Test Project

IT Network Systems Administration

Module A – Client Server Environment

Submitted by:
Troy Pretty AU
Mario González Vásquez CR
Ander GUERRA ES
Mikko Hiltunen FI
Vijay Gosavi IN
Atsuya Kamioka JP
Brendan Burns UK
Mbusi Makhanya ZA

WSC2022SE_TP39_MA_actual_en

Introduction to Test Project

The following is a list of sections or information that must be included in all Test Project proposals that are submitted to WorldSkills.

- Contents including list of all documents, drawings and photographs that make up the Test Project
- Introduction/overview
- Short description of project and tasks
- Instructions to the Competitor
- Equipment, machinery, installations and materials required to complete the Test Project
- Marking scheme (incl. assessment criteria)
- Other

Introduction

The competition has a fixed start and finish time. You must decide how to best divide your time.

Please **carefully read** the following instructions!

When the competition time ends, please leave your station in a running state. The assessment will be done in the state as it is. No reboot will be initiated as well as powered off machines will not be powered on!

Please use the information below for all the servers and clients.

LOGIN

Username:	root / user
Username:	Administrator / user
Password:	Skill39

*If you cannot use this password by group policy on Windows, you can use “P@ssw0rd” instead of “Skill39”

System Configuration

Region/timezone:	Korea
Locale:	English US (UTF-8)
Key Map:	English US

Software

For testing purpose, all linux 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

Description of project and tasks

Part 1 – wsc2022.kr domain

KR-EDGE

Routing

- Enable forwarding on this server to make this server act as a router.
- Configure the static routes for Public Internet Network.

NAT

- Configure NAT as below using nftables:
  - Configure PAT for all hosts of wsc2022.kr domain.
  - Configure port-forwarding for services.
  - Configure static NAT for fw.wsc2022.kr. When fw.wsc2022.kr communicate with public internet network, its own IP address should be translated to 210.103.5.10

Site-to-Site VPN

- Configure IKEv2 Site-to-Site VPN. Use certificate issued by SKILL39-CA for authentication.

fw

Routing

- Enable forwarding on this server to make this server act as a router.

Nftables

- All traffic should be blocked by default.
- Traffic originating from the 192.168.1.0/24, 192.168.3.0/24, 10.1.1.0/30 and 172.16.1.0/24 networks should always be allowed.
- Of all traffic originating from the dmzsrv host, only traffic required by services should be allowed.
- Of all traffic originating from the public internet network to dmzsrv host, only traffic required by services should be allowed.
- ICMP should be allowed.
- Rules should be documented and dropped connections logged.

DHCP

- Configure DHCP service for the hosts of 192.168.1.0/24 network in wsc2022.kr – internal network.
  - Use IP assignment range as 192.168.1.100-199 and set appropriate value for scope options.
  - A and PTR records should be updated automatically.

Remote Access VPN

- Configure Remote Access IKEv2 VPN.
  - Use RSA-SIG as local authentication method, and EAP-MSCHAPv2 as remote authentication method. FreeRADIUS should be used as authentication backend.
  - Use certificate generated by SKILL39-CA, FQDN is “**vpn.wsc2022.kr**”.
  - VPN client should be assigned IP address from 192.168.3.0/24. Also, after VPN client connect successfully, it should be able to use resources of wsc2022.kr and wsc2024.fr domains.

intsrv

OpenLDAP

- Install and configure OpenLDAP server.
  - Add user objects according to Appendix: wsc2022.kr users.
  - Never use plaintext password as user password.
  - Make anonymous user prohibited from getting objects information.

FreeRADIUS

- Install and configure FreeRADIUS server. FreeRADIUS should be able to bring account information from OpenLDAP database. Use “**Skill39**” as shared-secret.

