Конкурсное задание

ИТ Сетевое и системное

администрирование

Модуль А – Среда клиент-сервер

Представлено:
Troy Pretty AU
Mario González Vásquez CR
Ander GUERRA ES
Mikko Hiltunen FI
Vijay Gosavi IN
Atsuya Kamioka JP
Mohamad Ropi Abdullah MY
John Doyoyo ZA

Введение в конкурсное задание

Ниже приводится список разделов или информации, которые должны быть включены во все предложения по тестовым проектам, представляемые в WorldSkills.

- Содержание, включая список всех документов, рисунков и фотографий, составляющих Конкурсное задание.
- Введение/обзор
- Краткое описание задания и задач
- Инструкция для участника
- Оборудование, машины, установки и материалы, необходимые для выполнения Конкурсного задания.
- Схема выставления оценок (включая критерии оценки)
- Другое

Введение

Конкурс имеет фиксированное время начала и окончания. Вы должны решить, как лучше распределить свое время.

Пожалуйста, **внимательно прочтите** следующие инструкции!

Когда время соревнования закончится, пожалуйста, оставьте свою станцию в рабочем состоянии. Оценка будет сделана в том состоянии, в котором она есть. Никакая перезагрузка не будет инициирована, а выключенные машины не будут включены!

Пожалуйста, используйте приведенную ниже информацию для всех серверов и клиентов.

ВХОД

Имя пользователя :	root / user
Имя пользователя:	Administrator / user
Пароль:	Skill39

Конфигурация системы

Регион/ часовой пояс : Korea

Язык :	English US (UTF-8)
Ключевая карта:	English US

Программного обеспечения

В целях тестирования на все хосты Linux были установлены следующие инструменты тестирования: smbclient, curl, lynx, dnsutils, ldap-utils, ftp, lftp, wget, ssh, nfs -common, rsync, telent, traceroute, tcptraceroute.

Описание проекта и задач

Часть 1 – Домен wsc2022.kr

KR-EDGE

Маршрутизация

- Включите переадресацию на этом сервере, чтобы этот сервер работал в качестве маршрутизатора.
- Установите и настройте frr для получения маршрутов для общедоступной сети Интернет. Используйте BGP в качестве протокола динамической маршрутизации.

NAT

- Настройте NAT, как показано ниже, используя nftables:
  - Настройте PAT для всех хостов домена wsc2022.kr.
  - Настройте переадресацию портов для служб.
  - Настройте статический NAT для fw.wsc2022.kr. Когда fw.wsc2022.kr связывается с общедоступной интернет-сетью, его собственный IP-адрес должен быть преобразован в 210.103.5.10.

DHCP

- Настройте службу DHCP для хостов сети 192.168.1.0/24 в wsc2022.kr — внутренняя сеть.
  - Используйте диапазон назначения IP-адресов 192.168.1.100-199 и установите соответствующее значение для параметров области.
  - Записи A и PTR должны обновляться автоматически.

Site-to-site VPN

- Настройте GRE через IPsec VPN. Используйте аутентификацию с предварительным общим ключом и «**Skill39**» в качестве секрета. Используйте **tun0** в качестве имени интерфейса.

fw

Маршрутизация

- Включите переадресацию на этом сервере, чтобы этот сервер работал в качестве маршрутизатора.

Nftables

- Весь трафик через брандмауэр должен быть заблокирован по умолчанию.
- Трафик, исходящий из сетей 192.168.1.0/24, 192.168.3.0/24, 10.1.1.0/30 и 172.16.1.0/24, всегда должен быть разрешен.
- Из всего трафика, исходящего от хоста dmzsrv , должен быть разрешен только трафик, требуемый службами.
- Из всего трафика, исходящего из общедоступной интернет-сети на хост dmzsrv , должен быть разрешен только трафик, необходимый службам.
- fw должен иметь возможность пинговать любые хосты.

Агент DHCP- ретрансляции

- Настройте агент DHCP-ретрансляции, чтобы клиенты во внутренней сети могли автоматически получать IP-адреса.

