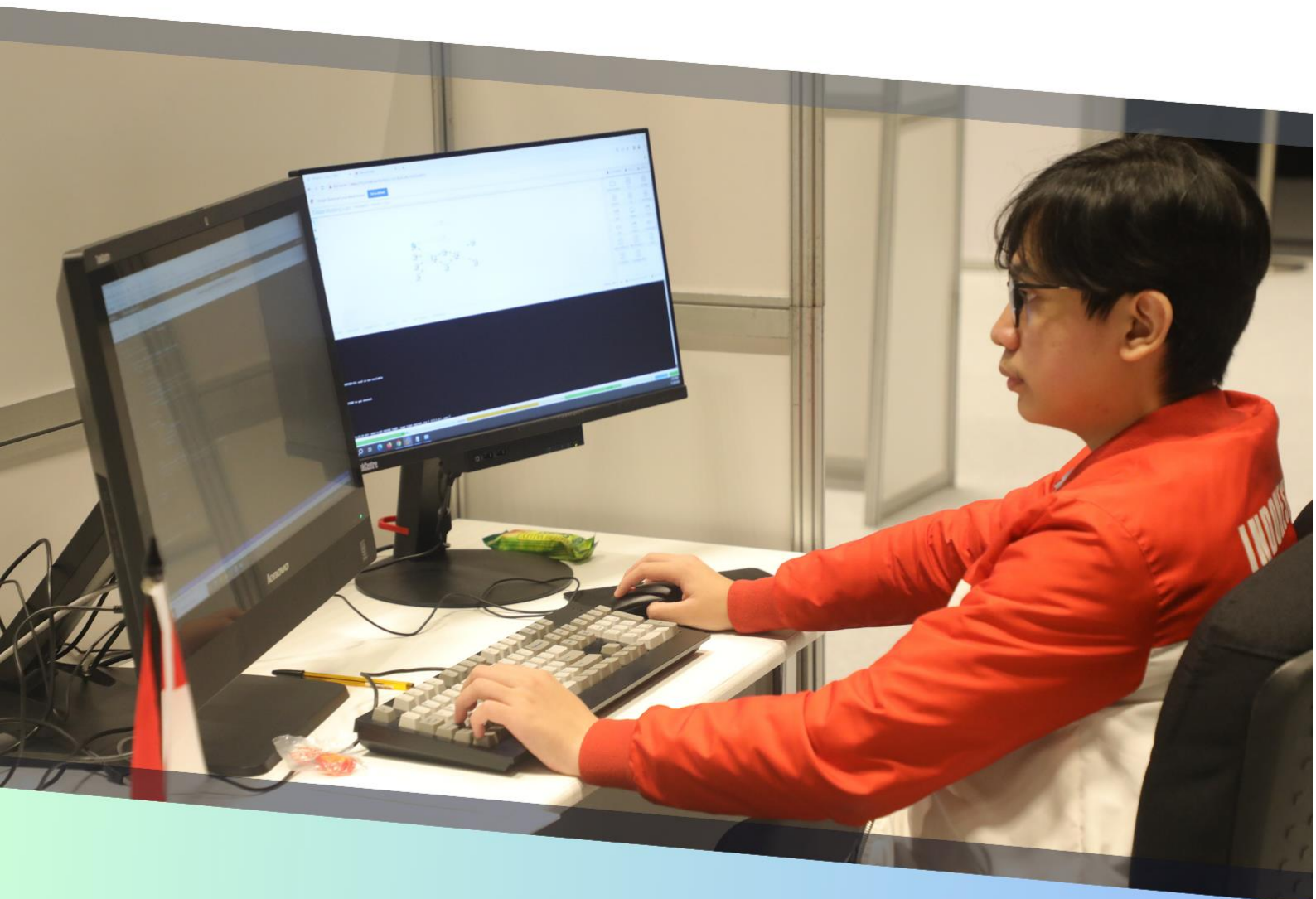




**TAHUN
2024**

TEST PROJECT SELEKDA CALON KOMPETITOR THE 14th WORLDSKILLS ASEAN IT NETWORK SYSTEMS ADMINISTRATION



**KEMENTERIAN KETENAGAKERJAAN R.I.
DIREKTORAT JENDERAL PEMBINAAN
PELATIHAN VOKASI DAN PRODUKTIVITAS
DIREKTORAT BINA STANDARDISASI KOMPETENSI DAN
PROGRAM PELATIHAN**

