



**TEST PROJECT**

**MODUL 4 – WINDOWS ENVIRONMENT**

**SELEKSI NASIONAL CALON KOMPETITOR**

**ASEAN SKILLS COMPETITION (ASC) XIII 2019**

**KEJURUAN IT NETWORK SYSTEMS**

**ADMINISTRATION**

**DIREKTORAT BINA STANDARDISASI KOMPETENSI DAN PELATIHAN KERJA**

**DIREKTORAT JENDERAL PEMBINAAN PELATIHAN DAN PRODUKTIVITAS**

**KEMENTERIAN KETENAGAKERJAAN R.I.**

Jl. Jenderal Gatot Subroto Kav. 51 Telp./Fax. 021-5262782 Jakarta Selatan 12950

## **Day 3 – Windows Environment IT Network Systems Administration**

## INTRODUCTION OF TEST PROJECT

### CONTENTS

This Test Project proposal consists of the following document/file:

1. Modul\_4\_Windows\_Environment.pdf
2. Modul\_4\_Users.xlsx
3. HTML.zip

You are the IT consultant responsible for Skill39. Use the password "**Skill39**"(without quotes) when no specific password has given. Please follow the instructions that follow to complete the project.

## DC1

### Configure to match the following requirements:

- Rename hostname and set IP address according to configuration table and network diagram.
- Configure Active Directory
  - Import users from included excel file
    - **Note: If you can't import from excel to Active Directory User, please make some users for each group according to the list below.**

User	Group
competitor	Competitors
expert	Experts
manager	Managers
volunteer	Volunteers
visitor	Visitors
agent	Agents

- Account should be enabled and have the properties listed in the spreadsheet including group membership and NOT be required to change password at first login
- Configure DNS Service
  - Create all appropriate A records for all servers on 172.18.15.0/24
  - Create all appropriate CNAME records according to the tasks.
    - A record for 172.18.15.20
      - adfs
    - CNAME records of dc2.inaskills.net:
      - work, csweb, www, intra, extra
  - Create a reverse lookup zone creating PTR records for all hosts.
- Configure DHCP Service
  - Configure failover scope with DC2 once it is installed. Set DC1 as the active server.
  - Total scope Range: 172.18.15.99 - 172.18.15.199
  - Give DC1 70% of this scope to DC1, and the rest to DC2
  - Configure the failover to use Hot Standby mode
  - Scope Options
    - DNS: 172.18.15.10, 172.18.15.20, Gateway: 172.18.15.1
- Configure Network Policy Server to authorize network access for VPN-connected users.
  - Users in the Competitor group are not allowed to connect to VPN server.
  - Agents and Experts can use VPN connection by username and password
- Configure and apply the following group policies:
  - Disable "**first sign-on animation**" on each domain joined client.
  - Change Power settings so machines do not go to sleep for each domain-joined client.
  - Create a GPO which is applied to all machines so that the firewall is modified to allow ping traffic between machines.
  - Automatically issue a certificate for the "**Manager**" group members.

- The work folder must be automatically connected when "**Experts**" group members logged on.
- Create and share a **C:\backups** folder as **\\DC1\Backups\**
  - Create a backup job to backup all users home folders located on DC2 at 4 PM daily.
  - Make sure the backup job is written to the event log.

## DC2

### Configure to match the following requirements:

- Rename hostname and set IP address according to configuration table and network diagram.
- Configure this server as a second domain controller for the **inaskills.net** domain.
- Configure DNS service
  - The records of Active Directory-Integrated zones should be replicated.
- Configure DHCP service
  - Configure failover scope - refer to the description for DC1
- Configure Active Directory Federation Service
  - This server provides federation service.
  - URL: **https://adfs.inaskills.net**
  - Display Name: **"INASKILLS2019 Single Sign-On"**
- Add three extra 10G drives
  - Format the attached disk with NTFS into a single RAID 5 array (**G:\**) and enable de-duplication on this volume
- Create file share for user's home drives:
  - Access URL: **dc2.inaskills.net\homes**
  - Local path: **"G:\homes\"**
- Configure Work folders:
  - Access URL: **https://work.inaskills.net/**
  - Local path: **"G:\work\"**
- Create file share for each group
  - Access URL: **dc2.inaskills.net\seleknas**
  - Local path: **"G:\seleknas\"**
  - Create three subfolders and configure access control:
    - Junior Skills
      - Allow read-only access for users who have **"Junior"** as the job title.
      - Allow full access to the users who are also part of the **"WSJ"** organizational unit and also belong to the **"Manager"** group.
    - Secret Challenges
      - Allow access only for **"Agent"** group.
      - This folder should be hidden for the user who has insufficient permission.
    - Public
      - Allow read-only access for domain users.
      - Create a file share for local path **G:\witness** and share it as **\\DC2\witness**.
- Install and configure IIS and its websites using given HTML files.
  - Use a single certificate that only has **"www.inaskills.net"** as a common name.
  - Configure the **"Default Web Site"** as described below.

