INSTITUTE OF ENGINEERING TECHNOLOGY - KATUNAYAKE

Department of Electrical Engineering

EE4050 - Network and System Administration

Network Assignment

Instructed By	**: MR. DILSHAN FERNANDO**
Student Name	**: G.K.R. PERERA**
Registration Number	**: EN/22/0075**
Date of Submission	**: 11/08/2025**

Table of Contents

Table of Figures

1. Introduction

1.1 Purpose of the Assignment

This assignment serves as a guide to the design, implementation, and ongoing management of a computer network with Linux-based and Windows-based. It covers the integration of Linux and Windows servers, emphasizing practical applications in network monitoring and security. All configurations and design choices are thoroughly documented for clarity and replicability.

1.2 Overview of the Designed Network

The network detailed in this documentation is a mixed-OS virtualized environment (VMware Workstation Pro and Cisco Packet Tracer) operating on the 192.168.x.x private IP range. It demonstrates enterprise network services through:

- Core network services provided by Ubuntu 24.04 LTS servers.
- Active Directory and domain management via Windows Server 2019/2022.
- Client connectivity validation using a Windows 7 client.
- Performance and security analysis with dedicated network monitoring tools.
- Robust security measures, including comprehensive policies and firewall configurations.

2. Network Design

2.1 Network Diagram

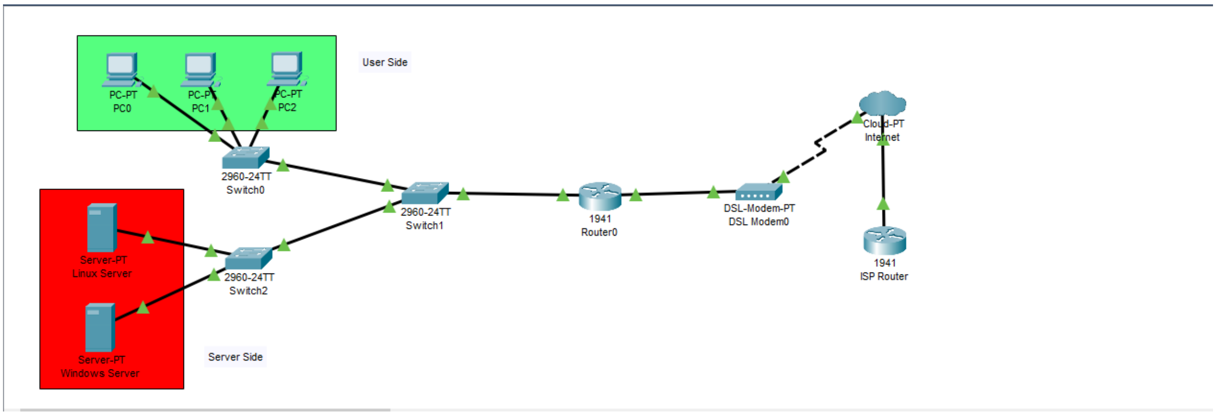


Figure 1: Network topology diagram with Cisco Packet Tracer

2.2 IP Addressing Scheme

The network utilizes the 192.168.100.0/24 subnet with the following IP allocation:

Device Category	IP Range	Purpose
Network Gateway	192.168.8.1	Router/Gateway
Linux Server	192.168.147.130	Core network services
Windows Server	192.168.8.101	Domain services
Client Machines	192.168.147.100-192.168.147.200	End-user devices

Detailed IP Plan:

- **Gateway:** 192.168.8.1/24
- **Ubuntu Server:** 192.168.147.130/24
- **DHCP Range:** 192.168.147.100-192.168.147.200
- **Windows Server (AD/Domain Controller):** 192.168.8.101/24

2.3 Rationale for Design Choices

2.3.1 Private IP Range Selection

The selection of the 192.168.x.x private IP address range was driven by several key factors:

- Ease of Use: This range offers straightforward configuration and memorability, particularly beneficial for a testing and demonstration network.
- Universal Compatibility: It ensures broad support across all utilized network devices and operating systems.
- Security by Design: Being a non-routable range, it inherently prevents direct internet access, enhancing the security posture of the network.
- Adequate Capacity: A /24 subnet within this range provides 254 usable IP addresses, which is more than sufficient for the current network's requirements.

2.3.2 Subnetting Strategy

A single /24 subnet was deployed due to its benefits in a controlled testing environment:

- Streamlined Deployment: This approach simplifies the initial network setup and subsequent troubleshooting processes.
- Direct Inter-Device Communication: It allows all connected devices to communicate directly without the need for complex routing protocols.
- Scalability: The address space provided by a /24 subnet is adequate for potential future additions to the network.
- Reduced Broadcast Domain Complexity: It helps to maintain a manageable broadcast domain, which is advantageous in a testing scenario

3. Linux Server Configuration

3.1 Distribution Choice and Rationale

Selected Distribution: Ubuntu 24.04 LTS (Both Desktop and Server editions)

Justification:

Ubuntu 24.04 LTS was chosen for this project due to its comprehensive set of features and benefits, which align with the network's requirements:

- Long-Term Support (LTS): The 5-year support lifecycle provides a stable and secure foundation, guaranteeing ongoing security updates and maintenance.
- Strong Community and Documentation: An extensive online community and rich documentation resources are available, facilitating troubleshooting and development.
- Optimized for Virtualization: Offers excellent compatibility and performance within virtualized environments, such as those used in this project.
- Efficient Package Management: The APT package manager simplifies the process of installing, updating, and managing software.
- Integrated Security: Features a suite of built-in security tools and benefits from consistent security patches, contributing to a robust security posture.
- Proven Enterprise Adoption: Its widespread use in production and enterprise settings underscores its reliability and readiness for complex network deployments.

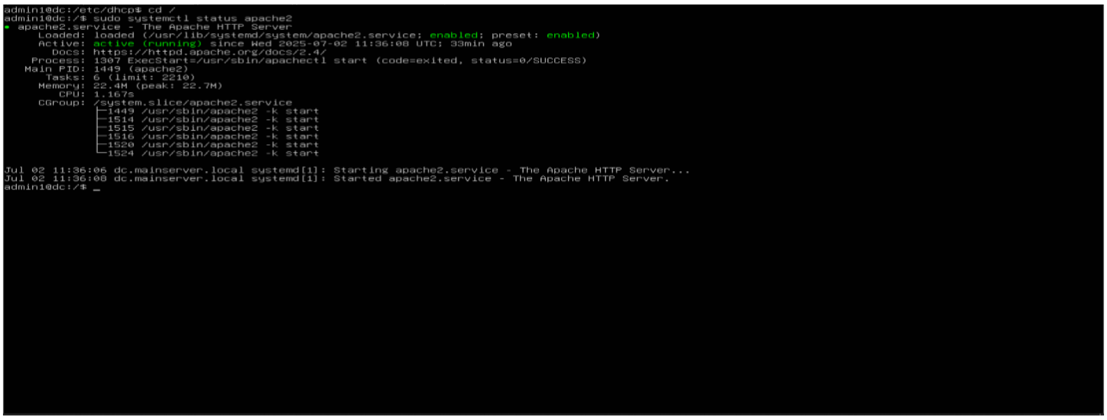
3.2 Server Services Configuration

3.2.1 Web Server (Apache2)

Installation and Configuration Steps:

The following commands applied for install and configure the Apache2 Web server in Ubuntu server.

1. Install Apache2: sudo apt install apache2
2. Check status: sudo systemctl status apache2



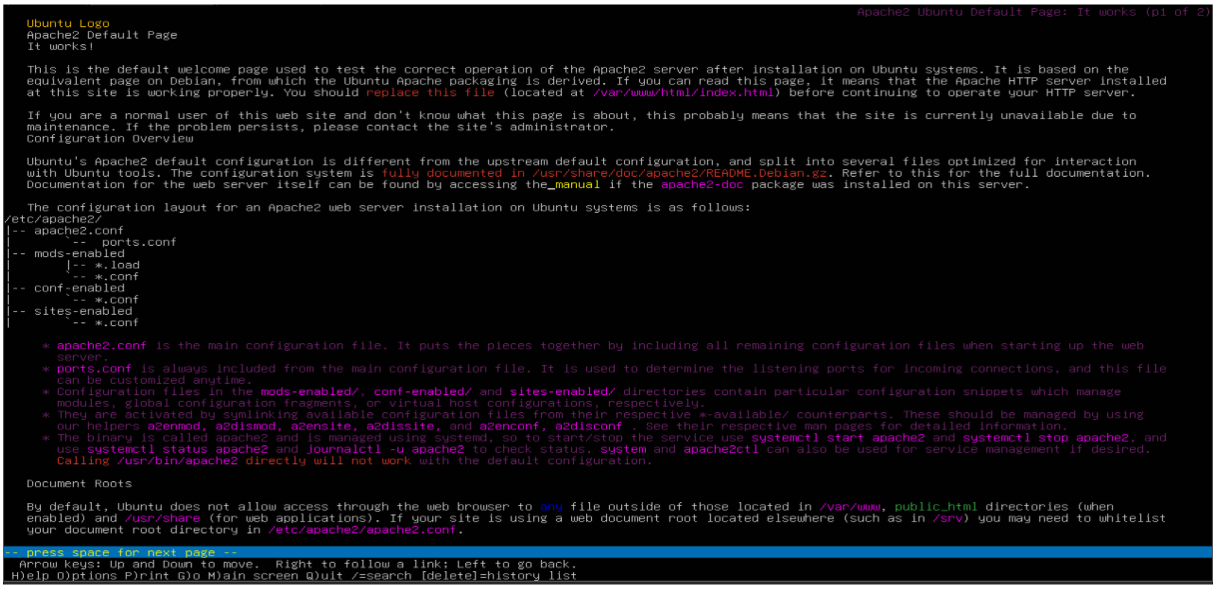
```
admin1@dc:/etc/dhcp$ cd /
admin1@dc:/$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Wed 2025-07-02 11:36:08 UTC; 33min ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 1307 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 1449 (apache2)
      Tasks: 6 (limit: 2210)
     Memory: 22.4M (peak: 22.7M)
        CPU: 1.167s
     CGroup: /system.slice/apache2.service
             ├─1449 /usr/sbin/apache2 -k start
             ├─1514 /usr/sbin/apache2 -k start
             ├─1515 /usr/sbin/apache2 -k start
             ├─1516 /usr/sbin/apache2 -k start
             ├─1520 /usr/sbin/apache2 -k start
             └─1524 /usr/sbin/apache2 -k start

Jul 02 11:36:06 dc.mainserver.local systemd[1]: Starting apache2.service - The Apache HTTP Server...
Jul 02 11:36:08 dc.mainserver.local systemd[1]: Started apache2.service - The Apache HTTP Server.
admin1@dc:/$ _
```

