Linux 명령어

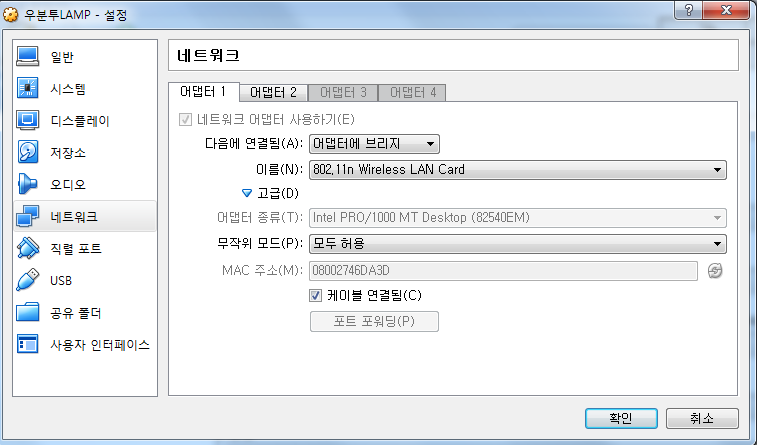
**Ubuntu server Tip**

1. 가상호스팅을 받은 우분투 서버를 보면, 글자가 영어임에도 불구하고 다이아몬드로 깨지는 현상이 발생합니다. 이런 경우 export LANG=C라고 명령어를 준 다음부터는 잘 나오지만 부팅을 다시 하면 또 다시 깨지게 된다. 이럴 경우 nano ~/.bashrc 하여 가장 마지막 줄에 export LANG=C를 추가하고 저장하면 깨짐 현상을 해결 할 수 있다.

