



Proyek Uji Lomba Kompetensi Siswa Nasional 2026

SMA/MA/SMK/MAK/Sederajat



Cabang Ajang

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

ACTUAL TEST PROJECT
MODUL C - WINDOWS ENVIRONMENT

IT NETWORK SYSTEMS ADMINISTRATION

**LOMBA KOMPETENSI SISWA DIKMEN
TINGKAT NASIONAL 2026**

Introduction

You are working as a system administrator for **itnsa.id**. This organization use Microsoft technologies to provide centralized management, file services, and web services. At the same time, Ansible is utilized to automate system configuration, deployment, and routine administrative tasks.

The infrastructure consists of two distinct sites operating across separate time zones. You are required to manage both environments and ensure that **cross-site communication** is established and maintained without interruption.

On every host, there is one network adapter called **Management**. This network adapter will be used for assessment or marking. **DO NOT CHANGE OR MODIFY IT!**

On each server there is an agent for marking that runs on port **8080**. **DO NOT DISABLE OR MODIFY IT!**

There is a **wita-router** that simulates internet router. It's already preconfigured with IP address, hostname and routing. **DO NOT DISABLE OR MODIFY IT!**

Consider **case-sensitive** for website configuration (site name, domain name, index content)

Credential Information

Windows

Username: User / Administrator

Password: Skill39@2026

Timezone: (UTC+07:00) Jakarta

Linux

Username: root / sysop

Password: Skill39@2026

Description of project and tasks

Basic Configuration

Configure **hostname**, **FQDN** and **IP address** on all hosts refer to the information table and set the timezone to **(UTC+07:00) Bangkok, Hanoi, Jakarta**.

Active Directory

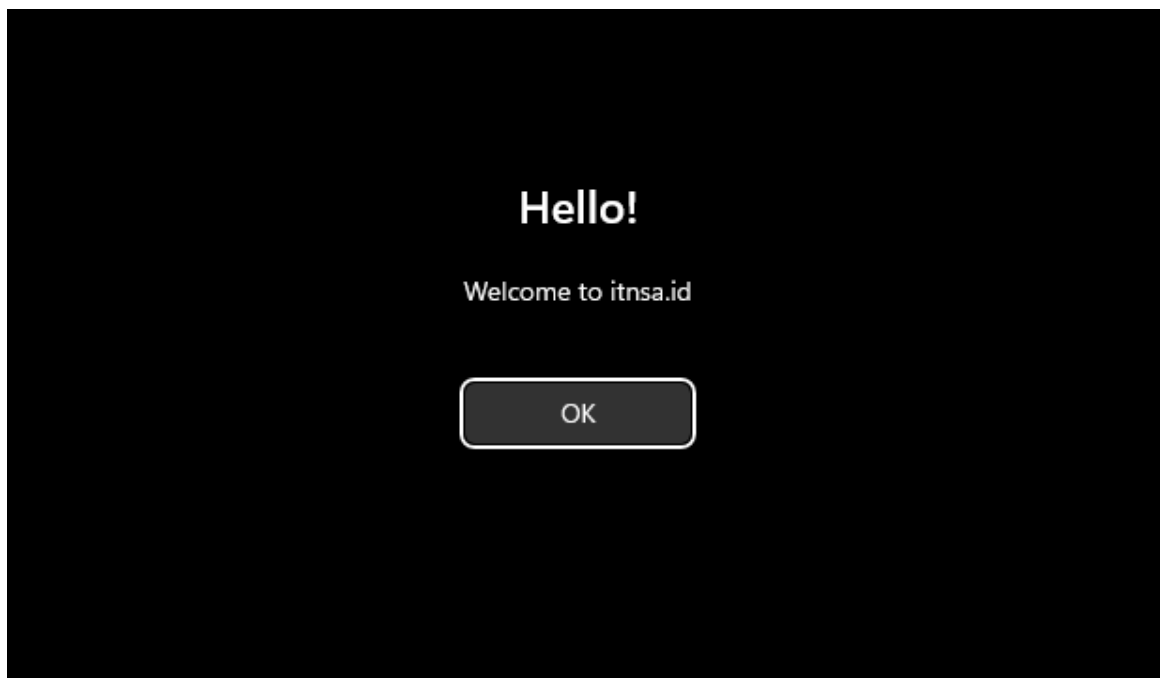
dc1

1. Configure this server as the initial domain controller for a new forest named **itnsa.id**.
2. Configure Active Directory Sites and Services:
 - a) Create a new site named **West-ITNSA**
 - b) Create and associate the following IP subnets with the **West-ITNSA** site:
 - **172.31.1.0/24**
 - **192.168.1.0/24**
 - **192.168.2.0/24**
 - c) Only **dc1** server assigned to the **West-ITNSA** site
3. Create the following Organizational Units (OU) inside the **itnsa.id** domain:
 - a) **Employees**
 - b) **ITs**
 - c) **Finances**
 - d) **Managers**
4. Inside each newly created OU, create a security group with the same name as its corresponding OU (e.g., create a group named **Employees** inside the **Employees** OU).
5. Create Active Directory user accounts according to the table below. Use **PowerShell script** to create all user accounts. Use password **Skill39@2026** and make sure users do not need to change their password at the next logon.

