.0	/24	255.255.255.0	192.168.1.1 — 192.168.1.254	192.168.1.255
IT Department	100	192.168.2.0	/25	255.255.255.128	192.168.2.1 — 192.168.2.126	192.168.2.127
Server Windows	10	192.168.2.128	/28	255.255.255.240	192.168.2.129 — 192.168.2.142	192.168.2.143
Server Debian	6	192.168.2.144	/29	255.255.255.248	192.168.2.145 — 192.168.2.150	192.168.2.151

- IPv6 Table Addressing

ROLE	INTERF ACE	IP ADDRESS	PR EFI X	DEFAULT GATEWAY	VLA N ID
Router HQ	Fa0/0.20	2001:3200:1000:2000::1 (IT Department)	/64	N/A	20
	Fa0/0.30	2001:3200:1000:3000::1 (Windows)	/64	N/A	30
	Fa0/0.40	2001:3200:1000:4000::1 (Debian)	/64	N/A	40
	S0/0	2001:db8:1:2::1	/64	N/A	
Router ISP	S0/0	2001:db8:1:2::2	/64	N/A	
	S0/1	2001:db8:5:6::5	/64	N/A	
Router Branch	Fa0/0.10	2001:3200:1000:1000::1 (Remote Access)	/64	N/A	
	S0/1	2001:db8:5:6::6	/64	N/A	

Remote Access (PC)	NIC	2001:3200:1000:1000::2 (Static before DHCP)	/64	2001:3200:1000:1000::1	10
IT Department (PC)	NIC	2001:3200:1000:2000::2 (Static before DHCP)	/64	2001:3200:1000:2000::1	20
Server Windows	NIC	2001:3200:1000:3000::2	/64	2001:3200:1000:3000::1	30
Server Debian	NIC	2001:3200:1000:4000::2	/64	2001:3200:1000:4000::1	40

- **VLSM IPv6**

SUBNET NAME	VLAN ID	NETWORK ADDRESS	PREFIX	DEFAULT GATEWAY
Remote Access	10	2001:3200:1000:1000::	/64	2001:3200:1000:1000::1
ITDepartment	20	2001:3200:1000:2000::	/64	2001:3200:1000:2000::1
Server Windows	30	2001:3200:1000:3000::	/64	2001:3200:1000:3000::1
Server Debian	40	2001:3200:1000:4000::	/64	2001:3200:1000:4000::1

Windows Server Hardening Checklist - Vulnerability Report

No.	Windows Server 2012	Before	After	Risk	Recommendation
Preparation and Installation					
1.	Using Security Configuration Wizard to harden the server	x	✓	High	No action needed
2.	Create the new policy for the server.	x	✓	High	No action needed
Role-Based Service Configuration					
3.	Select Server Roles	x	✓	High	No action needed
4.	Select Client Features	x	✓	High	No action needed
5.	Select Administration and Other Options	x	✓	High	No action needed
6.	Check error option in Administration and Other Options	x	✓	High	No action needed
	Handling Unspecified Service				

7.	Do not change the startup mode of the services when unspecified services is found	x	✓	Medium	No action needed
8.	Confirm Service Changes	x	✓	Medium	No action needed
	Network Security Settings				
9.	Enable the Windows Firewall in all profiles (domain, private, public). (Default)	x	✓	High	No action needed
10.	Configure the Windows Firewall in all profiles to block inbound traffic by default. (Default)	x	✓	High	No action needed
	Audit Policy Settings				
11.	Configure Account Logon audit policy.	x	✓	Low	No action needed
12.	Configure Account Management audit policy.	x	✓	Medium	No action needed
13.	Configure Logon/Logoff audit policy.	x	✓	Low	Audit privilege check “Successful” and “Failure”

14.	Configure Policy Change audit policy.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Medium	No action needed
15.	Configure Privilege Use audit policy.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Medium	No action needed
Network Access Control					
16.	Disable anonymous SID/Name translation. (Default)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Medium	No action needed
8.	Do not allow anonymous enumeration of SAM accounts. (Default)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High	No action needed
9.	Do not allow everyone permissions to apply to anonymous users. (Default)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	High	No action needed
10.	Require the "Classic" sharing and security model for local accounts. (Default)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Low	No action needed
User Account Policies					

11.	Set minimum password length.	x	✓	High	Set password minimum 10 characters including numbers, uppercase and lowercase words to produce a strong password.
12.	Enable password complexity requirements.	x	✓	High	No action needed
13.	Do not store password using reversible encryption. (Default)	x	✓	Medium	Disabled
14.	Configure account lockout policy.	x	✓	High	Set the account lockout with 3 attempts and 2 minutes duration session.
Security Settings					
15.	Disable the guest account.	✓	✓	Medium	No action needed
16.	Require Ctrl+Alt+Del for interactive logins	✓	✓	Medium	No action needed
17.	Configure machine inactivity limit to protect idle interactive sessions	✓	✓	Medium	No action needed