VPN с удаленным доступом

- Настройте удаленный доступ IKEv2 VPN.
  - MSCHAPv2 в качестве метода удаленной проверки подлинности. FreeRADIUS следует использовать в качестве серверной части аутентификации.
  - Используйте сертификат, созданный SKILL39-CA, полное доменное имя «**vpn.wsc2022.kr**».
  - VPN-клиенту должен быть назначен IP-адрес из 192.168.3.0/24. Кроме того, после успешного подключения VPN-клиент должен иметь возможность использовать ресурсы доменов wsc2022.kr и wsc2024.fr.

intsrv

DNS

- Настройте внутренний сервер имен **wsc2022.kr** .
  - Создайте статические записи A для всех серверов домена wsc2022.kr.
  - Создайте обратную зону и добавьте записи PTR.
  - Создайте записи CNAME, необходимые службам.
  - Создайте MX-запись.
- Настройте сервер пересылки с помощью **FR-DC.wsc2024.fr**
- Настройте «**INET**» как root-hint

OpenLDAP

- Установите и настройте сервер OpenLDAP.
  - Добавьте пользовательские объекты в соответствии с Приложением: пользователи wsc2022.kr.
  - Никогда не используйте открытый текстовый пароль в качестве пароля пользователя.
  - Запретить анонимному пользователю получать информацию об объектах.

FreeRADIUS

- Установите и настройте сервер FreeRADIUS. FreeRADIUS должен иметь возможность получать информацию об учетной записи из базы данных OpenLDAP. Используйте «**Skill39**» в качестве общего секрета.

Целевой сервер iSCSI

- Добавьте диск объемом 10 ГБ и настройте этот сервер в качестве цели iSCSI для **FR-FILE**.

SNMP-агент

- Настройте сообщество SNMPv2 «**public**».

dmzsrv

DNS

- Настройте внешний сервер имен **wsc2022.kr** .
  - Создайте записи CNAME, необходимые службам.
  - Создайте записи MX.

E-mail

- Настройте службу SMTPS и IMAPS для поддержки SSL/TLS для домена **wsc2022.kr**.

- Все пользователи должны иметь возможность свободно обмениваться электронными письмами с помощью почтового сервиса.
- Используйте сертификат, созданный центром сертификации **SKILL39-CA**.

Web

- Настройте сайт **https://www.wsc2022.kr**. Используйте сертификат, сгенерированный **SKILL39-CA**.
- Настройте сайт **http://intra.wsc2022.kr**.
  - Создайте подкаталог «**wsc2022**». Когда клиенты получают доступ к этому каталогу, он должен пройти аутентификацию LDAP с использованием пользовательских объектов OpenLDAP intsrv.
    - Хосты 192.168.1.0/24 должны иметь возможность просмотра без аутентификации.
  - Создайте подкаталог «**wsc2024**». Когда клиенты получают доступ к этому каталогу, он должен пройти аутентификацию LDAP с использованием пользователей в группе **FR_Managers** домена **wsc2024.fr.**

Мониторинг

- Установите и настройте сервис мониторинга Cacti.
  - Клиенты должны иметь доступ к этому сайту через **http://monitor.wsc2022.kr/monitor**.
  - Используйте «**Skill39**» в качестве пароля администратора.
  - Добавьте графики сетевого трафика **intsrv** и **FR-DC**.
  - Создайте дерево для каждого хоста.

intclnt

Конфигурация клиента

- Убедитесь, что пользователи OpenLDAP могут войти в систему intclnt . Вы должны войти в систему как пользователь james при выполнении задач.
- Установите сертификаты CA в firefox.
- Настройте почтовый клиент для **james@wsc2022.kr** с помощью Thunderbird. Не удаляйте электронные письма, которыми обменивались для тестирования.

Часть 2 – домен wsc2024.fr

FR-EDGE

Клиент члена домена

- Присоедините этот сервер к домену **wsc2024.fr**.

Маршрутизация

- Установите и настройте RRAS на этом сервере, чтобы этот сервер работал как маршрутизатор.
- Включите протокол маршрутизации для получения маршрутов для общедоступной сети Интернет. Используйте BGP в качестве протокола динамической маршрутизации.

NAT

- Настройте PAT для всех хостов домена **wsc2024.fr**.
- Настройте переадресацию портов для служб.

DHCP

- Настройте службу DHCP для хостов сети 172.16.1.0/24 домена wsc2024.fr.
  - Используйте диапазон назначения IP-адресов 172.16.1.100-199 и установите соответствующее значение для параметров области.

Site-to-site VPN

- Настройте GRE через IPsec VPN. Используйте аутентификацию с предварительным общим ключом и «**Skill39**» в качестве секрета. Используйте **VPN** в качестве имени интерфейса.

Web Application Proxy

- Настройте прокси веб-приложения. Используйте сертификат, сгенерированный **SKILL39-CA**.
  - **REMOTE** должен иметь доступ к **https://www.wsc2024.fr** после прохождения веб-аутентификации ADFS.
  - **REMOTE** также должен иметь доступ к веб-доступу к удаленным рабочим столам и использовать RemoteApp после прохождения веб-аутентификации ADFS.

