# Case Study: Setting Up and Configuring Apache Tomcat, Samba, DNS/LDAP Services, Firewall, and Proxy Server Configuration in a

**Networked Environment**

## Overview

This case study focuses on the implementation of a networked environment that includes Apache Tomcat for web applications, Samba for file sharing, DNS and LDAP for directory services, firewall configurations for security, and proxy server settings for controlled internet access. The environment is designed to support a medium-sized organization with a focus on security, performance, and ease of

management.

## Objectives

1. Deploy Apache Tomcat for hosting Java-based web applications.
2. Set up Samba for file sharing across different operating systems.
3. Implement DNS and LDAP for centralized user management and resource location.
4. Configure a firewall to secure the network.
5. Set up a proxy server for controlled internet access and monitoring.

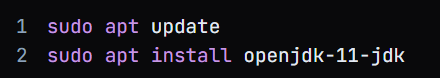
## Environment Setup

* + **Hardware**: A server with at least 16GB RAM, 4 CPU cores, and 500GB of storage.
  + **Operating System**: Ubuntu Server 22.04 LTS.
  + **Network Configuration**: Static IP addressing for servers, DHCP for client machines.

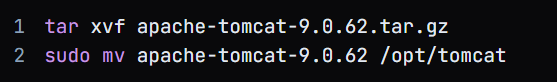
## Deploying Apache Tomcat

Installation Steps:

* 1. **Install Java Development Kit (JDK)**



* 1. **Download Apache Tomcat**:
     1. wget https://downloads.apache.org/tomcat/tomcat-9/v9.0.62/bin/apache-tomcat-9.0.62.tar.gz
  2. **Extract and Configure**:





1. **Start Tomcat**:



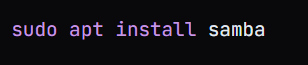
## Configuration:

* + Edit “server.xml” to configure the port and context paths.
  + Ensure proper security settings in “web.xml” for web applications.

## Setting Up Samba

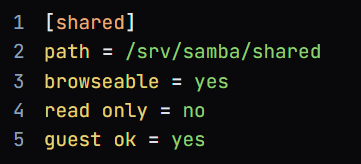
Installation Steps:

* 1. **Install Samba**

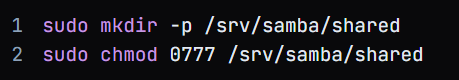


* 1. **Configure Samba:**

Edit /etc/samba/smb.conf to create a share**:**



* 1. **Create Shared Directory**:





## Implementing DNS and LDAP

Installation Steps for DNS (Bind9):

* 1. **Install Bind9**



* 1. **Configure Zone Files:**

Edit /etc/bind/named.conf.local to add zones.

* 1. **Restart Bind9**



Installation Steps for LDAP (OpenLDAP):

1. **Install OpenLDAP**



1. **Configure LDAP**:

Use dpkg-reconfigure slapd to set up the domain and admin password.

1. **Add Users:**

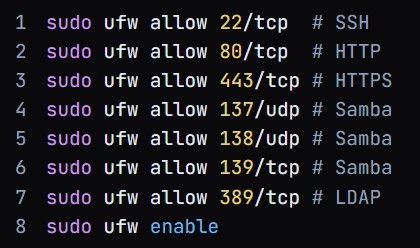
Create LDIF files and use ldapadd to populate the directory.

# Configuring the Firewall

Installation and Configuration:

* 1. **Install UFW**





## Setting Up a Proxy Server

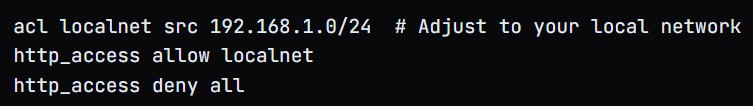
Installation Steps (Squid Proxy):

* 1. **Install Squid**



* 1. **Configure Squid:**

**Edit /etc/squid/squid.conf to set up ACLs and control access**



* 1. **Restart Squid Service:**



## Summary

This setup provides a secure, scalable infrastructure with Apache Tomcat for web applications,

Samba for file sharing, DNS and LDAP for centralized resource and user management, and firewall/proxy configurations for network security. Following best practices in securing access and monitoring logs helps in maintaining a reliable and compliant environment.