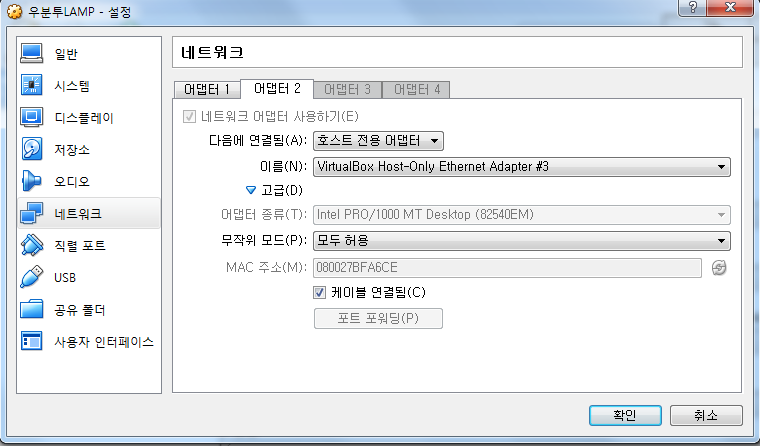
2. 콘솔에서 화면 scroll : shift + page up

3. Network방식을 변경하다 보면 network설정에서 많은 시간을 소요함 이럴 경우 network 아이콘 오른쪽 마우스버튼 네트워크 어댑터설정

4. virtual box

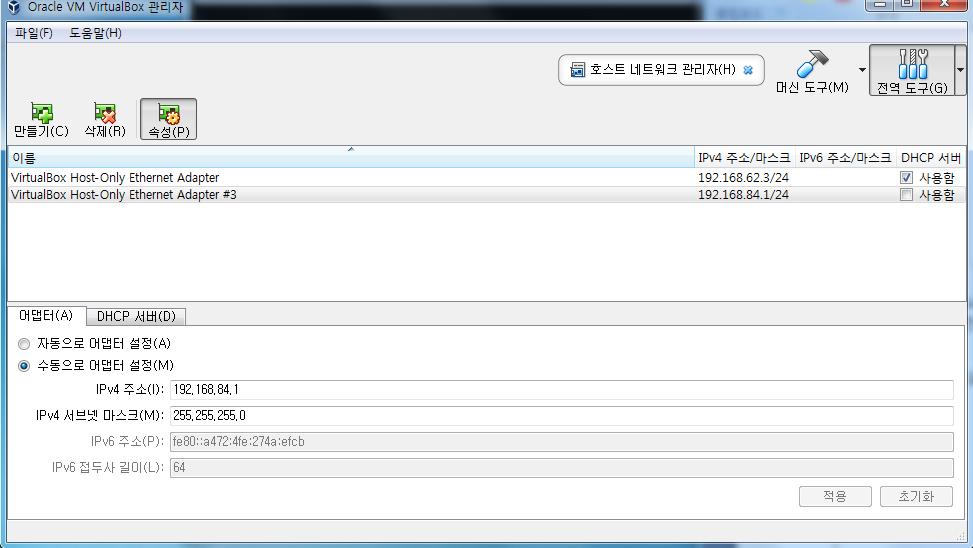


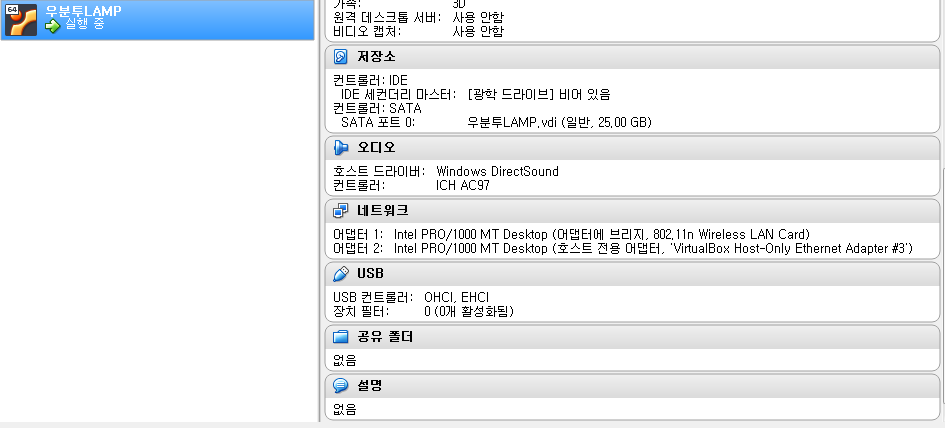
Adapter1 은 wireless로



adapter2는 host 전용으로

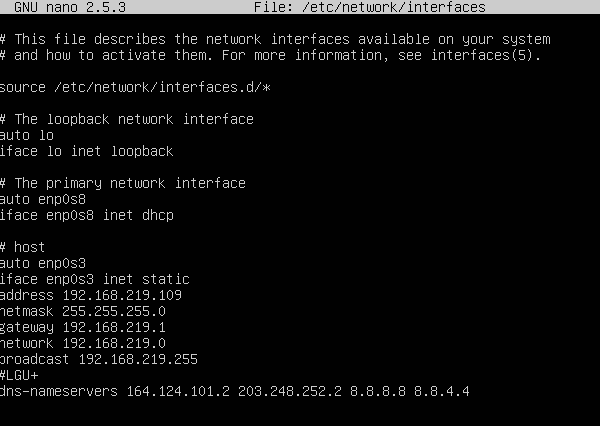
Virtual box의 전역도구에서 만들기 선택

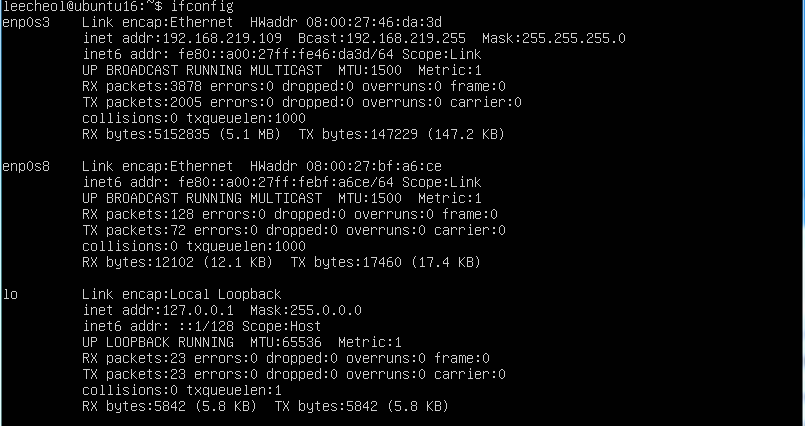


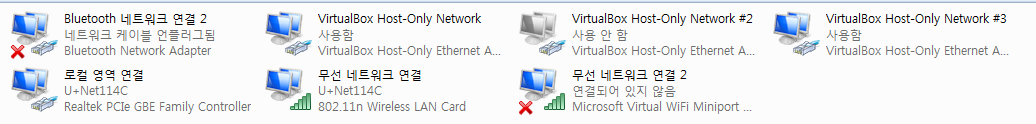


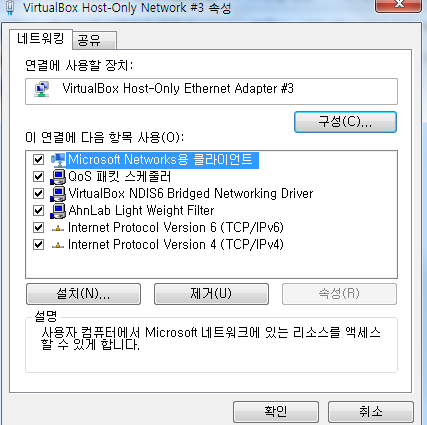
우분투 시작

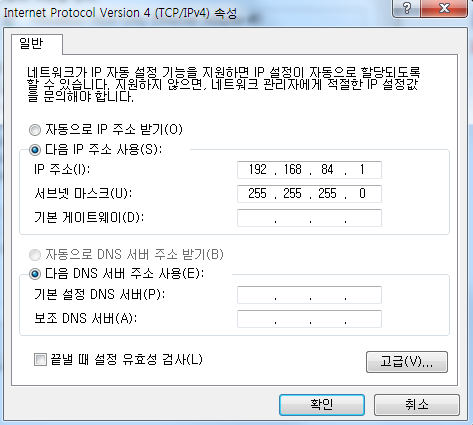
sudo nano /etc/network/interfaces

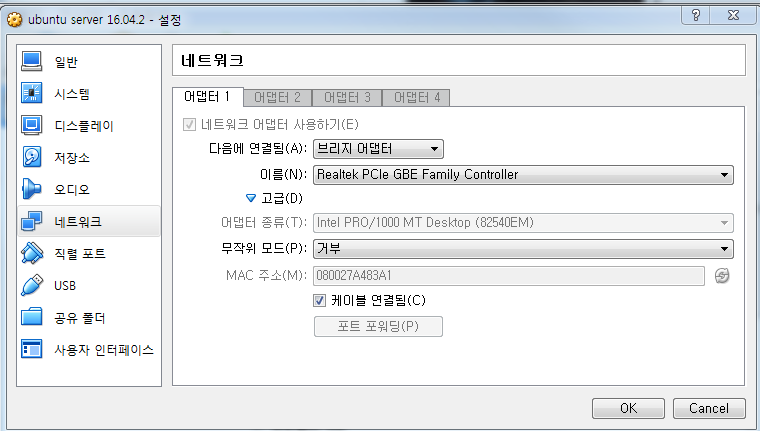












6. 무선공유기



Default gateway : 192.168.219.1

7.  [Virtual Box] : Host로부터 Guest로 고정 IP로 연결하기

/etc/network/interfaces

# The loopback network interface

auto lo

iface lo inet loopback

# The loopback network interface

auto enp0s3

#iface enp0s3 inet dhcp : original

iface enp0s3 inet static

address 192.168.219.109

netmask 255.255.255.0

gateway 192.168.219.1

network 192.168.219.0

broadcast 192.168.219.255

8.  sudo apt-get 실행시 error발생시

/etc/apt/sources.list에서

kr.archive.ubuntu.com 을 [ftp.daum.net](ftp://ftp.daum.net)으로 수정

/etc/resolv.conf를 수정

nameeserver 168.126.63.1

# 9. 한번에 끝내는 Ubuntu 웹서버세팅 (우분투 서버세팅) : <https://blog.lael.be/post/73>

# **0) root 권한으로 변경**

기본으로 주어진 계정이 root 가 아닐 경우에만 0번을 따라하세요.. 본문의 모든 명령어는 root 의 권한에서 실행해야 합니다. 자신에게 주어진 계정이 root 계정이 아니라면 다음의 명령어로 root 로 전환해 주도록 합시다.

자신의 계정 보기

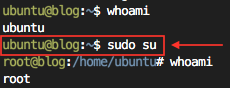
# whoami

sudo 명령어 실행. root 권한으로 root 로 로그인하는 명령어를 실행한다.

# sudo su

자신의 계정 보기

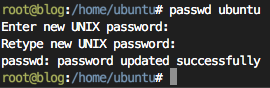
# whoami



기본 계정의 UserID 는 그림과 다를 수 있음. 위 예시에서 기본 아이디는 ubuntu 이다.

sudo 명령어를 사용할 수 있는 계정은 root 와 동급이니 비밀번호 관리에 신중해야한다. 기본 계정의 비밀번호를 매우 긴 어려운 것으로 변경해주도록 하자.

# passwd ubuntu



**1) 리눅스 버전체크**

#uname -a

Linux Lael-ubuntu-xenial 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:33:37 UTC 2016 x86\_64 x86\_64 x86\_64 GNU/Linux

### 2) Ubuntu 버전체크

#cat /etc/issue

Ubuntu 16.04.1 LTS \n \l

조금 더 자세하게 운영체제 버전정보를 알아보고 싶다면

# lsb\_release -a

해당 명령어는 Ubuntu 에서는 기본적으로 설치되어 있지만 CentOS 계열에서는 기본패키지가 아니니 사용하려면 다음 명령어로 설치해주어야 합니다.

# yum install redhat-lsb-core

### 3) 하드용량체크

#df -h

Filesystem Size Used Avail Use% Mounted on

udev 2.0G 0 2.0G 0% /dev

tmpfs 396M 6.2M 390M 2% /run

/dev/vda1 85G 3.6G 77G 5% /

tmpfs 2.0G 192K 2.0G 1% /dev/shm

tmpfs 5.0M 0 5.0M 0% /run/lock

tmpfs 2.0G 0 2.0G 0% /sys/fs/cgroup

tmpfs 396M 92K 396M 1% /run/user/1000

tmpfs 396M 0 396M 0% /run/user/0

대략 다 더하면 90G가 나온다.

### 4) 메모리 체크

#free -m

total used free shared buff/cache available

Mem: 3951 770 2262 10 918 3116

Swap: 4093 0 4093

3951M의 전체메모리중 현재 770M을 사용하고 있고 3116M가 비어있다.

### 4-1) CPU 코어수 확인

cpu정보 프로세스를 읽어서 processor 항목이 몇개인지 갯수를 셉니다.

#cat /proc/cpuinfo | grep processor | wc -l

g3

위의 사진은 6 core 를 뜻합니다.

한번 정도는 다음의 명령어를 확인해 보세요.

#cat /proc/cpuinfo | grep processor

#cat /proc/cpuinfo

### 5) 현재 서버에 설치된 패키지 최신버전으로 업그레이드

패키지 목록 갱신.

#apt-get update

현재 운영체제에 설치되어있는 프로그램 최신버전패치

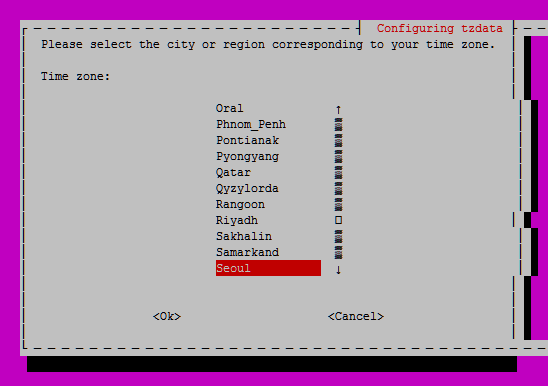
#apt-get upgrade

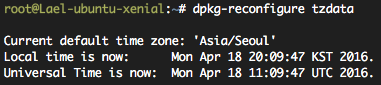
### 6) 시스템 시간 설정

물론 초기 설치할 때 Asia/Seoul 을 설정했다면 이 작업을 할 필요는 없다. 하지만 또 한다고 해서 문제되지는 않는다.

- 데비안 패키지 재설정 TimeZone Data 를 실행한다.

#dpkg-reconfigure tzdata

GUI 환경이 나올 텐데, 순서대로 Asia - Seoul 을 선택하면 된다.



7) Hostname 설정

이 서버에 이름을 정하는 것이다. 이름을 잘 정해 두어야 나중에 다중 서버작업을 할 때 헷갈리지 않는다.

g6

위의 뜻은 “li599-115 서버에 root 사용자” 라는 뜻이다.

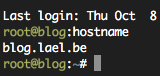
서버 이름은 FQDN(Fully Qualified Domain Name)을 쓰는 것이 좋다.

참고로 라엘이의 이 블로그 서버의 hostname은 blog.lael.be 이다.

#vi /etc/hostname

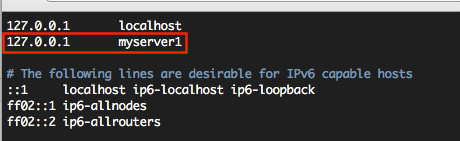
#hostname -F /etc/hostname

서버에 재 접속하면 적용된 것을 확인 할 수 있을 것이다.



서버의 /etc/hosts 에 해당 이름을 등록해두도록 하자.

127.0.0.1    myserver1



### 추가) 메일 발송프로그램 설치하기

많은 프로그램에서 mail() 함수를 사용한다. 이 함수는 서버의 sendmail 프로그램에게 메일발송을 요청한다.

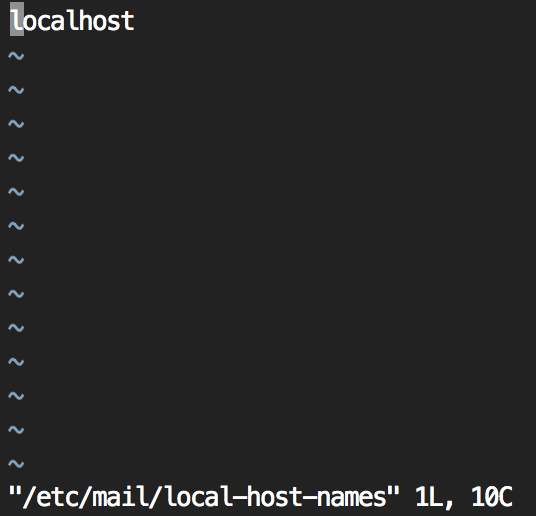
메일문의, 가입시 환영메일, 비밀번호 찾기 메일, 이메일인증 등 널리 사용된다. 서버가 메일 발송을 할 수 있게 sendmail 을 설치하자.