FR-DC

Active Directory

- Установите и настройте контроллер домена и глобальный каталог для **wsc2024.fr**.
  - Создайте следующие организационные единицы:
    - Managers
    - Competitors
    - Visitors
  - Создайте следующие глобальные группы AD:
    - FR_Managers (в OU Managers)
    - FR_Competitors (в OU Competitors)
    - FR_Visitors (в OU Visitors)
  - Создайте пользователей с помощью файла csv (файл csv находится в C:\FR-DC)
  - Все пользователи должны использовать «**\\FR-FILE\homes\%username%**» в качестве домашнего диска. Используйте **H:** в качестве буквы диска.
  - Все пользователи должны использовать «**\\FR-FILE\profiles\%username%**» в качестве перемещаемого профиля.

DNS

- Настройте внутренний сервер имен **wsc2024.fr** .
  - Создайте статические записи A для всех серверов домена wsc2024.fr.
  - Создайте обратную зону и добавьте записи PTR.
  - Создайте записи CNAME, необходимые службам.
  - Создайте MX-запись.
- Настройте внешний вид **домена** wsc2024.fr.
  - Создайте статические записи A.
  - Создайте записи CNAME, необходимые службам.
  - Создайте MX-запись.
- Настройте сервер пересылки с **помощью** intsrv.wsc2022.kr.
- Настройте «**INET**» как root-hint.

Групповая политика

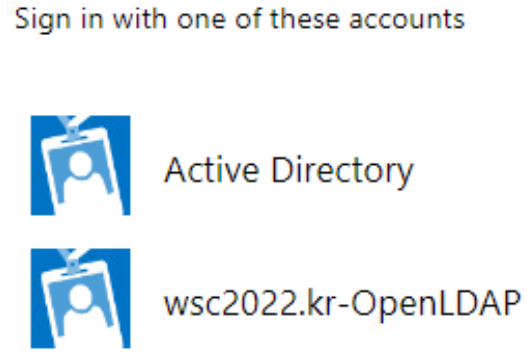
- Настройте групповую политику в соответствии со следующими требованиями:
  - От **worker** не должна отображаться анимация при первом входе в систему**.**
  - При входе в качестве пользователей в группу **FR_Managers** сертификат пользователя должен быть зарегистрирован автоматически с использованием шаблона **FR_USERS**.
  - Настройте сопоставление дисков, как показано ниже:
    - \\FR-FILE\WSC\Competitors -> G:\ (Только пользователи группы FR_Competitors)
    - \\FR-FILE\WSC\Managers -> G:\ (только пользователи группы FR_Managers)
    - \\FR-FILE\WSC\Visitors -> G:\ (Только пользователи группы FR_Visitors)

Центр сертификации

- Настройте подчиненный центр сертификации предприятия. Имя субъекта: «**CN=SKILL39-CA**».
  - Настройте CDP. URL-адрес: **«http://fr-dc.wsc2024.fr/certenroll/SKILL39-CA.crl»**.
  - Настройте AИA. URL-адрес: **«http://fr-dc.wsc2024.fr/certenroll/SKILL39-CA.crt»**.
  - Создайте шаблон «**FR_SERVER**» для сервисов.
  - Создайте шаблон «**FR_USERS**» для пользователей.

Служба федерации Active Directory

- Настройте службу федерации Active Directory. Используйте **https://adfs.wsc2024.fr** в качестве URL-адреса, а отображаемое имя должно быть «**WorldSkills Single Sign On**».
  - Добавьте OpenLDAP **intsrv.wsc2022.kr** в качестве Claim Provider. Объект LDAP user можно использовать для аутентификации ADFS. Используйте «**wsc2022.kr-OpenLDAP**» в качестве имени Claim Provider. Когда пользователи выполняют аутентификацию ADFS, пользователи должны иметь возможность выбирать Claim Provider между «**Active Directory**» и «**wsc2022.kr-OpenLDAP**», как показано на рисунке ниже.



  - Для тестирования включите IdpInitiatedSignonPage.

Службы удаленных рабочих столов

- Установите и настройте службы удаленных рабочих столов.
- Опубликуйте WordPad как программу RemoteApp. Убедитесь, что пользователи домена могут просматривать RD Web Access через **https://rds.wsc2024.fr/RDWeb/**.
- Установите и настройте шлюз удаленных рабочих столов для доступа из Интернета. Убедитесь, что RemoteApp можно использовать из REMOTE.

