Balai Pengembangan Talenta Indonesia
Kementerian Pendidikan Dasar dan Menengah

KEMENDIKDASMEN RAMAH #PENDIDIKAN BERMUTU UNTUK SEMUA

LKS DIKMEN
TINGKAT NASIONAL

TEST PROJECT

LOMBA KOMPETENSI SISWA DIKMEN 2025

SMK/SMA/MAK/MA

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 2025

Introduction

You have been appointed as the system administrator for **itnsa.id** and **lab.itnsa.id**. In this organization, Microsoft technologies are primarily used 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.

Your role is to ensure all services are properly configured, integrated, and operational within the given time constraints. Attention to detail and time management are critical to your success in this assignment.

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!**

There is also a pre-installed Root CA Certificate on all hosts called **ITNSA-CA** and it is used for services like IIS. **DO NOT REMOVE IT!**

For tasks related to Ansible, you can use pre-installed **Visual Studio Code** and **Zealdocs** on **ansible-srv**

All configuration on Windows Server and Client **MUST BE PERSISTS AFTER REBOOT!**

Credential Information

Windows

Username: User / Administrator
Password: Skill39@2025

Linux

Username: root / user
Password: Skill39@2025

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**. Also configure appropriate DNS servers on each host.

Active Directory

CORE.itnsa.id

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 **ITNSA-ID**.
   b) Create and associate the following IP subnets with the **ITNSA-ID** site:
      - **192.168.1.0/24**
      - **192.168.2.0/24**

   c) Only **CORE** server assigned to the **ITNSA-ID** site.

3. Create the following Organizational Units (OU) inside the itnsa.id domain:
   a) **Employee**
   b) **Finance**
   c) **Engineer**
   d) **Manager**

4. Inside each newly created OU, create a security group with the same name as its corresponding OU (e.g., create a group named **Finance** inside the **Finance** OU).

5. Create Active Directory user accounts according to the table below. Use **PowerShell script** to create all user accounts. Use password **Skill39@2025** and make sure users do not need to change their password at the next logon.

Username Format	Total Accounts	Target OU
employee-001 - employee-514	**514**	**Employee**
engineer-001 - engineer-182	**182**	**Engineer**
finance-001 - finance-056	**56**	**Finance**
manager-001 - manager-015	**15**	**Manager**

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 **Finance** OU must be members of the **Finance** group).

7. For users in the **Finance** and **Manager** groups, configure their home folder to be **\\itnsa.id\CSDrive\Home\%username%**, mapped into the **H:** drive letter.

8. Configure **SRV.itnsa.id**, **FW.itnsa.id** and **WORKSTATION.itnsa.id** as the domain members of **itnsa.id**

9. Configure group policy called **ITNSA GPO**. This policy must be applied only to the **WORKSTATION** with specification below:
   - Disable the first sign-in animation for users logging onto the workstation.
   - For any user logging into the workstation, automatically map the network path **\\itnsa.id\CSDrive\Group** to drive letter **G:**

DC.lab.itnsa.id

1. Promote this server as a new domain controller for a new child domain named **lab.itnsa.id** in the existing **itnsa.id** forest.

2. Configure Active Directory Sites and Services:
   a) Create a new site named **LAB-ITNSA-ID**
   b) Create and associate the IP subnet **10.1.1.0/24** with the **LAB-ITNSA-ID** site.
   c) Only **DC** server assigned to the **LAB-ITNSA-ID** site.

3. Inside the **lab.itnsa.id** domain, create the following Organizational Units (OU):
   a) **Operator**
   b) **Member**

4. Inside each created OU, create a security group with the same name as its corresponding OU.

5. Create Active Directory user accounts according to the table below. Use password **Skill39@2025** and make sure users do not need to change their password at the next logon.

Username Format	Total Accounts	Target OU
operator01 - operator02	**2**	**Operator**
member01 - member03	**3**	**Member**

6. Configure group membership for all created users. Each user must be a member of the security group corresponding to their OU.
7. Join **EDGE.lab.itnsa.id** into **lab.itnsa.id** domain.