Username Format	Total Accounts	Target OU
employee001 - employee100	100	Employees

it01 - it30	30	ITs
finance01 - finance15	15	Finances
manager01 - manager05	5	Managers

6. Configure group membership for all created users. Each user must be a member of the security group that corresponds with their OU (e.g., all users in the **Employees** OU must be members of the **Employees** group).
7. For users in the **Finances** and **Managers** groups, configure their home folder to be **\\itnsa.id\\Drive\\Home\\%username%**, mapped to the **H:** drive letter.
8. Join **dc1**, **file-srv** and **wib-router** as the domain members of **itnsa.id** through this **dc1**.
9. Configure group policy called **ITNSA_GPO**. This policy must be applied only to the **winc1t** with specification below:
 - Disable the first sign-in animation for users logging onto the workstation.
 - Set the login banner title into **Hello!**
 - Set the login banner text into **Welcome to itnsa.id**



dc2

1. Promote this server as the second domain controller of **itnsa.id**.
2. Configure Active Directory Sites and Services:
 - a) Create new site called **East-ITNSA**
 - b) Create and associate the IP subnet **192.168.100.0/24** with the **East-ITNSA** site
 - c) Only **dc2** server assigned to the **East-ITNSA** site
3. After **dc2** promoted as the secondary domain controller, join the **wit-router** into **itnsa.id** through this domain controller.
4. Configure **dc2** as a primary server for managing RID pools on **itnsa.id** domain.

Certificate Authority

dc1

1. Install and configure **Active Directory Certificate Services** to create Root CA certificates
2. Configure the **Root Certificate Authority (Root CA)** with the following specifications:
 - CA Type: **Enterprise Root CA**
 - Set CA common name to **ITNSA-ROOT-CA**
 - Validity period: **15 years**
3. Ensure the root certificate from this new CA is installed and trusted on **all hosts**. All service certificates (like **HTTPS**) must be issued by this CA. You can also use **wildcard certificates**.

DNS Service

dc1

1. Create the following Forward DNS records in the **itnsa.id** zone:

Type	Record Name	Value / Target
A	dc1	172.31.1.1
A	dc2	192.168.100.1
A	west	172.31.1.1
A	east	192.168.100.1
A	file-srv	192.168.1.10
A	wib-router	172.31.1.254
A	wit-router	192.168.100.254
CNAME	drive	file-srv.itnsa.id
CNAME	file	file-srv.itnsa.id
CNAME	www	file-srv.itnsa.id
CNAME	internal	file-srv.itnsa.id

2. Create the following Static Reverse DNS (PTR) records:

Record Name	IP Address
dc1.itnsa.id	172.31.1.1
dc2.itnsa.id	192.168.100.1
file-srv.itnsa.id	192.168.1.10
wib-router.itnsa.id	172.31.1.254
wit-router.itnsa.id	192.168.100.254

3. Make sure the **wincft** IP address is automatically created on the reverse DNS zone.

dc2

1. Make sure **itnsa.id** zone from **dc1** is replicated to this domain controller
2. Create **east-itnsa.id** primary zone on this server with record specified on the table below. This zone must not be replicated to the **dc1**

Type	Record Name	Value / Target
A	core	192.168.100.1
A	fw	192.168.100.254
CNAME	www	core.east-itnsa.id
CNAME	mgmt	core.east-itnsa.id

DHCP Service

wib-router

1. Install and configure DHCP services on this server. Create a new DHCP scope with the following specifications:

Scope Name	itnsa-id
Range	192.168.2.10 - 192.168.2.240
Subnet Mask	255.255.255.0
Excluded Address Range	192.168.2.110 - 192.168.2.120
DNS Servers	172.31.1.1, 192.168.100.1
Domain Name	itnsa.id
Gateway	192.168.2.254
Lease Time	1 day, 30 minutes

2. Configure the DHCP server to always perform dynamic DNS updates for clients.
3. Authorize this server in Active Directory as an authoritative DHCP server for the **itnsa.id** domain.