Additional Policy					
23.	Install and enable anti-virus software	x	x	High	Install the latest version of anti-virus software
24.	Configure anti-virus software to update daily	x	x	High	Update the anti-virus software daily
25.	Update Windows Server 2012	x	x	Medium	Request technician to allow the administrative permission to update Windows Server 2012.
Physical Security					
26.	Do not allow the system to be shut down without having to log on. (Default)	✓	✓	Medium	Configure to the “Disabled” setting
27.	Configure a screen-saver to lock the console’s screen automatically if the host is left unattended.	✓	✓	Medium	Configure to the “Enabled” setting

Registry Settings	

28.	Require SMB Security Signatures -check both of the attributes	x	✓	Medium	No action needed
29.	Outbound Authentication Methods -check Domain Account	x	✓	Medium	No action needed
30.	Outbound Authentication using Domain Account -check Windows NT 4.0 Service Pack 6a or late operating Systems	x	✓	Medium	No action needed
31.	Confirm Registry Settings in Registry Settings Summary	x	✓	Medium	No action needed

Table: Windows Server Hardening Checklist

Linux Server Hardening Checklist - Vulnerability Report

Task	Before	After
Software and Updates		
Search Software and Update	X	✓
Change from weekly to daily in automatically check for updates bar	X	✓
Check for updates	X	✓
Terminal		
Check password expiration with sudo chage -l (username)	X	✓
Change password expiration with sudo chage -M (max days_ -I (days inactive) -W (days for warning) (username)	X	✓
Install Nmap	X	✓

Scan ports with Nmap	<u>X</u>	✓
Disable CUPS service (for printing)	<u>X</u>	✓
Disable Bluetooth	<u>X</u>	✓
Enable ufw	<u>X</u>	✓

Table: Linux Server Hardening Checklist

Test Case 1: Maintenance

Test ID	Update01
Node List	Debian Server
Test Description	User use specific Software & Updates to verify does the software is up to date.
Test Data	Username: debian Password: Debian12345

Test Steps	<p>Step 1: Login into Debian Server with password</p> <p>Step 2: Search bar in Debian Software & Update</p> <p>Step 3: Go to Update</p> <p>Step 4: Change from weekly to daily in automatically check for updates bar.</p>
Expected Results	There will not have update package. Which show the software is up to date.
Observed Results	As Expected
Final Result	Pass

Table: Test case maintenance

Test Case 2: Password Expiration

Test ID	Password01
Node List	Debian Server
Test Description	Set the minimum password to avoid the password easy to crack.
Test Data	<p>Username: debian</p> <p>Password: Debian12345</p>

Test Steps	<p>Step 1: Login into Debain Server with password</p> <p>Step 2: Open terminal</p> <p>Step 3: Enter in sudo chage -l debian to view current status.</p> <p>Step 4: Set the password expiry sudo chage -M 180 -I 30 -W 14 debian</p> <p>Step 5: Enter sudo chage -l debian to verify the result.</p>
Expected Results	The password will expired after 180 days
Observed Results	As expected
Final Result	Pass

Table: Test case password expiration

Test Case 3: Disable Bluetooth

Test ID	Bluetooth01
Node List	Debian Server
Test Description	<p>It is to provide a minimum baseline standard for connecting Bluetooth enabled devices to the network or owned devices. The intent of the minimum standard is to ensure sufficient protection Personally Identifiable Information (PII) and confidential data.</p>

Test Data	Username: debian Password: Debian12345
Test Steps	<p>Step 1: Login into Debian Server with password</p> <p>Step 2: Open terminal</p> <p>Step 3: Type in nano /etc/rc.local and press Enter.</p> <p>Step 4: Insert text rfkill block Bluetooth</p> <p>Step 5: Save and exit</p> <p>Step 5: Open file Bluetooth sudo nano /etc/Bluetooth/main.conf</p>
Expected Results	The status Bluetooth will be show inactive (dead).
Observed Results	As Expected
Final Result	Pass

Table: Test case bluetooth

Test Case 4: Check on Network Port

Test ID	Port01
Node List	Debian Server

Test Description	User use Nmap to check port used on the Server.
Test Data	Username: debian Password:Debian12345
Test Steps	Step 1: Login into Debian Server with password Step 2: Open terminal Step 3: Type in sudo nmap -v -sS localhost and press Enter. Step 4: Insert password as Debian12345 Step 5: Verify the result
Expected Results	The terminal will show all the listening port that are used on the Server, such as SFTP, SSH and etc.
Observed Results	As Expected
Final Result	Pass

Table: Test case network port