Figure 2: Apache2 installation process

Configuration Details:

- Document Root: `/var/www/html`
- Port Configuration: 80 (HTTP), 443 (HTTPS)

Purpose and Role: This component offers HTTP/HTTPS services, crucial for deploying and managing web-based applications and content. It acts as the central access point for users and administrators interacting with the network's web services and management interfaces.



```
                                                                     Apache2 Ubuntu Default Page: It works (p1 of 2)
   Ubuntu Logo
   Apache2 Default Page
   It works!

   This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the
   equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed
   at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.

   If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to
   maintenance. If the problem persists, please contact the site's administrator.
   Configuration Overview

   Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction
   with Ubuntu tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation.
   Documentation for the web server itself can be found by accessing the_manual if the apache2-doc package was installed on this server.

   The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:
/etc/apache2/
|-- apache2.conf
|        `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf

       * apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web
         server.
       * ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file
         can be customized anytime.
       * Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage
         modules, global configuration fragments, or virtual host configurations, respectively.
       * They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using
         our helpers a2enmod, a2dismod, a2ensite, a2dissite, and a2enconf, a2disconf . See their respective man pages for detailed information.
       * The binary is called apache2 and is managed using systemd, so to start/stop the service use systemctl start apache2 and systemctl stop apache2, and
         use systemctl status apache2 and journalctl -u apache2 to check status. system and apache2ctl can also be used for service management if desired.
         Calling /usr/bin/apache2 directly will not work with the default configuration.

   Document Roots

   By default, Ubuntu does not allow access through the web browser to any file outside of those located in /var/www, public_html directories (when
   enabled) and /usr/share (for web applications). If your site is using a web document root located elsewhere (such as in /srv) you may need to whitelist
   your document root directory in /etc/apache2/apache2.conf.

-- press space for next page --
  Arrow keys: Up and Down to move.  Right to follow a link; Left to go back.
 H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
```

Figure 3: Apache2 configuration files and virtual host setup

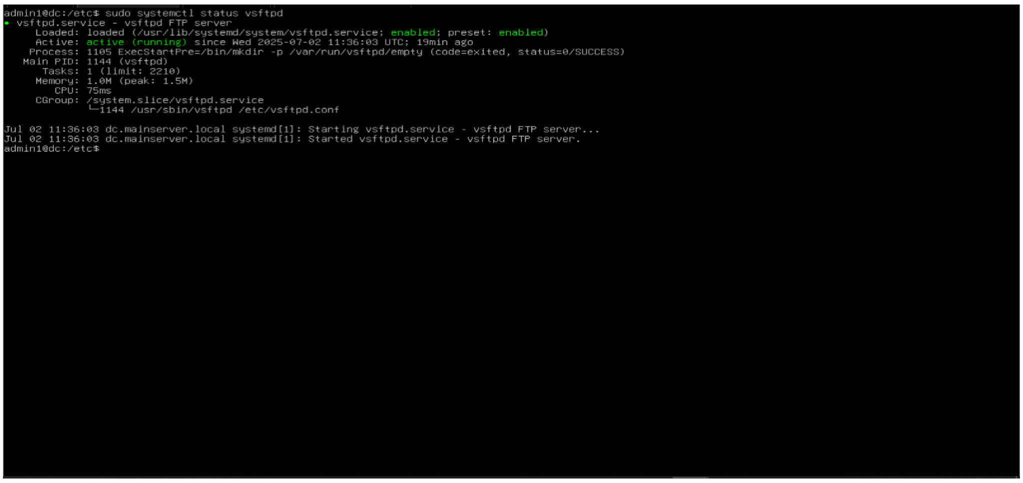
3.2.2 FTP Server (vsftpd)

Installation & Configuration Steps:

The following commands applied for install and configure the Apache2 Web server in Ubuntu server.

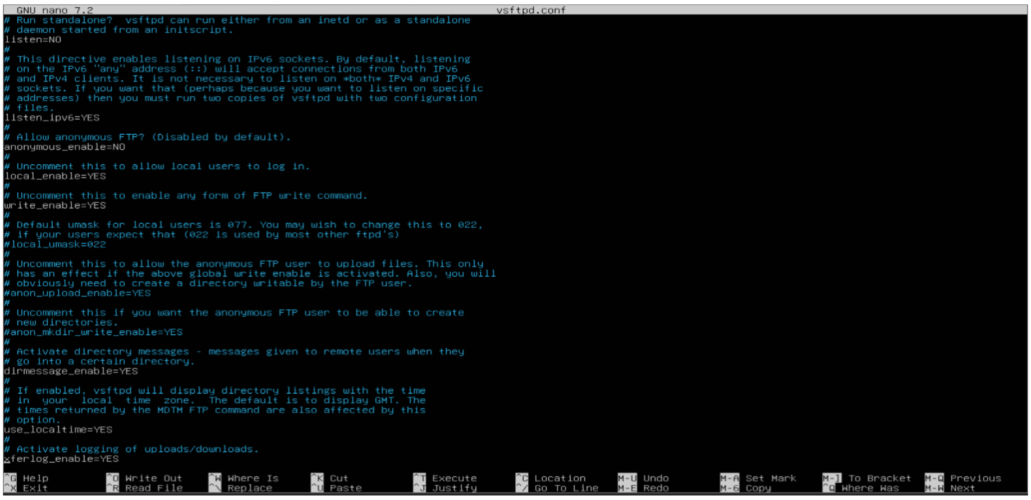
Install vsftpd File Server: sudo apt install vsftpd

Then, check the status of FTP server: sudo systemctl status vsftpd



```
admin1@dc:/etc$ sudo systemctl status vsftpd
● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; preset: enabled)
     Active: active (running) since Wed 2025-07-02 11:36:03 UTC; 19min ago
    Process: 1105 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
   Main PID: 1144 (vsftpd)
      Tasks: 1 (limit: 2210)
     Memory: 1.0M (peak: 1.5M)
        CPU: 75ms
     CGroup: /system.slice/vsftpd.service
             └─1144 /usr/sbin/vsftpd /etc/vsftpd.conf

Jul 02 11:36:03 dc.mainserver.local systemd[1]: Starting vsftpd.service - vsftpd FTP server...
Jul 02 11:36:03 dc.mainserver.local systemd[1]: Started vsftpd.service - vsftpd FTP server.
admin1@dc:/etc$
```

Figure 4: FTP server status



```
  GNU nano 7.2                                                        vsftpd.conf
# Run standalone?  vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
#local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
#anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
#anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
#
# If enabled, vsftpd will display directory listings with the time
# in  your  local  time  zone.  The default is to display GMT. The
# times returned by the MDTM FTP command are also affected by this
# option.
use_localtime=YES
#
# Activate logging of uploads/downloads.
xferlog_enable=YES
```

Figure 5: FTP server configuration

Security Configuration:

Enable firewall rules for block unauthorized access using following commands.

sudo ufw allow 20/tcp

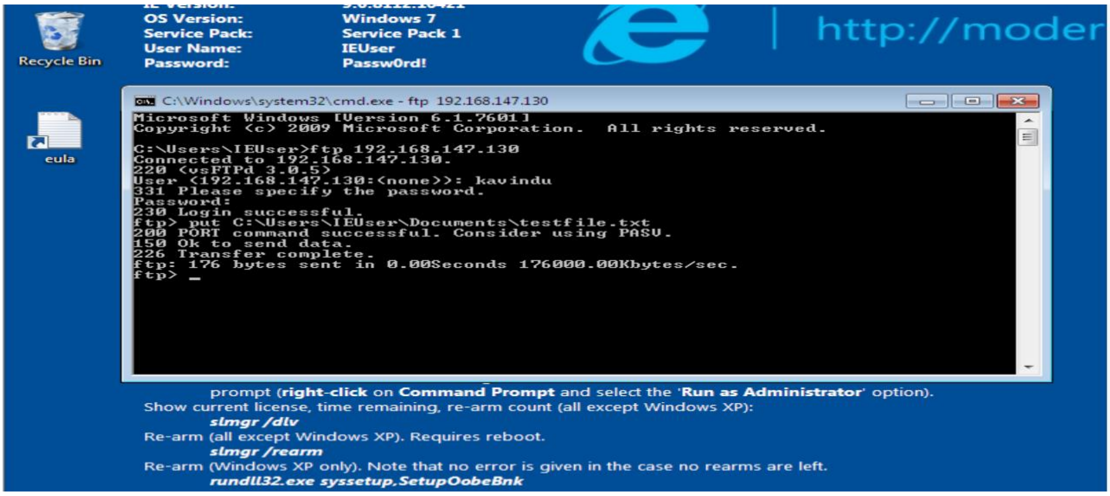
sudo ufw allow 21/tcp

Purpose:

Provides file transfer capabilities for network users and administrators.