# apt-get install sendmail

이것은 오직 웹사이트에서 메일을 보내기 위한 것이다.

아이디@당신의도메인.com 같은 것을 하고 싶다면 절대로 직접 구축하려고 하지 말고 [구글앱스](https://apps.google.com/intx/ko/pricing.html), 도메인 구입처, 클라우드서버 업체의 메일호스팅, 서버호스팅업체의 메일호스팅 을 사용하도록 하자.

# vi /etc/mail/local-host-names



localhost 를 제외하고 나머지 항목은 지운다. 이곳에 쓰여진 도메인은 sendmail 발송시 목적 메일서버조회(mx record query)를 하지 않고 로컬로 보낸다.

### 8) Apache2 설치

#apt-get install apache2

16.04 LTS 에서는 apache 2.4.x 가 설치된다. (2016년 4월 21일 현재 최신버전은 Apache 2.4.18 이다.)

가끔씩 apt-get update 및 apt-get upgrade 를 실행하면 아무런 문제없이 최신버전으로 업데이트 될 것이다. 설치가 완료되면 자동적용 및 시작된다.버전체크

apache2 -v

apache_1604  
확인해본다.

http:// 192.168.219.109 (서버의 아이피)  
웹브라우져에 기본 설명페이지가 뜨면 성공.  
(참고로 기본으로 보여지는 파일은 /var/www/html/index.html 이다.)  
기본 파일을 지운다.

#rm /var/www/html/index.html

기타 주로 사용되는 모듈을 활성화, 필요 없는 모듈은 비활성화 한다. 아래 모듈에 대한 자세한 설명은… 생략한다. 사용에 문제가 발생하지 않는 최상의 방식이라고 이해하면 된다.

#a2enmod rewrite

#a2enmod headers

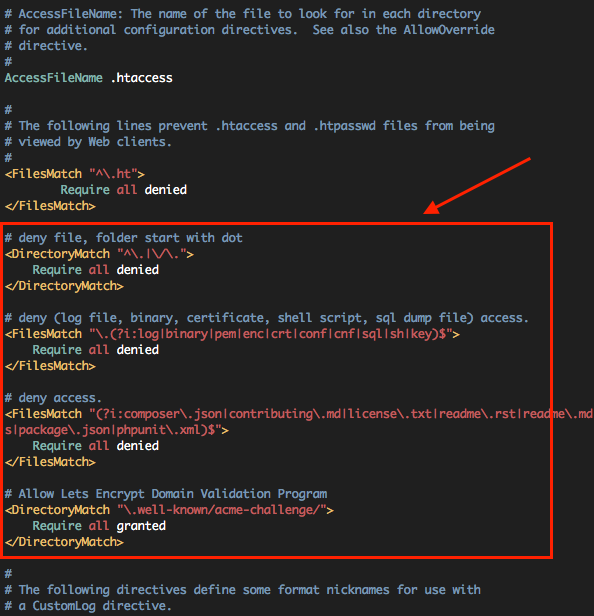
#a2enmod ssl

#a2dismod -f autoindex

 #추가 보안패치. (.git, .svn, .env 등 dot로 시작하는 파일 및 폴더 보호, Web Access가 되어서는 안될 파일들의 접근 제어)

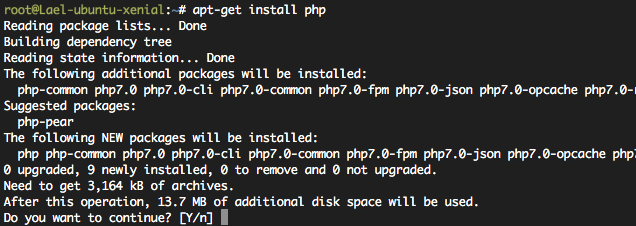
# vi /etc/apache2/apache2.conf

파일 중간의 <FilesMatch “^\.ht”> 구문 다음에 추가한다.



### 9) PHP 7.0설치

#apt-get install php



16.04 에서는 PHP 7.0.x 가 설치된다.

PHP-아파치 연동모듈 설치

#apt-get install libapache2-mod-php7.0

기타 주로 사용되는 모듈을 설치한다.

- 암호화 모듈

#apt-get install php-mcrypt

- 다국어 처리모듈

#apt-get install php-mbstring

- 이미지처리 모듈

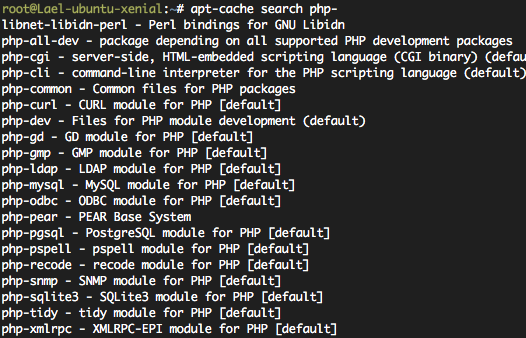
#apt-get install php-gd

- 원격지 정보 불러는 모듈 (워드프레스, 드루팔 등에서 쓰임)

#apt-get install php-curl php-xml

-추가로 설치하고 싶은 모듈이 있으면

#apt-cache search php-

라고 입력해서 설치가능한 패키지를 검색후 install 하도록 하자.  


- 아파치 재시작(적용을 위해서)

#service apache2 restart

버전체크

#php -v

PHP 7.0.4-7ubuntu2 (cli) ( NTS )  
Copyright (c) 1997-2016 The PHP Group  
Zend Engine v3.0.0, Copyright (c) 1998-2016 Zend Technologies  
with Zend OPcache v7.0.6-dev, Copyright (c) 1999-2016, by Zend Technologies

7.0.4 버전이다. (당신이 설치한 버전은 이것보다 높을 것이다.)

### 10 - 1) MariaDB 설치

mysql 과 mariadb 는 완전 API 호환된다.

#apt-get install mariadb-server

MariaDB 10.0.24 이 설치된다.

MariaDB 초기화.

14.04 LTS까지는 자동으로 처리되던 작업인데.. 분리되었다.

아무튼 데이터베이스 초기화 작업을 하도록 하자. 다음의 명령어 실행하자.

/usr/bin/mysql\_secure\_installation

모르면 엔터 누르면 된다. (비밀번호만 설정하고 나머지는 엔터) 잘못한 것 같으면 위 명령어를 다시 실행하면 된다.

:: root 의 인증 플러그인 정보 제거하기

MySQL에 플러그인이라는 개념이 생겼다. 그 중 하나가 서버사이드 인증이다.

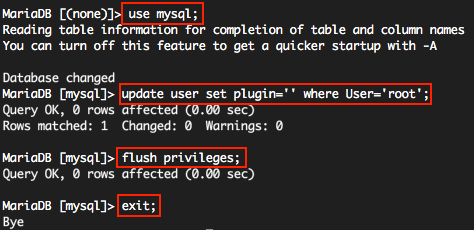
예를들어 Linux의 myuser1 사용자와 MySQL(MariaDB)의 myuser1 과 연결이 되는 경우이다. (비밀번호 필요없이 쉘인증)

root 사용자가 기본값으로 unix\_socket Auth Plugin 이 설정되어 있는데… 이건 실 사용에 많은 불편함을 준다. 기존과 같이 비밀번호 인증 방식으로 바꾸도록 하자.

Linux root 사용자로 로그인한 상태에서

# mysql

(현재는 unix\_socket 인증방식이라서 Linux root 사용자는 MySQL(MariaDB) root 계정에 비밀번호 없이 로그인 할 수 있다)



use mysql;

update user set plugin='' where User='root';

flush privileges;

exit;

#apt-get install php-mysql

DB 연동모듈 설치. 완전 호환되기 때문에 mysql 이라고 해도 mariadb 사용가능.

##### MYSQL 콘솔 클라이언트 버전체크

#mysql -V

mysql  Ver 15.1 Distrib 10.0.24-MariaDB, for debian-linux-gnu (x86\_64) using readline 5.2

### 10 - 2) 기본 언어셋 설정(중요)

이 단계를 건너뛰면 DB가 latin1 으로 생성되며 추후 DB작업에 문제가 생길 수 있다.

#vi /etc/mysql/mariadb.conf.d/50-server.cnf

(vi 에디터 사용방법을 모른다면 ftp 클라이언트를 사용하여 서버에 로그인 후 해당파일을 수정하고 덮어쓰기한다.)

[mysqld] 항목에 다음 2 줄을 추가한다.

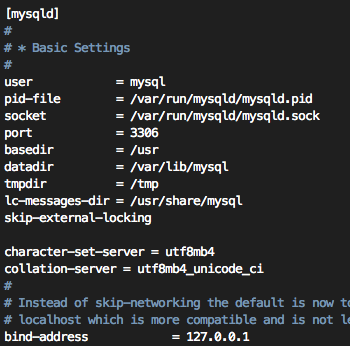
2015년도 부터는 아래와 같이 utf8mb4 속성을 사용하세요.