Gedung Vokasi, Jl. Jend Gatot Subroto Kav. 44
Jakarta Selatan 12710

<https://inaskills.kemnaker.go.id>

ACTUAL TEST PROJECT
MODUL A – CLIENT SERVER
ENVIRONMENT
(LINUX)

IT NETWORK SYSTEMS ADMINISTRATION

SELEKSI DAERAH
CALON COMPETITOR WORLD SKILLS ASEAN 2024

Introduction

Please carefully read the following instructions! Use the default value or adjust accordingly when no specific value is given. All configurations **must work & persist even after reboot**. Use the password **P@ssw0rd** as the default password if nothing is specified. Use the information below for login credentials into the servers

Username : root / competitor

Password : P@ssw0rd

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

SSH services with root login already pre configured on all hosts. **Do NOT turn off the SSH service!**

If you did not complete the CA task for services that need a certificate, you can use a self-signed certificate

Consider **case sensitive** for certificate subject, hostname, LDAP object and website content!

Basic Configuration

Configure basic configuration below on all servers :

- Configure hostname and IP address refer to the appendix
- Set domain name to **itnsa.id**
- Set time zone to **Asia/Jakarta**
- Set nameserver to IP address of WSSRV-LN and ESSRV-LN

Forwarding

- Enable packet forwarding on RO-LN (IPv4 only)
- Make sure it persists across reboot

HAProxy

Install and configure HAProxy on RO-LN to load balance HTTPS traffic to east and west server

- Configure HTTPS binding for **www.itnsa.id**. Use certificate signed by RootCA
- Use HTTPS with SSL verification for backend connection to east and west server
- Use round robin as the load balancing algorithm

DHCP Service

Install and configure DHCP service on RO-LN using isc-dhcp-server

- Configure DHCP scope for 172.1.100.0/28 network.
- Address lease should start from 172.1.100.2 – 172.1.100.9
- IP address 172.1.100.10 must always be leased to ESSRV-LN
- Set default gateway to IP address of RO-LN
- Set DNS server to IP address of WSSRV-LN and ESSRV-LN

Certificate Authority

Configure root certificate authority on WSSRV-LN

- Use directory **/etc/ssl/RootCA** and save the root certificate as **/etc/ssl/RootCA/RootCA.crt**
- Set subject name of root certificate to **"C=ID, O=ITNSA.ID, CN=RootCA"**
- Root certificate must be valid for 10 years
- Distribute and trust root certificate on all servers
- Create a shell script **/usr/local/bin/generate_cert.sh** to generate certificate signed by RootCA with it's private key
 - When this script is executed, it will receive an argument subject name of generated certificate. For example, certificate with subject **test.itnsa.id** can be generated by execute:
`/usr/local/bin/generate_cert.sh test.itnsa.id`
 - Certificate and private key should be saved with certificate subject name as the filename followed by **.crt** and **.key** extension. For example, certificate **test.itnsa.id** generated by script will be saved as :
 - **/etc/ssl/RootCA/issued/test.itnsa.id.crt** for the certificate file
 - **/etc/ssl/RootCA/issued/test.itnsa.id.key** for the private key file
 - If certificate subject already exists, display this message:
Certificate with subject <SUBJECT_NAME> already exists!

DNS Service

Install and configure DNS services on WSSRV-LN and ESSRV-LN using Bind9. All domain zone must be created inside `/etc/bind` directory

- Configure **itnsa.id** domain zone and create domain record below:

Type	Record	Value
NS	@	WSSRV-LN.itnsa.id.
NS	@	ESSRV-LN.itnsa.id.
A	WSSRV-LN	10.200.50.1
A	ESSRV-LN	172.1.100.10
A	www	172.1.100.1 10.200.50.2
CNAME	east.itnsa.id.	ESSRV-LN.itnsa.id.
CNAME	west.itnsa.id.	WSSRV-LN.itnsa.id.
A	mail	10.200.50.1
MX	@	39, mail.itnsa.id.