Testing:

First, created a sample text file in another host machine (Windows 7), named it as testfile.txt and save it in the Documents folder. Then, log in to the FTP server via the Windows command prompt and uploaded the file as below figure.



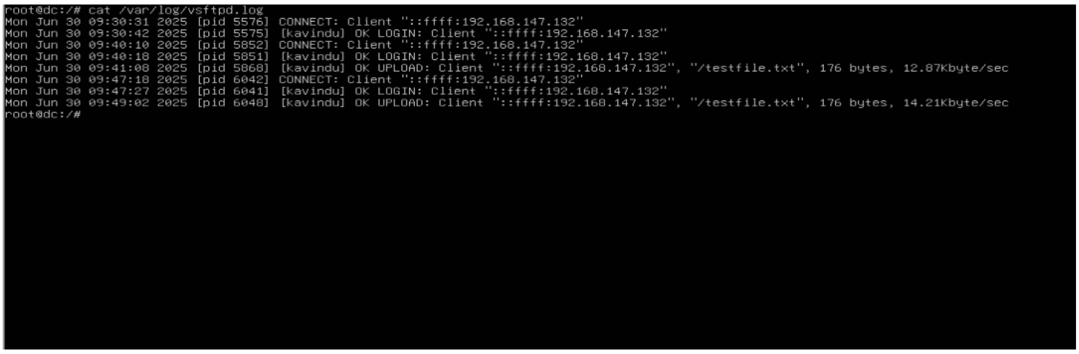
OS Version: Windows 7
Service Pack: Service Pack 1
User Name: IEUser
Password: Passw0rd!

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\IEUser>ftp 192.168.147.130
Connected to 192.168.147.130.
220 (vsFTPd 3.0.5)
User (192.168.147.130:(none)): kavindu
331 Please specify the password.
Password:
230 Login successful.
ftp> put C:\Users\IEUser\Documents\testfile.txt
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
ftp: 176 bytes sent in 0.00Seconds 176000.00Kbytes/sec.
ftp> _
```

prompt (**right-click** on **Command Prompt** and select the '**Run as Administrator**' option).
Show current license, time remaining, re-arm count (all except Windows XP):
slmgr /dlv
Re-arm (all except Windows XP). Requires reboot.
slmgr /rearm
Re-arm (Windows XP only). Note that no error is given in the case no rearms are left.
rundll32.exe syssetup,SetupOobeBnk

Figure 6: Upload a file to FTP server

Finally, verified the file that uploaded in the Ubuntu server.



```
root@dc:/# cat /var/log/vsftpd.log
Mon Jun 30 09:30:31 2025 [pid 5576] CONNECT: Client "::ffff:192.168.147.132"
Mon Jun 30 09:30:42 2025 [pid 5575] [kavindu] OK LOGIN: Client "::ffff:192.168.147.132"
Mon Jun 30 09:40:10 2025 [pid 5852] CONNECT: Client "::ffff:192.168.147.132"
Mon Jun 30 09:40:18 2025 [pid 5851] [kavindu] OK LOGIN: Client "::ffff:192.168.147.132"
Mon Jun 30 09:41:08 2025 [pid 5868] [kavindu] OK UPLOAD: Client "::ffff:192.168.147.132", "/testfile.txt", 176 bytes, 12.87Kbyte/sec
Mon Jun 30 09:47:18 2025 [pid 6042] CONNECT: Client "::ffff:192.168.147.132"
Mon Jun 30 09:47:27 2025 [pid 6041] [kavindu] OK LOGIN: Client "::ffff:192.168.147.132"
Mon Jun 30 09:49:02 2025 [pid 6048] [kavindu] OK UPLOAD: Client "::ffff:192.168.147.132", "/testfile.txt", 176 bytes, 14.21Kbyte/sec
root@dc:/#
```

Figure 7: Verify the upload status of the file to FTP server

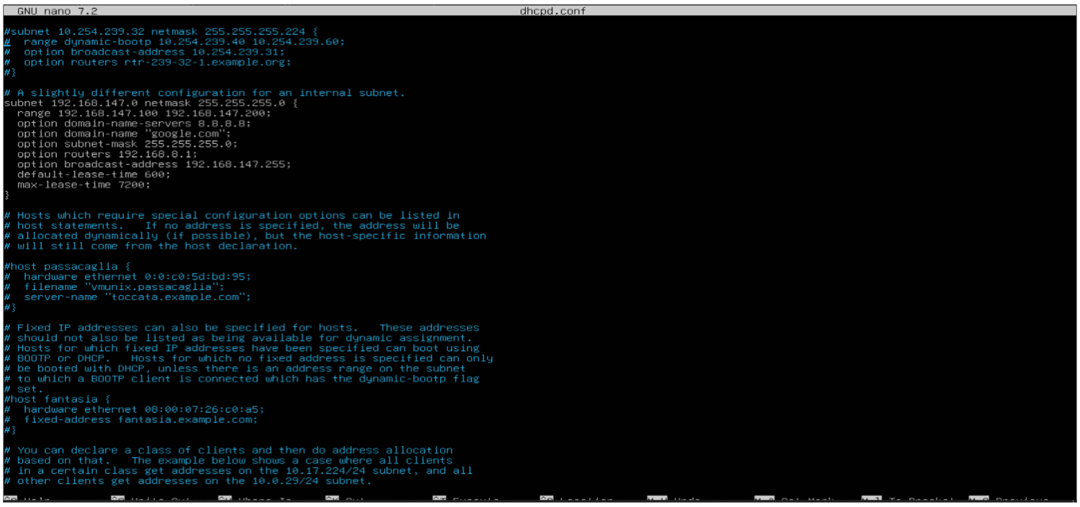
3.2.3 DHCP Server

Installation and Configuration:

The following commands applied for install and configure the DHCP server in Ubuntu server.

- ➢ sudo apt install isc-dhcp-server -y

Then edited the dhcpd.conf file as following figure.



```
#subnet 10.254.239.32 netmask 255.255.255.224 {
#  range dynamic-bootp 10.254.239.40 10.254.239.60;
#  option broadcast-address 10.254.239.31;
#  option routers rtr-239-32-1.example.org;
#}

# A slightly different configuration for an internal subnet.
subnet 192.168.147.0 netmask 255.255.255.0 {
  range 192.168.147.100 192.168.147.200;
  option domain-name-servers 8.8.8.8;
  option domain-name "google.com";
  option subnet-mask 255.255.255.0;
  option routers 192.168.8.1;
  option broadcast-address 192.168.147.255;
  default-lease-time 600;
  max-lease-time 7200;
}

# Hosts which require special configuration options can be listed in
# host statements.   If no address is specified, the address will be
# allocated dynamically (if possible), but the host-specific information
# will still come from the host declaration.

#host passacaglia {
#  hardware ethernet 0:0:c0:5d:bd:95;
#  filename "vmunix.passacaglia";
#  server-name "toccata.example.com";
#}

# Fixed IP addresses can also be specified for hosts.   These addresses
# should not also be listed as being available for dynamic assignment.
# Hosts for which fixed IP addresses have been specified can boot using
# BOOTP or DHCP.   Hosts for which no fixed address is specified can only
# be booted with DHCP, unless there is an address range on the subnet
# to which a BOOTP client is connected which has the dynamic-bootp flag
# set.
#host fantasia {
#  hardware ethernet 08:00:07:26:c0:a5;
#  fixed-address fantasia.example.com;
#}

# You can declare a class of clients and then do address allocation
# based on that.   The example below shows a case where all clients
# in a certain class get addresses on the 10.17.224/24 subnet, and all
# other clients get addresses on the 10.0.29/24 subnet.
```

Figure 8: Edit dhcpd.conf file

Configuration Parameters:

- IP Pool: 192.168.147.100-192.168.147.200
- Gateway: 192.168.8.1
- DNS Servers: 8.8.8.8

Purpose:

A DHCP server automatically assigns IP addresses and network configuration settings to client devices, eliminating the need for manual configuration and reducing administrative workload.

3.2.4 DNS Server (BIND9)

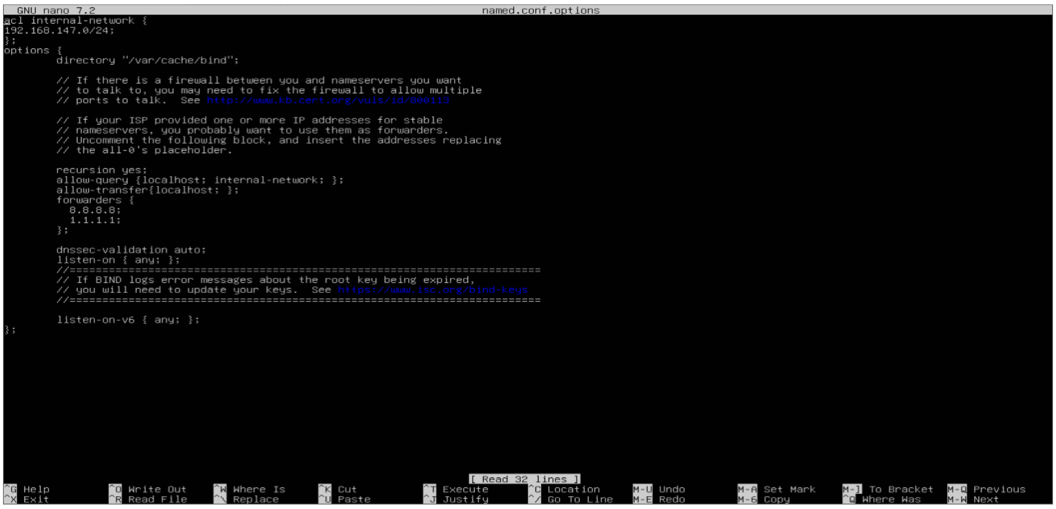
Installation Steps:

Installed BIND9 and DNS utilities from following command.

- sudo apt install bind9 bind9utils bind9-doc -y

Then edited following configuration files.

- named.conf.local
- named.conf.options
- forward.kavindu.org



