

구름수비대

○ 2025.06 ○

HYBRID CLOUD

“ 네트워크와 서버, AWS를 활용한 클라우드 인프라 구축 ”

팀명 : 구름수비대(CloudGuardians)

팀원 : 김형주, 신예은, 여인수, 최지원

• INDEX

목차



01

개요

02

네트워크

03

서버

04

클라우드

05

결론

01 ➤ 개요

- 프로젝트 개요 및 시나리오
- 팀원 소개 & 역할 분담

01

프로젝트 개요 및 시나리오

프로젝트 개요

- **프로젝트 목적**

가상의 기업 환경을 기반으로 서버, 네트워크, 클라우드 인프라를 직접 설계하고 구축하며, IT 인프라에 대한 실무형 이해와 문제 해결 역량을 향상시키는 것을 목표로 함

- **구현 방향**

- **서버** : 리눅스 환경에서 Web, DB, Log, DNS, DHCP, Proxy 등을 구축하여 시스템 운영 역량을 실습
- **네트워크** : VLAN 기반 망 분리, HSRP, 라우팅 및 Redistribute 구성으로 안정적인 네트워크 환경 구현
- **클라우드** : AWS EKS에서 Kubernetes 기반 Web 서버를 배포하며 클라우드 웹 서비스 운영과 확장성 실습

프로젝트 시나리오 (고객 요청사항)

- **고객사명** : YSCK

- **사업명** : 물류/유통

- **조직 구성**

- 본사(인사부, 마케팅부, 운영부, 서버관리부서)
- 지사1(물류운송팀, 관리팀, 서버관리실)
- 지사2(관리부, Log 감사팀)