SNMP Agent

- Configure SNMPv2 community “**public**”.

dmzsrv

DNS

- Configure a view of internal **wsc2022.kr** name server.
  - Create static A records for all servers of wsc2022.kr domain.
  - Create reverse zone and add PTR records.
  - Create CNAME records required by services.
  - Create MX record.
- Configure a view external **wsc2022.kr** name server.
  - Create CNAME records required by services.
  - Create MX records.
- Configure forwarder with **FR-DC.wsc2024.fr**
- Configure “**INET.**“ as root-hint

E-Mail

- Configure SMTPS and IMAPS service support SSL/TLS for **wsc2022.kr** domain.
  - All users should be able to freely exchange emails using Mail service.
  - Use certificate generated by **SKILL39-CA** Certificate Authority.

Web

- Configure **https://www.wsc2022.kr** site. Use certificate generated by **SKILL39-CA**.
  - Create sub directory “**wsc2022**”. When clients access this directory, it should be passed ADFS authentication on FR-DC using only claim provider "**wsc2022.kr-OpenLDAP**".
    - The hosts of 192.168.1.0/24 should be able to browse without authentication.
  - Create sub directory “**wsc2024**”. When clients access this directory, it should be passed ADFS authentication on FR-DC using only claim provider "**Active Directory**".

FTP

- Install and configure FTP server using vsftpd.
  - Make sure the users are jaild in the same directory as the web-root for www.wsc2022.kr.
  - The OpenLDAP users should be able to upload the files.

Monitoring

- Install and configure Cacti monitoring service.
  - Clients should be able to access this site via **http://monitor.wsc2022.kr/monitor**.
  - Use “**Skill39**” as administrator’s password.
  - Add graphs of network traffic of **intsrv** and **FR-DC**.
  - Create tree per host.

intclnt

Client Configuration

- Make sure OpenLDAP users can login to intclnt. You should login as james user when performing tasks.
- Install CA certificates to firefox.
- Configure mail client for **james@wsc2022.kr** using thunderbird. Do not delete the emails that have been exchanged for testing.

Part 2 – wsc2024.fr domain

FR-EDGE

Domain member client

- Join this server into **wsc2024.fr** domain.

Routing

- Install and configure RRAS on this server to make this server acts as a router.
- Configure the static routes for Public Internet Network.

NAT

- Configure PAT for all hosts of **wsc2024.fr** domain.
- Configure port-forwarding for services.

DHCP

- Configure DHCP service for the hosts of 172.16.1.0/24 network of wsc2024.fr domain.
  - Use IP assignment range as 172.16.1.100-199 and set appropriate value for scope options.

Site-to-Site VPN

- Configure IKEv2 Site-to-Site VPN. Use certificate issued by SKILL39-CA for authentication.

Web Application Proxy

- Configure Web Application Proxy. Use certificate generated by **SKILL39-CA**.
  - **REMOTE** should be able to access RD Web Access and use RemoteApp after passing ADFS web authentication.

FR-DC

Active Directory

- Install and configure Domain controller and Global catalog for **wsc2024.fr**.
  - Create the following OUs:
    - Managers
    - Competitors
    - Visitors
  - Create the following global AD groups:
    - FR_Managers (Under Managers OU)
    - FR_Competitors (Under Competitors OU)
    - FR_Visitors (Under Visitors OU)
  - Create users using csv file (csv file is located in C:\ of FR-DC)
    - Configure the account so that the users are not prompted to change the password on first login.
  - All users have to use "**\\FR-FILE\homes\%username%**" as their home drive. Use **H:\** as drive letter.

DNS

- Configure internal **wsc2024.fr** name server.
  - Create static A records for all servers of wsc2024.fr domain.
  - Create reverse zone and add PTR records.
  - Create CNAME records required by services.
  - Create MX record.
- Configure external view of **wsc2024.fr** domain.
  - Create static A records.
  - Create CNAME records required by services.
  - Create MX record.
- Configure forwarder with **dmzsrv.wsc2022.kr.**
- Configure "**INET.**" as root-hint.