IIS Web Service

file-srv

1. Install and configure the **Internet Information Services (IIS)** web server role on this server.
2. All websites created on this server must be secured using a certificate issued by the **Root Certificate Authority**. Enable HTTP to HTTPS redirection.
3. Create and configure websites according to the specifications in the table below:

Website Name	Path	Content
internal.itnsa.id	C:\www\internal	Internal site of itnsa.id
www.itnsa.id	C:\www\public	Welcome to itnsa.id

4. Only client from 192.168.1.0/24, 192.168.2.0/24 and 172.31.1.0/24 can access **internal.itnsa.id**

dc2

1. Install and configure the **Internet Information Services (IIS)** web server role on this server.
2. All websites created on this server must be secured using a certificate issued by the **Certificate Authority**. Enable HTTP to HTTPS redirection.
3. Create website with specification refer to the list below:
 - **Website name:** www.east-itnsa.id
 - **Path:** C:\public\www
 - **Content:** <h1>Welcome to east-itnsa.id</h1>

Shared Folder

file-srv

1. Create a new root directory for all shared folders at the following path: **C:\Shares**
2. Create two shared folders refer to the list below:
 - Shared folder named **Home** pointing to the **C:\Shares\Home** directory. This share will be used for users' personal home folders mounted as home drives.
 - Shared folder named **Group** pointing to the **C:\Shares\Group** directory. This share will be used for group-specific data.
3. On **Group** shared folder, create folder with NTFS permission refer to the list below:
 - The **Employees** folder must grant **Full Control** to the **Employees** and **Managers** groups.
 - The **ITs** folder must grant **Full Control** to both **ITs** and **Managers** groups.
 - The **Finances** folder must grant **Full Control** to the **Finances** and **Managers** groups.
 - The **Managers** folder is restricted so only the **Managers** group has **Full Control**.

File Server Resource Manager

file-srv

1. Configure Quota Management to enforce storage limits:
 - Apply a **100MB** hard limit to **each user's personal folder** inside the **Home** shared folder.
 - Apply a **250MB** hard limit quota directly to **each group folder** inside the **Group** shared folder.
2. Configure File Screening to control file types:
 - On the **Home** folder, apply a file screen to **block executable** files from being saved.
 - On the **Group** folder, apply a file screen that only permits files with the **.txt**, **.doc** and **.xlsx** extensions to be saved.

Distributed File System

file-srv

1. Configure a new domain-based DFS Namespace with name **Drive**
2. Create the following folders within the **Drive** namespace with their respective targets:
 - **\\itnsa.id\Drive\Home** targeting **\\file-srv.itnsa.id\Home**
 - **\\itnsa.id\Drive\Group** targeting **\\file-srv.itnsa.id\Group**
3. After the DFS folder is configured, make sure all assigned permissions on the shared folder are properly inherited.

Routing and Remote Access

wib-router & wit-router

1. **Routing and Remote Access** already installed on both servers with routing enabled.
2. Configure **Network Address Translation (NAT)** to allow clients from their respective internal networks to communicate with the internet.

Site-to-Site VPN Configuration

Configure site-to-site VPN tunnel between **wib-router** and **wit-router**. The connection must use the following parameters on both servers:

- **VPN Protocol:** IKEv2
- **Authentication:** Pre-Shared Key (PSK)
- **Pre-Shared Key:** Skill39@VPN
- Set it as **Persistent Connection**

Note: If you are unable to configure the Site-to-Site VPN using **IKEv2**, you may use any alternative protocol; however, you will not receive points for this task.

Client Configuration

winclt

1. Ensure this client is joined to the **itnsa.id** domain to test deployed services.
2. Install Root CA certificates on this machine to prevent **HTTPS SSL errors**.

Ansible Automation

ansible-srv

The **ansible-srv** host is pre-configured with the necessary inventory and credentials to connect to the Windows servers in the **itnsa.id** domain. You can check it in the **/opt/ansible** directory. **Zealdocs** and **Visual Studio** already preinstalled on this machine.

Your task is to create and execute Ansible playbooks to automate the following administrative tasks. All playbooks should be created in the **/opt/ansible/playbooks/** directory with **.yml** format.