DNS Service

CORE.itnsa.id

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

Type	Record Name	Value / Target
A	**CORE**	**192.168.1.1**
A	**SRV**	**192.168.1.100**
A	**FW**	**192.168.1.254**
A	**CLIENT-GW**	**192.168.2.254**
CNAME	**CSDRIVE**	**SRV.itnsa.id**
CNAME	**FILE**	**SRV.itnsa.id**
CNAME	**www**	**SRV.itnsa.id**
CNAME	**internal**	**SRV.itnsa.id**

CNAME	**extra**	**SRV.itnsa.id**
CNAME	**DC**	**CORE.itnsa.id**

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

Record Name	IP Address
CORE.itnsa.id	**192.168.1.1**
SRV.itnsa.id	**192.168.1.100**
FW.itnsa.id	**192.168.1.254**
CLIENT-GW.itnsa.id	**192.168.2.254**

3. Make sure **WORKSTATION** IP address automatically created on reverse DNS zone.

DC.lab.itnsa.id

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

Type	Record Name	Value / Target
A	**DC**	**10.1.1.10**
A	**EDGE**	**10.1.1.1**

2. Configure a DNS forwarder pointing to the IP address of **CORE.itnsa.id**.

DHCP Service

FW.itnsa.id

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

Scope Name	**itnsa.id_Client**
Range	**192.168.2.10 - 192.168.2.200**
Subnet Mask	**255.255.255.0**
Excluded Address Range	**192.168.2.110 - 192.168.2.120**
DNS Servers	**192.168.1.1, 10.1.1.10**
Domain Name	**itnsa.id**
Gateway	**192.168.1.254**
Lease Time	**1 day, 39 minutes, 39 seconds**

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

SRV.itnsa.id

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 pre-installed certificate with appropriate subject name for **HTTPS** connections.
3. Use the provided website content files located in the **"Content"** directory on the desktop for the corresponding websites.
4. Create and configure websites according to the specifications in the table below:

Website Name (Binding)	Path	Default Index File
internal.itnsa.id	**C:\www\internal**	**Internal.html**
www.itnsa.id	**C:\www\public**	**Index.html**
extra.itnsa.id	**C:\www\extra**	**Extra.html**

5. Configure Windows Authentication for **internal.itnsa.id** and make sure domain users can access this site after authentication.

DC.lab.itnsa.id

1. Install **Internet Information Services (IIS)** web server role on this server for future website deployment using playbook.
2. For easier management, install and configure IIS Management Service.

Shared Folder

SRV.itnsa.id

1. Create a new root directory for all shared folders at the following path: **C:\Shared Folder**

2. Create two shared folders refer to the list below:
   - Shared folder named **Home** pointing to the **C:\Shared Folder\Home** directory. This share will be used for users' personal home folders mounted as home drives.
   - Shared folder named **Group** pointing to the **C:\Shared Folder\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:
   - **Employee** directory with **Employee & Manager** group has Full permission.
   - **Engineer** directory with **Engineer & Manager** group has Full permission
   - **Finance** directory with **Finance & Manager** group has Full permission
   - **Manager** directory with **Manager & Manager** group has Full permission

4. Configure permissions on the **Home** shared folder so that each user can only access their own personal folder within the share.

5. On all created shared folders, remove the default **Everyone** account share permission.

File Server Resource Manager

SRV.itnsa.id

1. Configure Quota Management to enforce storage limits:
   - Apply a **50MB** hard limit to **each user's personal folder** inside the **Home** shared folder.
   - Apply a **100MB** 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** and **.doc** extensions to be saved.

Distributed File System

SRV.itnsa.id

1. Configure a new domain-based DFS Namespace.with name **CSDrive**
2. Create the following folders within the **CSDrive** namespace with their respective targets:
   - **\\itnsa.id\CSDrive\Home** targeting **\\SRV.itnsa.id\Home**
   - **\\itnsa.id\CSDrive\Group** targeting **\\SRV.itnsa.id\Group**
3. Configure this server as the primary member for DFS replication. Set up replication for the following folders:

Source Directory	Target Directory
C:\Shared Folder\Group\Manager	**C:\Backup\Manager**
C:\Shared Folder\Group\Finance	**C:\Backup\Finance**
C:\Shared Folder\Group\Engineer	**C:\Replica\Engineer**
C:\Shared Folder\Group\Employee	**C:\Replica\Employee**

FW.itnsa.id

1. Add this server as a second namespace server for the **\\itnsa.id\CSDrive** namespace to provide redundancy.
2. Configure this server as the target replication server for the DFS replication configured on **SRV.itnsa.id**.
3. Ensure that DFS Replication is configured to synchronize automatically and continuously between the primary member and this target server.

Routing and Remote Access

FW.itnsa.id & EDGE.lab.itnsa.id:

1. Install and configure the **Routing and Remote Access** service.
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 **FW.itnsa.id** and **EDGE.lab.itnsa.id**. 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**
- You may use any name for the VPN demand-dial interfaces.

***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.*

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** and **lab.itnsa.id** domain. You can check it in the **/etc/ansible** directory. **DO NOT MODIFY THE INVENTORY FILE!**

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

1. **Checking Playbook**

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

   - Ensure the directory **C:\ITNSA** exists
   - Create a file at **C:\ITNSA\ansible_ready.txt**
   - The content of the file must be the text: **Ansible Connected**

2. **Shared Folder Deployment**

   Create a playbook named **deploy_project.yml** that targets **SRV.itnsa.id**. This playbook must read variables from a file located at **/etc/ansible/itnsa_project.json** to create one or more shared folders that are used for future projects. Use directory **C:\Shared Folder** as the root directory for created shared folders.