- **요청사항**

- 본사와 지사 구분

- 고객 데이터와 업무 데이터를 관리 및 감시할 데이터 센터 구축
- 각 부서별로 사용하는 네트워크 망 분리

01. 개요

02

팀원 소개 & 역할 분담

여인수



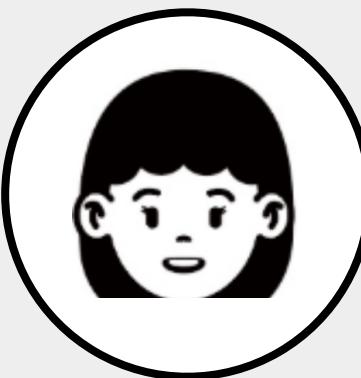
팀장 - 총괄
기획

최지원



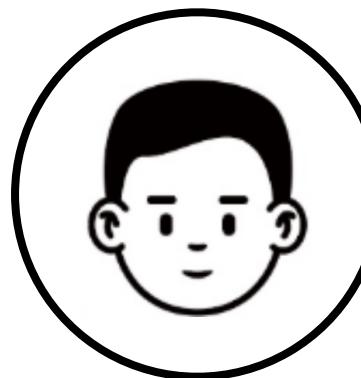
로컬 서버
PPT

신예은



네트워크
보안

김형주



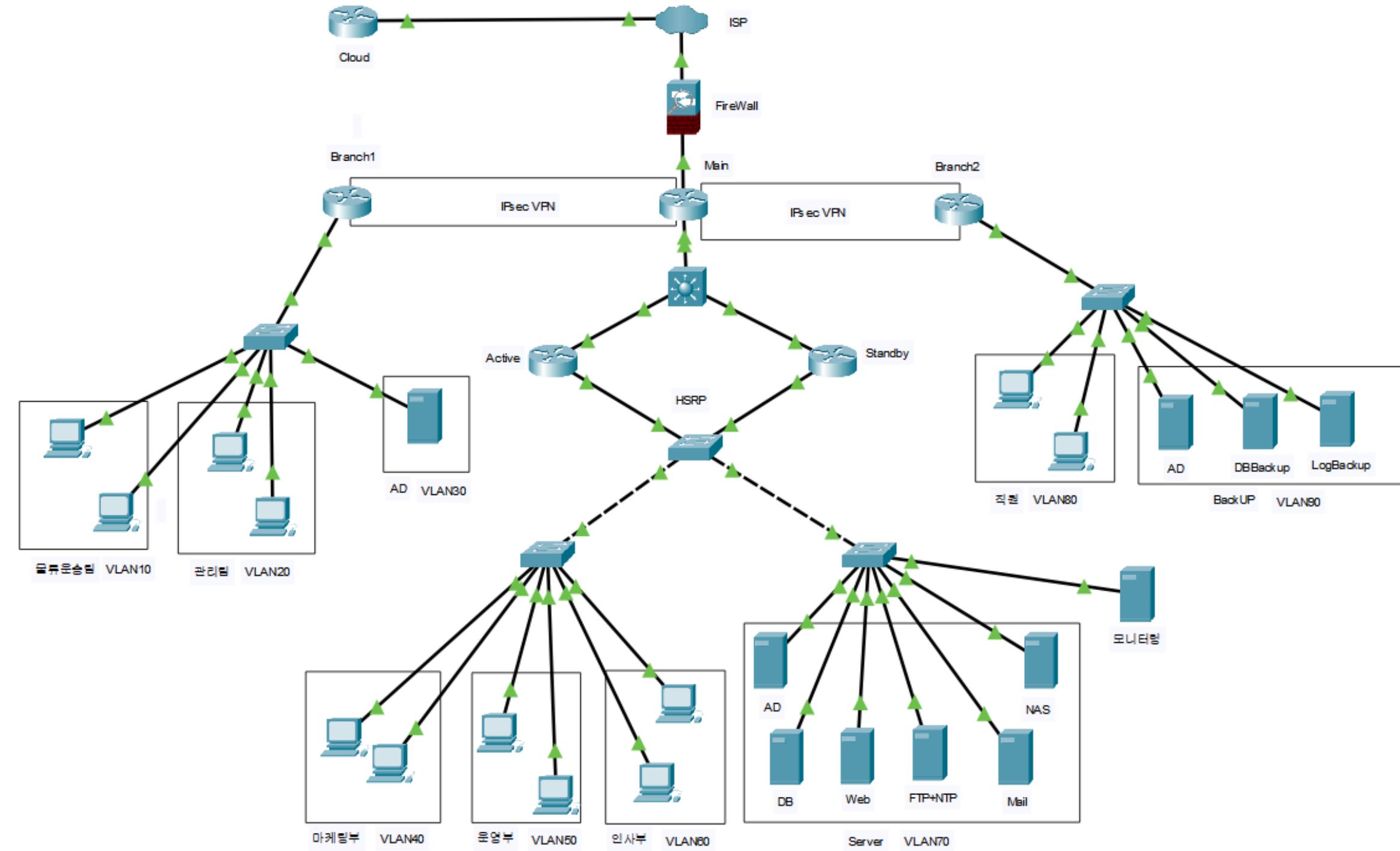
로컬 서버
AWS

02 ➤

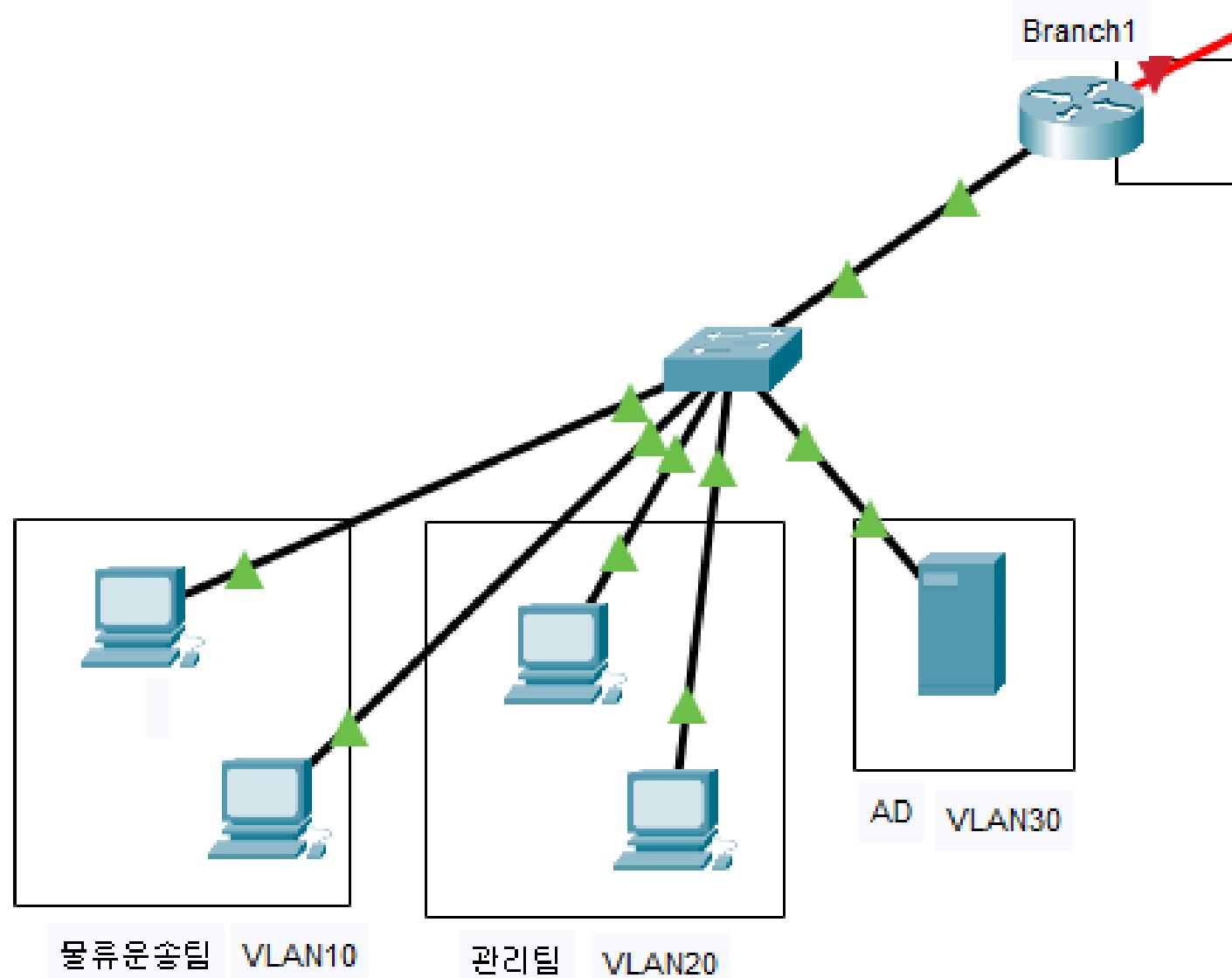
네트워크

- Network Topology
- VLAN
- HSRP
- IPsec VPN

01 Network Topology



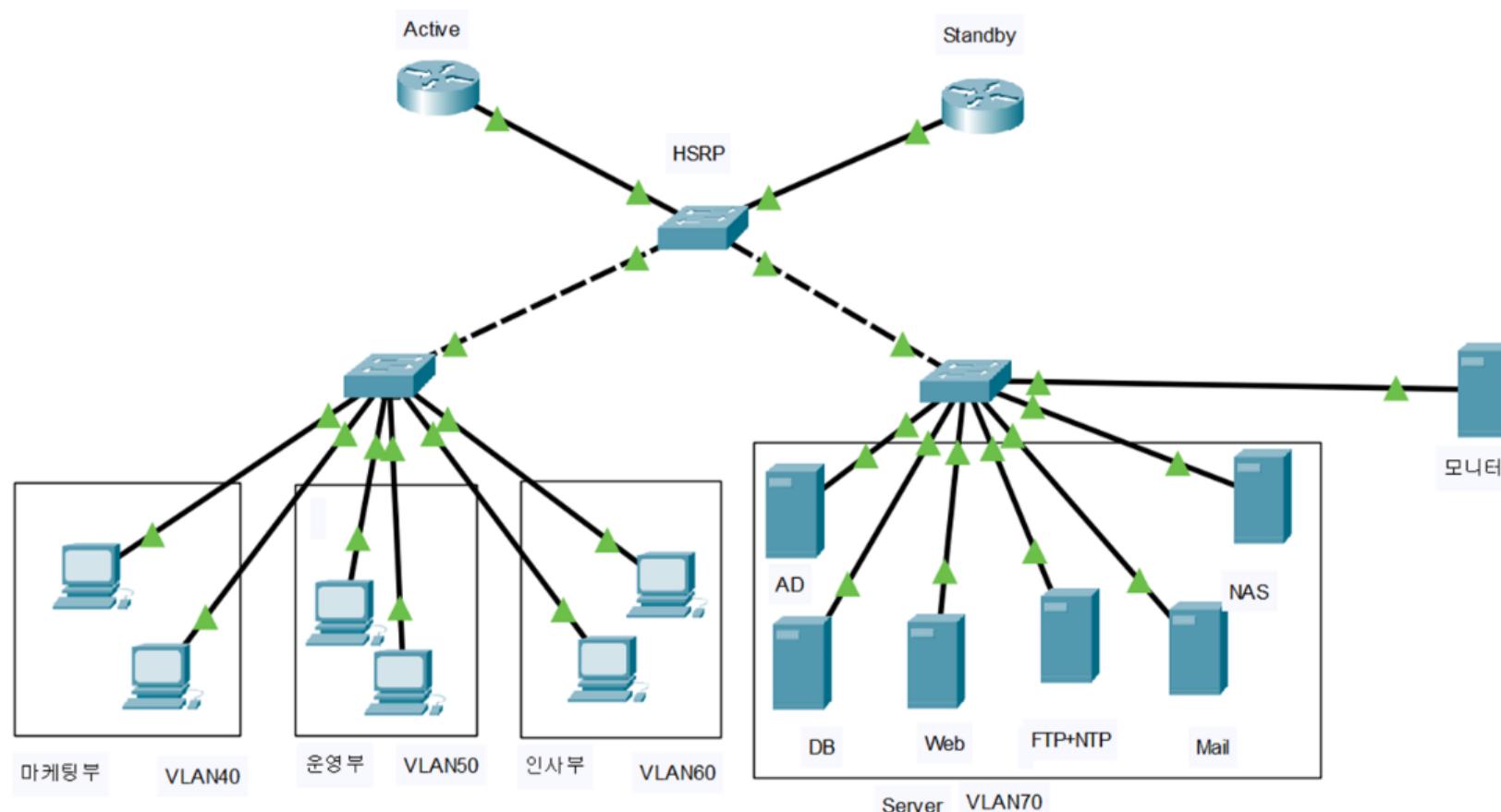
02 VLAN



Switch#sh vlan			
VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig0/1 Gig0/2
10	TRANS	active	Fa0/2, Fa0/3
20	MAN	active	Fa0/4, Fa0/5
30	AD	active	Fa0/6
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

- 부서별로 VLAN10~VLAN90으로 분리하여 보안성과 네트워크 효율성을 높임
- 내부망을 구분하여 서버 접근 제어를 용이하게 하고,
브로드캐스트 트래픽을 최소화해 성능을 최적화함

03 HSRP



● Active

State가 Active이고 우선순위(110)가 높아서 Active 라우터로 동작함.

Router#sh standby br						
P indicates configured to preempt.						
Interface	Grp	Pri	P	State	Active	Standby
Gig	40	110	P	Active	local	192.168.40.2
Gig	50	110	P	Active	local	192.168.50.2
Gig	60	110	P	Active	local	192.168.60.2
Gig	70	110	P	Active	local	192.168.70.2

Virtual IP

192.168.40.254
192.168.50.254
192.168.60.254
192.168.70.254

● Standby

State가 Standby이고 우선순위(100)가 낮아서 대기(Standby) 라우터로 설정됨.

Router#sh standby br						
P indicates configured to preempt.						
Interface	Grp	Pri	P	State	Active	Standby
Gig	40	100	P	Standby	192.168.40.1	local
Gig	50	100	P	Standby	192.168.50.1	local
Gig	60	100	P	Standby	192.168.60.1	local
Gig	70	100	P	Standby	192.168.70.1	local

Virtual IP

192.168.40.254
192.168.50.254
192.168.60.254
192.168.70.254

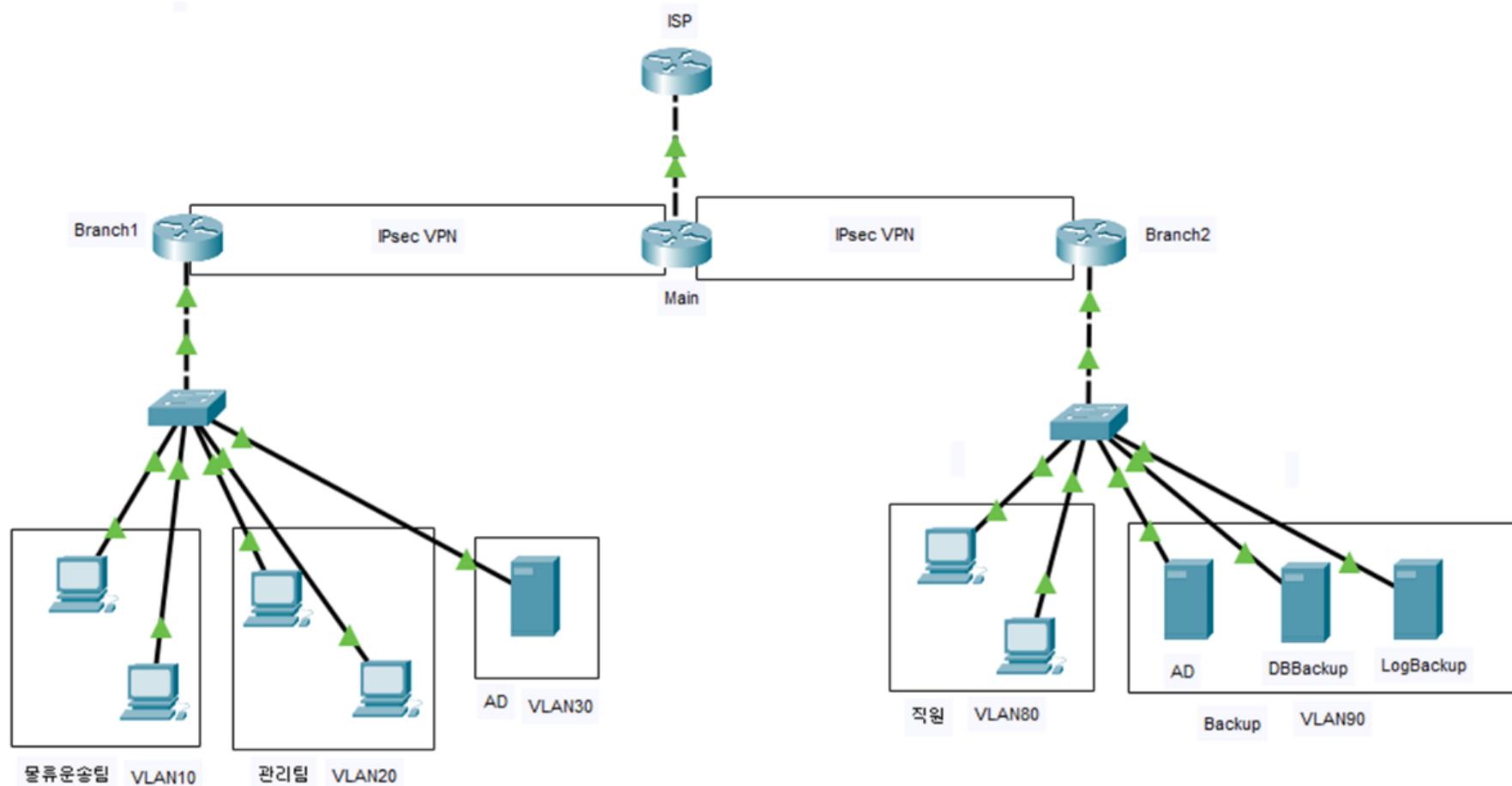
● 가상 gateway

Active Router 의 물리적 주소	ip address 192.168.70.1 255.255.255.0
Active Router의 가상 게이트웨이 주소	standby 1 ip 192.168.70.254
서버의 게이트웨이 주소는 가상 게이트웨이 주소로 설정	IPv4 Address 192.168.70.101 Subnet Mask 255.255.255.0 Default Gateway 192.168.70.254

- Active 장애 시 자동으로 Standby로 전환함
- 장애 발생시 다운타임 없이 지속적으로 운영될 수 있도록 고가용성 제공(High Availability)

