



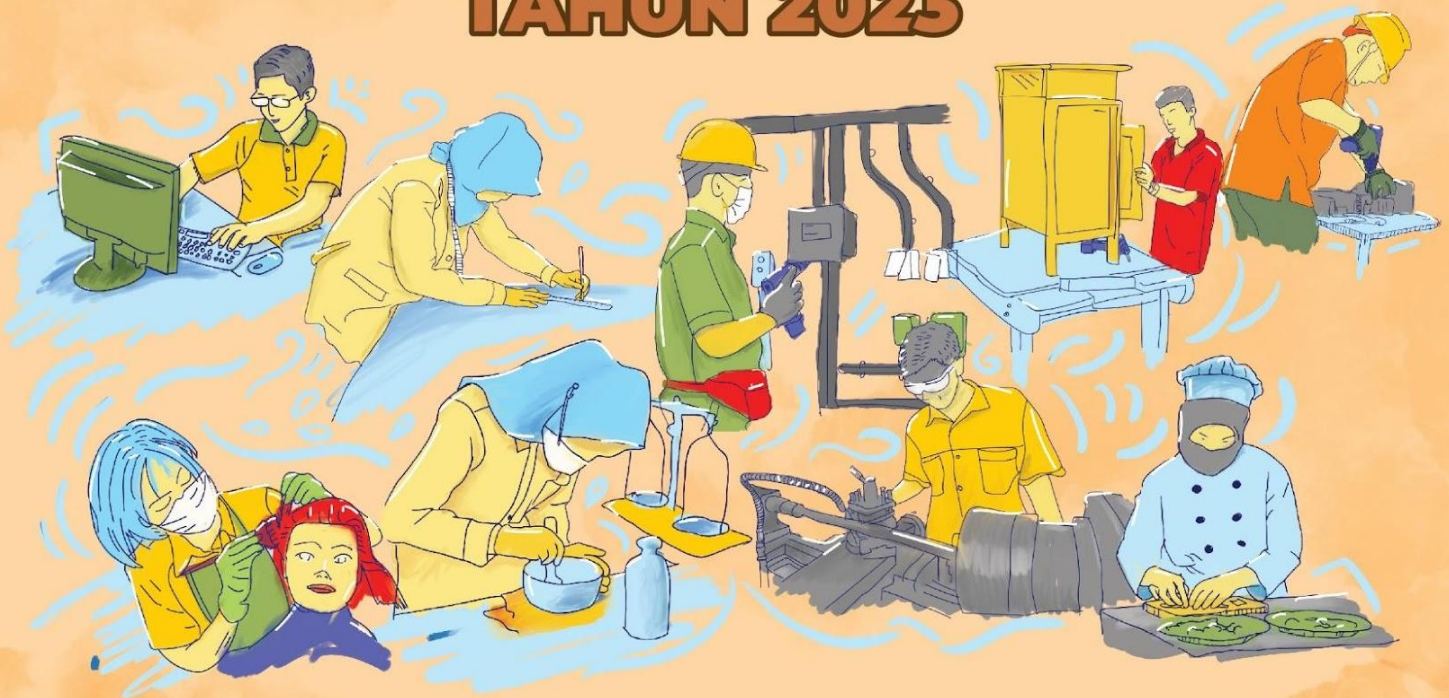
**BALAI PENGEMBANGAN TALENTA INDONESIA**  
PUSAT PRESTASI NASIONAL  
SEKRETARIAT JENDERAL  
KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI

**MERDEKA  
BELAJAR**



# SOAL

## LOMBA KOMPETENSI SISWA SMK TINGKAT NASIONAL TAHUN 2023



### BIDANG LOMBA

**Teknologi Informasi Sistem Administrasi Jaringan**  
(IT Network System Administration)

**MERDEKA BERPRESTASI**  
Talenta Vokasi Menginspirasi

# **ACTUAL TEST PROJECT** **MODUL A - CLIENT SERVER**

## ***IT NETWORK SYSTEMS ADMINISTRATION***

**KELOMPOK INFORMATION AND COMMUNICATION TECHNOLOGY**

# Introduction

An e-commerce company just bought some servers to create on-premise infrastructure for their application. They require both Linux servers and Windows servers for their business operation. You will be responsible for configuring the servers according to their requirements.

## Configuration Guidelines

- Make sure all configuration is permanent and able to survive reboot.
- **ALL servers will be rebooted before marking.**
- If no information or instruction is provided, you should use the default configuration.
- If you require a password for some tasks, you can use **Skills39s**
- Do not change anything related to the SSH configuration in all Linux Servers.

# Description of project and tasks

## General Configuration

- Configure all servers with hostname and IP Address(es), refer to the Appendix for detailed information.
- Configure all windows servers to be pingable.
- Do not change anything related to the SSH configuration in all Linux Servers.

