

PRA TEST PROJECT

MODUL B – Client Server

IT NETWORK SYSTEMS ADMINISTRATION

LOMBA KOMPETENSI SISWA SMK TINGKAT NASIONAL 2024

*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 tersebut 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.

Instructions to the Competitor

Login credentials

Debian 12

Username : **root/user**

Password : **P@ssw0rd**

Windows Server 2022

Username : **Administrator**

Password : **P@ssw0rd**

System environments

WIB site

Region/Time zone: **Asia/Jakarta**

WITA site

Region/Time zone: **Asia/Makassar**

WIT site

Region/Time zone: **Asia/Jayapura**

Software

For testing purpose, all hosts have been installed with the following test tools: **smbclient, curl, lynx, dnsutils, ldap-utils, ftp, lftp, wget, ssh, nfs-common, rsync, telnet, traceroute, tcptraceroute**

WIB SITE

DHCP Server

FW-WIB

- Configure the DHCP service on FW-WIB by referring to the below table

Option	Value
Subnet	/24
Range	10.10.10.100 - 10.10.10.200
Domain Name Server	10.10.10.10 10.10.10.20
Domain Name	barat.id
Gateway	10.10.10.254

- Configure static DHCP IP Address for LINSRV2 10.10.10.20
- Enable Dynamic DNS (DDNS) to automatically update DNS records barat.id for clients receiving DHCP leases.

DNS Server

LINSRV1

- Set up the barat.id domain on LINSRV1 using Bind9
 - the server works as the master DNS server
 - add domain records

Type	Record	Value
NS	barat.id	ns1.barat.id
		ns2.barat.id
A	ns1	10.10.10.10
	ns2	10.10.10.20
	LINSRV1	10.10.10.10
	LINSRV2	10.10.10.20
	www	32.12.10.110
	file	10.10.10.20
	mail	10.10.10.10
MX	barat.id	10, mail.barat.id

- Configure name server forwarder so can resolve domain tengah.id
 - the target address is 32.12.10.120

LINSRV2

- Set up the barat.id domain on LINSRV2

- the server works as the slave DNS server from LINSRV1

Certificate Authority

LINSRV2

- Set up root certificate authority on LINSRV2 using OpenSSL on directory /root/ca.
- Create Root Certificate cacert.pem and cacert.key with attributes should be set as follows.
 - Country Code: ID
 - Organization: ITNSA
 - Common Name: LKSN 2024 CA
- Create additional certificate

Issued Certificate	Note
CN=WIB	OpenVPN Server
CN=WITA	OpenVPN Client
CN=BUDI	OpenVPN Client
CN = mail.barat.id	Mail Server
CN = www.barat.id	Web
CN = file.barat.id	Web
CN = www.tengah.id	Web

RAID

LINSRV2

- Add two disk with size 5gb
- Configure raid 1 and mount on directory /data

WEB Server

LINSRV1

- Configure web server on LINSRV1 using apache2
 - Create a virtual host HTTP only for serving www.barat.id
 - The website page should display “Hello World from barat”
 - Add the HTTP header “X-Served-By” with the server hostname as the value

LINSRV2

- Configure web server on LINSRV2 using nginx
 - Create a virtual host HTTP only for serving www.barat.id
 - The website page should display “Hello World from barat”
 - Add the HTTP header “X-Served-By” with the server hostname as the value
 - Create a virtual host on LINSRV2 for serving file.barat.id
 - Enable HTTPS using the Certificate Authority from LKSN 2024 CA

- Redirect all HTTP requests to HTTPS.
- This virtual host is set as a file server for directory /data/file/
- Add basic authentication using username rahasia with password Skills39
- Make sure LINCLT can access without any warning

SSH

LINSRV2

- Install and configure the SSH Server on LINSRV2
 - Create a user file with the password Skills39 and set the home directory to /data/file/
 - Make sure to configure the file user not to be able to use sudo and become root
- Configure the user "user" in LNXCLT SSH to file@linsrv2.barat.id without a password and use key-based SSH authentication
- Change SSH port default to 2024

MAIL Server

LINSRV1

- Install and configure Postfix and Dovecot on LINSRV1
 - Use the domain barat.id so that email can be sent to user@barat.id email address.
 - Enable SMTP with negotiable TLS on port 25
 - Enable IMAP with negotiable TLS on port 143
 - Use certificates from LKSN 2024 CA
- Enable web-based email using Roundcube
 - Make it accessible using the domain mail.barat.id.
 - Enable HTTPS access using a certificate LKSN 2024 CA
 - Make sure LINCLT can access the web-based email Roundcube
- Create two mail users: admin@barat.id and user@barat.id with password Skills39s
 - Send a test mail from user@barat.id to admin@barat.id.
- Create email alias contact@barat.id should be received by admin@barat.id
 - Send a test mail from user@barat.id to contact@barat.id