```
  GNU nano 7.2                                   named.conf.options
acl internal-network {
192.168.147.0/24;
};
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        recursion yes;
        allow-query {localhost; internal-network; };
        allow-transfer{localhost; };
        forwarders {
          8.8.8.8;
          1.1.1.1;
        };

        dnssec-validation auto;
        listen-on { any; };
        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================

        listen-on-v6 { any; };
};

                                      [ Read 32 lines ]
^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark   M-] To Bracket M-Q Previous
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy       ^Q Where Was   M-W Next
```

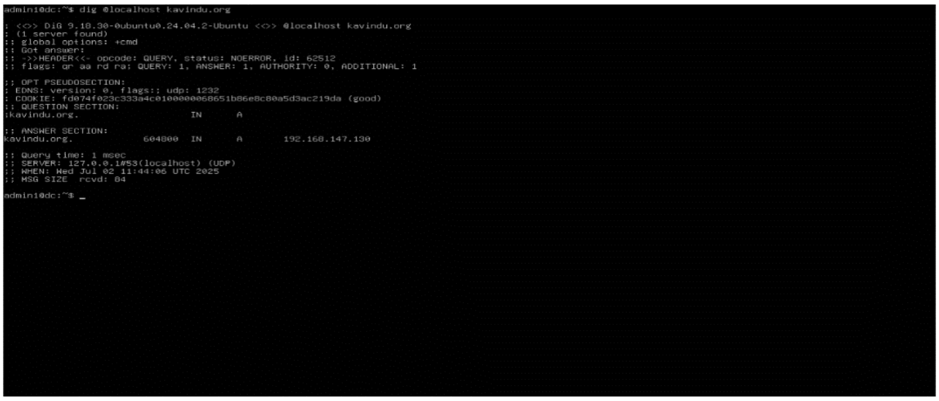
Figure 9: Edit named.conf.options file

Then started and enabled BIND9 service.

- sudo systemctl start bind9
- sudo systemctl enable bind9

Finally, tested the DNS queries by following command.

- dig @localhost kavindu.org



```
admin1@dc:~$ dig @localhost kavindu.org

; <<>> DiG 9.18.30-0ubuntu0.24.04.2-Ubuntu <<>> @localhost kavindu.org
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62512
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: fd074f023c333a4c0100000068651b86e8c80a5d3ac219da (good)
;; QUESTION SECTION:
;kavindu.org.                   IN      A

;; ANSWER SECTION:
kavindu.org.            604800  IN      A       192.168.147.130

;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(localhost) (UDP)
;; WHEN: Wed Jul 02 11:44:06 UTC 2025
;; MSG SIZE  rcvd: 84

admin1@dc:~$ _
```

Figure 10: Test DNS Query

Purpose:

BIND9 (Berkeley Internet Name Domain, version 9) is a widely used open-source Domain Name System (DNS) server software. It translates human-readable domain names (e.g., example.com) into IP addresses, enabling devices to locate and communicate with each other over networks. It supports features like DNSSEC, IPv6, dynamic updates, and zone transfers, making it suitable for both small networks and enterprise-level deployments.

3.2.5 NTP Server

Installation and Configuration:

The following commands applied for install and configure the NTP server in Ubuntu server.

- sudo apt install ntp -y
- sudo systemctl start ntp
- sudo systemctl enable ntp

Purpose:

A Network Time Protocol (NTP) server synchronizes the system clocks of devices across a network to a common time source. Accurate timekeeping is critical for event logging, authentication systems, database transactions, and coordination between networked devices. NTP servers can synchronize time from reliable external sources or act as a local time reference for internal clients.

3.2.6 Email Server (Postfix)

Installation Steps:

First, installed Postfix and mail utilities.

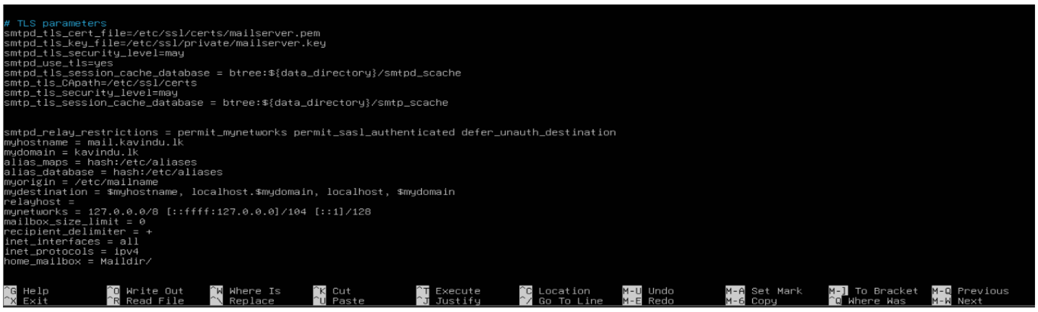
- sudo apt install postfix mailutils -y

During installation, will be prompted with a configuration screen. In this screen,

- General type of mail configuration: Choose Internet Site
- System mail name: kavindu.lk

Then, edit the main.cf file actual domain.

- sudo nano /etc/postfix/main.cf



```
# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/mailserver.pem
smtpd_tls_key_file=/etc/ssl/private/mailserver.key
smtpd_tls_security_level=may
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_CApath=/etc/ssl/certs
smtp_tls_security_level=may
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache


smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = mail.kavindu.lk
mydomain = kavindu.lk
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = ipv4
home_mailbox = Maildir/
```

Figure 11: Postfix configuration

Purpose:

A mail server handles the sending, receiving, and storage of email messages over a network. It enables communication between users by using standardized protocols such as SMTP (Simple Mail Transfer Protocol) for sending, and IMAP/POP3 for receiving. Postfix is a widely used, secure, and high-performance open-source mail transfer agent (MTA) that routes and delivers email efficiently.

3.3 Firewall Configuration (UFW)

Firewall Rules Implementation:

A firewall controls incoming and outgoing network traffic based on predefined security rules, acting as a barrier between trusted and untrusted networks. Implementing firewall rules enhances network security by restricting unauthorized access, allowing only permitted services, and preventing malicious activity. On Linux systems, tools like UFW (Uncomplicated Firewall) or iptables are commonly used to configure and enforce these rules.

3.4 Port Configuration and Security

Service	Port(s)	Protocol	UFW Command
Apache2 (HTTP)	80	TCP	sudo ufw allow 80/tcp
Apache2 (HTTPS)	443	TCP	sudo ufw allow 443/tcp
FTP	21	TCP	sudo ufw allow 21/tcp
DNS	53	TCP/UDP	sudo ufw allow 53
DHCP	67 (server), 68 (client)	UDP	sudo ufw allow 67/udp sudo ufw allow 68/udp
Mail (SMTP)	25	TCP	sudo ufw allow 25/tcp
Mail (IMAP)	143	TCP	sudo ufw allow 143/tcp
Mail (IMAPS)	993	TCP	sudo ufw allow 993/tcp
Mail (POP3)	110	TCP	sudo ufw allow 110/tcp
Mail (POP3S)	995	TCP	sudo ufw allow 995/tcp

3.5 Configuration Issues and Solutions

Issues Encountered:

1. BIND9 (DNS Server)
    - Issue: DNS queries not resolving.
    - Cause: Incorrect zone file configuration or missing forwarders.

Solution:

Check configuration syntax:

```
sudo named-checkconf
```

```
sudo named-checkzone example.com /etc/bind/db.example.com
```

Add valid DNS forwarders in /etc/bind/named.conf.options.

Restart service:

```
sudo systemctl restart bind9
```

2. NTP Server
    - Issue: Time not synchronizing with clients.
    - Cause: NTP service not started or blocked by firewall.

Solution:

Ensure service is running:

```
sudo systemctl status ntp
```

Open NTP port (123/UDP) in firewall:

```
sudo ufw allow 123/udp
```

3. Postfix (Mail Server)
    - Issue: Emails not being sent.
    - Cause: Incorrect relay configuration or port blocked by ISP/firewall.

Solution:

Verify /etc/postfix/main.cf settings for myhostname, mydomain, and relayhost.

Allow SMTP ports in firewall:

```
sudo ufw allow 25/tcp
```

```
sudo ufw allow 587/tcp
```

Restart Postfix:

```
sudo systemctl restart postfix
```

4. Apache2 (Web Server)
    - Issue: Website not loading.
    - Cause: Apache service stopped or port blocked.

Solution:

Start Apache:

```
sudo systemctl start apache2
```

Enable on boot:

```
sudo systemctl enable apache2
```

Allow HTTP/HTTPS in firewall:

```
sudo ufw allow 80/tcp
```

sudo ufw allow 443/tcp

5. FTP Server
   - Issue: Cannot connect via FTP client.
   - Cause: Firewall blocking port 21 or passive ports not configured.

Solution:

Allow port 21 in firewall:

sudo ufw allow 21/tcp

Configure passive mode in /etc/vsftpd.conf and open the port range.

6. DHCP Server
   - Issue: Clients not receiving IP addresses.
   - Cause: DHCP service not running or another DHCP server interfering.

Solution:

Start and enable service:

sudo systemctl start isc-dhcp-server

sudo systemctl enable isc-dhcp-server

Verify /etc/dhcp/dhcpd.conf for correct subnet configuration.

4. Network Monitoring and Management

4.1 Monitoring Tools Implementation

Selected tool: Nagios

Nagios is an open-source network monitoring tool that helps administrators track the availability, health, and performance of network services, hosts, and devices. It provides real-time alerts for failures, latency, or performance degradation, enabling quick response to network issues. Nagios supports monitoring via agents, SNMP, and direct service checks, and offers a web-based dashboard for centralized management.

Installation Process:

- ➢ sudo apt install autoconf gcc make wget unzip apache2 php libapache2-mod-php php-gd libgd-dev libmcrypt-dev libssl-dev bc gawk dc build-essential snmp libnet-snmp-perl gettext -y

Create Nagios User and Group

- ➢ sudo useradd nagios
- ➢ sudo groupadd nagcmd
- ➢ sudo usermod -a -G nagcmd nagios

- sudo usermod -a -G nagcmd www-data

Download and Extract Nagios Core

- cd /tmp
- wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.14.tar.gz
- tar xzf nagios-4.4.14.tar.gz
- cd nagios-4.4.14

Compile and Install Nagios

- ./configure --with-command-group=nagcmd
- make all
- sudo make install
- sudo make install-init
- sudo make install-commandmode
- sudo make install-config
- sudo make install-webconf

Create Nagios Web Interface User

- sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin

  (Replace nagiosadmin with preferred username.)

Enable and Start Services

- sudo systemctl enable apache2
- sudo systemctl start apache2
- sudo systemctl enable nagios
- sudo systemctl start nagios

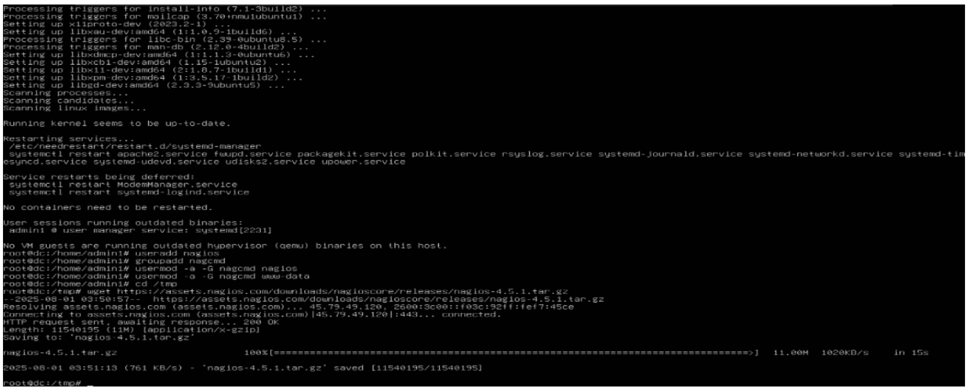
Access the Web Interface

Open the browser and go to:

- http://<server-ip>/nagios

Login with the web user credentials that created.

- 192.168.147.130/nagios



```
Processing triggers for install-info (7.1-3build2) ...
Processing triggers for mailcap (3.70+nmu1ubuntu1) ...
Setting up x11proto-dev (2023.2-1) ...
Setting up libxau-dev:amd64 (1:1.0.9-1build6) ...
Processing triggers for libc-bin (2.39-0ubuntu8.5) ...
Processing triggers for man-db (2.12.0-4build2) ...
Setting up libxdmcp-dev:amd64 (1:1.1.3-0ubuntu6) ...
Setting up libxcb1-dev:amd64 (1.15-1ubuntu2) ...
Setting up libx11-dev:amd64 (2:1.8.7-1build1) ...
Setting up libxpm-dev:amd64 (1:3.5.17-1build2) ...
Setting up libgd-dev:amd64 (2.3.3-9ubuntu5) ...
Scanning processes...
Scanning candidates...
Scanning linux images...

Running kernel seems to be up-to-date.

Restarting services...
 /etc/needrestart/restart.d/systemd-manager
 systemctl restart apache2.service fwupd.service packagekit.service polkit.service rsyslog.service systemd-journald.service systemd-networkd.service systemd-tim
esyncd.service systemd-udevd.service udisks2.service upower.service

Service restarts being deferred:
 systemctl restart ModemManager.service
 systemctl restart systemd-logind.service

No containers need to be restarted.

User sessions running outdated binaries:
 admin1 @ user manager service: systemd[2231]

No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@dc:/home/admin1# useradd nagios
root@dc:/home/admin1# groupadd nagcmd
root@dc:/home/admin1# usermod -a -G nagcmd nagios
root@dc:/home/admin1# usermod -a -G nagcmd www-data
root@dc:/home/admin1# cd /tmp
root@dc:/tmp# wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.5.1.tar.gz
--2025-08-01 03:50:57--  https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.5.1.tar.gz
Resolving assets.nagios.com (assets.nagios.com)... 45.79.49.120, 2600:3c00::f03c:92ff:fef7:45ce
Connecting to assets.nagios.com (assets.nagios.com)|45.79.49.120|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11540195 (11M) [application/x-gzip]
Saving to: 'nagios-4.5.1.tar.gz'

nagios-4.5.1.tar.gz                 100%[===========================================================================>]  11.00M  1020KB/s    in 15s

2025-08-01 03:51:13 (761 KB/s) - 'nagios-4.5.1.tar.gz' saved [11540195/11540195]