## OS Configuration

- Please create a disk partition in muna.lks.id with RAID technology with two disks mirroring, so that it tolerates single disk failure.
  - Use two available unused disks.
  - Mount in /data
- Install sudo in buton.lks.id.
  - Make sure to configure **competitor** user to be able to use sudo and become root.

## Karimata DNS

- Configure rote.lks.id to serve DNS for karimata.id
- Configure to forward all requests to (sub)domains other than karimata.id to Lombok DNS.
- Create records needed by the Karimata Web Service.

## Karimata Web Service

- Configure rote.lks.id as a web server serving all requests for all \*.karimata.id websites.
- Serve www.karimata.id with the default html file.
  - Enable HTTPS using the Certificate Authority with wildcard domain \*.karimata.id.
  - Redirect all HTTP requests to HTTPS.
  - Create the necessary DNS record at Karimata DNS

## Karimata Networking

- Configure DHCP server in muna.lks.id.
  - You can freely use any tools/package that provides standard DHCP.
  - Respond only to requests received in the Karimata Network.
  - Use the IP range: 10.200.2.40-10.200.2.50
  - Give DNS Address to Karimata DNS
  - Give default gateway to muna.lks.id.
- Make sure muna.lks.id can route traffic from the Karimata Network to two other networks.

## Karimata Root Certificate

- Use rote.lks.id as the certificate issuer for all services.
  - Configure as Root CA.
  - Use Common Name: Karimata-RootCA
- Issue all required certificates for services in other tasks.
  - Send all generated certificates in PEM format in muna.lks.id /opt/certs
    - Make sure it's also include the Root Certificate
  - Also place all generated certificate's private keys in muna.lks.id /opt/keys
    - Make sure it's also include the Root Certificate Key

## Lombok DNS

- Configure jukung.lks.id and komodo.lks.id as DNS servers for two domains.
  - Both servers need to have identical records.
  - Both are the authoritative servers of the lombok.id domain and lks.id domain.
  - Create both server records in the lombok.id domain as jukung.lombok.id and komodo.lombok.id that points to the Lombok Network IP address.
- Create records of all servers in lks.id domain according to their hostname.
  - Those records should point to all available IP Addresses in each server.
- Create records for all other tasks required in the Lombok Network, including but not limited to:
  - Email
  - Webmail
- Configure to forward all requests to (sub)domains other than karimata.id, lombok.id and lks.id to Malaka DNS.
- Configure to forward all requests to karimata.id (sub)domains to Karimata DNS.

## Company Mail

- Configure buton.lks.id as the central mail server.
  - Use any application that supports both SMTP and IMAP using negotiable TLS
  - Use the domain lks.id, so email can be sent to user@lks.id email address.
  - Enable SMTP with negotiable TLS on port 25
  - Enable IMAP with negotiable TLS on port 143
  - Use certificates from Karimata Root Certificate
- Enable web-based email using roundcube
  - Make it accessible using the domain mail.lks.id.
  - Enable HTTPS access using a certificate from Karimata Root Certificate
  - Do not respond to HTTP requests.
- Make sure the SMTP and IMAP only respond to requests from Karimata Network.
- Make sure the web-based email is accessible via any network.
- Create two mail users: admin@lks.id and user@lks.id with password Skills39s
  - Send a test mail from user@lks.id to admin@lks.id.
- Create email alias contact@lks.id should be received by admin@lks.id
  - Send a test mail from user@lks.id to contact@lks.id

## Additional Storage

- Configure muna.lks.id disk to be shared via iSCSI
  - Share two disks that RAID or the OS does not use.
  - Make sure the disk is accessible by jukung.lks.id and komodo.lks.id
- Setup iSCSI in jukung.lks.id and komodo.lks.id to access the previous disk.
  - There are two disks, one for jukung.lks.id and one for komodo.lks.id.
  - Mount the disk at the same F: drive using a suitable filesystem
- Share these folders to be able to read and write anonymously:
  - F:\backup at jukung.lks.id
  - F:\backup at komodo.lks.id
  - C:\backup at jukung.lks.id
- Create the folder if it does not exist.
- Make sure the folder is accessible from linux using standard SMB client.



