PRA TEST PROJECT
MODUL A - CLIENT SERVER

IT NETWORK SYSTEMS ADMINISTRATION

KELOMPOK INFORMATION AND COMMUNICATION TECHNOLOGY

Dokumen ini merupakan Pra-Test Project yang menjadi subject perubahan maksimal 30% untuk Actual Test Project. Pelaksanaan kompetisi LKS Nasional nanti akan menggunakan Actual Test Project yang akan dipublikasi pada saat kompetisi. Perubahan itu meliputi Topology, Functionality, Aplikasi dan Task yang diminta.

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 password for some tasks, you can use **Skills39**

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.
- Configure all linux servers to be accessed using SSH from non-root user only.
    - Disable root login via SSH.

OS Configuration

- Please create 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 and restrict login using root in anywhere (console, SSH, etc,)
    - Make sure to configure other 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 and Karimata Shared Folder.

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 non-https request to https.
    - Put all website content in C:\webdir\www\
    - 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 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 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 certificate for services in other tasks.
    - For the record, place all generated certificates and their private keys in C:\internal\cert

Lombok DNS

- Configure jukung.lks.id and komodo.lks.id as DNS server.
    - Both needs to have identical record.
    - Both are the authoritative server of the lombok.id domain and lks.id domain.
    - Create both server record 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.
    - The record should points 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
    - Web
- Configure to forward all requests to lombok.id (sub)domains to Lombok DNS.
- Configure to forward all requests to (sub)domains other than lombok.id and karimata.id to Malaka 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 certificate from Karimata Root Certificate
    - Do not respond to HTTP requests.
- Make sure the SMTP and IMAP only respond to request 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 Skills39
- Create email alias contact@lks.id should be received by admin@lks.id

Additional Storage

- Configure muna.lks.id disk to be shared via iSCSI
    - Share two disks that is not used by RAID or the OS.
    - Make sure 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 suitable filesystem
- Share these folders to be able to read-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.

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 OU VPN to store all VPN users.
    - Create user remote with password Skills39 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 have access to both Karimata Network and Lombok Network after VPN established.
    - Use IP range 10.250.1.0/24 for site-to-site connectivity.
    - Keep the VPN connection running.
- Configure Remote-Access VPN in buton.lks.id
    - Use openvpn.
    - Allow clients to connect via Malaka Network only.
    - Only users in VPN OU are able to use the VPN.
    - Distribute client configuration file to connect to the VPN to cilik.lks.id
        - Also install openvpn client in cilik.lks.id.
        - Put the file in /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
    - Point mail.lks.id to buton.lks.id’s address in Malaka Network.
    - Do not respond to query 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 with content specified in the appendix.
    - Use HTTPS with certificate from Karimata Root Certificate
    - Serve the page in both HTTP and HTTPS.
    - Use /var/www/home to store all this 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 Skills39
  - For user02.malaka.id, use username user02 and password Skills39
  - For user03.malaka.id, use username user03 and password Skills39
  - …
  - For user09.malaka.id, use username user09 and password Skills39
  - For user10.malaka.id, use username user10 and password Skills39
- All user website content is the same:
  - **<html><h1>This is user website. The content is not yet changed </h1></html>**
- Add all required DNS record in Malaka DNS.

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.
  - Incoming ICMP request.
- Enable IP Forwarding in the required servers to 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.
  - Lombok Network must not be able to reach Malaka Network.
  - Karimata Network must not be able to reach Malaka Network.