VPN

FW-WIB

- This device works as OpenVPN server.
- Configure site to site VPN to communicate between WIB Site and WITA Site.
 - port 1195
 - use certificate for authentication
 - VPN subnet : 10.255.255.0/28
 - use tun interface
- Configure remote-access vpn for WIT site
 - port 1194
 - use authentication user budi with password Skills39
 - VPN subnet : 10.100.100.0/25
 - use tun interface

Firewall

FW-WIB

- Make sure that the firewall operates in stateful mode.
- Configure DNAT for DNS using external IP.
- Configure WIB site can ping to public networks.

Active Directory Server

WINSRV1

- Configure this server as the initial domain controller (new forest) for tengah.id
- Add users and groups belongs to

User	Password	Group
drs1-3	Skills39	Direksi
mng1-10	Skills39	Manager
kyw1-100	Skills39	Karyawan

- Configure all users in the domain must have a home folder under the C:\Homes directory.
- the users home directory can only be accessed by the user and is set to have a quota of 100MB.
- Configure group policy for prevents the Welcome animation from appearing on first login in all clients in tengah.id domain

WINSRV2

- Configure an addition domain controller for tengah.id

DNS Server

WINSRV1

- Configure DNS for tengah.id
- Create a reverse Zone for the 172.31.16.0/24 network
- Add domain records.

Type	Record	Value
NS	tengah.id	ns1.tengah.id ns2.tengah.id
A	ns1	172.31.16.10
	ns2	172.31.16.20
	www	32.12.10.120
	manager	172.31.16.10

- Configure name server forwarder so we can resolve domain barat.id
 - The target address is "32.12.10.110"

WEB Server

WINSRV1

- Install IIS web service
- Create web for host www.tengah.id
 - Path C:\inetpub\wwwroot
 - The website page should display “Hello World from tengah”
- Create internal web with host manager.tengah.id
 - Path C:\inetpub\manager
 - The website page should display “Hello Managers !”
 - Enable basic authentication and allow user from group Manager only

FW-WIB

- Configure HTTP/HTTPS reverse proxy for www.tengah.id, hosted by WINSRV1
 - User certificate from LKSN 2024 CA
 - Make sure WINCLT can access without any warning

iSCSI

WINSRV2

- add disk 10gb on WINSRV2
- create virtual disk iSCSI with size 5gb
- Create an iSCSI target on the virtual disk
 - Name the iSCSI target ‘BACKUP-TG’
 - Configure the iSCSI target BACKUP-TG to allow access only from WINSRV1

Windows Backup

WINSRV1

- Create a backup job to backup folder C:\inetpub\wwwroot to folder C:\backup at 4 PM daily.

DFS Replication

WINSRV1 & WINSRV2

- configure folders synchronized
 - C:\Homes at WINSRV1
 - G:\Homes at WINSRV2

WINSRV1

- Set up the iSCSI initiator to connect to the iSCSI target BACKUP-TG on WINSRV2
- Mount the iSCSI target as disk H: on WINSRV1
- format the disk with the NTFS file system and name it backup

OpenVPN

FW-WITA

- This device works as OpenVPN Client.
- Configure Site to Site VPN to communicate between WITA site and WIB site.
 - same configuration policies as the server.

Firewall

FW-WITA

- Make sure that the firewall operates in stateful mode.
- Configure DNAT for DNS using external IP.
- Configure WITA site can ping to public networks.

WIT SITE

Firewall

FW-WITA

- Make sure that the firewall operates in stateful mode.
- Configure DNAT for DNS using external IP.
- Configure WITA site can ping to public networks.

BUDI-CLT

- configure OpenVPN remote access client
- make sure ssh to LINSRV1 success with user rahasia

Appendix

Device	OS	IP Address
LINSRV1	Debian 12.x	10.10.10.10/24
LINSRV2	Debian 12.x	10.10.10.20/24 (DHCP)
FW-WIB	Debian 12.x	10.10.10.254/24 32.12.10.110/23
LINCLT	Debian 12.x GUI	10.10.10.200/24
WINSRV1	Windows Server 2022	172.31.16.10/24
WINSRV2	Windows Server 2022 Core	172.31.16.20/24
FW-WITA	Debian 12.x	172.31.16.254/24 32.12.10.120/23
WINCLT	Windows 11	172.31.16.200/24
FW-WIT	Debian 12.x	192.168.101.254/24 32.12.10.130/23
BUDI-CLT	Debian 12.x GUI	192.168.101.200/24

Topology

