# 제52회 전국기능경기대회 과제

| 직 종 명 | IT Network System | 과제명 | Window Environments | 과제번호 | 제 2 과제 |
|---|---|---|---|---|---|
| 경기시간 | 4시간 | 비번호 | | 심사위원 확 인 | (인) |

## 1. 과제 개요

당신은 ISP 에 근무하는 네트워크 엔지니어입니다. 이번에 새로 생긴 Right 그룹의 네트워크를 구축하는 업무를 맡게 되었습니다. Right 그룹은 본사와 지사로 나뉘어져 있으며, 지사는 Hyper-V를 이용하여 구축되어야 합니다.

지사는 가상 스위치를 이용하여 네트워크를 구성하게 되며, 내부 Cloud 서버는 본사의 파일 서버를 통해 클러스터링 합니다. 내부와 지사는 Site-to-Site Secure Tunnel을 이용하여 연결되도록 하며, 외부 클라이언트(Ex-Client)에서 내부로 접근하기 위해 DirectAccess를 이용하여 연결합니다.

## 2. 배포자료(USB에 복사하여 배포)

- Windows Server 2016 ISO 이미지
- Windows 10 Enterprise K x64 ISO 이미지
- VMware Workstation 12

## 3. 주의 사항

- 암호를 필요로 하는 곳에 암호가 지정되지 않을 경우 "Hyper12$$를 기본 값으로 사용합니다.
- Ex-Client 호스트는 채점 시 네트워크 인터페이스를 바꿀 수 있습니다.
- 특별하게 지정되지 않은 옵션 또는 설정은 시스템이 추천하는 기본 값을 사용합니다. 기본 설정이 없을 경우 사용자 임의로 설정합니다.
- 모든 Guest OS의 프린터 포트, 사운드 장치 및 플로피드라이브를 제거합니다.
- 정해진 USB장치 이외의 저장장치의 반입을 금지합니다.
- 휴대폰등과 같은 스마트기기는 경기시작 전 심사위원(또는 관리위원)에게 보관하도록 합니다.
- 모든 서버에 ICMPv4및 ICMPv6에 대한 방화벽을 허용하도록 합니다.

# 4. 과제 내용

## 가. 운영체제 설치 및 네트워크 구성

1) 운영체제 설치

부록의 운영체제 설치 항목을 참고하여 운영체제를 설치하도록 합니다.

2) 라우팅

Right 그룹이 인터넷 구간과 원활히 통신할 수 있도록 ISP에서 Routing을 합니다.

3) NAT

내부가 외부와 통신을 할 수 있도록 Hyper 및 Router에서 NAT을 합니다.

지사 내부의 호스트는 Hyper Server을 통해 NAT되어 외부와 통신하며, 본사 내부의 호스트는 Router Server을 통해 NAT되어 외부와 통신합니다.

4) Site-To-Site Secure Tunnel

본사.지사 간 보안된 통신을 위해 Router 와 Hyper 서버에 Secure Tunnel을 구성합니다. L2TP/IPSEC을 이용하며, 인증서를 이용하여 인증합니다.

EAP로 PEAP-MS-CHAPv2를 사용하도록 하며 NPS 서버를 통해 처리되어야 합니다.

Tunnel 서버 재시작 후 자동으로 연결되도록 하며, 영구적인 연결로 구성합니다.

## 나. Hyper-V

1) Hyper 서버에 Hyper-V 서비스를 설치하고 아래의 서버를 운영합니다.

| Host | 운영체제 |
|---|---|
| Hyper-AD | Window Server 2016 with GUI |
| Cloud01 | Window Server 2016 Core |
| Cloud02 | Window Server 2016 Core |

2) Router 서버에 Hyper-V 서비스를 설치하고 아래의 서버를 운영합니다.

| Host | 운영체제 |
|---|---|
| File01 | Window Server Nano Standard |
| File02 | Window Server Nano Standard |

3) Host와 Hyper-V Guest간의 Clipboard를 공유할 수 있게 합니다.