root@dc:/tmp# _
```

Figure 12: Nagios installation

Basic Configuration for Monitoring

Add Hosts to Monitor

- Edit /usr/local/nagios/etc/objects/hosts.cfg (create if not exists).

Add Services to Monitor

- Edit /usr/local/nagios/etc/objects/services.cfg.

Verify Configuration

- sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

Restart Nagios to Apply Changes

- sudo systemctl restart nagios

4.2 Monitoring Network Performance with Nagios

- Availability Checks – Monitor host up/down status using ICMP (ping) or service checks.
- Service Monitoring – Track performance of HTTP, FTP, DNS, SMTP, and other protocols.
- Resource Usage – Monitor CPU, RAM, disk space, and bandwidth usage.
- Alert Notifications – Configure email or SMS alerts for downtime or performance issues.
- Historical Reports – View uptime history, response times, and trends to identify recurring problems.

4.3 Monitoring Tools Contribution to Security

The deployed monitoring tools play a vital role in enhancing network security by:

- Real-Time Threat Detection – Identifying unusual or suspicious traffic patterns that may indicate potential security threats.
- Incident Response Support – Providing comprehensive logs and alerts to facilitate timely investigation and resolution of security incidents.
- Performance Baseline Establishment – Defining normal network behavior to quickly detect anomalies and deviations.
- Compliance Monitoring – Verifying that network operations adhere to established security policies and regulatory requirements.

5. Windows Server Setup

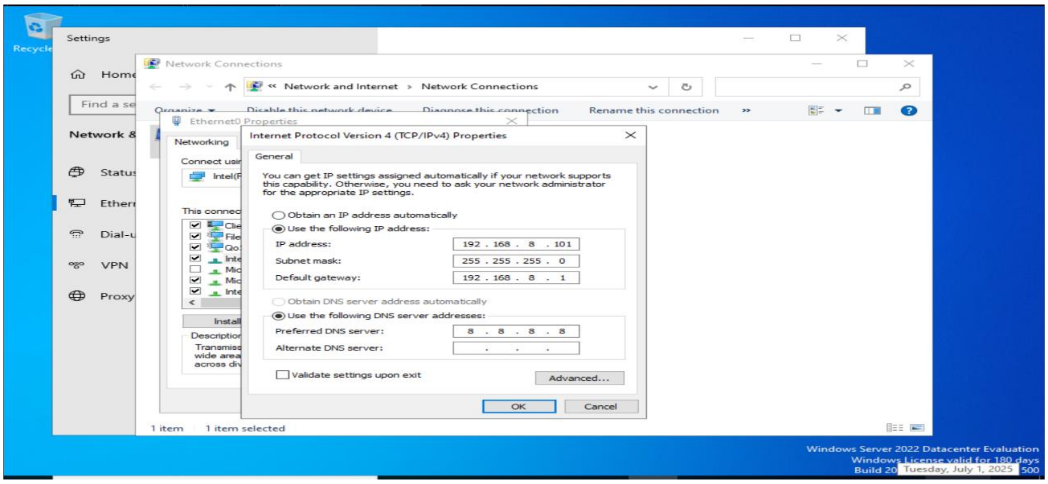
Windows Server 2022 is Microsoft’s latest long-term servicing channel (LTSC) release for enterprise-grade server operating systems, designed to deliver enhanced security, performance, and scalability. It introduces advanced security features such as Secured-core server, TLS 1.3, and improved Windows Defender capabilities to protect against modern cyber threats. Windows Server 2022 also offers hybrid cloud integration with Azure, improved container support, and better storage performance through SMB compression and faster file transfers. It is suitable for roles such as Active Directory Domain Services (AD DS), file and print services, web hosting, and application deployment, making it a versatile choice for modern IT infrastructure.

5.1 Windows Server Installation

Operating System: Windows Server 2019/2022 Evaluation Edition

Virtual Machine Specifications:

- RAM: 2GB
- Storage: 60GB
- Network: Bridged Adapter
- IP Address: 192.168.8.101



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 8 . 101
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 8 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 8 . 8 . 8 . 8
Alternate DNS server: . . .

□ Validate settings upon exit

Advanced...   OK   Cancel

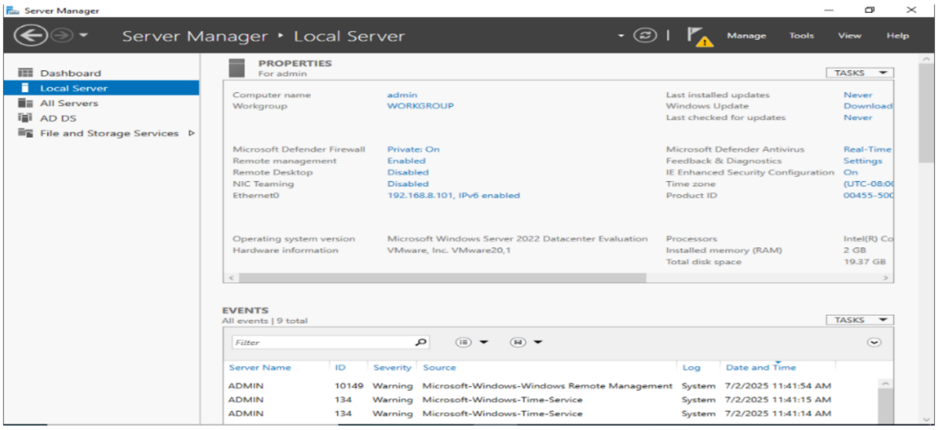
Figure 13: Static IP for Windows Server

5.2 Active Directory Configuration

5.2.1 Active Directory Domain Services Installation

Installation Steps:

1. Server Manager → Add Roles and Features
2. Select Active Directory Domain Services
3. Promote server to Domain Controller
4. Create new forest: `kavindu.local`



PROPERTIES
For admin

Computer name admin
Workgroup WORKGROUP

Last installed updates Never
Windows Update Download
Last checked for updates Never

Microsoft Defender Firewall Private: On
Remote management Enabled
Remote Desktop Disabled
NIC Teaming Disabled
Ethernet0 192.168.8.101, IPv6 enabled

Microsoft Defender Antivirus Real-Time
Feedback & Diagnostics Settings
IE Enhanced Security Configuration On
Time zone (UTC-08:0
Product ID 00455-50

Operating system version Microsoft Windows Server 2022 Datacenter Evaluation
Hardware information VMware, Inc. VMware20,1

Processors Intel(R) Co
Installed memory (RAM) 2 GB
Total disk space 19.37 GB

EVENTS
All events | 9 total

Server Name	ID	Severity	Source	Log	Date and Time
ADMIN	10149	Warning	Microsoft-Windows-Windows Remote Management	System	7/2/2025 11:41:54 AM
ADMIN	134	Warning	Microsoft-Windows-Time-Service	System	7/2/2025 11:41:15 AM
ADMIN	134	Warning	Microsoft-Windows-Time-Service	System	7/2/2025 11:41:14 AM

Figure 14: Windows Server Manager wizard

5.2.2 Domain Configuration

Domain Details:

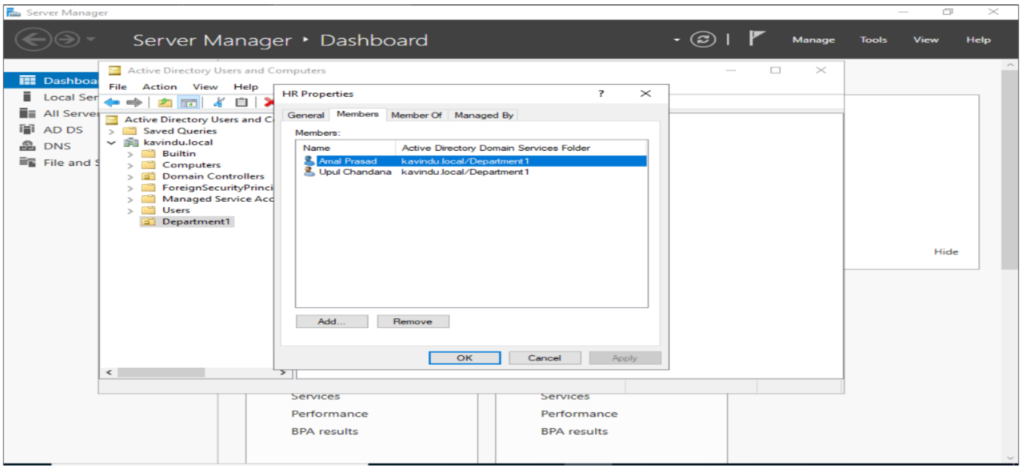
- **Domain Name:** kavindu.local
- **NetBIOS Name:** KAVINDU
- **Forest Functional Level:** Windows Server 2022
- **Domain Functional Level:** Windows Server 2022

5.3 Users and Groups Management

5.3.1 Organizational Units (OUs)

Created OUs for organizational structure:

- **Department1**



Members:

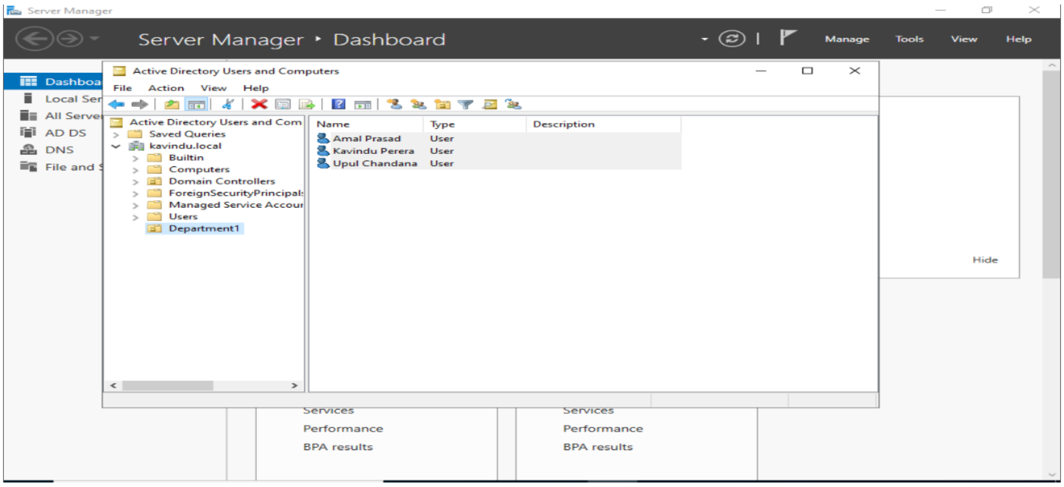
Name	Active Directory Domain Services Folder
Amal Prasad	kavindu.local/Department1
Upul Chandana	kavindu.local/Department1

Figure 15: Group creation in Windows Server

5.3.2 User Account Creation

Sample Users Created:

- kperera@kavindu.local
- aprasad@kavindu.local
- uchandana@kavindu.local



Name	Type	Description
Amal Prasad	User	
Kavindu Perera	User	
Upul Chandana	User	

Figure 16: User creation in Windows Server

5.4 Client Domain Integration

5.4.1 Windows 7 Client Configuration

A Windows 7 virtual machine was installed and configured to act as the client system for domain login testing. The client VM's network settings were adjusted to ensure it operated within the same network as the Windows Server 2022 domain controller. The machine was then joined to the domain by navigating to Control Panel → System and Security → System, selecting Change settings under the computer name, choosing Domain, and entering the configured domain name. When prompted, domain administrator credentials were provided to authorize the join operation. After restarting the client machine to apply the changes, login tests were conducted for each of the three newly created user accounts. Using the Other User option on the Windows 7 login screen, domain credentials were entered, and successful logins confirmed that user profiles were created correctly and network access permissions were functioning as intended.

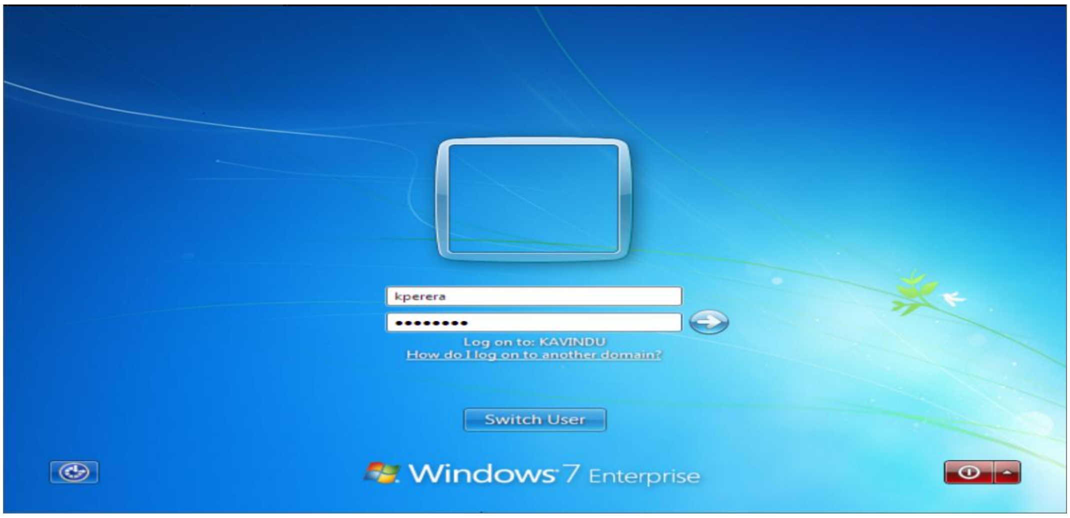
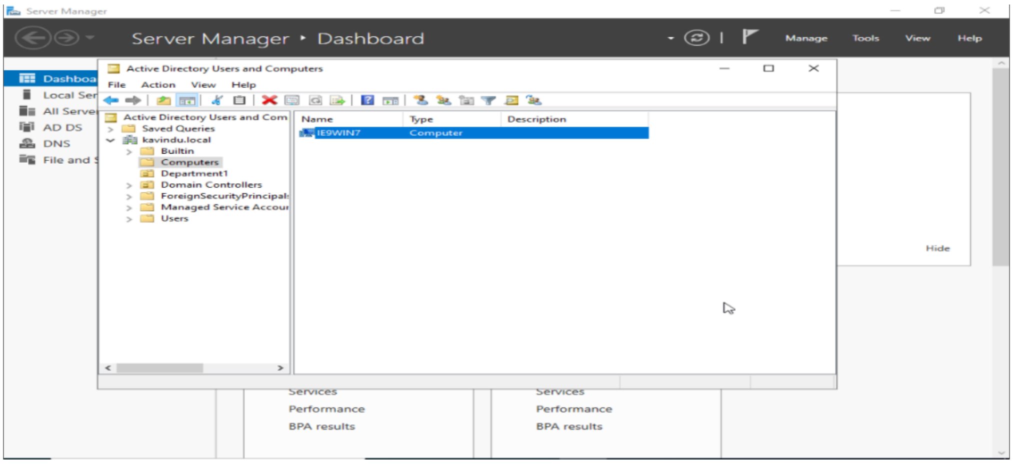

kperera
•••••••••
Log on to: KAVINDU

Figure 17: Client login to server



Active Directory Users and Computers
- Saved Queries
- kavindu.local
  - Builtin
  - Computers
  - Department1
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Managed Service Accounts
  - Users

Name	Type	Description
IE9WIN7	Computer	

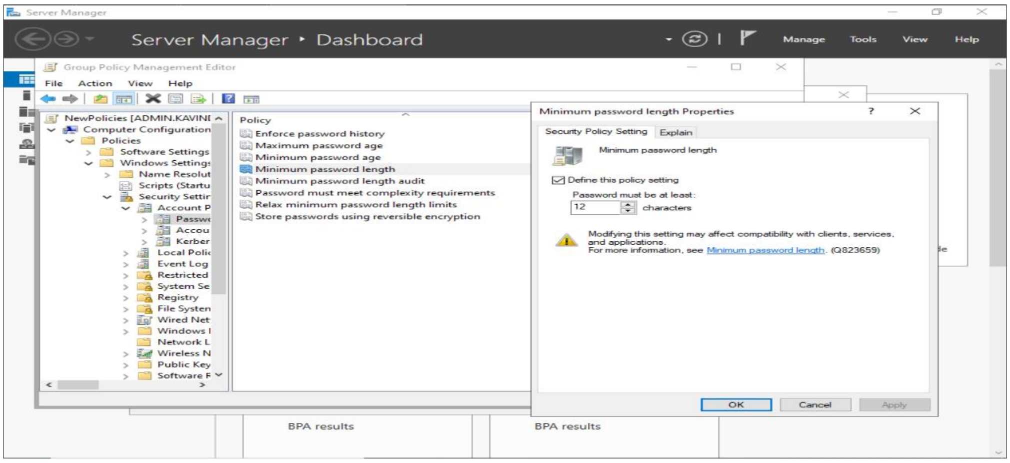