04

IPsec VPN



- IPsec VPN을 사용함으로써 VLAN10의 사용자(192.168.10.10)는 원격지 VLAN80(192.168.80.10)과 안전하게 통신할 수 있으며, 중간 경로(IP: 10.10.10.1, 20.20.20.2)를 지나며 암호화된 터널을 통해 데이터가 보호됨
- 데이터 기밀성, 무결성, 송신자 인증을 보장하여 보안성과 안정성이 향상됨

- paul이라는 사용자로 VPN 가입

VPN Configuration

Client IP:

192.168.2.101

- 192.168.10.10이라는 가상 VPN을 정상적으로 할당받았는지 확인

```
Tunnel Interface IP Address.....: 192.168.2.101
```

- VPN 터널을 통해 원격지 간 암호화된 안전한 통신이 이루어지는 것을 보여줌

```
PC>tracert 192.168.80.10
```

```
Tracing route to 192.168.80.10 over a maximum of 30 hops:
```

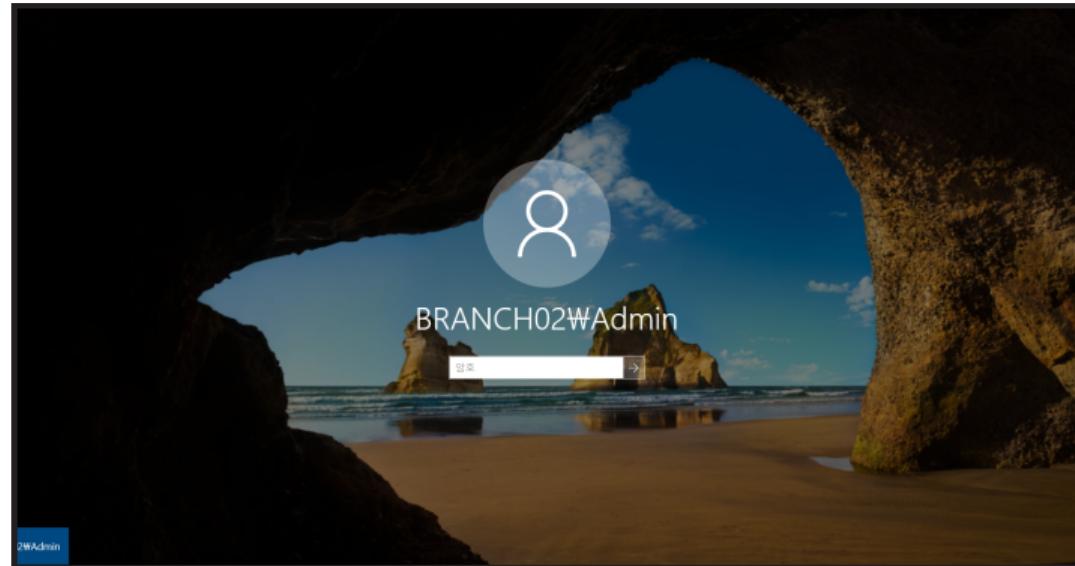
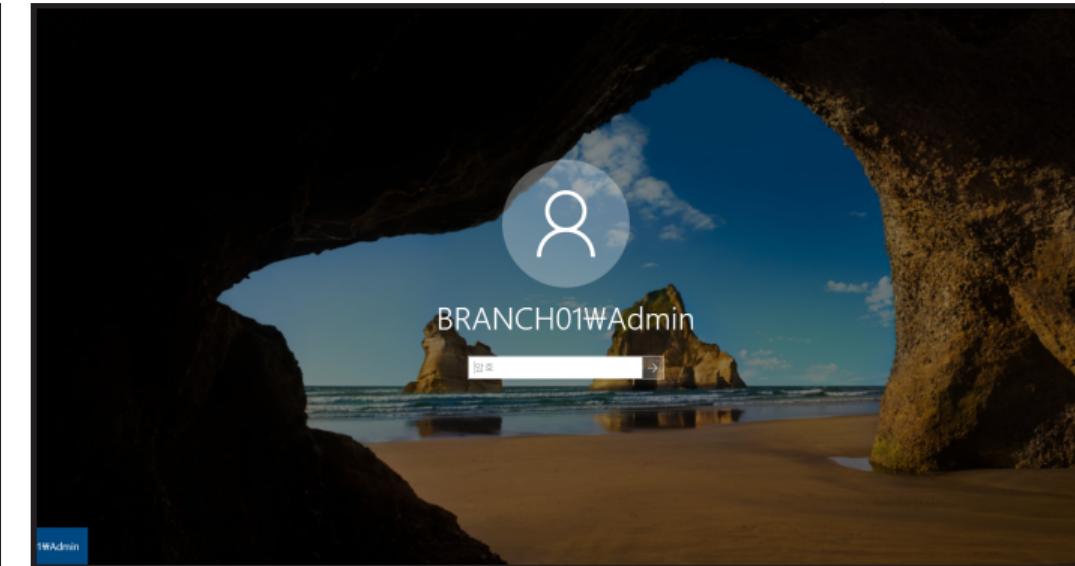
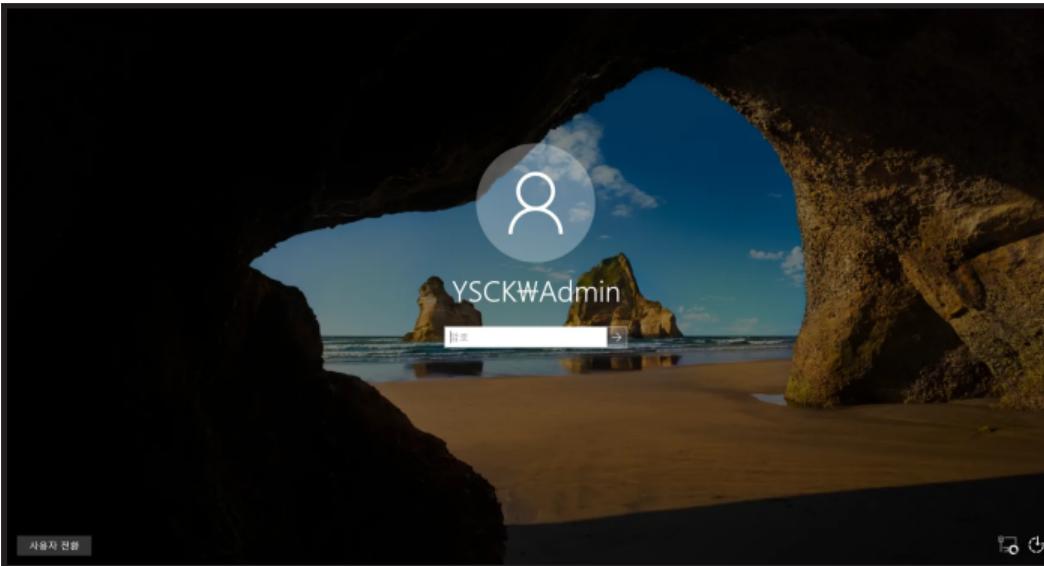
1	0 ms	0 ms	1 ms	192.168.10.254
2	1 ms	0 ms	0 ms	10.10.10.1
3	0 ms	5 ms	1 ms	20.20.20.2
4	1 ms	*	15 ms	192.168.80.10

03> 서버

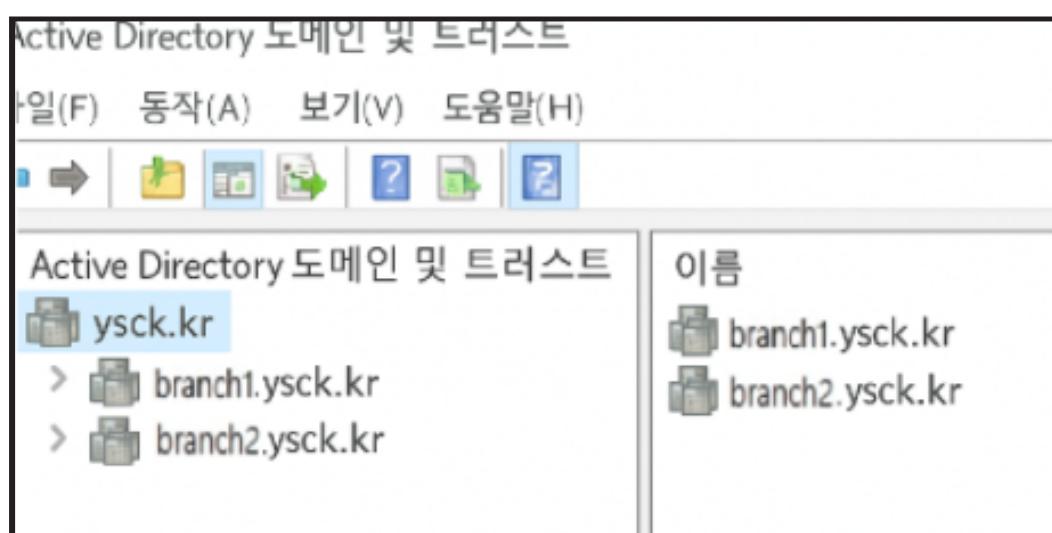
- AD server
- Log server
- NAS server
- MAIL server
- Web server
- DB server
- Bacula backup server
- FTP & NTP
- DNS & DHCP & Proxy

01 AD server

- 도메인 기반 로그인 환경 구성



- Active Directory 도메인 및 트러스트 설정



- AD 서버는 본사에 메인 도메인을 구성하고, 지사 AD 서버는 '기존 도메인에 도메인 컨트롤러 추가' 방식으로 보조 DC로 구성됨
- 이 구조를 통해 각 지사에서도 독립적으로 인증 서비스를 제공하며, 본사와 동일한 도메인 환경 내에서 안정적인 로그인과 정책 적용이 가능함
- 전체 시스템은 도메인 컨트롤러 간 복제를 통해 계정, 권한, 정책을 일관되게 유지하며, 트래픽 분산 및 인증 속도 향상 효과를 제공함

02

Log server

- Log server 정보

Server OS	Ubuntu 18.04
Server IP	192.168.90.93
Client IP	192.168.70.71 (DB)
사용 포트	rsyslog(514), Apache(80)

- rsyslog
: 원격 로그 수집 용도
- 주요 설정 파일
: /etc/rsyslog.comf

- TCP/UDP 로그 수신 활성화 (514번 포트)

```
#####
#### MODULES #####
#####

module(load="imuxsock") # provides support for local system logging
#module(load="immark") # provides --MARK-- message capability

# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")
```