Group Policy

- Configure Group Policy according to the below requirements:
  - From **worker**, First-Login animation should not be displayed.
  - When login as users in **FR_Managers** group, user certificate should be enrolled automatically using **FR_USERS** template.
  - Configure drive mapping as the below:
    - \\FR-FILE\WSC\Competitors -> G:\ (Only users of FR_Competitors group)
    - \\FR-FILE\WSC\Managers -> G:\ (Only users of FR_Managers group)
    - \\FR-FILE\WSC\Visitors -> G:\ (Only users of FR_Visitors group)
  - Configure folder redirection for "Desktop" to "\\FR-FILE\redirected\%username%".

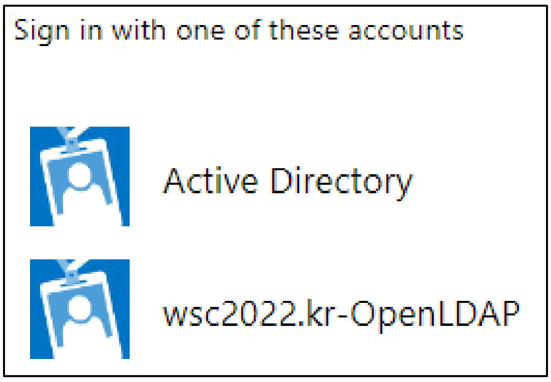
  - Configure password policy so that require 7 characters non-complex password for domain users, and complex password for members of FR_Managers.

Certificate Authority

- Configure Enterprise Subordinate Certificate Authority. Subject-Name is “**CN=SKILL39-CA**”.
  - Configure CDP. URL is “**http://fr-dc.wsc2024.fr/certenroll/SKILL39-CA.crl**”.
  - Configure AIA. URL is “**http://fr-dc.wsc2024.fr/certenroll/SKILL39-CA.crt**”.
  - Create “**FR_SERVER**” template for services.
  - Create “**FR_USERS**” template for users.

Active Directory Federation Service

- Configure Active Directory Federation Service. Use **https://adfs.wsc2024.fr** as URL, and Display Name should be “**WorldSkills Single Sign On**”.
  - Add OpenLDAP of **intsrv.wsc2022.kr** as Claim Provider. LDAP user object can be used for ADFS authentication. Use “**wsc2022.kr-OpenLDAP**” as the name of claim provider. When users perform ADFS authentication, users should be able to choose claim provider between “**Active Directory**” and “**wsc2022.kr-OpenLDAP**” as the below picture.



Sign in with one of these accounts

Active Directory

wsc2022.kr-OpenLDAP

  - For testing, enable IdpInitiatedSignonPage.

Remote Desktop Services

- Install and configure Remote Desktop Services.
- Publish WordPad as RemoteApp program. Make sure domain users can browse RD Web Access via “**https://rds.wsc2024.fr/RDWeb/**”.
- Install and configure Remote Desktop Gateway for access from the internet. Make sure RemoteApp can be used from REMOTE.

SNMP Agent

- Configure SNMPv2 community “**public**”.

FR-FILE

Active Directory

- Join this server into **wsc2024.fr** domain.
- Install and configure additional Domain Controller for wsc2024.fr. (No Global Catalog!)

RAID5

- Add 4 2GB disks and configure them as RAID5, NTFS format and mounted as **V:\**

File Server

- Configure “**WSC**” shared folder. Local path is “**V:\WSC\**”.
  - Create 3 subfolders “**Managers**”, “**Competitors**” and “**Visitors**” in “**V:\WSC\**”.
    - These subfolders should be able to access from only users in group under OU with the same name as the shared folders.
    - These subfolders should be hidden for all users who have insufficient permission to access the folder. (For instance, a user in FR_Managers group should be able to see only “Managers” folder.)
- Configure “**Resource**” shared folder. Local path is “**V:\Resource\**”. Only users in **FR_Managers** and **FR_Competitors** group should be able to access this share.
- Configure File Resource Manager so that all users cannot save the executable files (.exe, .bat, .cmd, etc…) and more than 100MB of data on their home drive.

FR-SRV

Domain member client

- Join this server into **wsc2024.fr** domain. Make sure the domain users can login to this server.