1. Checking Playbook

As an introduction, create a playbook named **01-check.yml**. This playbook must perform the following actions on all Windows hosts defined in the inventory file:

- Ensure the directory **C:\Testing** exists
- Create a file **C:\Testing\ansible_ready.txt**

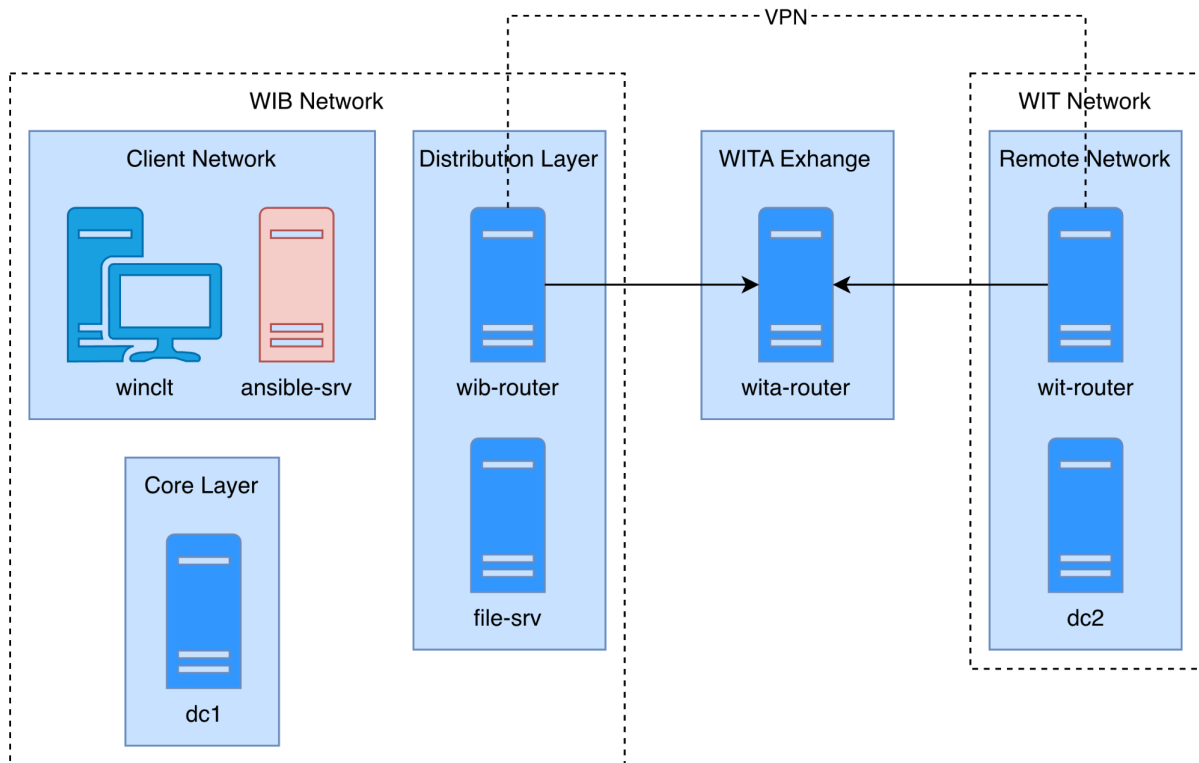
2. Active Directory Object Playbook

Create a playbook called **02-imports.yml** to create Organizational Units, Security Groups, and Users on **itnsa.id** domain. This playbook targets **dc1**:

- This playbook will read user data from a variable file located at **/opt/ansible/users.yml**
- The playbook must perform the following steps in order:
 - Create each Organizational Unit defined in the variable file under the **DC=itnsa,DC=id** path.
 - Create each Security Group with global scope and security category, placed inside its corresponding **OU**.
 - Create each AD User account with the specified **username** and **password**, placed inside its corresponding **OU**. Ensure the user does not need to change password at the next logon.
 - Add each user as a member of the security group corresponding to their OU.

Appendix

Topology



Addressing Table

Hostname	FQDN	IP Address
dc1	dc1.itnsa.id	Management: 10.10.11.1/24 Ethernet0: 172.31.1.1/24
file-srv	file-srv.itnsa.id	Management: 10.10.11.2/24 Ethernet0: 192.168.1.10/24
wib-router	wib-router.itnsa.id	Management: 10.10.11.3/24 Ethernet0: 15.66.12.1/30 Ethernet1: 172.31.1.254/24 Ethernet2: 192.168.1.254/24 Ethernet3: 192.168.2.254/24

wita-router	wita-router	<i>*Preconfigured</i> Ethernet-0: 15.66.12.2/30 Ethernet-1: 34.77.41.1/30
wit-router	wit-router.itnsa.id	Management: 10.10.11.4/24 Ethernet0: 34.77.41.2/30 Ethernet1: 192.168.100.254/24
dc2	dc2.itnsa.id	Management: 10.10.11.5/24 Ethernet0: 192.168.100.1/24
winclt	winclt.itnsa.id	Management: 10.10.11.6/24 Ethernet0: DHCP
ansible-srv	ansible-srv	Management: 10.10.11.7/24 ens256: 192.168.2.222/24