- rsyslog 설정을 통해 로그를 대시보드 템플릿 경로에 저장하여, 시스템 모니터링과 추적이 용이함

- 로그 저장 경로 지정

```
# 원격 로그 저장 템플릿
$template RemoteHost,"/var/log/remote/%HOSTNAME%/syslog.log"
$template RemoteHostAuth,"/var/log/remote/%HOSTNAME%/secure.log"
$template RemoteHostNormalized,"/var/log/remote/%HOSTNAME:::secpath-replace%syslog.log"
$template RemoteHostAuthNormalized,"/var/log/remote/%HOSTNAME:::secpath-replace%secure.log"

#####
#### RULES #####
#####

# 원격 호스트에서 온 로그 처리
if $fromhost-ip != '127.0.0.1' then {
    # CentOS의 인증 관련 로그 (authpriv facility 사용)
    authpriv.*                                ?RemoteHostAuth
    # Ubuntu의 인증 관련 로그 (auth facility 사용)
    auth.*                                     ?RemoteHostAuth
    # 기타 모든 로그
    *.*                                         ?RemoteHost
    # 원격 로그는 로컬 로그 파일에 중복 저장하지 않음
    stop
}
```

- Apache2를 이용한 간단한 로그 확인용 대시보드 제작 후 Kali에서 DB서버에 ssh 접속 시도
(고의로 비밀번호 한 번 틀리고 접속)

- 고의로 비밀번호 1회 틀린 후 접속

```
[root@kali]# ssh root@192.168.70.71
root@192.168.70.71's password:
Permission denied, please try again.
root@192.168.70.71's password:
Last failed login: Wed Jun 18 17:31:35 KST 2025 from 192.168.70.128 on ssh:notty
There was 1 failed login attempt since the last successful login.
Last login: Wed Jun 18 17:23:49 2025 from 192.168.70.128
```

- 원격 서버 : /var/log/secur에 로그가 저장됨

```
[root@dbserver centos1]# sudo tail -10 /var/log/secur
Jun 18 17:31:32 dbserver sshd[3456]: Connection from 192.168.70.128 port 34484 on 192.168.70.71 port 2
Jun 18 17:31:33 dbserver unix_chkpwd[3458]: password check failed for user (root)
Jun 18 17:31:33 dbserver sshd[3456]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=
Jun 18 17:31:33 dbserver sshd[3456]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by u
Jun 18 17:31:35 dbserver sshd[3456]: Failed password for root from 192.168.70.128 port 34484 ssh2
Jun 18 17:31:40 dbserver sshd[3456]: Accepted password for root from 192.168.70.128 port 34484 ssh2
Jun 18 17:31:40 dbserver sshd[3456]: pam_unix(sshd:session): session opened for user root by (uid=0)
Jun 18 17:31:40 dbserver sshd[3456]: Starting session: shell on pts/1 for root from 192.168.70.128 por
Jun 18 17:37:10 dbserver sudo:    root : TTY=pts/0 ; PWD=/home/centos1 ; USER=root ; COMMAND=/bin/tail
Jun 18 17:37:10 dbserver sudo: pam_unix(sudo:session): session opened for user root by centos1(uid=0)
```

- 로그 서버 : 원격 서버의 SSH 인증 로그 확인

SSH 인증 로그 (secure.log)

```
Jun 18 17:31:32 dbserver sshd[3456]: Connection from 192.168.70.128 port 34484 on 192.168.70.71 port 22
Jun 18 17:31:28 dbserver systemd-logind: Removed session 4.
Jun 18 17:31:33 dbserver sshd[3456]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=ss
Jun 18 17:31:33 dbserver sshd[3456]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "roo
Jun 18 17:31:35 dbserver sshd[3456]: Failed password for root from 192.168.70.128 port 34484 ssh2
Jun 18 17:31:40 dbserver sshd[3456]: Accepted password for root from 192.168.70.128 port 34484 ssh2
Jun 18 17:31:40 dbserver systemd-logind: New session 6 of user root.
Jun 18 17:31:40 dbserver pam_unix(sshd:session): session opened for user root by (uid=0)
```

- 원격 서버 (192.168.70.71)
로그를 기록할 대상 서버

- 로그 서버 (192.168.90.93)
로그가 저장되는 서버

03

NAS server

- NAS server 정보

Server OS	Rocky Linux 8
IP	192.168.70.203
사용 포트	445(SMB), 139(NetBIOS), 2049(NFS)

- 부서 그룹별로 공유 폴더 생성 후 권한(770) 부여
- 개인 별로 공유 폴더 생성 후 권한(700) 부여
- 사용자를 만들고 각 부서 그룹에 추가하면, 해당 사용자는 부서 공유 폴더에 접근 가능

```
[root@nas ~]# tree /nas
/nas
  ├── public
  └── shared
      ├── backup
      ├── development
      ├── documents
      ├── management
      ├── media
      ├── readonly
      ├── sales
      └── software
  └── users
      ├── developer
      │   └── manager
      └── sales
14 directories, 0 files
```

부서별(또는 일반) 공유 디렉터리

개인 공유 디렉터리

/etc/samba/smb.conf

[global] 섹션: 전역 설정

```
[global]
workgroup = WORKGROUP
server string = Rocky NAS Server
netbios name = ROCKY-NAS
security = user
map to guest = bad user
dns proxy = no

# 네트워크 설정
interfaces = 192.168.70.203/24
bind interfaces only = yes
hosts allow = 192.168.70. 127.0.0.1

# 로그 설정
log file = /var/log/samba/log.%m
max log size = 1000

# 성능 최적화
socket options = TCP_NODELAY IPTOS_LOWDELAY
read raw = yes
write raw = yes
```

공유 섹션: 각 공유 폴더별 설정

```
# 매니저 공유
[management]
comment = Management Share
path = /nas/shared/management
valid users = @managers
browseable = yes
writable = yes
create mask = 0660
directory mask = 0770

# 개발자 공유
[development]
comment = Development Share
path = /nas/shared/development
valid users = @developers
browseable = yes
writable = yes
create mask = 0660
directory mask = 0770

# 영업부 공유
[sales]
comment = sales man Share
path = /nas/shared/sales
valid users = @sales
```

/etc/exports

공유 디렉토리 네트워크 대역

옵션

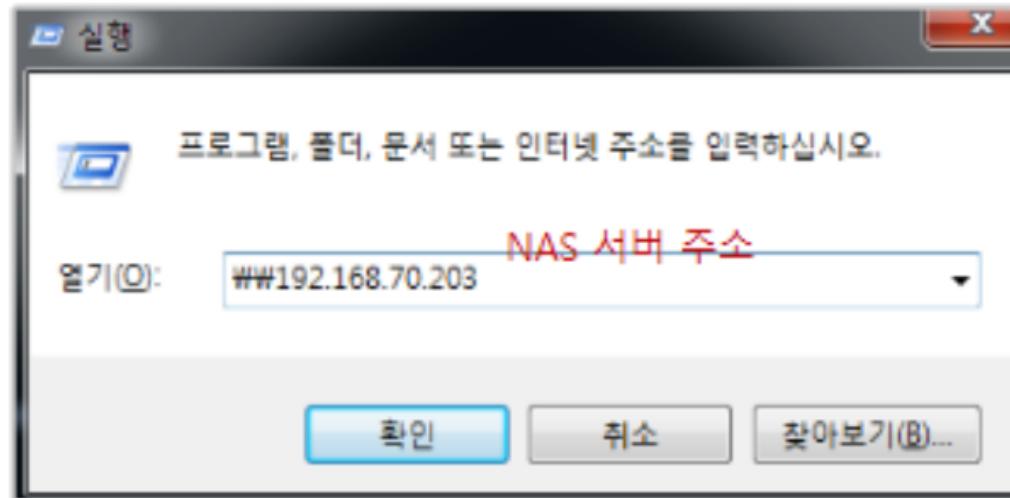
/nas/shared	192.168.70.0/24	rw, sync, no_root_squash, no_subtree_check
/nas/public	192.168.70.0/24	rw, sync, no_root_squash, no_subtree_check
~		

옵션 설명

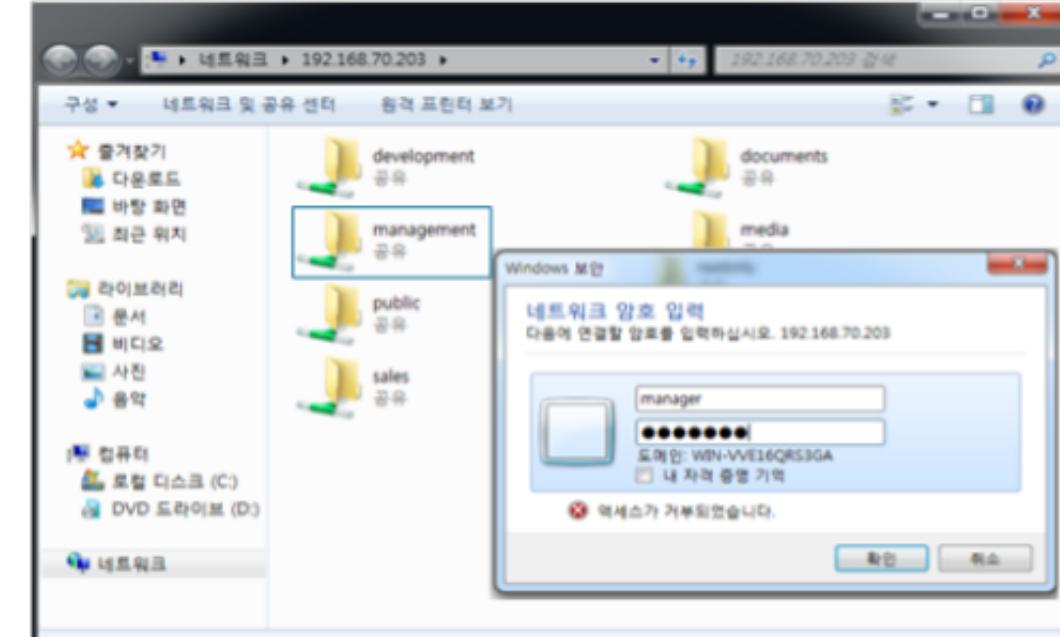
rw : 읽기/쓰기 권한
sync : 동기 쓰기 모드(데이터가 디스크에 완전히 쓰여진 후 응답 반환)
no_root_squash : 클라이언트의 root 사용자를 서버의 root로 맵핑
no_subtree_check : 서브트리 검사 비활성화