## 다. DNS 및 IP 주소 할당

1) Internet DNS

- ISP 서버에 msftncsi.com 도메인의 DNS 서비스를 아래의 조건에 따라 구성합니다. (필요할 경우 레코드를 추가할 수 있습니다.)

| FQDN | TYPE | IP |
|---|---|---|
| www.msftncsi.com | A | 1.1.1.2 |
| | | 2.2.2.2 |
| ca.msftncsi.com | A | 1.1.1.2 |
| | | 2.2.2.2 |
| dns.msftncsi.com | A | 131.107.255.255 |

또한, 해당 서버를 Root 서버로 구성합니다.

2) 내부 DNS

File01서버에 내부 클라이언트를 위한 right.loc 도메인 서버를 구성합니다. 필요한 레코드를 적절히 구성합니다. 외부 레코드는 Root DNS를 통해 쿼리합니다.

Hyper-AD 서버에 right.loc 도메인 서버를 구성합니다. 필요한 레코드를 적절히 구성합니다. 외부에 대한 레코드는 File01 서버를 Forwarder로 사용하여 쿼리합니다.

3) 외부 DNS

File01서버에 외부에 대한 right.loc 도메인 서버를 구성합니다. 필요한 레코드를 적절히 구성합니다.

| FQDN | TYPE | IP |
|---|---|---|
| da1.right.loc | A | 1.1.1.1 |
| da2.right.loc | A | 2.2.2.1 |

4) IP 주소 자동할당

Router 서버에서 아래의 조건에 맞게 IPv4주소를 배포하도록 합니다.

| | |
|---|---|
| 범위 | 192.168.0.100 - 192.168.0.150 |
| Default Gateway | 192.168.0.254 |
| DNS Server | 192.168.0.10 |

Router 서버에서 아래의 조건에 맞게 IPv6주소를 배포하도록 합니다.

| | |
|---|---|
| Prefix | 2100:f89:23::/64 |
| DNS Server | 2100:f89:23::10 |

5) IP 주소 수동할당

Ex-Client에 IP를 할당하기 위해 스크립트를 작성하여 C:₩ 폴더에 저장하도록 합니다. 해당 스크립트 실행 시 자동으로 아래 표에 제시된 IP가 할당 되어야 합니다.

| 파일 이름 | IP address | Default Gateway | DNS Server |
|---|---|---|---|
| branch.bat | 1.1.1.10 | 1.1.1.2 | 1.1.1.2 |
| head.bat | 2.2.2.10 | 2.2.2.2 | 2.2.2.2 |

## 라. 파일 시스템

1) ISCSI

Hyper 서버에 C:₩cluster.vhdx 가상 하드디스크를 만든 뒤 해당 디스크를 이용하여 ISCSI 서비스를 구성합니다.

가상 하드디스크 cluster.vhdx는 50GB의 고정된 용량을 가지도록 합니다.

2) Scale-Out File Server

File01과 File02서버에 CSV를 활용한 Scale-Out File Server를 구성합니다.

Scale-Out File Server는 “file.right.loc”도메인으로 접근가능해야 하며, AD 서버에서 관리할 수 있어야합니다.

공유 경로는 “₩₩file.right.loc₩data” 입니다.

## 마. 도메인 구성

1) Active Directory 구성

AD 서버에 right.loc 도메인을 구성하도록 합니다. 도메인 표를 참조하여 사용자를 추가합니다. 모든 클라이언트는 right.loc 도메인에 가입합니다.

2) Domain Controller

Hyper-AD 서버를 추가 DC로 사용합니다.

3) 도메인 사용자

Guest 사용자들은 평일 오전 6시 ~ 오후 6시까지만 로그인 될 수 있도록 합니다.