## Integrated Backup

- Use Windows Backup to backup C:\internal\cert from rote.lks.id to these destinations daily at any hour:
  - F:\backup at komodo.lks.id
  - C:\backup at jukung.lks.id
- Execute the backup at least once to have immediate backup.
- Use DFS-Replication or something similar to keep these folders synchronized:
  - F:\backup at komodo.lks.id
  - F:\backup at jukung.lks.id

## Company VPN

- Install and configure LDAP with OpenLDAP in buton.lks.id
  - Use domain dc=lks,dc=id
  - Create admin user cn=admin,dc=lks,dc=id with password Skills39s
  - Use simple authentication.
  - Create OU VPN to store all VPN users.
  - Create a user remote with password Skills39s in the VPN OU to be used during VPN authentication.
- Configure Site-to-Site VPN from buton.lks.id to aur.lks.id
  - Use OpenVPN.
  - Make sure aur.lks.id traffic to Karimata Network and Lombok Network is tunneled via VPN.
  - Use IP range 10.250.1.0/24 for site-to-site connectivity.
  - Keep the VPN connection running.
  - Use tun interface
  - Make sure the vpn can be started/stopped via systemctl <start/stop> openvpn@sitetunnel
- Configure Remote-Access VPN in buton.lks.id
  - Use OpenVPN.
  - Use a different port from Site-to-Site VPN.
  - When connected to VPN, allow clients to connect only to Malaka Network.
  - Only users in VPN OU are able to use the VPN.
  - Distribute the client configuration file to connect to the VPN to cilik.lks.id
    - Also install openvpn client in cilik.lks.id.
    - Put the file in cilik.lks.id at /etc/openvpn/client.ovpn
    - You can test the connection, but don't forget to disconnect again.
  - Make sure clients have access to both Karimata Network and Lombok Network after VPN is established.

## Malaka DNS

- Configure buton.lks.id as DNS Server for all malaka.id records.
  - You can use any service/application.
  - Add all records required for Malaka Website.
  - Add NS record to buton.lks.id
  - Add server records: buton.malaka.id, aur.malaka.id, and cilik.malaka.id with address in Malaka Network.
  - REFUSE all queries for (sub)domains other than malaka.id

## Malaka Website

- Configure aur.lks.id to serve a bunch of user websites
  - You can use any service/application.
- Add the homepage [www.malaka.id](http://www.malaka.id) with content specified in the appendix.
  - Use HTTPS with a certificate from Karimata Root Certificate
  - Serve the website in both HTTP and HTTPS.
  - Use /var/www/home to store all these website files.
- Add 10 user websites:
  - user01.malaka.id stored at /var/www/user01
  - user02.malaka.id stored at /var/www/user02
  - user03.malaka.id stored at /var/www/user03
  - ...
  - user09.malaka.id stored at /var/www/user09
  - user10.malaka.id stored at /var/www/user10
- Enable basic authentication for all 10 user websites.
  - For user01.malaka.id, use username user01 and password Skills39s
  - For user02.malaka.id, use username user02 and password Skills39s
  - For user03.malaka.id, use username user03 and password Skills39s
  - ...
  - For user09.malaka.id, use username user09 and password Skills39s
  - For user10.malaka.id, use username user10 and password Skills39s
- All user website content is the same:
  - **<html><h1>This is a user website. The content is not yet changed </h1></html>**
- Add all required DNS records in Malaka DNS.
- Make sure all user websites are accessible via HTTP plaintext.

## Firewall and IP Forwarding

- Configure buton.lks.id with iptables LOG module to log these traffics:
  - Traffic from Malaka Network to Karimata Network.
  - Incoming DNS request
    - Use log-prefix DNS
  - Incoming ICMP request
    - Use log-prefix ICMP
- Configure IP Addressing and IP Forwarding with the following conditions:
  - Lombok Network must be able to reach Karimata Network.
  - Karimata Network must be able to reach Lombok Network
  - Malaka Network must not be able to reach Lombok Network without using VPN.
  - Malaka Network must not be able to reach Karimata Network without using VPN.

# Appendix

## IP Address Design

Hostname	OS	IP Addresses
aur	Debian 11 Server	45.8.17.23/24
buton	Debian 11 Server	45.8.17.115/24
		10.196.10.1/25
cilik	Debian 11 Server	45.8.17.31/24
jukung	Windows Server 2019 Desktop	10.196.10.10/25
komodo	Windows Server 2019 Desktop	10.196.10.11/25
ligitan	Windows 10	10.196.10.80/25
muna	Debian 11 Server	10.196.10.12/25
		10.200.2.2/25
rote	Windows Server 2019 Desktop	10.200.2.13/25
sipadan	Debian 11 Client	10.200.2.XX/25 (DHCP)

## Network Detail

Malaka Network	Subnet	45.8.17.0/24
	Default Gateway	-
	DNS Servers	45.8.17.31
Lombok Network	Subnet	10.196.10.0/25
	Default Gateway	10.196.10.1
	DNS Servers	10.196.10.10
		10.196.10.11
Karimata Network	Subnet	10.200.2.0/25
	Default Gateway	10.200.2.2
	DNS Servers	10.200.2.13



## Website Content

**www.malaka.id**

```
<html><head>  
  
<title>Malaka Homepage</title>  
  
</head><body>  
  
<h1>PT Malaka</h1>  
  
<p>Copyright 2023. Hak Cipta dilindungi oleh undang-undang.</p>  
  
</body> </html>
```

## Topology