03. Server

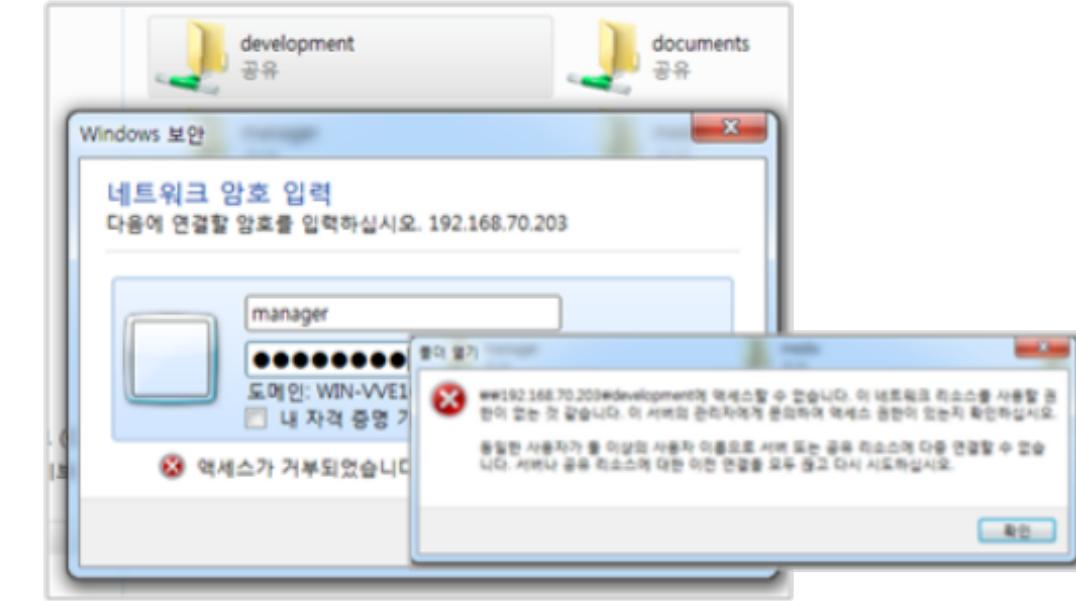
• Windows와 Linux에서 테스트



1. NAS server 접속



2. 자신의 부서 공유 폴더 접근



3. 다른 부서에 접근 시도(막힘)

```
root@ubuntu1:/home/ubuntu1# smbclient //192.168.70.203/shared -U developer
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\developer's password:
Try "help" to get a list of possible commands.
smb: \>
smb: \> ls
.
..
documents
media
backup
software
management
development
sales
readonly
D      0  Wed Jun  4 17:15:31 2025
D      0  Wed Jun  4 17:15:31 2025
D      0  Wed Jun  4 16:27:38 2025
D      0  Wed Jun  4 17:11:03 2025
D      0  Wed Jun  4 17:15:31 2025
```

1. Developer 사용자가 Smbclient로 접속

```
smb: \> cd sales\
smb: \sales\> ls
NT_STATUS_ACCESS_DENIED listing \sales\*
```

2. 다른 부서 접근 시도 → ACCESS_DENIED

```
smb: \sales\> cd ../development\
smb: \development\> ls
.
..
requirements.txt
D      0  Wed Jun  4 18:58:37 2025
D      0  Wed Jun  4 17:15:31 2025
A      13  Wed Jun  4 17:35:57 2025
5231616 blocks of size 1024. 5161972 blocks available
smb: \development\>
smb: \development\> get requirements.txt /home/ubuntu1/Downloads/requirement
getting file \development\requirements.txt of size 13 as /home/ubuntu1/Down
```

3. development 부서 이동 후 파일 다운로드

04

Mail server

- NAS server 정보

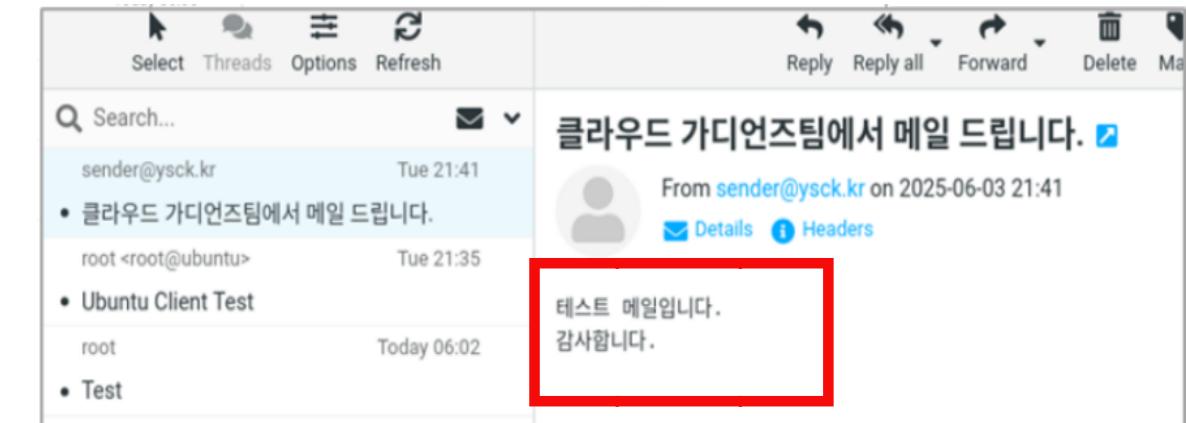
Server OS	Rocky Linux 8
Server IP	192.168.70.172
사용 포트	SMTP(25), IMAP(143), Apache(80) 등
호스트명	mail.ysck.kr

- 사용 프로그램



- 내부 직원과 원격지 지점(Branch1, Branch2) 간의 메일 송수신을
증가하는 역할을 함
- 오픈소스 웹 메일 프로그램(Roundcube)을 통해 메일을 주고 받을 수 있음

- GUI 환경에서 메일 송수신 테스트



1. 메일 발송

메일 발송 폼

보내는 사람:

받는 사람:

제목:

내용:

감사합니다.

메일 발송 폼

✓ 메일이 성공적으로 발송되었습니다!
보내는 사람:

받는 사람:

2. 메일 확인

05 Web server

- Web server 정보

Server OS	Ubuntu 18.04
Server IP	192.168.70.66
사용 포트	Apache(80), AJP(8009), Tomcat(8080)

- 외부 요청 처리

Web 서버는 사용자의 요청에 따라서 내부 리소스를 제공해주는 역할을 수행함

- 정적·동적 콘텐츠 분리 처리

Apache는 정적 콘텐츠(HTML, 이미지 등), Tomcat은 JSP 등 동적 콘텐츠를 처리함

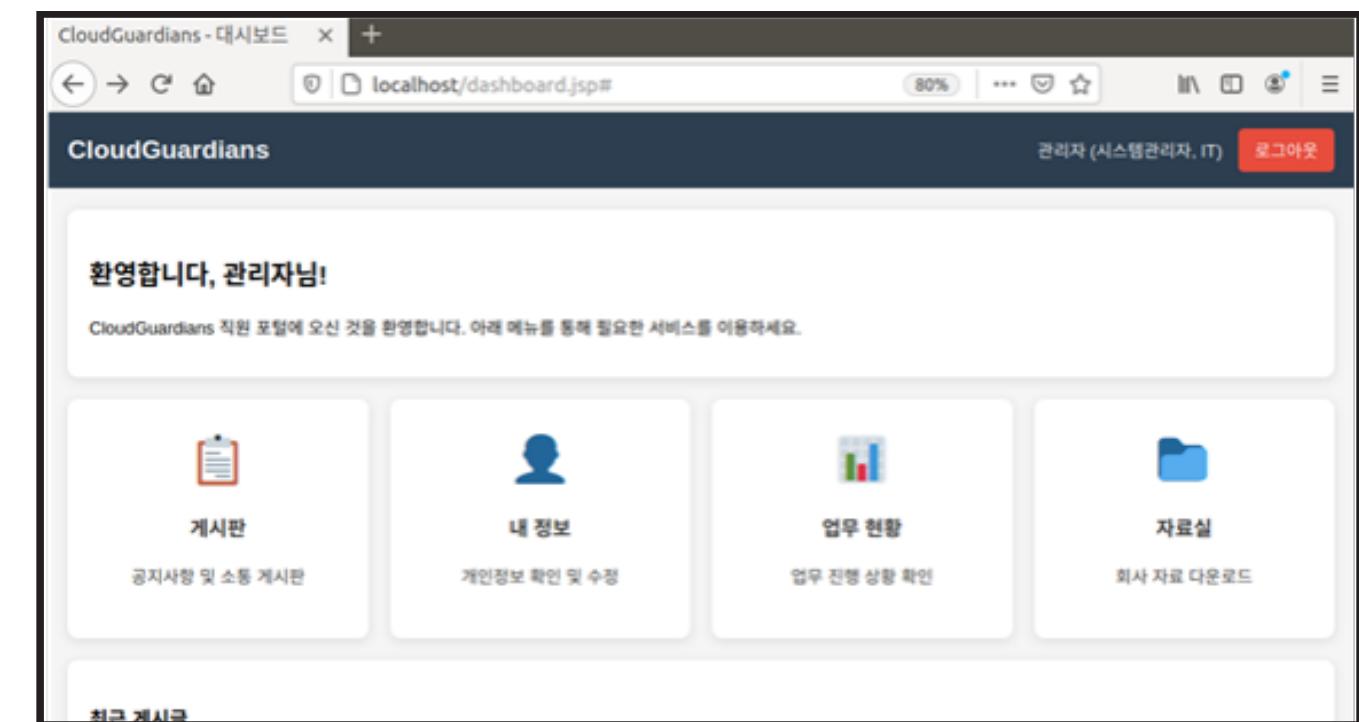
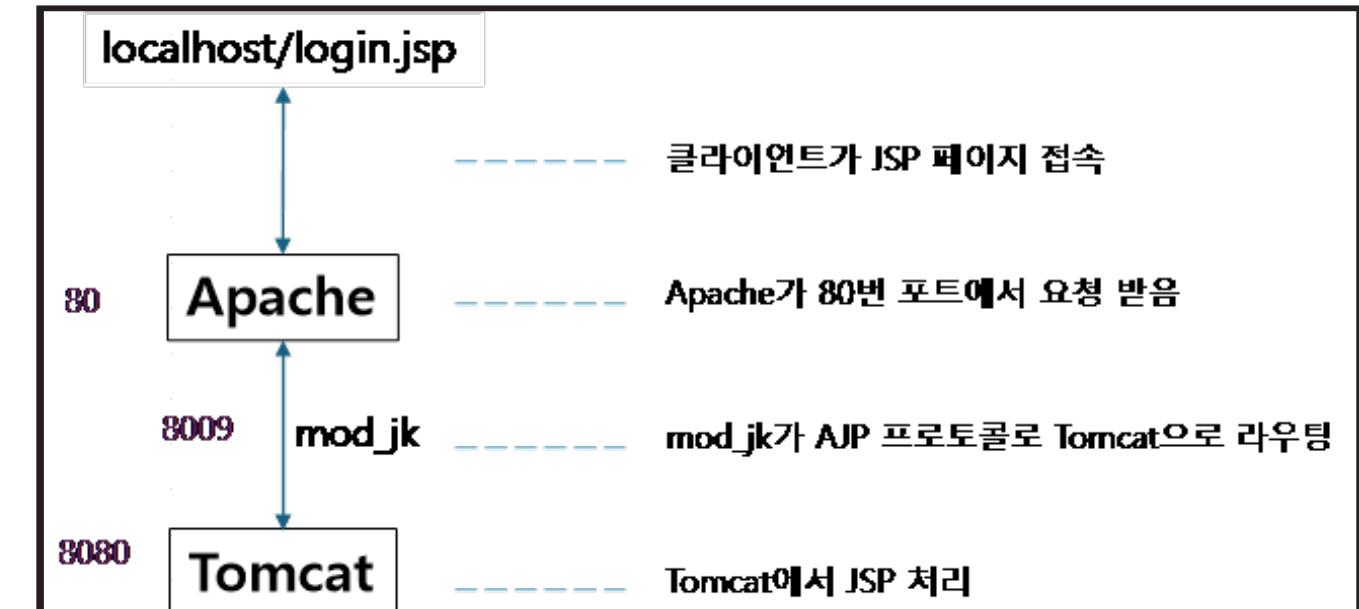
- Apache와 Tomcat 간 연동