지사의 서버를 위하여 “cn=brmgmt, ou=RIGHT, dc=right, dc=loc” 유저를 생성하도록 하며, 해당 유저를 이용하여 지사의 서버를 관리할 수 있도록 합니다. 해당 유저는 본사 서버에서 로그인 할 수 없습니다.

## 바. 그룹정책

1) 모든 클라이언트는 처음 시작 애니메이션이 비활성화 되어야 합니다.

2) 60초간 입력이 없을 시 화면보호기가 실행되어야 하며, 암호로 보호되어야 합니다.

3) 파일 삭제 시 휴지통에 저장되지 않고, 바로 삭제합니다.

4) Guest 사용자는 Internet Explorer을 실행할 수 없습니다.

5) Guest 사용자는 이동식 디스크의 읽기/쓰기를 할 수 없습니다.

6) worker 그룹의 사용자는 1분간 2번 로그인 실패 시 2분간 로그인이 되지 않습니다.

7) 서버를 관리하는 사용자는 1분간 1번 로그인 실패 시 2분간 로그인이 되지 않습니다.

## 사. 공유자원관리

1) 사용자 홈 디렉터리

도메인 내의 모든 사용자는 "₩₩shared.right.loc₩home₩사용자 이름"에 자신의 홈 디렉터리를 가진다. 도메인 로그인 시 자신의 홈 디렉터리가 "H:" 드라이브로 자동 연결될 수 있도록 합니다.

₩₩shared.right.loc₩home₩

모든 사용자는 홈 디렉토리에 대해 50MB의 할당량을 가집니다.

2) 사용자 프로필

도메인 내의 모든 사용자는 "₩₩shared.right.loc₩profile"에 자신의 프로필을 저장합니다.

## 아. 사이트 구성

1) Right 그룹의 사용자가 가까운 DC에서 로그인 정보를 받을 수 있도록 적절히 Site를 구성합니다.

2) 지사의 사이트는 Branch, 본사의 Site 는 Head 라는 이름을 사용합니다.

## 자. 인증 기관

1) 인증 기관 구성

ISP 서버에 아래 조건에 따라 Root 인증기관을 설치하여 SSL/TLS통신을 위한 인증서를 제공할 수 있도록 합니다.

| | |
|---|---|
| 인증기관 이름 | Root-CA |
| 인증기관 유형 | Standalone CA |
| Online Certificate Status Protocol | http://ca.msftncsi.com/ocsp |

Cloud01과 Cloud02 서버에 아래 조건에 따라 Intermediate 인증기관을 설치하여 SSL/TLS통신을 위한 인증서를 제공할 수 있도록 하며, 인증기관의 고가용성을 위해 Failover Cluster를 구성합니다. 서비스를 위한 모든 인증서는 해당 서버를 통해 발급합니다.

| | |
|---|---|
| 인증기관 이름 | Right-CA |
| 인증기관 유형 | Enterprise CA |
| Online Certificate Status Protocol | http://ca.right.loc/ocsp |

2) 인증 기관 웹 게시

right.loc 그룹의 사용자는 https://ca.right.loc로 접근하여 인증서를 발급받을 수 있도록 합니다.

## 차. 웹 서비스

1) NCSI 구성

ISP에 NCSI를 위한 웹사이트를 구성하도록 합니다.

2) FTP 구성

Cloud01과 Cloud02 서버에 FTP 사이트를 게시합니다. "ftp.right.loc" URL을 통해 접근하며, "ftpuser" 사용자를 추가하여 서비스를 이용할 수 있도록 합니다.

"ftp.right.loc" 사이트는 부하 분산되어야 하며, FTP 서비스를 위한 저장 공간은 Scale-out File Server를 이용하도록 합니다.

부하 분산 시 Cloud01 서버 접근 시에는 "Cloud01 Server is Running" 메세지가 출력되어야하고, Cloud02 서버에 접근 시에는 "Cloud02 Server is Running" 메세지가 출력되어야 합니다.

## 카. NTP

ISP 서버를 NTP 서버로 사용하여 Right 그룹 호스트의 시간을 동기화 합니다.