이 속성은 utf8확장입니다. 기존의 모든 utf8과 상위 호환됩니다. (utf8 에서 utf8mb4 로의 변환은 손실이 일어나지 않습니다.)

utf8mb4 속성은 스마트폰 이모티콘 문자(emoji)를 저장할 수 있습니다.

자세한 설명은 이곳에(<https://blog.lael.be/post/917>) 있습니다.

|  |  |
| --- | --- |
| /etc/mysql/mariadb.conf.d/50-server.cnf 에 추가 | |
| 1  2 | character-set-server = utf8mb4  collation-server = utf8mb4\_unicode\_ci |



변경사항 적용

#service mysql restart

### 11) PHP 권한 설정

웹 서비스 구동시 발생할 수 있는 Nobody 퍼미션 관련 문제를 해결하기 위해 관련 프로그램을 설치한다.  
이 세팅을 하면 shell의 권한과 sftp의 권한과 web의 권한이 동일하게 취급되며 보안도 좋게 된다.  
순서대로 쓰면 된다.

# apt-cache search mpm-itk

libapache2-mpm-itk - multiuser module for Apache

mpm_1604

#apt-get install libapache2-mpm-itk

#chmod 711 /home

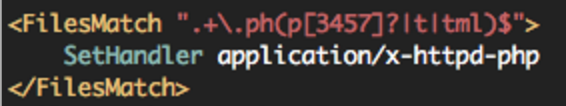
#chmod -R 700 /home/\*

(/home/\* 안에 아무 파일도 없을 경우 마지막 구문은 에러가 날 수 있다. 에러가 나면 무시하도록 하자.)

### 11-1) PHP 실행확장자 변경

php 를 해석하는 확장자가 꽤 많이 있다.

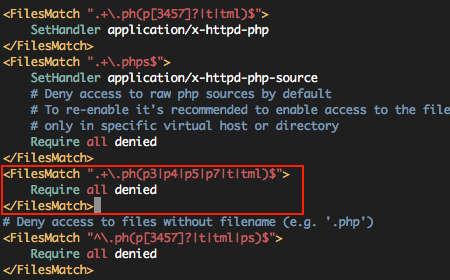
#vi /etc/apache2/mods-available/php7.0.conf



.php .php3 .php4 .php5 .php7 .pht .phtml 확장자 파일이 기본적으로 php를 해석할 수 있게 되어있다. 웹페이지에서 파일업로드 구현시 이 확장자 파일을 제대로 막아주지 못하면 사이트가 위험하게 된다.

 .php 를 제외한 나머지의 접근을 차단하자.

|  |  |
| --- | --- |
|  |  |



적용을 위해서 아파치 재시작

#service apache2 restart

### 11-2) PHP Default timezone 설정하기.

이 값을 설정하지 않으면 시스템 timezone 을 사용합니다. PHP Default timezone 을 설정하는 것은 필수는 아니지만 매우 권장하는 작업입니다. 설정해주세요.

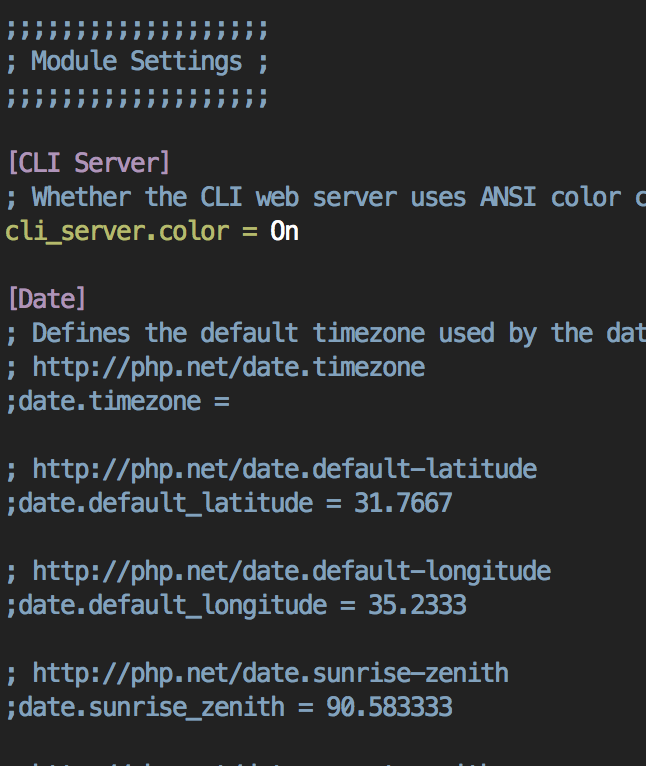
동일한 작업을 2개의 파일에 적용해 주어야 합니다. 이건 Apache2 - PHP때 참조하는 설정파일입니다.

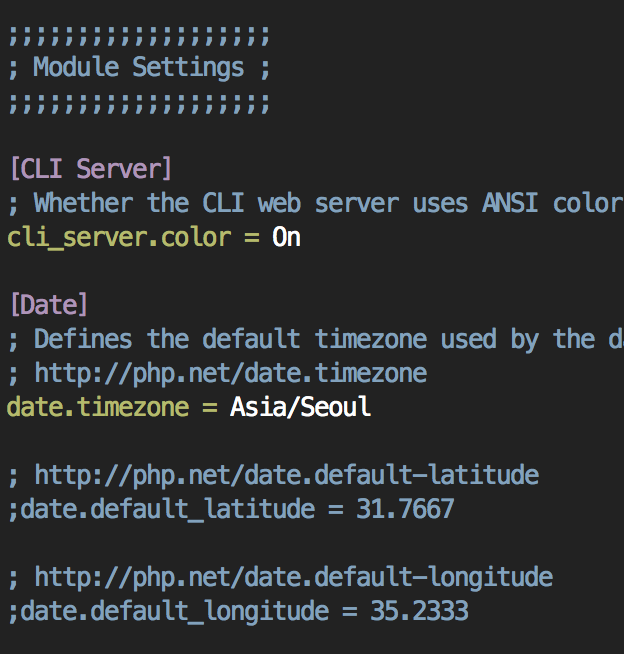
#vi /etc/php/7.0/apache2/php.ini

이건 Cron이나 Console에서 PHP를 직접 실행 할 때 참조하는 설정파일입니다.

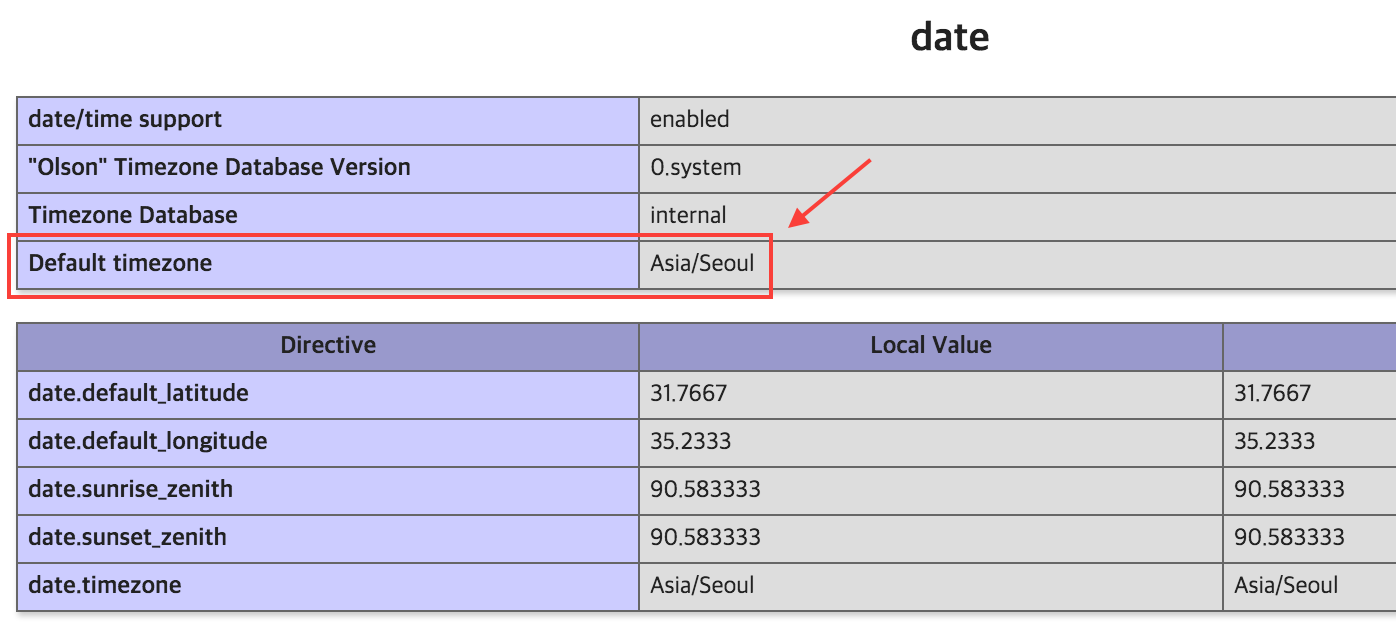
#vi /etc/php/7.0/cli/php.ini

date.timezone 값을 찾아서 주석을 제거하고 시간을 설정해주세요.