mod_jk와 AJP 프로토콜을 사용해 Apache와 Tomcat 간 효율적인 연동을 함으로써

개발자들의 웹서비스 처리 기반을 마련함

- 내부 시스템 연동 및 인증

직원 로그인, 게시판 등의 내부 시스템과 연결되며, 인증 기능을 통해 사용자 접근을 제어함



03. Server

● 로그인 및 직원 게시판

직원은 웹 페이지에서 로그인 후 게시판을 통해 글을 작성하고 조회할 수 있으며, 사용자 정보는 내부 DB와 연동됨. 이 기능은 인증 기반으로 동작하여 구성원 간 정보 공유와 접근 제어를 동시에 수행함

The image displays four screenshots of the CloudGuardians web application:

- Login Page:** A browser window showing the URL `localhost/login.jsp`. It contains fields for 'Username' (admin) and 'Password' (*****), and a blue 'Login' button.
- Employee List:** A table view of employee data. The columns are: A-Z username, A-Z password, A-Z name, A-Z email, A-Z department, and A-Z position. The data includes:

A-Z username	A-Z password	A-Z name	A-Z email	A-Z department	A-Z position
admin	admin	관리자	admin@clouddguardians. IT	IT	시스템관리자
rocky	pwrocky	테스터	tester@clouddguardians. IT	IT	개발자
guardian	user123	테스터	jane.smith@clouddguardians. HR	HR	인사담당자
- Post Creation Page:** A form titled '게시글 작성' (Post Creation). It has fields for '작성자' (admin), '제목' (신입사원 환영), and '내용' (새로 입사한 직원들을 환영합니다!). The entire form area is highlighted with a red box.
- Post List:** A browser window showing the URL `localhost/board.jsp`. It lists three posts in a table:

번호	제목	작성자	작성일	조회
3	신입사원 환영	admin	2025-06-04 13:42:17.0	0
1	CloudGuardians 포털 오픈	admin	2025-06-04 10:42:53.0	1
2	시스템 점검 안내	admin	2025-06-04 10:43:53.0	0

06 DB server

- DB server 정보

Server OS	CentOS7
Server IP	192.168.70.71
사용 포트	mariadb(3306)

- Bacula, Web 등 다른 ip에서 접근을 허용하기 위해 nano /etc/my.cnf에서 bind-address 설정 변경

```
[mysqld]
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
bind-address = 0.0.0.0
port = 3306
log-bin = mysql-bin
server-id = 1
```

127.0.0.1 → 로컬 접속만 허용
0.0.0.0 → 외부 IP에서 접속 허용

- 이후 web, bacula에 필요한 사용자 및 데이터베이스 생성

- CentOS7 기반 MariaDB 서버로, 포트 3306을 통해 외부 접근을 허용하도록 설정
- Web, Bacula 백업 서버가 접근할 수 있도록 bind-address를 0.0.0.0으로 설정
- 필요한 사용자 계정 및 데이터베이스를 사전에 생성하여 연동 준비 완료

```
MariaDB [(none)]> SELECT User, Host FROM mysql.user;
+-----+-----+
| User   | Host    |
+-----+-----+
| root   | 127.0.0.1
| webuser | 192.168.70.%
| backup_user | 192.168.70.96
| bacula  | 192.168.70.96
| root   | ::1
| root   | localhost
+-----+-----+
6 rows in set (0.00 sec)
```

사용자

```
MariaDB [(none)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| information_schema |
| bacula |
| log4j_demo |
| mysql |
| performance_schema |
| testdb |
+-----+
6 rows in set (0.00 sec)
```

데이터베이스

07

Bacula backup server

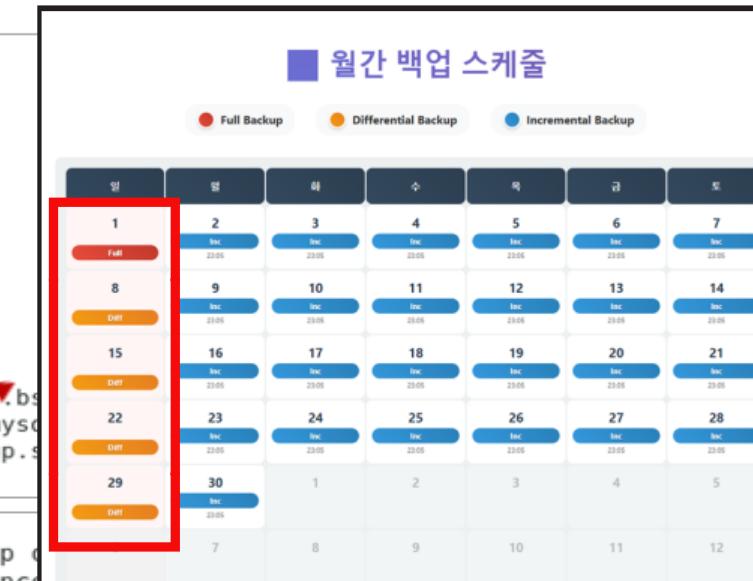
- Bacula 백업/복원 서버

Server OS	Ubuntu 18.04
Server IP	192.168.90.96 (Bacula)
Client IP	192.168.70.71 (DB)
사용 포트	Bacula Daemon(9101), Storage Daemon(9103), File Daemon(9102)

- Backup과 Restore에 대한 Job 정의

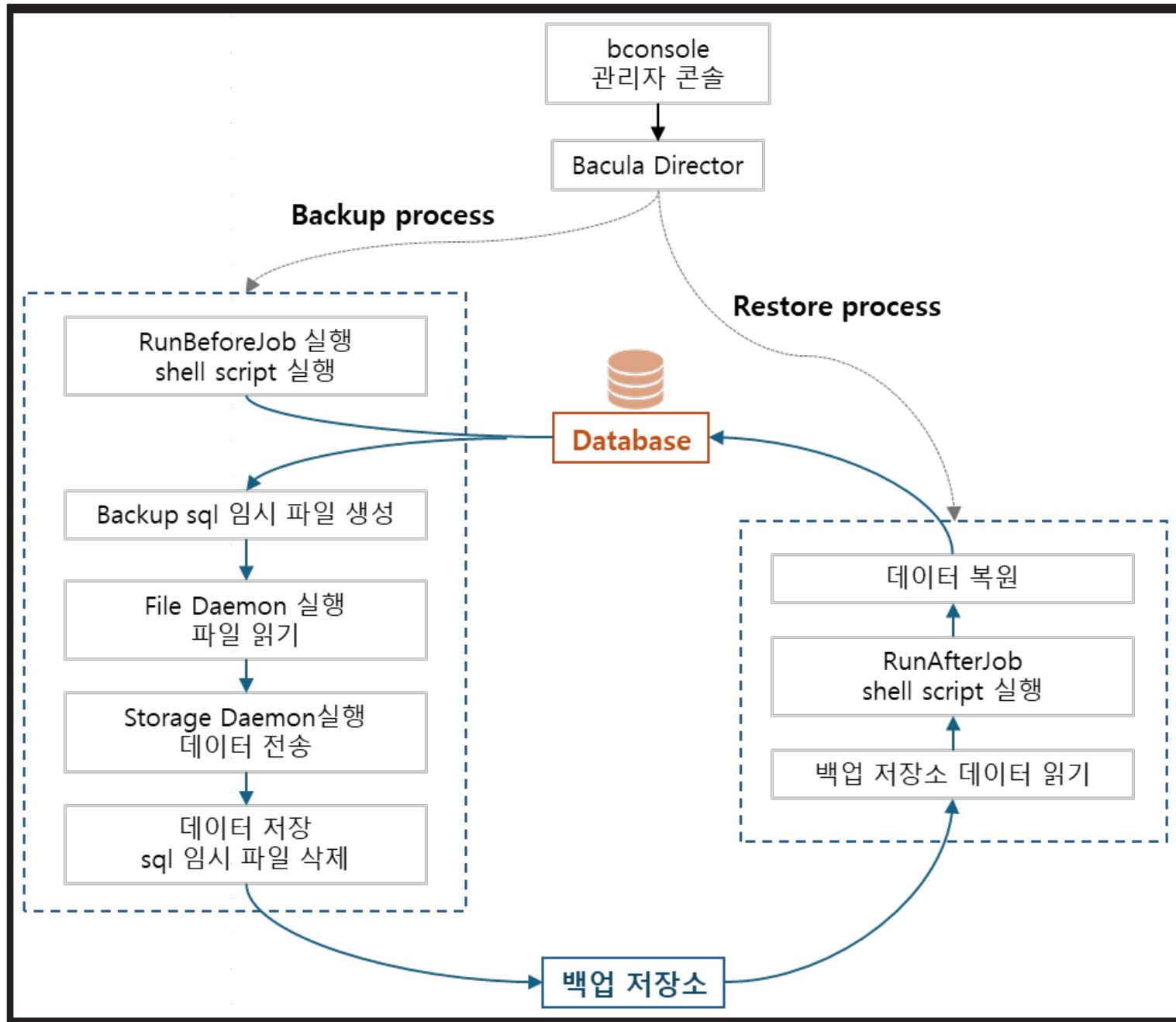
```
# MySQL 백업용 Job 정의 추가
Job {
  Name = "MySQL-Backup"
  Type = Backup
  Level = Full
  Client = bacula-fd
  FileSet = "MySQL-FileSet"
  Schedule = "WeeklyCycle"
  Storage = FileStorage
  Messages = Standard
  Pool = File
  SpoolAttributes = yes
  Priority = 10
  Write Bootstrap = "/var/lib/bacula/%.bs"
  RunBeforeJob = "/opt/bacula/scripts/mysql_start.sh"
  RunAfterJob = "rm -f /tmp/mysql_backup.sql"
}

#
# When to do the backups, full backup on
# differential (i.e. incremental since)
# and incremental backups other days
Schedule {
  Name = "WeeklyCycle"
  Run = Full 1st sun at 23:05
  Run = Differential 2nd-5th sun at 23:05
  Run = Incremental mon-sat at 23:05
}
```