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

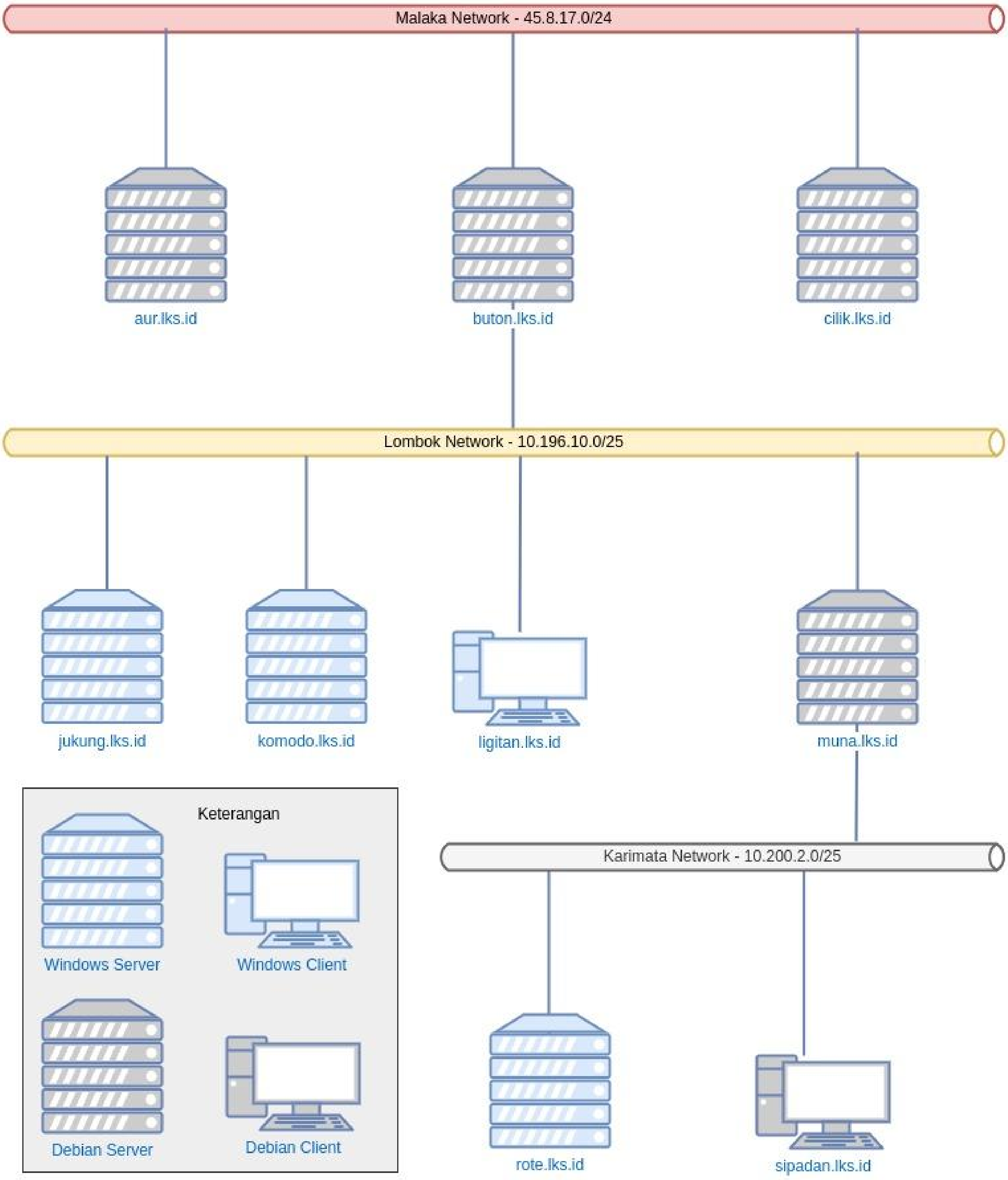
Karimata Network	Subnet	10.200.2.0/25
	Default Gateway	10.200.2.2
	DNS Servers	10.200.2.13

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



Malaka Network - 45.8.17.0/24
aur.lks.id
buton.lks.id
cilik.lks.id
Lombok Network - 10.196.10.0/25
jukung.lks.id
komodo.lks.id
ligitan.lks.id
muna.lks.id
Keterangan
Windows Server
Windows Client
Debian Server
Debian Client
Karimata Network - 10.200.2.0/25
rote.lks.id
sipadan.lks.id