## 타. Direct Access

1) Direct Access 구성

Hyper-AD 및 AD 서버에 Direct Access 서비스를 제공합니다.

"CN=Direct Client, OU=RIGHT, DC=RIGHT, DC=LOC" 그룹을 추가한 후 해당 그룹에 포함된 클라이언트들이 DA를 이용할 수 있게 합니다.

Direct Access 연결이름은 "DA Connect"로 설정합니다.

2) Direct Access 연결

지사 연결용으로는 da1 사이트의 da1.right.loc 도메인을 사용하며, 본사 연결용으로 da2 사이트의 da2.right.loc 도메인을 사용합니다.

Direct Access 사용자는 가까운 Direct Access 서버를 이용하여 Direct Access 서비스를 이용하도록 합니다.

3) NLS 구성

https://nls.right.loc를 nls로 사용합니다.

4) 사용자 홈 디렉터리 및 사용자 프로필

Direct Access 연결이 끊어지더라도 사용자 홈 디렉터리 및 사용자 프로필을 정상적으로 사용할 수 있어야합니다.

## 파. NPS

1) RADIUS 구성

AD 서버에 RADIUS 서비스를 구성합니다. AD 서버는 Router의 요청에만 서비스를 제공합니다.

Router 서버에 RADIUS Proxy 서비스를 구성합니다. Router는 모든 요청을 AD 서버에게 전달해야 하며, RADIUS Proxy관련 정책을 제외한 어떠한 정책도 존재하지 않아야 합니다.

2) 정책 구성

AD 서버에 Site-to-Site Secure Tunnel을 위한 정책을 추가합니다.

Site-to-Site Secure Tunnel 연결 시 EAP로 PEAP-MS-CHAPv2만 사용가능 해야 합니다.

## 하. Failover Cluster

1) 클러스터 구성

Cloud01과 Cloud02 서버를 이용하여 “cluster”라는 이름의 Failover Cluster을 운영합니다. 클러스터의 IP는 172.16.0.100을 사용합니다.

클러스터를 위해 Scale-out File Server에 가상 하드 디스크를 추가하도록 합니다.

가상 하드 디스크 이름은 “cluster”를 사용합니다.

Hyper 서버에서 클러스터를 관리할 수 있어야합니다.

2) 인증기관 클러스터

CA라는 이름을 사용하며, 172.16.0.102 IP를 사용합니다.

한 서버가 서비스 불가 상태가 되어도 인증기관 서비스를 정상적으로 이용 가능해야 합니다.

3) 파일서버 클러스터

shared라는 이름을 사용하며, 172.16.0.101 IP를 사용합니다.

home, profile, share 폴더를 폴더의 이름을 공유이름으로 사용하여 공유합니다.

4) 공유폴더

shared 폴더 내에 AE폴더와 KR 폴더 값을 각각 만든 후 User의 Country 값이

폴더 이름과 일치할 경우 해당 폴더가 보이도록 합니다.

(기본적으로 폴더가 보이지 않습니다.)

## 가. Remote Desktop

Hyper 서버의 가상화 호스트를 이용하여 Remote Desktop을 운영합니다.

1) Remote Desktop 구성

Collector 이름으로 “RDC”를 사용하며, 템플릿을 이용하여 가상 호스트를 추가할 수 있도록 합니다.

Domain-users에 소속된 사용자는 Remote-Desktop을 이용할 수 있도록 합니다.