매월 첫째주 일요일 Full backup
그 다음주 일요일부터는 Differential backup
월-토 23:05에 Incremental backup 진행

- Bacula 백업/복구 전체 구조도



03. Server

● 백업 / 복원 테스트

1. 기존 데이터 확인

A-Z username	A-Z password	A-Z email	A-Z role
admin	\$2a\$10\$N.zmdr9k7uOCQb376NoUnuTj8iAt6Z5EHsM	admin@example.com	ADMIN
user1	\$2a\$10\$N.zmdr9k7uOCQb376NoUnuTj8iAt6Z5EHsM	user1@example.com	USER
user2	\$2a\$10\$N.zmdr9k7uOCQb376NoUnuTj8iAt6Z5EHsM	user2@example.com	USER
user3	\$2a\$10\$N.zmdr9k7uOCQb376NoUnuTj8iAt6Z5EHsM	user3@example.com	USER
user4	\$2a\$10\$N.zmdr9k7uOCQb376NoUnuTj8iAt6Z5EHsM	user4@example.com	USER
user5	\$2a\$10\$N.zmdr9k7uOCQb376NoUnuTj8iAt6Z5EHsM	user5@example.com	USER
user6	\$2a\$10\$N.zmdr9k7uOCQb376NoUnuTj8iAt6Z5EHsM	user6@example.com	USER
user7	\$2a\$10\$N.zmdr9k7uOCQb376NoUnuTj8iAt6Z5EHsM	user7@example.com	USER

2. DB 데이터 백업 진행

```
1000 OK: 103 bacula-dir Version: 9.0.6 (20 November 2017)
Enter a period to cancel a command.
*run job=MySQL-Backup
Using Catalog "MyCatalog"
Run Backup job
JobName: MySQL-Backup
Level: Full
Client: bacula-fd
FileSet: MySQL-FileSet
Pool: File (From Job resource)
Storage: FileStorage (From Job resource)
When: 2025-06-01 07:00:09
Priority: 10
OK to run? (yes/mod/no): yes
Job queued. JobId=26
*■
```

3. 데이터 일부 삭제

QL expression to filter results (use Ctrl+Space)			
A-Z username	A-Z password	A-Z email	A-Z role
admin	\$2a\$10\$N.zmdr9k7uOCQb376NoUnuTj8iAt6Z5EHsM	admin@example.com	ADMIN
user1	\$2a\$10\$N.zmdr9k7uOCQb376NoUnuTj8iAt6Z5EHsM	user1@example.com	USER

4. 데이터 복원 진행

```
*restore
First you select one or more JobIds that contain files
to be restored. You will be presented several methods
of specifying the JobIds. Then you will be allowed to
select which files from those JobIds are to be restored.

To select the JobIds, you have the following choices:
  1: List last 20 Jobs run
  2: List Jobs where a given File is saved
  3: Enter list of comma separated JobIds to select
  4: Enter SQL list command
  5: Select the most recent backup for a client
 cwd is: /
$ mark *
1 file marked.
$ done
Bootstrap records written to /var/lib/bacula/bacula-dir.restore.2.bsr

The Job will require the following (*=>InChanger):
  Volume(s)          Storage(s)          SD Device(s)
=====
  Vol-0001           FileStorage        FileChgr1-Dev1

Volumes marked with "*" are in the Autochanger.

1 file selected to be restored.

The defined Restore Job resources are:
  1: RestoreFiles
  2: MySQL-Restore
Select Restore Job (1-2): 1
Run Restore job
```

5. 데이터 복원 확인

A-Z username	A-Z password	A-Z email	A-Z role
admin	\$2a\$10\$N.zmdr9k7uOCQb376NoUnuTj8iAt6Z5EHsM	admin@example.com	ADMIN
user1	\$2a\$10\$N.zmdr9k7uOCQb376NoUnuTj8iAt6Z5EHsM	user1@example.com	USER
user2	\$2a\$10\$N.zmdr9k7uOCQb376NoUnuTj8iAt6Z5EHsM	user2@example.com	ADMIN
user3	\$2a\$10\$N.zmdr9k7uOCQb376NoUnuTj8iAt6Z5EHsM	user3@example.com	USER
user4	\$2a\$10\$N.zmdr9k7uOCQb376NoUnuTj8iAt6Z5EHsM	user4@example.com	ADMIN
user5	\$2a\$10\$N.zmdr9k7uOCQb376NoUnuTj8iAt6Z5EHsM	user5@example.com	USER
user6	\$2a\$10\$N.zmdr9k7uOCQb376NoUnuTj8iAt6Z5EHsM	user6@example.com	ADMIN
user7	\$2a\$10\$N.zmdr9k7uOCQb376NoUnuTj8iAt6Z5EHsM	user7@example.com	USER

08

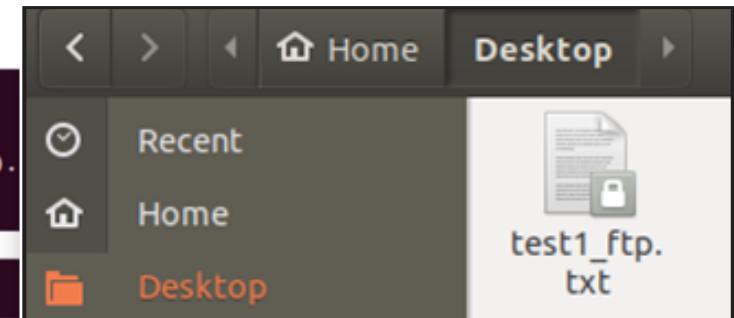
FTP & NTP

● FTP

```
# When "listen" directive is enabled, vsftpd runs in standalone mode and
# listens on IPv4 sockets. This directive cannot be used in conjunction
# with the listen_ipv6 directive.
listen=YES
```

FTP 서버에서 IPv4 접속을 허용

```
root@ubuntu:/home/ubuntu# ftp 192.168.70.101
ftp> get Desktop/test1.txt Desktop/test1_ftp.txt
local: Desktop/test1_ftp.txt remote: Desktop/test1.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for Desktop/test1.txt (205558 bytes).
226 Transfer complete.
205558 bytes received in 0.01 secs (18.7648 MB/s)
ftp> !ls Desktop/
test1_ftp.txt
ftp>
```



Ubuntu Client에서 서버의 "test1_ftp.txt" 파일을 get 명령어로 가져옴

● NTP

```
server kr.pool.ntp.org iburst
server ntp.kornet.net iburst
server ntp.bora.net iburst
```

NTP패키지는 chrony로 사용

서버는 kr.pool.ntp.org 외 2곳에서 시간데이터를 가져옴

```
root@ubuntu:/home/ubuntu# chronyc sources -v
210 Number of sources = 1
MS Name/IP address          Stratum Poll Reach LastRx Last sample
===== ====== ====== ====== ====== ====== ====== ====== ======
^* www.ysck.kr               3      6    377    55 +136us[ -63us] +/- 6481us
```

Ubuntu Client에서 시간데이터 소스를 가져올 서버의 주소를 확인

```
Allow NTP client access from local network.
allow 192.168.10.0/24
```

서비스를 허용할 네트워크 대역대를 지정

```
root@ubuntu:/home/ubuntu# timedatectl
Local time: 목 2025-06-05 15:29:24 KST
Universal time: 목 2025-06-05 06:29:24 UTC
RTC time: 목 2025-06-05 15:29:24
Time zone: Asia/Seoul (KST, +0900)
```

chrony 서버에서 UTC기준으로 시간데이터를 가져온 후,
Client의 Time zone 정보(Asia/Seoul)에 따라서
시간데이터를 KST로 변환하여 Client에게 표시해줌

09

DNS & DHCP & Proxy

● DNS

```
$TTL 86400
@ IN SOA centos.ysck.kr. admin.ysck.kr. (
    0001 ; Serial
    3600 ; Refresh
    1800 ; Retry
    604800 ; Expire
    86400 ; Minimum TTL
)

@ IN NS centos.ysck.kr.
centos IN A 192.168.70.101
www IN A 192.168.70.101
ftp IN A 192.168.70.102
```