- Path for website root: "C:\inetpub\intranet\".
  - Enable Windows Internal authentication.
    - Use certificate authentication for "/manager/" subdirectory
- Create "https://extra.inaskills.net" website with the name "Extranet".
  - Path for website root: "C:\inetpub\extranet\".
  - Enable ADFS web authentication via the Web Application Proxy for clients on the Internet.
- Create "https://www.inaskills.net" website with the name "Public".
  - Path for website root: "C:\inetpub\internet\".
- Configure Certificate Enrolment Web Service (CES) and Certificate Enrolment Policy Web Service (CEP).
  - URL: "https://cswb.inaskills.net" for both CES and CEP.
  - Computers that are not in inaskills.net domain should be able to get a certificate through this server.
  - Authentication should be done by username and password.
  - Friendly Name: "INASKILLS2019 Enrollment Policy"
  - Make only "\_External\_Client" template visible.
- Configure IP Address and Domain Restrictions.
  - The "https://intra.inaskills.net" website can be accessible from: 172.18.15.0/24, 10.12.3.0/24

## CERT

### Configure to match the following requirements:

- Rename hostname and set the IP address according to configuration table and network diagram
- Configure the Certificate Authority service
  - Install Enterprise Root CA
  - Name: **"INASKILLS2019-CA"**
  - Lifetime: 60 months
  - Enable extensions for CDP and AIA URL through HTTP
    - URL for CDP:
      - `http://cert.inaskills.net/CertEnroll/<CaName><CRLNameSuffix><Delta CRLAllowed>.crl`
    - URL For AIA
      - `http://cert.inaskills.net/CertEnroll/<ServerDNSName>_<CaName><CertificateName>.crl`
- Create these templates:
  - **"\_INASKILLS\_Manager"**
    - For users in the **"Manager"** group.
  - **"\_INASKILLS\_Server"**
    - To provide a certificate for servers/services inaskills.net domain.
  - **"\_External\_Client"**
    - To provide a certificate for computers on the Internet.
    - Enable key-based renewal.
    - Enable certificate manager approval to issue a certificate.

## FIREWALL

### Configure to match the following requirements:

- Rename hostname and set the IP address according to configuration table and network diagram
- Enable Routing
- Configure DNS server for the public Internet.
  - Create primary zone **"inaskills.net"** and add these A records of 200.150.15.1.
    - ns,vpn,csweb,work,extra
  - Add an A record **"www.inaskills.net"** of 172.18.15.20.
  - SOA record of the **"inaskills.net"** should be **"ns.inaskills.net"**.
- Configure Routing and Remote Access Service
  - Users and computers on the Internet should be able to establish VPN connection to this server.
  - IKEv2 clients can connect to the intranet through this server.
  - Authorize VPN access through the NPS.
  - IP address pool for remote access clients: 10.12.3.1 - 10.12.3.254



- Configure the Web Application Proxy.
  - Clients on the Internet should be able to:
    - Access "**https://extra.inaskills.net**" website after passing the ADFS web authentication.
    - Access "**https://csweb.inaskills.net**" to reach to the Certification Enrolment Policy and Certification Enrolment Service.
    - Access "**https://work.inaskills.net**" to use work folders for each user.
    - Configure firewall rules to prevent unauthorized access.
    - Allow HTTPS traffic from 200.150.15.0/24 to 172.18.15.20.
    - Block any other traffics sourced from 200.150.15.0/24 to 172.18.15.0/24.

## INTCLT

Configure to match the following requirements:

- Rename hostname and set IP address according to configuration table and network diagram.
- Join to inaskills.net domain.
- Use this machine to:
  - Test access to Manager/Intranet/Extranet websites.
  - Test GPOs.
  - Test home and Work Folders.
  - Ensuring users have been imported correctly.

## PUBCLT

Configure to match the following requirements:

- Rename hostname and set IP address according to configuration table and network diagram.
- Do not join this client to the domain.
- Set the firewall on this machine to allow inbound and outbound “ping” traffic.
- Set the power settings to “never sleep”.
- Test Work Folders service is available via <https://work.inaskills.net>.
  - ADFS web authentication should be work.
  - Work Folders should be accessible and writable.
- This client should be able to receive a certificate from CES.
  - Create a local Enrolment Policy.
  - Get a certificate contains CN=PUBCLIENT from CES.
- Create an IKEv2connection "INASKILLS2019-VPN" for test purpose and make don't remember credential.

## CONFIGURATION TABLE

Hostname	Operating System	Domain	IP Address(es)	VM Connection
<b>DC1</b>	Windows Server 2016 (Desktop)	INASKILLS.NET	172.18.15.10	Bridged
<b>DC2</b>	Windows Server 2016 (Core)	INASKILLS.NET	172.18.15.20	Bridged
<b>CERT</b>	Windows Server 2016 (Desktop)	INASKILLS.NET	172.18.15.30	Bridged
<b>FW</b>	Windows Server 2016 (Desktop)	INASKILLS.NET	- 200.150.15.1 - 172.18.15.1	- LAN Segment EXTERNAL - Bridged
<b>INTCLT</b>	Windows 10 Enterprise	INASKILLS.NET	DHCP	Bridged
<b>PUBCLT</b>	Windows 10 Enterprise	WORKGROUP	200.150.15.10	LAN Segment EXTERNAL

## NETWORK DIAGRAM