#service apache2 restart



나중에 mytest.php 파일을 만들고 웹브라우져에서 실행시킨 뒤 위와 같이 설정되어 있으면 정상이다.

|  |  |
| --- | --- |
| mytest.php | |
| 1 | <?php phpinfo(); ?> |

Default timezone 이 설정되어 있으면 정상.

**12) 계정생성 및 동작테스트**

원래 표준명령어는 useradd 이지만    ubuntu는 사용하기 좋게 adduser 를 지원한다. 리눅스 관련 서적을 보면 **둘다** 계정생성용 명령어라고 되어있다. 쉬운 설정을 위해 adduser를 사용

#adduser myuser1

위와 반대동작을 하는 계정삭제 명령어는 - 계정을 삭제하고 홈디렉토리도 삭제함 -

#userdel -r myuser1

입니다.)

보통 웹루트는 홈디렉토리에 하지 않습니다. 저는 주로 www 디렉토리를 사용합니다. 사용자변경 후 www 디렉토리를 생성하고 빠져나오기

#su -l myuser1

#mkdir www

#exit

### 13) 웹사이트 Apache 환경설정파일 작성

#### #16.12.20 설정 가이드가 추가됨

환경설정을 쉽게하도록 도와주는, 환경설정 생성기가 추가되었습니다.

<https://blog.lael.be/demo-generator/apache/my-example-site.com.php>

다음의 내용을 작성한다.  
아래 예제에서는 사이트 환경설정파일명을 192.168.219.109로 가정하고 진행한다. 당신의 도메인, 사용자 아이디, 별도의 구분단어로 설정해서 사용하도록 하자.

#vi /etc/apache2/sites-available/192.168.219.10.conf

/etc/apache2/sites-available/192.168.219.10**.conf**에 저장한다.

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  21  22  23 | <VirtualHost \*:80>      #main domain      ServerName 192.168.219.10        #additional domain      ServerAlias www.xxx.xxx      ServerAlias my-anotherdomain.com        #document Root      DocumentRoot /home/leecheol/www/        #additional setting      <Directory /home/leecheol/www/>          Options FollowSymLinks MultiViews          AllowOverride All          require all granted      </Directory>        AssignUserID leecheol lwwcheol        ErrorLog ${APACHE\_LOG\_DIR}/lael.be-error.log      CustomLog ${APACHE\_LOG\_DIR}/lael.be-access.log combined  </VirtualHost> |

ServerAlias 는 사용안하면 빼도 되는 줄이다.

당신이 만약 SSL(https) 를 적용하고자 한다면 192.168.219.10**.conf  파일 하단**에 다음의 코드를 추가하세요. 즉 VirtualHost 영역을 하나 더 추가.

|  |  |
| --- | --- |
|  | <VirtualHost \*:443>      #main domain      ServerName lael.be        #additional domain      ServerAlias www.lael.be      ServerAlias my-anotherdomain.com        #document Root      DocumentRoot /home/myuser1/www/        #additional setting      <Directory /home/myuser1/www/>          Options FollowSymLinks MultiViews          AllowOverride All          require all granted      </Directory>        AssignUserID myuser1 myuser1        ErrorLog ${APACHE\_LOG\_DIR}/lael.be-error.log      CustomLog ${APACHE\_LOG\_DIR}/lael.be-access.log combined        Header always set Strict-Transport-Security "max-age=31536000"        SSLEngine on        SSLProtocol all -SSLv2 -SSLv3        SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:  ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:  ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:  ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:  DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:  DHE-RSA-AES256-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:  AES:CAMELLIA:DES-CBC3-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!aECDH:!EDH-DSS-DES-CBC3-SHA:  !EDH-RSA-DES-CBC3-SHA:!KRB5-DES-CBC3-SHA        SSLHonorCipherOrder on        SSLCertificateFile "/home/myuser1/ssl/mysite\_ssl.crt"      SSLCertificateKeyFile "/home/myuser1/ssl/mysite\_ssl.key"      SSLCertificateChainFile "/home/myuser1/ssl/mysite\_ssl.certchain.crt"    </VirtualHost> |

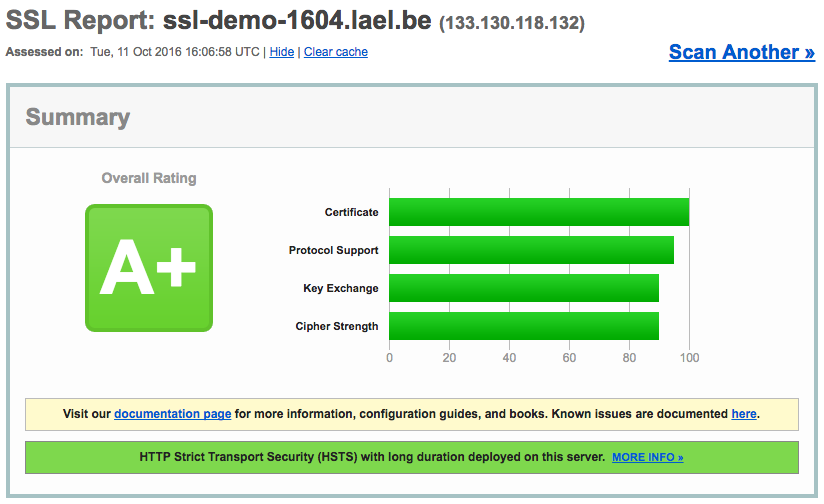
<https://www.sslshopper.com/ssl-checker.html#hostname=blog.lael.be>  (SSL Chain test - 인증서가 올바르게 설치되어 있는지)

<https://www.ssllabs.com/ssltest/analyze.html?d=blog.lael.be> (SSL Algorithm test - 안전한 암호화 통신이 설정되어 있는지)

Chain test 는 모두 Valid 이어야하고, SSL Algorithm test 는 A 이상이면 정상적인 운영이 가능하다.

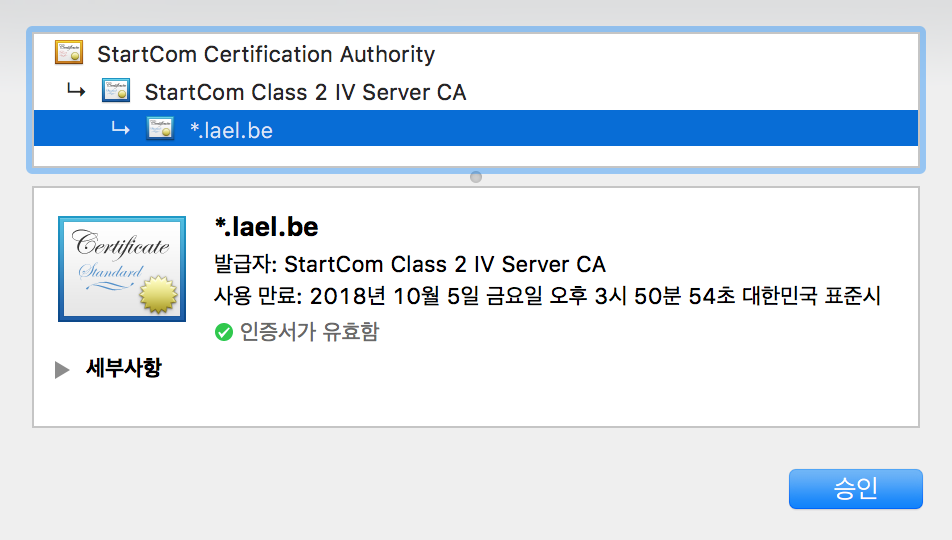
라엘이가 여러 설정 값에 대해서 테스트를 해 보았고, 최적의 권장설정 값을 위와 같이 적어두었으니 그대로 쓰면 된다.

위의 설정값으로 SSL을 설치하면 A+등급을 받을 수 있을 것이다.



.

인증서 적용 테스트는 위의 사이트를 이용하여라. 인증서 체인 파일이란 “인증서에 대한 인증서” 파일이다.



< 그림 : 이 블로그는 위의 단계를 거쳐 인증된다. 이것을 체인 인증 이라고 한다. >

대통령이 당신을 인증할 때 직권으로 인증하는 것이 아니라, 대통령 -> 서울시장 -> 강남구청장 -> 삼성동장 -> 당신 의 단계를 거친다. 검증하려면 모든 단계의 보증 증서를 제공해야 하는 것이다.

인증서 파일에는 삼성동장 -> 당신  의 정보가 들어있고, (암호화 통신시 공개됨)

인증서 키 파일에는 암호화 통신을 위한 정보가 들어있고 (은행 보안카드 로 비유. 외부에 공개되지 않음.)

인증서 체인 파일에는 대통령 -> 서울시장, 서울시장 -> 강남구청장, 강남구청장 -> 삼성동장 의 정보가 들어있다. (체인 인증이라고 한다. 연결고리 인증)

인증서 체인을 올바르게 작성하지 않으면 Firefox 브라우저와 Android Chrome 브라우저에서 “인증서 정보부족” 오류가 발생하게 된다.

### 14) 사이트 활성화 및 적용

명령어는  
#a2ensite 사이트환경설정파일명  
입니다.

#a2ensite **lael.be**

(참고로 사이트 비활성화는

#a2dissite lael.be

입니다.)

- 아파치 설정 다시 불러오기(적용을 위해)

#service apache2 reload

### 15) 연동테스트

apache 와 php, 그리고 mariadb 를 모두 사용하는 프로그램을 실행시켜보자.

phpmyadmin 공식사이트 : <https://www.phpmyadmin.net/>

설치 못하시는 분이 꽤 있으셔서 따로 설치법을 적습니다.