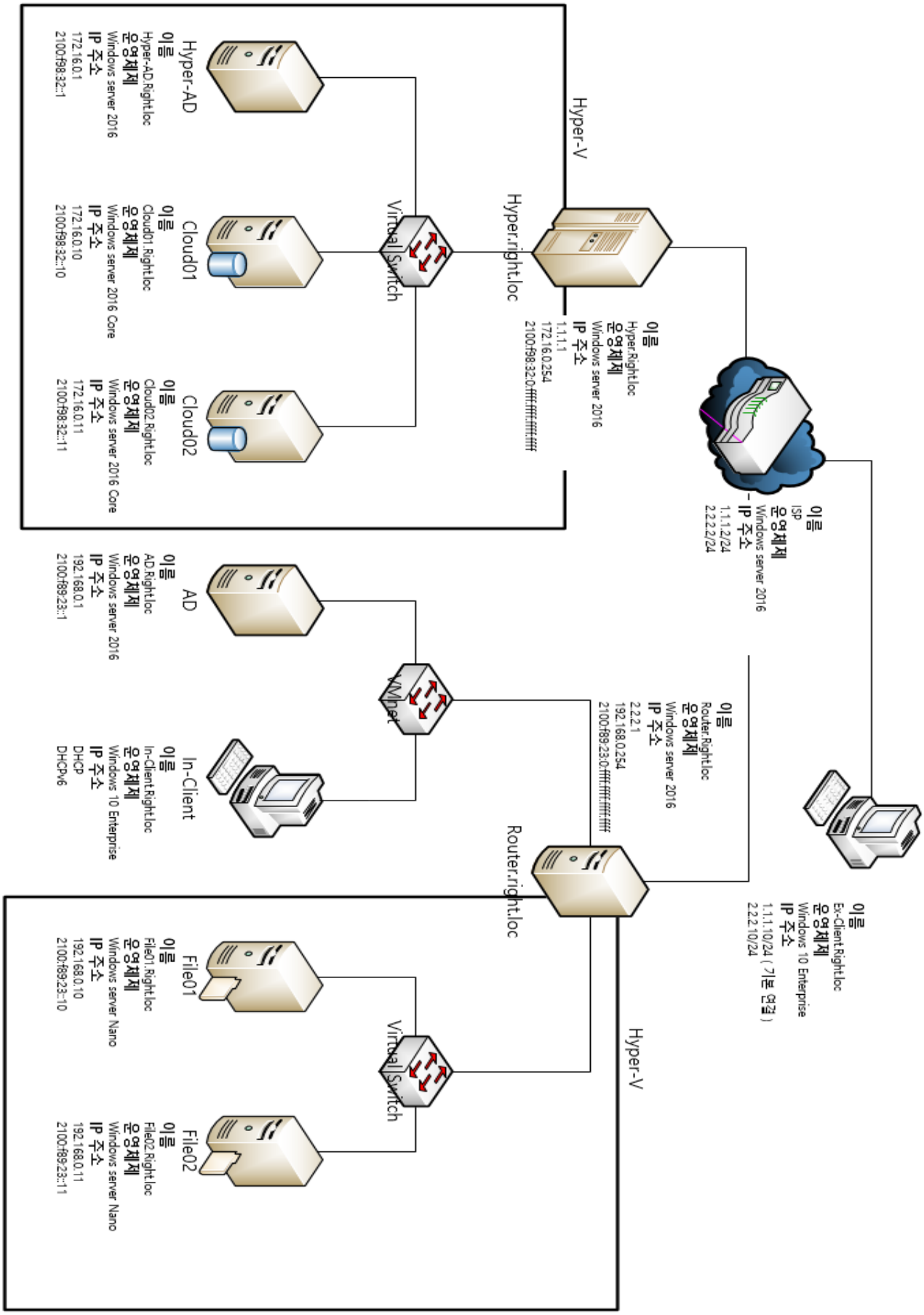
호스트를 여러 사용자가 이용할 수 있게 하며, 자동 롤백되도록 구성합니다.

2) Web Access

https://remote.right.loc을 통해 Remote Desktop Service를 이용할 수 있습니다. 내부에서만 접근하여 사용할 수 있습니다.