SNMP- агент

- Настройте сообщество SNMPv2 «**public**».

FR-FILE

Активный каталог

- Присоедините этот сервер к домену **wsc2024.fr**.
- Установите и настройте дополнительный контроллер домена для wsc2024.fr. (Нет глобального каталога!)

iSCSI-инициатор

- Настройте этот сервер для подключения к серверу iSCSI intsrv. Отформатируйте диск с помощью файловой системы NTFS и смонтируйте в **V:**

Файловый сервер

- Настройте общую папку «**WSC**». Локальный путь: «**V:\WSC**».
  - Создайте 3 подпапки «**Managers**», «**Competitors**» и «**Visitors**» в «**V:\WSC**».
    - Доступ к этим подпапкам должны иметь только пользователи в группе под OU с тем же именем, что и у общих папок.
    - Эти вложенные папки должны быть скрыты для всех пользователей, у которых недостаточно прав для доступа к папке. (Например, пользователь в группе FR_Managers должен видеть только папку «Managers».)
- Настройте общую папку «**Resource**». Локальный путь: «**V:\Resources**». Только пользователи из групп **FR_Managers** и **FR_Competitros** должны иметь доступ к этому общему ресурсу.
- Настройте диспетчер файловых ресурсов таким образом, чтобы все пользователи не могли сохранять исполняемые файлы (.exe, .bat, .cmd и т.д.) и данные объемом более 100 МБ на своем домашнем диске.

FR-SRV

Клиент члена домена

- Присоедините этот сервер к домену **wsc2024.fr**. Убедитесь, что пользователи домена могут войти на этот сервер.

Интернет

- Настройте сайт **https://www.wsc2024.fr** . Используйте **/var/www** в качестве физического пути и используйте сертификат, сгенерированный **SKILL39-CA** .
  - Создайте подпапку «**managers**» в **/var/www**. Когда пользователи обращаются к **https://www.wsc2024.fr/managers**, должна выполняться аутентификация сертификата клиента.

Эл. почта

- Настройте службы SMTPS и IMAPS, поддерживающие SSL/TLS, для домена **wsc2024.fr**.
  - Все пользователи должны иметь возможность свободно обмениваться электронными письмами с помощью почтовой службы.

- Используйте сертификат, созданный центром сертификации **SKILL39-CA**.
- Настройте службы SMTP в качестве вторичного почтового сервера для домена **wsc2022.kr**. Если служба SMTP на dmzsrv выходит из строя, любая почта на домен wsc2022.kr должна отправляться на FR-SRV. Убедитесь, что он отправлен на dmzsrv сразу после восстановления.

worker

Конфигурация клиента

- Присоедините этого клиента к домену **wsc2024.fr**.
- Войдите в этот клиент как mgr-001 и настройте почтовый клиент для **mgr-001@wsc2024.fr** с помощью почтового приложения. Не удаляйте электронные письма, которыми обменивались для тестирования.
- Установите сертификаты ЦС.

Часть 3 – Public Internet Network

ISP

Маршрутизация

- Включите переадресацию на этом сервере, чтобы этот сервер работал в качестве маршрутизатора.
- Установите и настройте frr для отправки маршрутов в общедоступную интернет-сеть. Используйте BGP в качестве протокола динамической маршрутизации.

INET

DNS

- Настройте сервер имен для домена **internet.com.**
  - Создайте статические записи A для всех серверов общедоступной сети Интернет .
  - Создайте записи CNAME, необходимые службам.
  - Создайте MX-запись.
- Настройте сервер имен для Microsoft NCSI.
- Настройте серверы пересылки для доменов **wsc2022.kr** и **wsc2024.fr**.

Центр сертификации

- Настройте корневой центр сертификации.
  - Имя субъекта — «**C=KR, O=WSI, CN=Root-CA**», и используйте «**/etc/ssl/CA** » в качестве каталога CA.
  - Настройте CDP. URL-адрес: «**http://www.internet.com/Root-CA.crl»** .
  - Настройте AИA. URL-адрес «**http://www.internet.com/Root-CA.crt**».

Веб сервер

- Настройте веб-сайт для Microsoft NCSI.
- Настройте сайт **https://www.internet.com**. Используйте сертификат, созданный **Root-CA**.

Эл. почта

- Настройте службы SMTP и IMAP для домена **internet.com.**
  - Все пользователи должны иметь возможность свободно обмениваться электронными письмами с помощью почтовой службы.