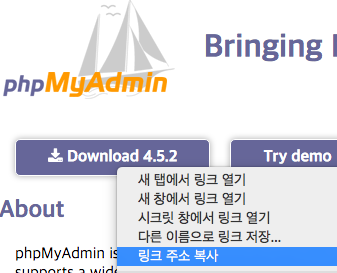
여러 설치방법이 있겠지만 저는 다음과 같이 설치합니다.

#### 압축해제 프로그램 설치

# apt-get install unzip

#### 압축파일 다운로드

# cd /var/www/html



<https://www.phpmyadmin.net/> 사이트로 이동 후 위의 그림과 같이 입력하여 최신버전을 설치할 수 있도록 하자.

이 글에서는 글 작성 시각 현재 최신버전인 4.5.2 를 설치할 것이다. phpmyadmin 은 매우 견고하게 만들어진 프로그램으로써 4.5.2를 설치해도 보안취약점이 있지는 않겠지만 최신버전을 설치하는 습관을 기르도록 하자. (혹시나 말하지만, Alpha나 Beta 같은 개발자-최신버전을 설치하라는 뜻이 아니라 널리 사용되어 검증된 Release Channel 최신버전 를 사용하라는 것이다.)

# wget https://files.phpmyadmin.net/phpMyAdmin/4.5.2/phpMyAdmin-4.5.2-all-languages.zip

압축해제

# unzip phpMyAdmin-4.5.2-all-languages.zip

폴더 이름변경

# mv phpMyAdmin-4.5.2-all-languages dbmyadmin

다운받은파일 삭제

# rm phpMyAdmin-4.5.2-all-languages.zip

http://111.222.333.444/dbmyadmin/



**[TIP]** 간혹 방금 설치한 디비의 root 비밀번호가 기억이 안나는 분들도 있을 것이다. 이 경우에는 다음의 명령어를 사용하여 mariadb 를 재설치 하도록 하자.  
- 제거  
# apt-get purge mariadb-server  
- 설치  
# apt-get install mariadb-server

#### - 재부팅

복잡한 세팅이 끝났으니 한번 숨을 고르고 가자.

# reboot

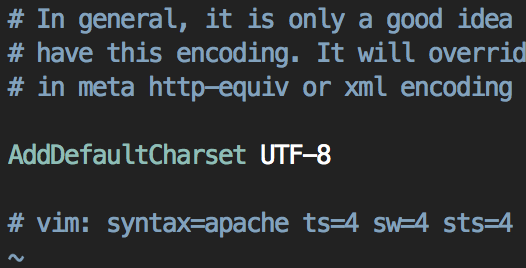
재부팅 후에 phpinfo 페이지와 phpmyadmin 가 잘 실행된다면 “재부팅이 가능한 서버” 라고 볼 수 있다.

### 16) Apache 추가 보안 설정

- 기본 언어셋 설정

#vi /etc/apache2/conf-available/charset.conf

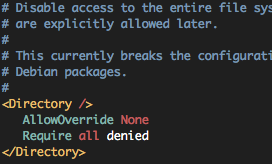
기본 언어값 UTF-8 에 대해서 주석처리되어 있을 텐데 주석(#)을 제거해 준다.

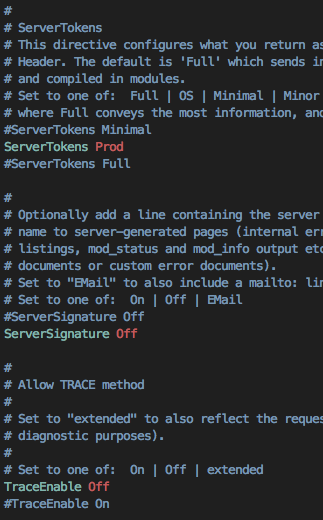


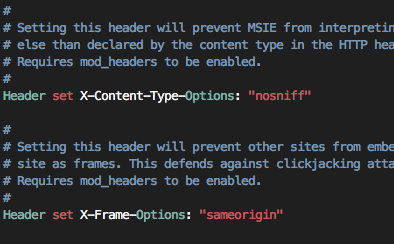
- 추가 보안 설정

#vi /etc/apache2/conf-available/security.conf

매우 권장하는 보안설정이므로 Ubuntu Apache 패키지 제작자가 미리 써두었다.  
이미 다 쓰여 있으니까 주석(#) 만 제거하자.







- 아파치 설정 다시 불러오기(적용을 위해)

#service apache2 reload

### 옵션) SSH 기본 포트번호 변경

#이 작업은 무작위 대입공격(Brutu force attack)의 시도를 차단해줍니다.  
보통 IP주소 : 22번 포트를 스캔해서 ssh와 연결되면 무작위 로그인 시도를 하는 프로그램이 엄청 많은데,  
포트번호만 바꾸어주어도 방어가 되거든요.

!! IPTABLES 방화벽, SSH 포트번호 변경, Fail2ban 중에서 **하나만** 적용하세요!!

1) 나는 KS 클라우드 or 아마존 클라우드를 사용하고 있어! -> 클라우드 방화벽 쓰세요 !!  
2) 나는 허용된 IP만 서버에 접속하게 할거야 -> IPTABLES !!  
3) 나는 사용자의 IP를 특정지을 수 없는데 무차별대입 공격은 방어할거야 -> Fail2ban !!  
4) 나는 나만 아는 포트번호로 서버에 접속할 거야 -> SSH 포트변경!!

[개인 프로젝트, 회사의 서비스 -> IPTABLES]  
[웹호스팅 -> Fail2ban 또는 SSH 포트변경]

SSH 기본 포트번호인 22번을 다른 번호로 바꿉니다.  
기억하기 쉬운 숫자로 변경하세요.

#vi /etc/ssh/sshd\_config

Port 22   를 찾아서 임의의 숫자 : 10022, 34522 등 기억하기 쉬운 숫자로 설정.

포트번호는 10000번 이상의 숫자를 선택하시길 권장합니다.

#service ssh restart

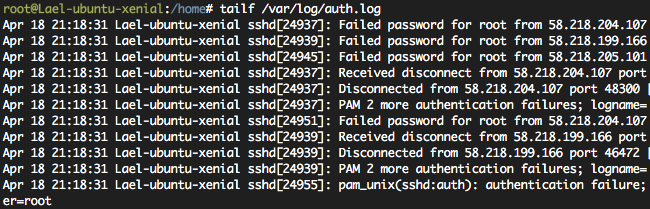
### 옵션) 방화벽 적용하기

방화벽의 중요성을 알고 싶다면

# tailf /var/log/auth.log

를 입력해보도록 하자.  (Control + C 를 눌러 프로그램 종료)

별도의 방화벽 설정이 없었다면 벌써 중국에서 서버에 로그인 시도를 하고 있을 것이다.

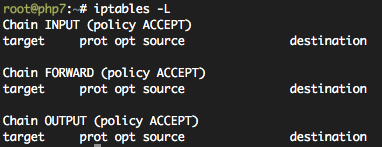


이러한 무차별 로그인 시도를 다음 중 어느 하나를 사용해서 막을 수 있다.

가장 편한 것은 fail2ban 이다. (한줄만 타이핑하면 방어됨)  
(<https://blog.lael.be/post/858#fail2ban>) 로 이동해서 설정하세요.  
\* 접속자의 IP 가 고정되어 있으면 방화벽 설정을 통해, 특정 아이피에서만 서버에 접속할 수 있도록 설정해주세요.

현재 방화벽 설정 보기. (List)

#iptables -L



INPUT (서버로 들어오는 것 관리), FORWARD (서버에서 내부망으로 연결관리;잘 안씀), OUTPUT (서버에서 나가는 것 관리)  
로 이루어져 있다.

보통 FORWARD와 OUTPUT은 건들이지 않고 INPUT 만 수정한다.  
policy ACCEPT 라는 뜻은 아무 조건도 해당하지 않았을 때 ACCEPT 하라는 것이다.

먼저 현재 방화벽 설정을 파일로 저장한다. 언제든 현재의 상태로 되돌릴 수 있기 위해서 이다.

#cd ~

#mkdir firewall\_rules

#cd firewall\_rules

#iptables-save > 151214.rules                 현재 날짜 쓰세요.

이제 방화벽을 복구해 보자.

#iptables-restore < 151214.rules

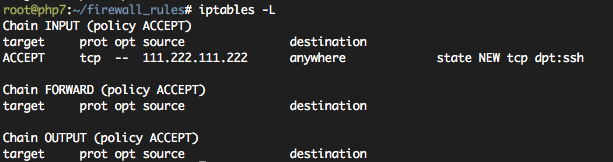
#iptables -L

>>설정 시작.  
규칙 : 아이피 111.222.111.222 에 대해서 destination port 가 22 이면 ACCEPT 하여라.

#iptables -A INPUT -s 111.222.111.222/32 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT

아이피 바꾸지 마시고 위의 예시 (111.222.111.222) 그대로 입력하세요.

#iptables -L



이제 현재 상태에 대해서 방화벽 설정파일을 다시 생성해보도록 하자.

#iptables-save > 151214.rules

SFTP나 vi, cat 으로 해당 151214.rules 를 열어보자.