/var/named/fwd.ysck.kr 정방향 DNS Zone 설정

```
ubuntu@ubuntu:~$ nslookup google.com www.ysck.kr
Server:      www.ysck.kr
Address:     192.168.70.101#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.206.238
Name:   google.com
Address: 2404:6800:400a:804::200e
```

www.ysck.kr로 dns query를 보내면
192.168.70.101에서 query response를 응답

● DHCP

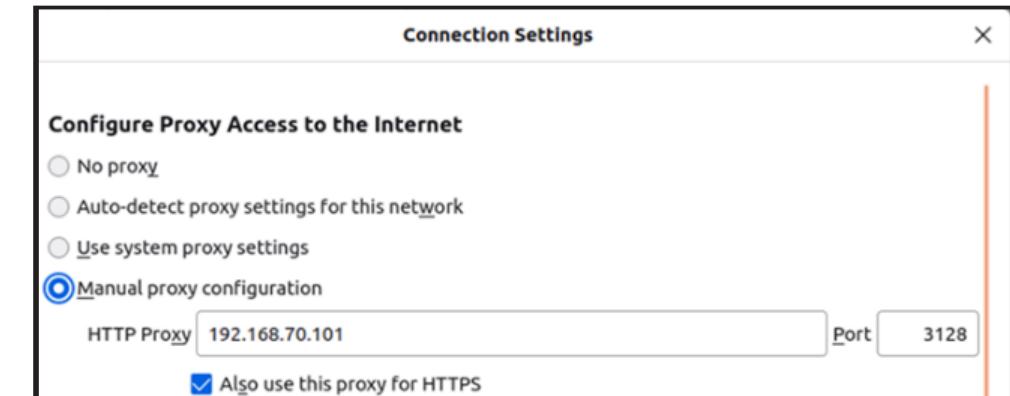
```
# DHCP Server Configuration file.
# see /usr/share/doc/dhcp*/dhcpd.conf.example
# see dhcpd.conf(5) man page
#
subnet 192.168.10.0 netmask 255.255.255.0 {
    range 192.168.10.10 192.168.10.100;
    option subnet-mask 255.255.255.0;
    option routers 192.168.10.254;
    option broadcast-address 192.168.10.255;
    option domain-name-servers 192.168.70.101;
    default-lease-time 6000;
}
```

192.168.10.10부터 192.168.10.100 까지
총 91개 주소를 임대해줄 수 있도록 설정

```
lease 192.168.10.10 {
    starts 2 2025/06/03 13:57:40;
    ends 2 2025/06/03 15:37:40;
    cltt 2 2025/06/03 13:57:40;
    binding state active;
    next binding state free;
    rewind binding state free;
    hardware ethernet 00:0c:29:48:f2:35;
    client-hostname "ubuntu";
}
```

/var/lib/dhcpd/dhcpd.leases에서 IP주소 임대 이력을 확인

● Proxy



Ubuntu Client에서 Proxy 설정



proxy 서버로부터 Ubuntu Client에 서비스됨

192.168.10.10 TCP MISS/302 1234 GET http://www.google.com/ - HIER DIRECT/142.250.198.164 text/html

/var/log/squid/access.log에서 서비스 해준 이력 확인

04>

클라우드

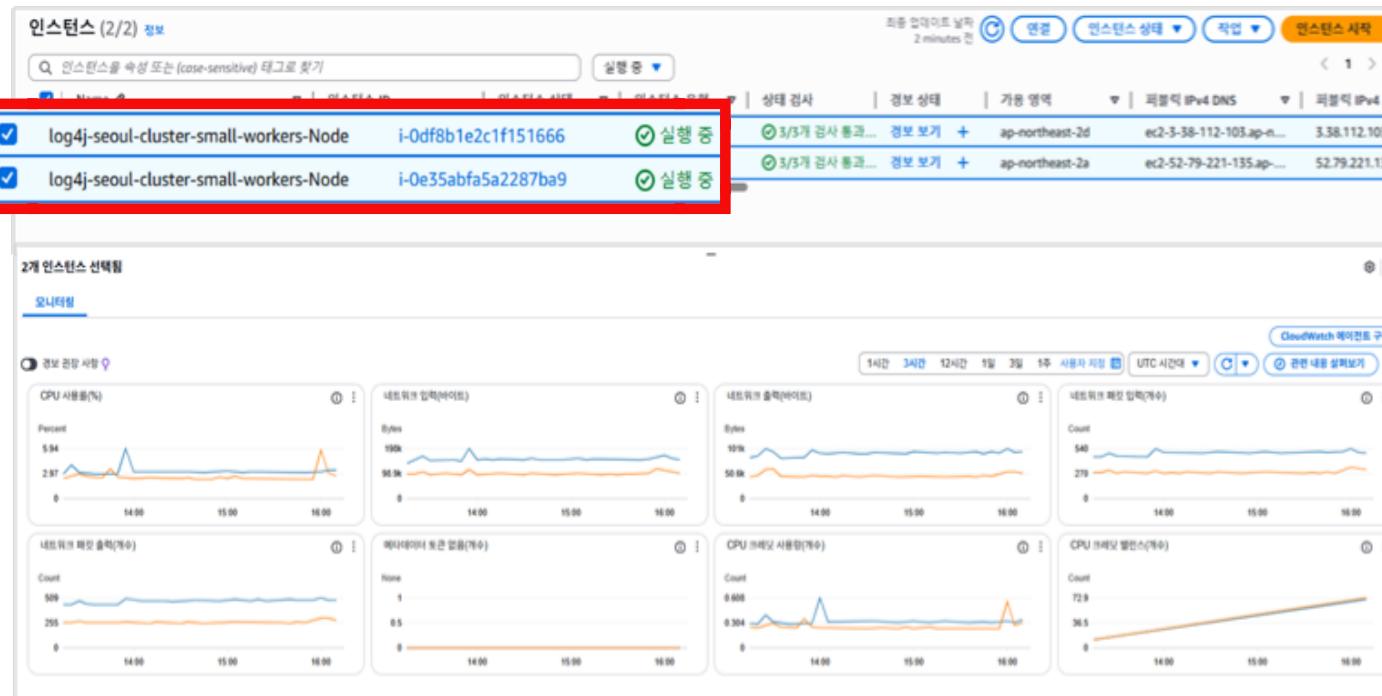
- AWS

01 AWS

- eksctl로 클러스터 생성

```
ubuntu1@guardians:~/EKS$ eksctl create cluster \
>   --name log4j-seoul-cluster \
>   --version 1.29 \
>   --region ap-northeast-2 \
Seoul 리전에서 생성
>   --nodegroup-name small-workers \
비용과 pod 제한을 고려하여 t3.small 타입 사용
>   --node-type t3.small \
>   --nodes-min 1 \
>   --nodes-max 3 \
>   --nodes 2 \
worker 인스턴스 2개 생성
>   --managed
```

- 생성된 인스턴스



- yaml파일로 배포

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: log4j-app
  namespace: log4j-demo
  labels:
    app: log4j-web
    version: v1
spec:
  replicas: 3
  selector:
    matchLabels:
      app: log4j-web
  template:
    metadata:
      labels:
        app: log4j-web
        version: v1
```

Replicas는 3으로 설정하여 고가용성 테스트

- 생성된 pods

```
ubuntu1@guardians:~/EKS$ kubectl get pod -o wide -n log4j-demo
NAME                               READY   STATUS    RESTARTS   AGE     NODE
log4j-app-7765f985d6-d74pv       1/1    Running   0          9m52s   ip-192-168-56-135.ap-northeast-2.compute.internal
log4j-app-7765f985d6-mqwbb       1/1    Running   0          9m52s   ip-192-168-15-89.ap-northeast-2.compute.internal
log4j-app-7765f985d6-pwxrv       1/1    Running   0          9m52s   ip-192-168-56-135.ap-northeast-2.compute.internal
```

ip-192-168-56-135.* 인스턴스에서 2개의 pod가 생성 되었으며,
ip-192-168-15-89.* 인스턴스에서 1개의 pod가 생성됨

04. Cloud

● 최종 배포 결과: 실시간 물류 관리 시스템

www.ysck.kr 로 접속시 나오는 웹페이지

The screenshot shows the homepage of the 'Cloud-GUARDIANS!' real-time logistics management system. The URL in the browser is https://www.ysck.kr. The top navigation bar includes links for 대시보드 (Dashboard), 입고관리 (Inbound Management), 출고관리 (Outbound Management), 재고조회 (Inventory Inquiry), 배송추적 (Delivery Tracking), 시스템관리 (System Management), and 로그인 (Login). A yellow banner at the top left reads '▲ Log4j 취약점 실효성을 위한 테스트 페이지' (▲ Test page for Log4j vulnerability effectiveness). The main title '통합물류관리시스템' (Integrated Logistics Management System) is displayed prominently. Below it, a sub-header says '실시간 물류 현황 모니터링 및 효율적인 재고 관리' (Real-time logistics status monitoring and efficient inventory management). On the left, a red box labeled '보안 상태' (Security Status) indicates that the Log4j vulnerability has been mitigated. To the right, there is a search bar for '보안 점검' (Security check). Four key metrics are displayed in cards: '1,234' (오늘 입고) with a download icon, '897' (오늘 출고) with an upload icon, '156' (대기 중) with a clock icon, and '23' (보안 이벤트) with an exclamation mark icon. Below these, a chart titled '물류 현황' (Logistics Status) shows '오늘의 물류 현황' (Today's logistics status) with two lines: a teal line for '입고' (Inbound) and a red line for '출고' (Outbound). The final section on the right is titled '빠른 작업' (Quick Work) with four buttons: '+ 입고 등록' (+ Inbound Registration), '🔍 재고 검색' (🔍 Inventory Search), '🚚 배송 조회' (🚚 Delivery Inquiry), and '✿ 취약점 실효성' (✿ Vulnerability Effectiveness).

05 ➔ 결론

- 프로젝트 성과 및 의의

01

프로젝트 성과 및 의의

“ 통합 인프라 설계 및 운영 경험 ”

- 본 프로젝트는 가상환경 상에서 서버, 네트워크, 클라우드 환경을 설계하고 구축해볼 수 있었음.
- VLAN 망 분리, HSRP 게이트웨이 이중화, AWS EKS 상의 컨테이너 배포 등 실제 인프라와 유사한 환경을 실습함
- 구축 과정에서 역할 분담과 협업을 통해 문제 해결 능력과 시스템 운영의 중요성을 체감함
- 결과적으로 인프라를 구성하는 다양한 기술들을 하나의 시스템으로 연결해보는 의미 있는 실습이었으며, 실무에 가까운 감각과 팀워크의 중요성을 확인할 수 있는 경험을 함

구름수비대

Thank you