REMOTE

Конфигурация клиента

- Установите сертификаты ЦС.
- Настройте почтовый клиент для **user@internet.com** с помощью почтового приложения. Не удаляйте электронные письма, которыми обменивались для тестирования.
- Настройте VPN-адаптер «**WSC**».
  - Он не должен запоминать учетные данные.

Приложение

Топология

Физическая топология

Логическая топология

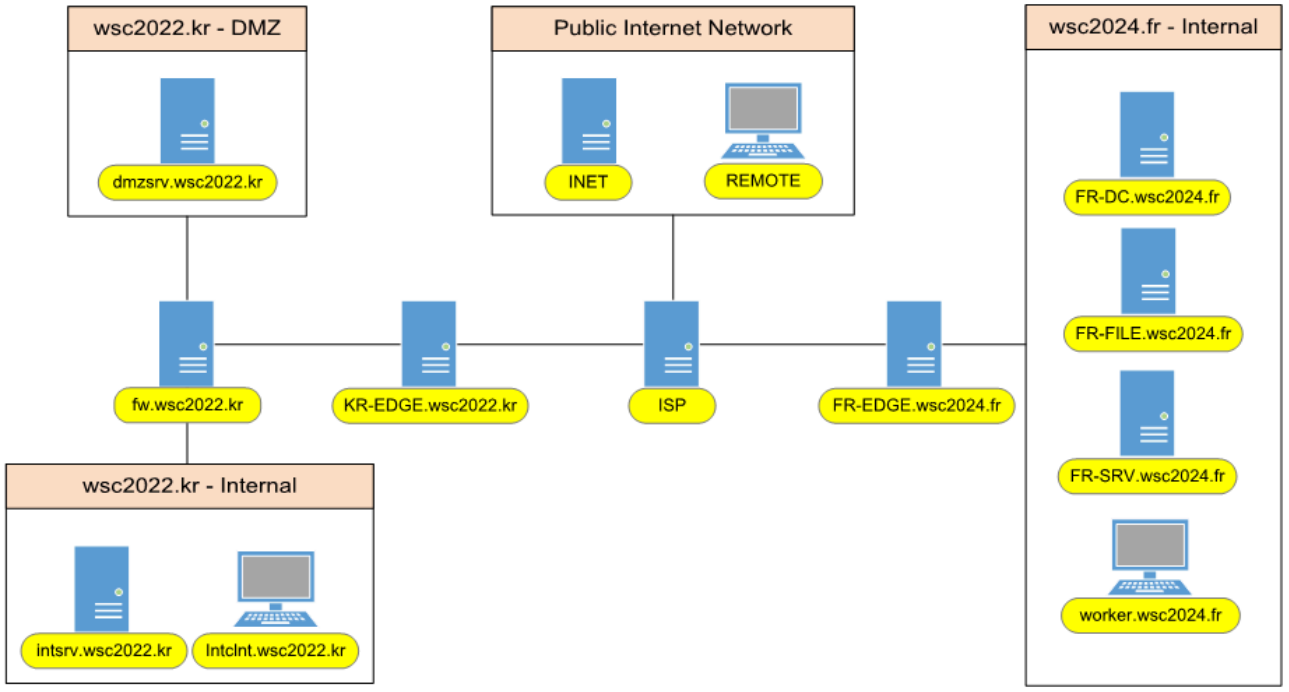


Таблица конфигурации

Полное доменное имя	IP адрес	Службы	Операционная система
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	DHCP, S2S VPN	Debian Linux 11.3 (CUI)
FW.WSC2022.KR	192.168.1.254 192.168.2.254 10.1.1.1	Firewall, DHCP Relay Agent, Remote Access VPN	Debian Linux 11.3 (CUI)
INTSRV.WSC2022.KR	192.168.1.1	DNS, OpenLDAP, FreeRADIUS, SNMP Agent, iSCSI Target Server	Debian Linux 11.3 (CUI)
INTCLNT.WSC2022.KR	DHCP	----	Debian Linux 11.3 (GUI)
DMZSRV.WSC2022.KR	192.168.2.1	DNS, WEB, 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, iSCSI Initiator, 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

Сети

Сеть	CIDR	Домен
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	---

Пользователи wsc2022.kr

Имя пользователя	Пароль	Эл. почта	Домашний каталог
JAMES	Pa$$worD	james@wsc2022.kr	/home/james
DONALD	Pa$$worD	donald@wsc2022.kr	/home/donald