   - Create the directory first on the target server with the **same name** as the project name.
   - Configure the shared folder with the **appropriate** permissions, ensure it points to the project directory that has been created on the first step.

3. **Website Deployment**

   Create a playbook named **deploy_website.yml** that targets **DC.lab.itnsa.id**. This playbook must be able to deploy a new website by using a variable for the site name.

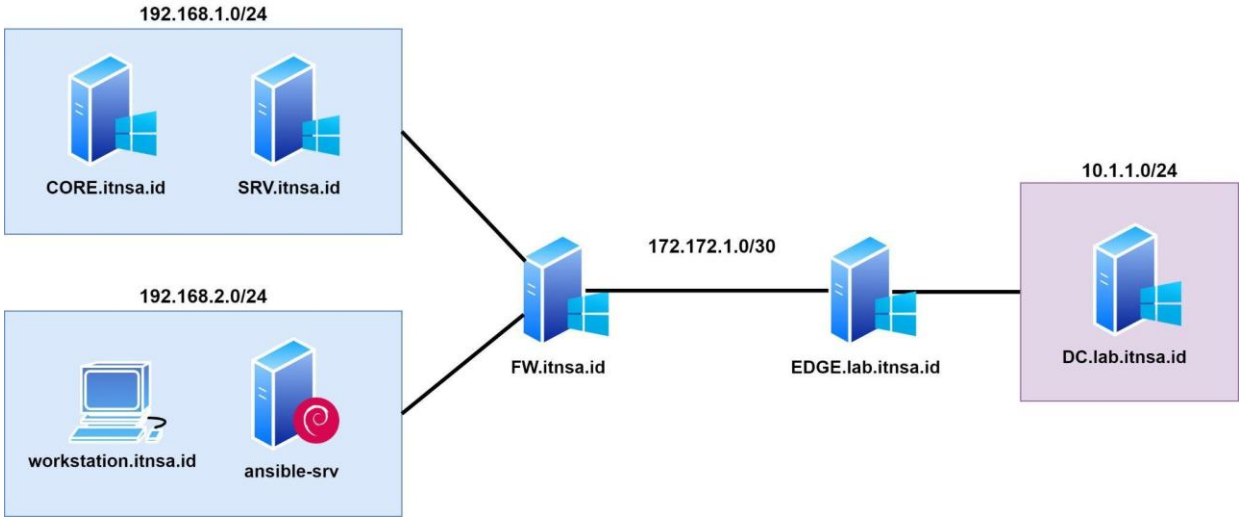
   - The playbook should accept the following variable `site_name` as the website name. Example execution:

     ```
     # ansible-playbook /etc/ansible/playbooks/deploy_website.yml \
       -e site_name=test.lab.itnsa.id
     ```

   - The created playbook must perform this step:
     1. Create a **DNS A record** in the **lab.itnsa.id** zone for the `site_name`, pointing to the IP address of DC.lab.itnsa.id. Based on example execution, DNS A record *test.lab.itnsa.id* will be created pointing to 10.1.1.10
     2. Create a root directory for the website at **C:\project_website**`site_name`. Based on example execution, *C:\project_website\test.lab.itnsa.id*\ will be created.
     3. Configure default index content to the value of `site_name`. Based on example execution, content of created website will be **test.lab.itnsa.id**
     4. Create a new IIS website that listens on HTTP, using the `site_name` as the hostname and the corresponding directory for its content.

Appendix

Topology



Addressing Table

Hostname	FQDN	IP Address
CORE	**CORE.itnsa.id**	**Ethernet0**: 192.168.1.1/24 **Management**: 10.10.10.1/24
SRV	**SRV.itnsa.id**	**Ethernet0**: 192.168.1.100/24 **Management**: 10.10.10.2/24
FW	**FW.itnsa.id**	**Ethernet0**: 172.172.1.1/30 **Ethernet1**: 192.168.1.254/24 **Ethernet2**: 192.168.2.254/24 **Management**: 10.10.10.3/24
EDGE	**EDGE.lab.itnsa.id**	**Ethernet0**: 172.172.1.2/30 **Ethernet1**: 10.1.1.1/24 **Management**: 10.10.10.4/24
DC	**DC.lab.itnsa.id**	**Ethernet0**: 10.1.1.10/24 **Management**: 10.10.10.5/24
WORKSTATION	**WORKSTATION.itnsa.id**	**Ethernet0**: DHCP **Management**: 10.10.10.6/24
ansible-srv	N/A	**ens160**: 192.168.2.222/24 **ens192**: 10.10.10.7/24