열고나서 코드의 뜻을 대충 해석해보아라. (간단하다.)

하단 \*filter 부분에

-A INPUT -s 111.222.111.222/32 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT

가 보이는가?

여러분은 이곳에 아래의 코드를 집어넣어야 한다.

순서가 중요하다. IF-ELSE 같이 동작하기 때문에 조건에 맞으면 바로 지정된 동작을 한다.

211.105.192.168 아이피만 지정하고 싶을 때 -> -s 211.105.192.168/32

211.105.192.\* 아이피 그룹을 지정하고 싶을 때 -> -s 211.105.192.0/24

211.105.\*.\* 아이피 그룹을 지정하고 싶을 때 -> -s 211.105.0.0/16

목적지 포트가 22번(ssh) 포트일 때 -> -dport 22

목적지 포트가 80번(http) 포트일 때 -> -dport 80

목적지 포트가 443번(https) 포트일 때 -> -dport 443

아래는

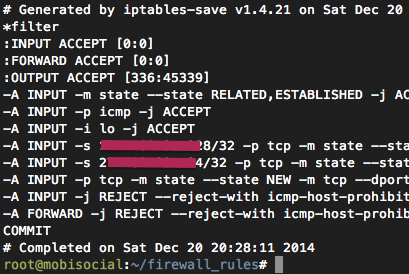
1. 이미 연결된 것은 허용  
2. ping 허용  
3. loopback 허용  
4. 111.222.111.222 의 22번 포트 접근 허용  
5. 123.111.123.111 의 22번 포트 접근 허용  
6. 80 포트 접근 허용 (-s 옵션이 없으므로 누구나 허용)  
7. 443 포트 접근 허용 (-s 옵션이 없으므로 누구나 허용)  
8. 차단  
9. FORWARD 차단

의 코드이다.

아까 생성한 .rules 파일을 열어서 아래의 코드를 그림과 같이 코드를 추가하여라. 이때 반드시 당신의 아이피를 추가하여라.

추가가 잘못되어도 어차피 1번의 조건에 의해서 당신의 연결이 끊기지는 않겠지만 새로운 연결은 차단될 것이다.

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9 | -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT  -A INPUT -p icmp -j ACCEPT  -A INPUT -i lo -j ACCEPT  -A INPUT -s 111.222.111.222/32 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT  -A INPUT -s 123.111.123.111/32 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT  -A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT  -A INPUT -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT  -A INPUT -j REJECT --reject-with icmp-host-prohibited  -A FORWARD -j REJECT --reject-with icmp-host-prohibited |



#iptables-restore < 151214.rules

#iptables -L

!!!반드시 현재 쉘 연결을 끊지 말고!!!

현재 연결은 1번 조건에 의해서 반드시 허용이기 때문에 괜찮다.

새로 연결창 띄워서 테스트해 보아라.

만약 원하는대로 동작하지 않는다면 다시 .rules 파일을 수정하고 iptables-restore 하여라.

방화벽 설정이 머리가 아프다면

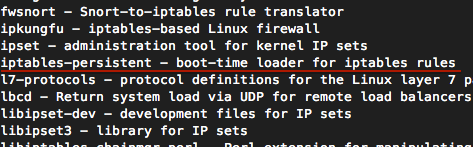
# iptables -F

로 초기화 하고 내일 다시 시도해 보아라.

이 설정은 재부팅이 되면 초기화 된다.

설정을 지속시키도록 하자.

iptables-persistent 설치



#apt-get install iptables-persistent

Yes (엔터), Yes (엔터)

/etc/iptables 라는 폴더가 생성되고

rules.v4, rules.v6 가 생성된다.

부팅시 실행되는 파일을 갱신하자.

#iptables-save > /etc/iptables/rules.v4

ipv6 차단하기

#vi /etc/sysctl.conf

맨 밑에

|  |  |
| --- | --- |
| 1  2  3 | net.ipv6.conf.all.disable\_ipv6 = 1  net.ipv6.conf.default.disable\_ipv6 = 1  net.ipv6.conf.lo.disable\_ipv6 = 1 |

추가.

설정파일 적용

#sysctl -p

검사

#cat /proc/sys/net/ipv6/conf/all/disable\_ipv6

1 이면 disable 된 상태이다.

q30

재부팅

#reboot

재부팅 후에 방화벽 규칙이 유지가 되면 성공이다.

#iptables -L

### 옵션) 계정별 트래픽 양 제한하기. Apache Mod Cband install.

- 2015.06.01. Ubuntu 14.04 LTS 테스트 완료.   
- 순간속도(대역폭), 총 전송량(쿼터), 동시접속연결을 제한하는 모듈입니다.  
장애가 일어날 것 같은 값들을 Hard Boundary 로 정해놓으면 장애가 일어날 것 같은 환경에서 서버가 잘 돌아가는 것을 볼 수 있을 것입니다.

저도 서버 서비스의 장애를 막기 위해서 실 서비스에 이것을 사용하고 있습니다.  
다만 저 같은 경우 분산처리를 해 두었기 때문에 개별 서버에 적용한 제한치보다 실제 서비스는 더 높은 처리를 보여줍니다. (100의 제한을 건 서버 5대에 분산처리하면 전체적으로 500의 제한이 걸린 것 처럼 보이겠죠?)

Mod Cband 는 Apache2 모듈입니다.

다음의 기능이 가능합니다.

1) 대역폭 제한 (Bandwidth limit)  
2) 동시 접속자 제한 (Concurrent user)  
3) 트래픽 제한 (Transfer quota)  
통계 용도로만 사용할 수도 있다.

현재 공식사이트가 닫혀있어서 대체할 만한 다운로드 경로를 적는다.

1) mod cband 공식사이트 :   (안열림.)  
2) mod cband 메인 개발자 블로그 : http://dembol.org/blog/mod\_cband/ (다운로드 링크가 동작안함)  
3) source forge 링크 : http://sourceforge.net/projects/cband/files/ (최신버전이 아님)

4) 현존하는 것 중에서 가장 최선의 선택 : <https://fossies.org/linux/www/apache_httpd_modules/mod-cband-0.9.7.5.tgz/>

5) 라엘이 블로그 백업용 파일 (4번과 완전히 동일한 파일) [mod-cband-0.9.7.5.zip](https://blog.lael.be/wp-content/uploads/2014/10/mod-cband-0.9.7.5.zip)

##### 1] mod cband 는 apxs 라는 아파치 확장 개발 라이브러리를 필요로 합니다.

#apt-get install apache2-dev

##### 2] apache cband module 다운로드

#wget https://fossies.org/linux/www/apache\_httpd\_modules/mod-cband-0.9.7.5.tgz

##### 3] 압축을 풀고 설치

#tar -xzvf mod-cband-0.9.7.5.tgz

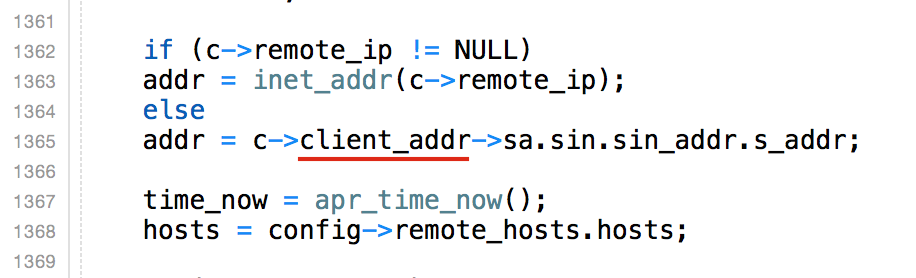
#cd mod-cband-0.9.7.5

##### 3-1] 패치.

apxs 가 업데이트 되면서 변수명이 몇개 바뀌었다.

#vi src/mod\_cband.c

찾기 : remote\_addr      ,    바꾸기 : client\_addr       1365번째줄, 1회만 치환되어야 함.