Web

- Configure **https://www.wsc2024.fr** site. Use **/var/www** as physical path, and use certificate generated by **SKILL39-CA**.
  - Create subfolder “**managers**” in **/var/www**. When users access **https://www.wsc2024.fr/managers**, client certificate authentication should be done.
- http://www.wsc2024.fr must redirect to https://www.wsc2024.fr.

E-Mail

- Configure SMTPS and IMAPS service that support SSL/TLS for **wsc2024.fr** domain.
  - All users should be able to freely exchange emails using Mail Service.
  - Use certificate generated by **SKILL39-CA** Certificate Authority.
- Configure SMTP services as secondary mail server for **wsc2022.kr** domain. If SMTP service on dmzsrv goes down, any mail to wsc2022.kr domain should be sent to FR-SRV. Make sure it is sent to dmzsrv immediately after recover.

worker

Client Configuration

- Join this client into **wsc2024.fr** domain.
- Log in to this client as mgr-001 and configure mail client for **mgr-001@wsc2024.fr** using Mail Application. Do not delete the emails that have been exchanged for testing.
- Install CA certificates.

Part 3 – Public Internet Network

ISP

Routing

- Enable forwarding on this server to make this server act as a router.
- Configure the static routes for Public Internet Network.

INET

DNS

- Configure name server for **internet.com** domain.
  - Create static A records for all servers of public internet network.
  - Create CNAME records required by services.
  - Create MX record.
- Configure name server for Microsoft NCSI.
- Configure forwarders for **wsc2022.kr** and **wsc2024.fr** domains.

Certificate Authority

- Configure Root Certificate Authority.
  - Subject Name is "**C=KR, O=WSI, CN=Root-CA**", and use "**/etc/ssl/CA**" as CA directory.
  - Configure CDP. URL is "**http://www.internet.com/Root-CA.crl**".
  - Configure AIA. URL is "**http://www.internet.com/Root-CA.crt**".

Web Server

- Configure web site for Microsoft NCSI.
- Configure **https://www.internet.com** site. Use certificate generated by **Root-CA**.

E-Mail

- Configure SMTP and IMAP service for **internet.com** domain.
  - All users should be able to freely exchange emails using Mail Service.

REMOTE

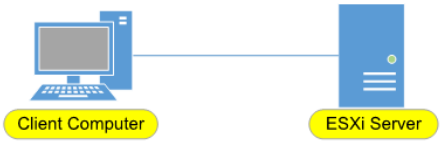
Client Configuration

- Install CA certificates.
- Configure mail client for **user@internet.com** using Mail Application. Do not delete the emails that have been exchanged for testing.
- Configure VPN adapter "**WSC**".
  - It should not remember credential.