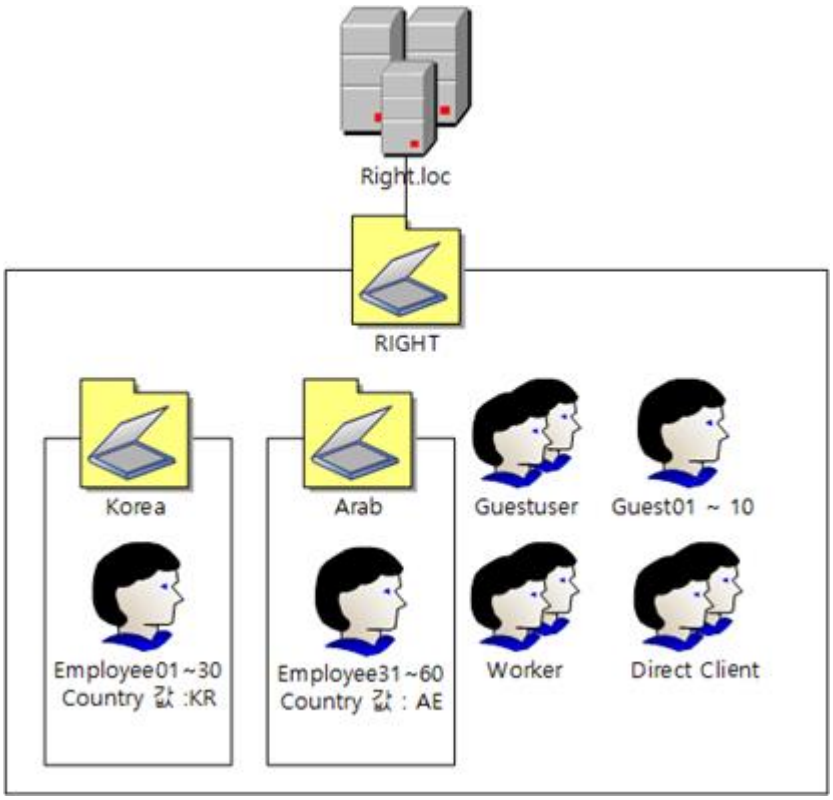
3) Single Sing On

Right.loc의 사용자는 로그온 시 바로 Remote Desktop을 이용할 수 있도록 Single Sign On을 설정합니다.


Hyper-V
Hyper.right.loc
이름
Hyper.Right.loc
운영체제
Windows server 2016
IP 주소
1.1.1.1
172.16.0.254
2100:f98:32:0:ffff:ffff:ffff:ffff
Virtual Switch
Hyper-AD
이름
Hyper-AD.Right.loc
운영체제
Windows server 2016
IP 주소
172.16.0.1
2100:f98:32::1
Cloud01
이름
Cloud01.Right.loc
운영체제
Windows server 2016 Core
IP 주소
172.16.0.10
2100:f98:32::10
Cloud02
이름
Cloud02.Right.loc
운영체제
Windows server 2016 Core
IP 주소
172.16.0.11
2100:f98:32::11
이름
ISP
운영체제
Windows server 2016
IP 주소
1.1.1.2/24
2.2.2.2/24
이름
Ex-Client.Right.loc
운영체제
Windows 10 Enterprise
IP 주소
1.1.1.10/24 ( 기본 연결 )
2.2.2.10/24
이름
Router.Right.loc
운영체제
Windows server 2016
IP 주소
2.2.2.1
192.168.0.254
2100:f89:23:0:ffff:ffff:ffff:ffff
Router.right.loc
VMnet
AD
이름
AD.Right.loc
운영체제
Windows server 2016
IP 주소
192.168.0.1
2100:f89:23::1
In-Client
이름
In-Client.Right.loc
운영체제
Windows 10 Enterprise
IP 주소
DHCP
DHCPv6
Hyper-V
Virtual Switch
File01
이름
File01.Right.loc
운영체제
Windows server Nano
IP 주소
192.168.0.10
2100:f89:23::10
File02
이름
File02.Right.loc
운영체제
Windows server Nano
IP 주소
192.168.0.11
2100:f89:23::11