Figure 18: Check Client login status

5.5 Group Policy Configuration

5.5.1 Security Policies

Password Policy Configuration:

- Minimum password length: 12 characters
- Password complexity requirements: Enabled



NewPolicies [ADMIN.KAVINDU...]
- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Security Settings
        - Account Policies
          - Password Policy
          - Account Lockout Policy
          - Kerberos Policy
        - Local Policies
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Wired Network
        - Windows Firewall
        - Network List Manager
        - Wireless Network
        - Public Key Policies
        - Software Restriction

Policy
- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length
- Minimum password length audit
- Password must meet complexity requirements
- Relax minimum password length limits
- Store passwords using reversible encryption

Minimum password length Properties

Security Policy Setting | Explain

Minimum password length

☑ Define this policy setting

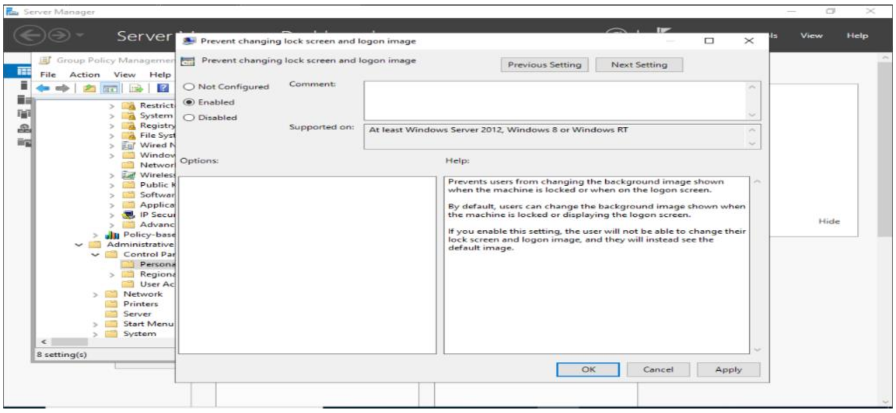
Password must be at least:
12 characters

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Minimum password length. (Q823659)

Figure 19: Setup Password policy

5.5.2 User Rights Assignment

Prevent changing log screen and logon image



Prevent changing lock screen and logon image

Prevent changing lock screen and logon image

Previous Setting | Next Setting

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2012, Windows 8 or Windows RT

Options:

Help:

Prevents users from changing the background image shown when the machine is locked or when on the logon screen.

By default, users can change the background image shown when the machine is locked or displaying the logon screen.

If you enable this setting, the user will not be able to change their lock screen and logon image, and they will instead see the default image.

OK | Cancel | Apply

Figure 20: Setup lock screen policy

5.6 Authentication System Benefits

5.6.1 Centralized Authentication

In a domain environment, user identity verification can be unified under a single directory service, removing the need for separate logins for each system or application. Instead of managing credentials in multiple places, administrators can update permissions, reset passwords, and track account activity from one management interface. This approach reduces administrative effort, minimizes user confusion, and allows the infrastructure to grow without significant changes to the authentication process.

5.6.2 LDAP Integration

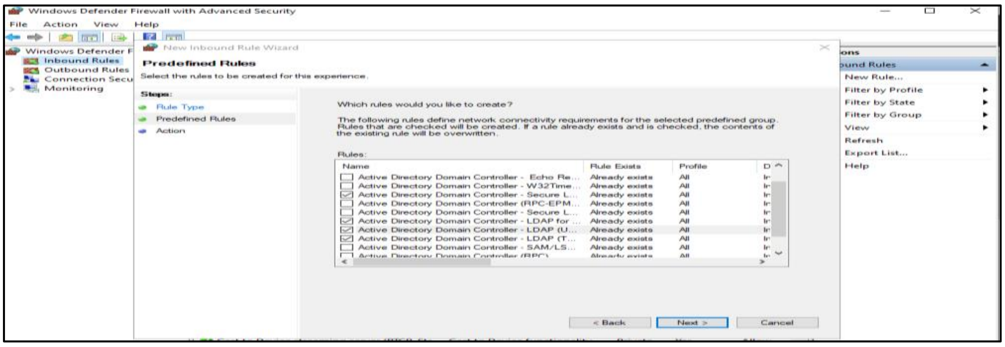
By implementing directory-based protocols such as LDAP, authentication and resource lookups can be extended beyond the Windows ecosystem. This makes it possible for mixed environments—where Linux servers, web applications, and other non-Microsoft platforms are present—to verify user access against the same trusted source. It also enables consistent identity data to be shared across multiple tools and services, supporting both security enforcement and operational efficiency.

5.7 Windows Firewall Configuration

5.7.1 Firewall Rules

Inbound Rules:

- Allow Active Directory (TCP 389, 636, 3268)
- Allow DNS (TCP/UDP 53)
- Allow Kerberos (TCP/UDP 88)
- Allow LDAP (TCP 389)
- Allow RPC (TCP 135)



Predefined Rules

Select the rules to be created for this experience.

Which rules would you like to create?

The following rules define network connectivity requirements for the selected predefined group. Rules that are checked will be created. If a rule already exists and is checked, the contents of the existing rule will be overwritten.

Rules:

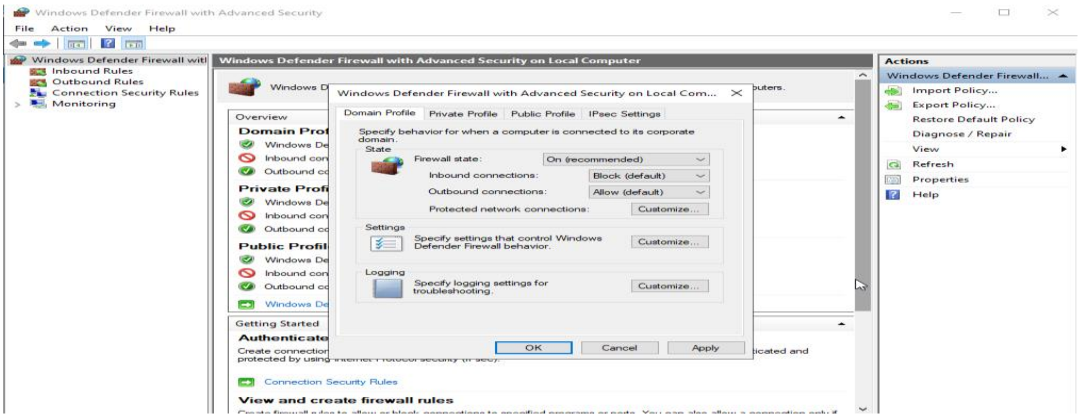
Name	Rule Exists	Profile	D
☐ Active Directory Domain Controller - Echo Re...	Already exists	All	Ir
☐ Active Directory Domain Controller - W32Time...	Already exists	All	Ir
☑ Active Directory Domain Controller - Secure L...	Already exists	All	Ir
☐ Active Directory Domain Controller (RPC-EPM...	Already exists	All	Ir
☐ Active Directory Domain Controller - Secure L...	Already exists	All	Ir
☑ Active Directory Domain Controller - LDAP for ...	Already exists	All	Ir
☑ Active Directory Domain Controller - LDAP (U...	Already exists	All	Ir
☑ Active Directory Domain Controller - LDAP (T...	Already exists	All	Ir
☐ Active Directory Domain Controller - SAM/LS...	Already exists	All	Ir
☐ Active Directory Domain Controller (RPC)	Already exists	All	Ir

Figure 21: Firewall configuration

5.7.2 Domain Profile Configuration

Security Settings:

- Firewall enabled for all profiles
- Default inbound action: Block
- Default outbound action: Allow
- Logging enabled for troubleshooting



Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall wit
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Defender Firewall with Advanced Security on Local Computer
Overview
Domain Prof
Private Profi
Public Profil
Getting Started
Authenticate
Connection Security Rules
View and create firewall rules
Actions
Windows Defender Firewall...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help

Windows Defender Firewall with Advanced Security on Local Com...

Domain Profile | Private Profile | Public Profile | IPsec Settings

Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections: Customize...

Settings

Specify settings that control Windows Defender Firewall behavior. Customize...

Logging

Specify logging settings for troubleshooting. Customize...

OK | Cancel | Apply

Figure 22: Enable firewall

6. Security and Access Control

6.1 Firewall Rules Summary

6.1.1 Linux Server (UFW) Rules

Service	Port(s)	Protocol	UFW Command
Apache2 (HTTP)	80	TCP	sudo ufw allow 80/tcp
Apache2 (HTTPS)	443	TCP	sudo ufw allow 443/tcp
FTP	21	TCP	sudo ufw allow 21/tcp
DNS	53	TCP/UDP	sudo ufw allow 53
DHCP	67 (server), 68 (client)	UDP	sudo ufw allow 67/udp sudo ufw allow 68/udp
Mail (SMTP)	25	TCP	sudo ufw allow 25/tcp
Mail (IMAP)	143	TCP	sudo ufw allow 143/tcp
Mail (IMAPS)	993	TCP	sudo ufw allow 993/tcp
Mail (POP3)	110	TCP	sudo ufw allow 110/tcp
Mail (POP3S)	995	TCP	sudo ufw allow 995/tcp

6.1.2 Windows Server Firewall Rules

Service	Port	Protocol	Action	Purpose
Active Directory	389, 636	TCP	ALLOW	LDAP/LDAPS
Global Catalog	3268, 3269	TCP	ALLOW	AD Global Catalog
Kerberos	88	TCP/UDP	ALLOW	Authentication
DNS	53	TCP/UDP	ALLOW	Name resolution
RPC	135	TCP	ALLOW	Remote procedure calls
SMB	445	TCP	ALLOW	File sharing
NetBIOS	137-139	TCP/UDP	ALLOW	Legacy networking

6.2 Authentication and Authorization Methods