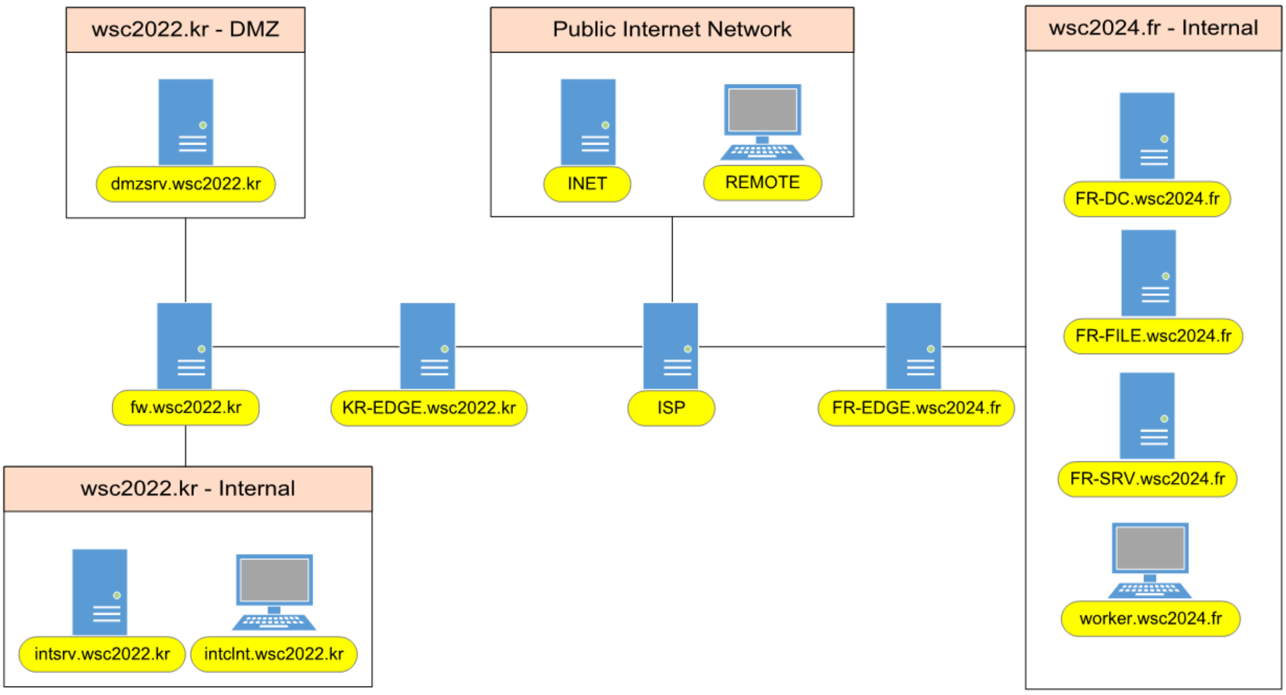
Appendix

Topology

Physical topology



Logical topology



Configuration Table

FQDN	IP Address	Services	Operating System
ISP	210.103.5.254 210.103.5.62 210.103.5.126	---	Debian Linux 11.3 (CUI)
KR-EDGE.wsc2022.kr	10.1.1.2 210.103.5.1	S2S VPN	Debian Linux 11.3 (CUI)
fw.wsc2022.kr	192.168.1.254 192.168.2.254 10.1.1.1	Firewall, DHCP, Remote Access VPN	Debian Linux 11.3 (CUI)
intsrv.wsc2022.kr	192.168.1.1	OpenLDAP, FreeRADIUS, SNMP Agent	Debian Linux 11.3 (CUI)
intclnt.wsc2022.kr	DHCP	----	Debian Linux 11.3 (GUI)
dmzsrv.wsc2022.kr	192.168.2.1	DNS, WEB, FTP, MAIL, Monitoring	Debian Linux 11.3 (CUI)
FR-EDGE.wsc2024.fr	172.16.1.254 210.103.5.65	DHCP, S2S VPN, Web Application Proxy	Windows Server 2019 Datacenter (Core)
FR-DC.wsc2024.fr	172.16.1.1	DC, Sub CA, ADFS, Remote Desktop, SNMP Agent	Windows Server 2019 Datacenter (GUI)
FR-FILE.wsc2024.fr	172.16.1.2	DC, RAID5, File Server	Windows Server 2019 Datacenter (Core)
FR-SRV.wsc2024.fr	172.16.1.3	WEB, MAIL	Debian Linux 11.3 (CUI)
worker.wsc2024.fr	DHCP (172.16.1.100)	---	Windows 10 Enterprise
INET	210.103.5.129	DNS, WEB, MAIL, Root CA	Debian Linux 11.3 (CUI)
REMOTE	210.103.5.210	---	Windows 10 Enterprise

Networks

network	CIDR	domain
wsc2022.kr - Internal	192.168.1.0/24	wsc2022.kr
wsc2022.kr - DMZ	192.168.2.0/24	wsc2022.kr
wsc2022.kr - Edge	10.1.1.0/30	wsc2022.kr
wsc2024.fr - Internal	172.16.1.0/24	wsc2024.fr
Public Internet Network	210.103.5.0/26 210.103.5.64/26 210.103.5.128/25	---

wsc2022.kr users

Username	Password	E-mail	Home Directory
james	Skill39	james@wsc2022.kr	/home/james
donald	Skill39	donald@wsc2022.kr	/home/donald