- Configure reverse zone for **10.200.50.0/30** network and create domain record below:

Type	Record	Value
NS	@	WSSRV-LN.itnsa.id.
NS	@	ESSRV-LN.itnsa.id.
PTR	WSSRV-LN.itnsa.id.	10.200.50.1
PTR	RO-LN.itnsa.id.	10.200.50.2

- Configure reverse zone for **172.1.100.0/28** network and create domain record below:

Type	Record	Value
NS	@	WSSRV-LN.itnsa.id.
NS	@	ESSRV-LN.itnsa.id.
PTR	ESSRV-LN.itnsa.id.	172.1.100.10
PTR	RO-LN.itnsa.id.	172.1.100.1

- Ensure WSSRV-LN is configured as the primary name server and ESSRV-LN as the secondary name server for the corresponding forward and reverse domain zone
- WSSRV-LN should always notify ESSRV-LN if there is any domain record update
- On WSSRV-LN, only permit ESSRV-LN to perform zone transfer

Web Service

Install and configure web service on WSSRV-LN and ESSRV-LN using any package of your choice

- Create “**www.itnsa.id**” virtual host on both WSSRV-LN and ESSRV-LN server
 - This virtual host must listen on port 80 and 443
 - Redirect any HTTP request to HTTPS
 - Use certificate signed by Root Certificate Authority
 - Set website content to **Welcome to www.itnsa.id**
- Create “**east.itnsa.id**” virtual host on ESSRV-LN
 - This virtual host must listen on port 80
 - Set website content to **East region of itnsa.id**
- Create “**west.itnsa.id**” virtual host on WSSRV-LN
 - This virtual host must listen on port 80
 - Set website content to **West region of itnsa.id**
- Every HTTP response must return HTTP header called **server_name** with value hostname of the corresponding web server

LDAP Service

Install and configure LDAP service on ESSRV-LN for centralized authentication

- Use **itnsa.id** as the domain name for LDAP service
- Create **HQ** and **Branch** organizational unit
- Create LDAP user object below:

Distinguished Name	Username (UID)	Password
uid=jack,ou=Branch,dc=itnsa,dc=id	jack	Skill39
uid=jane,ou=HQ,dc=itnsa,dc=id	jane	P@ssw0rd
uid=john,ou=HQ,dc=itnsa,dc=id	john	P@ssw0rd

- Create shell script **/usr/local/bin/add_ldap_user.sh** to create LDAP user object
 - When this script is executed, it will receive an argument organizational unit name followed by LDAP username. For example, creating **testuser** inside **HQ** organizational unit can be done by execute :
/usr/local/bin/add_ldap_user.sh HQ testuser
 - If user created in **HQ** organizational unit, set user password to **P@ssw0rd**
 - If user created in **Branch** organizational unit, set user password to **Skill39**
 - In case the shell script receive invalid organizational unit name, display this message:
Invalid organizational unit!
 - If user already exists, display this message :
User <USERNAME> already exists!
- Create shell script **/usr/local/bin/delete_ldap_user.sh** to delete LDAP user object
 - When this script is executed, it will receive an argument LDAP username. For example:
/usr/local/bin/delete_ldap_user.sh testuser
 - If LDAP user object has been successfully deleted, display this message:
User <USERNAME> has been deleted!
 - If corresponding LDAP user doesn't exists, display this message :
User <USERNAME> doesn't exists on LDAP database!

File Service

Install and configure Samba service on ESSRV-LN

- Create user **jane** and **john** on Samba database for authentication. Use password **P@ssw0rd**
- Create Samba shared folder called **public**
 - Use **/smb/public** for **public** shared folder
 - Permit everyone to access this shared folder (read only)
 - Authenticated user can upload file to this shared folder
- Create Samba shared folder called **private**
 - Use **/smb/private** for **private** shared folder
 - Only authenticated user can access this shared folder
- Create shell script **/usr/local/bin/sync_user.sh** to synchronize user between LDAP database and Samba database
 - Only synchronize LDAP user inside **HQ** organizational unit
 - When LDAP user has been deleted from LDAP database, the corresponding user must also be deleted on Samba database
 - Use default password **P@ssw0rd** for created user inside Samba database
 - This script must be executed every minute using cron as root user (Use **crontab -e**)

Mail Service

Install and configure mail service for **itnsa.id** on WSSRV-LN using Postfix and Dovecot

- Client should use Submission and IMAP port for accessing the mail service. Secure it using certificate signed by RootCA
- For easy management, use **Maildir** as the mail directory and mailbox format
- Only LDAP user can use this mail service. It must be authenticated through PAM
- Make sure user can login using username appended with **@itnsa.id** domain

Appendix

Addressing Table

Hostname	IP Address	Services
WSSRV-LN	10.200.50.1/30	DNS, Web, Certificate Authority, Mail Service
RO-LN	10.200.50.2/30 172.1.100.1/28	DHCP, HAProxy
ESSRV-LN	172.1.100.10/28	DNS, Web, LDAP, File Service

Topology Diagram