6.2.1 Layered Access Verification

A tiered security model can be applied to verify identity at multiple stages within the network and system environment.

- **Infrastructure-Level Controls** – Implement measures such as device whitelisting by hardware address, logical separation of network zones through VLAN configurations, and encrypted wireless connectivity using protocols like WPA2 or WPA3.
- **System-Level Verification** – Enforce secure sign-in to operating systems with robust password policies, enable public key authentication for Linux-based platforms, and integrate Windows endpoints into a centralized domain service for credential management.
- **Application-Level Checks** – Protect individual services with dedicated login processes, ensure databases require authenticated user sessions, and configure service-specific access controls tailored to their function.

6.2.2 Domain-Based Authentication Sequence

When resources are protected through a directory service, the verification process follows a defined exchange:

1. A user or device initiates a request to access a protected service.
2. The request is relayed to the directory service controller for identity validation.
3. If credentials are valid, a secure ticket is issued to prove authentication status.
4. A secondary request is made to obtain permission for the exact resource needed.
5. The service grants or denies access based on predefined authorization rules associated with the account.

7. Conclusion

7.1 Summary of Work Done

This project showcased the successful planning, deployment, and testing of a multi-platform computer network infrastructure that utilized both Linux-based and Windows-based server environments. The key goals set at the beginning were met, resulting in a fully operational and secure network.

Network Infrastructure:

- Designed and implemented a structured network based on the 192.168.147.0/24 subnet.
- Configured switching and routing functionalities using Cisco Packet Tracer to simulate network behavior.
- Verified end-to-end connectivity between all network nodes and services.

Linux Server Services:

- Deployed Ubuntu 24.04 LTS servers with multiple critical services
- Configured Apache2 web server, BIND9 DNS, ISC DHCP server, Postfix mail server and vsftpd FTP server
- Implemented comprehensive firewall security using UFW
- Established network time synchronization with NTP

Windows Active Directory:

- Installed Windows Server and deployed Active Directory Domain Services (AD DS).
- Created and managed users, groups, and organizational units to establish structured access control.
- Successfully joined a Windows 7 client machine to the domain.
- Configured Group Policy Objects (GPO) to enforce centralized security and administrative settings.

Network Monitoring:

- Configured Nagios for real-time network and system performance monitoring.
- Set up log tracking and alert notifications for proactive issue detection.
- Verified network security and availability through continuous observation.

7.2 Challenges Faced and Lessons Learned

7.2.1 Technical Challenges

Virtual Machine Resource Usage:
Running multiple servers and clients simultaneously required optimization of virtual machine configurations and a staggered startup schedule to conserve host system resources.

Service Configuration Errors:
Initial misconfigurations in **DNS** and **DHCP** caused connectivity issues. These were corrected through step-by-step troubleshooting and service revalidation.

Active Directory Domain Join Failures:
Issues with client integration into the domain were traced back to DNS settings. Adjustments to DNS forwarding and server time synchronization resolved the problem.

7.3 Key Takeaways

- **Cross-Platform Integration:** Combining Linux and Windows environments requires thorough planning, documentation, and testing to ensure smooth interoperability.
- **Security at Multiple Layers:** Implementing firewall rules, secure authentication methods, and proper network segmentation reinforced the importance of layered security in infrastructure design.
- **Proactive Monitoring:** Using **Nagios** emphasized the need for continuous system health checks and prompt issue detection to maintain network reliability and security.

8. References

1. "Introduction | Server documentation," *Ubuntu*, 2024. https://ubuntu.com/server/docs
2. Microsoft, "Windows Server documentation," *learn.microsoft.com*. https://learn.microsoft.com/en-us/windows-server/
3. "Nagios Core. Download Nagios Core For Free Here.," *Nagios*. https://www.nagios.org/projects/nagios-core/
4. GeeksforGeeks, "How to Configure DNS on Linux," *GeeksforGeeks*, Feb. 15, 2024. https://www.geeksforgeeks.org/techtips/how-to-configure-dns-in-linux/ (accessed Aug. 11, 2025).
5. L. Reynolds, "What is DHCP and how to configure DHCP server in Linux - LinuxConfig.org," *linuxconfig.org*, Jun. 15, 2021. https://linuxconfig.org/what-is-dhcp-and-how-to-configure-dhcp-server-in-linux
6. GeeksforGeeks, "How to setup and configure an FTP server in Linux?," *GeeksforGeeks*, Jan. 26, 2022. https://www.geeksforgeeks.org/linux-unix/setup-and-configure-an-ftp-server-in-linux/ (accessed Aug. 11, 2025).
7. "How to Install and Configure NTP on Linux | TimeTools Ltd," *TimeTools*, Feb. 15, 2019. https://timetoolsltd.com/ntp/how-to-install-and-configure-ntp-on-linux/
8. Orin-Thomas, "Manage user accounts with Active Directory Users and Computers in Windows Server," *Microsoft.com*, Apr. 04, 2025. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage-user-accounts-in-windows-server

9. Appendices

Appendix A: Configuration Files

A.1 DNS Zone Files

[SCREENSHOT PLACEHOLDER: Capture_forward.kavindu.org_config.png] *Configuration files: /etc/bind/forward.kavindu.org*

A.2 DHCP Server Configuration

[SCREENSHOT PLACEHOLDER: Capture_dhcpd.conf_Config.png] *Configuration file: /etc/dhcp/dhcpd.conf*

Appendix B: Command Outputs

B.1 DNS Query Test

[SCREENSHOT PLACEHOLDER: Capture_Test_DNS_Query.png] *Test DNS queries using dig command*

B.2 Verify File Upload

[SCREENSHOT PLACEHOLDER: Capture_verify_upload.png] *Verify the file uploaded successfully using windows 7 client*

Appendix C: Network Diagrams and Screenshots

C.1 Packet Tracer Network Topology

[SCREENSHOT PLACEHOLDER: packet_tracer_topology.png] *Complete network topology in Cisco Packet Tracer*

C.2 Active Directory Management Console

[SCREENSHOT PLACEHOLDER: Capture_Server_setup.png] *Active Directory Users and Computers management interface*