5-1. 네트워크 구성도

## 5-2. 도메인 구성




| 그룹 | 구성원 |
|---|---|
| Guestuser | Guest01 ~ Guest10 |
| Worker | Employee01 ~ Employee30 |
| | Employee31 ~ Employee60 |

## 5-4. 운영체제 설치

### 가. ISP

| | |
|---|---|
| 컴퓨터이름 | ISP |
| 운영체제 | Windows Server 2016 |
| WorkGroup | ISP-WORK |

### 나. Hyper

| | |
|---|---|
| 컴퓨터이름 | Hyper |
| 운영체제 | Windows Server 2016 |
| 도메인이름 | right.loc |

### 다. Router

| | |
|---|---|
| 컴퓨터이름 | Router |
| 운영체제 | Windows Server 2016 |
| 도메인이름 | right.loc |

### 라. AD

| | |
|---|---|
| 컴퓨터이름 | AD |
| 운영체제 | Windows Server 2016 |
| 도메인이름 | right.loc |

마. Hyper-AD

| 컴퓨터이름 | Hyper-AD |
|---|---|
| 운영체제 | Windows Server 2016 |
| 도메인이름 | right.loc |

바. Cloud01

| 컴퓨터이름 | Cloud01 |
|---|---|
| 운영체제 | Windows Server 2016 Core |
| 도메인이름 | right.loc |

사. Cloud02

| 컴퓨터이름 | Cloud02 |
|---|---|
| 운영체제 | Windows Server 2016 Core |
| 도메인이름 | right.loc |

아. File01

| 컴퓨터이름 | File01 |
|---|---|
| 운영체제 | Windows Server Nano |
| 도메인이름 | right.loc |

자. File02

| 컴퓨터이름 | File02 |
|---|---|
| 운영체제 | Windows Server Nano |
| 도메인이름 | right.loc |

차. In-Client

| 컴퓨터이름 | In-Client |
|---|---|
| 운영체제 | Windows 10 Enterprise K x64 |
| 도메인이름 | right.loc |
| 추가사용자 | Client |

카. Ex-Client

| 컴퓨터이름 | Ex-Client |
|---|---|
| 운영체제 | Windows 10 Enterprise K x64 |
| 도메인이름 | right.loc |
| 추가사용자 | Client |

## 5-5. 네트워크 할당

| 영역 | 네트워크 | 호스트 | IP 주소 |
|---|---|---|---|
| right.loc | 172.16.0.0/24 | Hyper | 172.16.0.254 |
| | | Hyper-AD | 172.16.0.1 |
| | | Cloud01 | 172.16.0.10 |
| | | Cloud02 | 172.16.0.11 |
| | 192.168.0.0/24 | AD | 192.168.0.1 |
| | | In-Client | DHCP |
| | | Router | 192.168.0.254 |
| | | File01 | 192.168.0.10 |
| | | File02 | 192.168.0.11 |
| | 2100:f98:32::/64 | Hyper | 2100:f98:32::ffff:ffff:ffff:ffff |
| | | Hyper-AD | 2100:f98:32::1 |
| | | Cloud01 | 2100:f98:32::10 |
| | | Cloud02 | 2100:f98:32::11 |
| | 2100:f89:23::/64 | AD | 2100:f89:23::1 |
| | | In-Client | DHCP |
| | | Router | 2100:f89:23::ffff:ffff:ffff:ffff |
| | | File01 | 2100:f89:23::10 |
| | | File02 | 2100:f89:23::11 |
| Internet | 1.1.1.0/24 | ISP | 1.1.1.2 |
| | | Hyper | 1.1.1.1 |
| | | Ex-Client | 1.1.1.10 |
| | 2.2.2.0/24 | ISP | 2.2.2.2 |
| | | Router | 2.2.2.1 |
| | | Ex-Client | 2.2.2.10 |