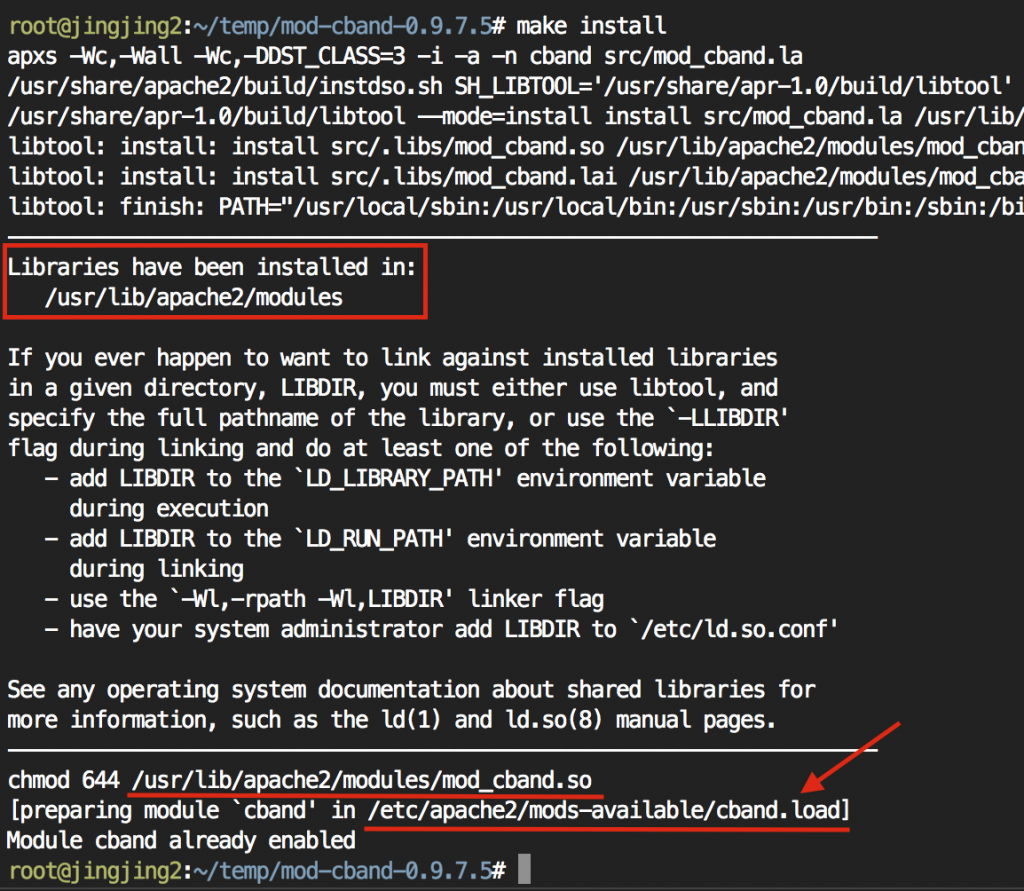
찾기 : remote\_ip       ,    바꾸기 : client\_ip     4회 치환되어야 함.

##### 3-2]  설치 계속 진행.

#./configure

#make

#make install



##### 4] cband 모니터링 페이지 생성

#vi /etc/apache2/mods-available/cband.conf

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15 | <IfModule mod\_cband.c>      <Location /cband-status>          SetHandler cband-status          AuthName "adminpage"          AuthType Basic          AuthUserFile /home/.htpasswd          require valid-user      </Location>      <Location /cband-status-me>          SetHandler cband-status-me          Order deny,allow          Deny from all          Allow from all      </Location>  </IfModule> |

#htpasswd -c -m /home/.htpasswd admin

##### 5] 아파치 모듈 켜기

#a2enmod cband

##### 6] 적용을 위해서 아파치 재시작

#service apache2 restart

##### 7] 확인

웹브라우져로

서버아이피/cband-status-me

서버아이피/cband-status

에 들어가 보자.

지금은 모두 무제한이므로 아무 항목이 뜨지 않을 것이다.

##### 8] 설정하기.

<https://www.linux.co.kr/home/lecture/?leccode=10588>

위의 링크 글을 참조하여 이미 생성해서 사용중인 sites-available 안의 virtualhost 파일을 수정한다.

##### 9] 설정 예제.

각 사이트의 <virtualhost> 구문에 Cband 설정 값을 추가한다. 다 쓸 필요는 없다. 필요한 제한만 두도록 하자.

당신이 웹호스팅을 운영중이라면 CBandLimit 구문과 CBandPeriod 구문을 사용하여라.

당신이 동영상 사이트나, 자료실을 운영중이라면 CBandSpeed 와 CbandExceededSpeed 를 사용하여라.

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  21  22 | <VirtualHost \*:80>      #main domain      ServerName lael.be      #something      #~~~      #~~~        <IfModule mod\_cband.c>          #4주동안 6GB 전송량 제한을 둠. 초과시 503 Service 에러페이지가 뜸.          CBandLimit 6G          CBandPeriod 4W          #트래픽 조각. 이 상황의 경우 1주일마다 1.5GB 가 보급된다.          #트래픽이 CbandPeriod 기간동안 골고루 사용되기를 원할때 설정한다.          CBandPeriodSlice 1W            #동영상(flv, mp4)이나 자료실 서비스를 하고 싶을때에만 아래의 속도제한 구문작성          CBandSpeed 500kbps 10 30          CBandExceededSpeed 128kbps 5 15          #CBandScoreboard /var/www/scoreboard/domain.com.scoreboard      </IfModule>    </VirtualHost> |

#### 옵션 ) 서버 동시접속자 설정 변경하기. (15.11.20 추가)

다음의 페이지를 많이 참조했습니다. (<http://www.zarafa.com/wiki/index.php/Apache_tuning>)

문의주시는 분들 중에 간혹 의도치않은 대박(?)이 일어나신 분들이 있더라. 동시접속 튜닝법을 설명하고자 한다.

##### 몇가지 배경지식 설명.

- http 웹페이지는 stateless(connectionless) 입니다. 즉 페이지 불러올 때에만 서버와 연결하고 페이지 로드가 끝난 후에는 연결을 끊습니다.

- 1개의 연결당 평균 메모리 소모량은 20MB 입니다. (라엘이가 관리하는 여러서버의 평균값을 내보았음)

- Ubuntu Apache 의 기본 동시접속자 제한은 150개 입니다. 1000개의 동시접속이 연결되면 150개는 즉시 처리진행되고, 나머지 850개는 대기열에서 대기하다가 차례대로 처리됩니다.

##### 1] 서버 연결당 얼마나 메모리를 소모하는지 확인

|  |  |
| --- | --- |
| 1 | ps -ylC apache2 | awk '{x += $8;y += 1} END {print "Apache Memory Usage (MB):  "x/1024; print "Average Proccess Size (MB): "x/((y-1)\*1024)}' |

q34

##### 2] 서버에 여유 메모리 자원이 얼마나 있는지 확인

서버를 재부팅한 후에 아파치를 종료후 서버의 메모리를 확인해본다.

# free -m

##### 3] 하드웨어 자원을 고려한 가용 동시연결수 계산

여유 메모리 / 1연결당 메모리     하면 된다.

2000MB free memory 가 있고, 1연결당 20MB 를 사용한다면 = 100개의 동시연결 가능. (300~500 동시접속자 처리가능)

##### 4] 사이트의 필요 동시연결수 계산

450명의 사용자가 있고 3초주기로 페이지 이동이 일어난다고 가정하자. 페이지 출력 실행시간은 2초라고 가정하자.

필요 동시연결수 = 450 / 3 \* 2 = 300

##### 5] 동시연결수 설정 변경.

# vi /etc/apache2/mods-available/mpm\_prefork.conf

MaxRequestWorkers 값을 수정해야 합니다.

ServerLimit 라는 옵션의 기본값이 256이기 때문에 MaxRequestWorkers 값이 256보다 작으면 따로 적을 필요가 없으며, 256보다 크면 그와 같은 값으로 ServerLimit 도 설정해야 합니다.

동시연결 제한 300 예제 설정법.

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8 | <IfModule mpm\_prefork\_module>      StartServers 5      MinSpareServers 5      MaxSpareServers 10      MaxRequestWorkers 300      ServerLimit 300      MaxConnectionsPerChild 0  </IfModule> |

**Linux 명령어**

1. mkdir : directory 만들기

2. ls -al : dir/w

ls -l

ls

3. touch :file 만들기

4. cd directory명 일부 + tab key :

5. rm : file 삭제

rm - r hello\_linux : directory삭제

rm -rf / : 묻지도 않고 root의 모든 것을 삭제함... 주의

6. 명령어 --help

rm --help

7. man 명령어 : Manual

8. mv : 화일을 리네임하거나 다를 곳으로 이동시킬 때 사용.

9. sudo : super관리자의 권한으로 명령을 실행하는 방법

super user do

Unix계열은 주로 다중사용자 용이었으며 따라서 각각의 사용자마다

permission(권한)을 부여 하였음.

apt-get install git : 권한이 없으면 실행을 할 수 없으나 sudo apt-get install

git을 할 수 있음.

10. Utility

1) grep : 해당 파일을 읽어서 해당 패턴을 검색하고, 패턴을 포함하는 줄의

내용을 출력한다.

grep xxx you.txt : you.txt에서 xxx가 포함된 Text를 출력

grep - : option

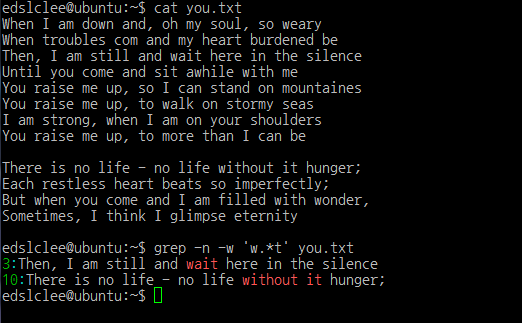
-i : 대소문자 구별 안 함.

-n: 라인 번호 포함

-w: 단어로 검색

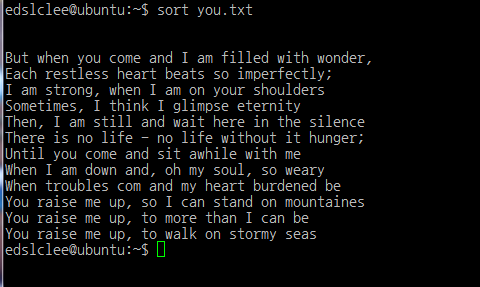
-v: reverse 조건으로 검색

-w ‘w.\*t’처럼 정규표현식으로 검색할 수 도 있음.



2) Sort : Text파일을 줄 단위로 정렬한다

- 기본 Format : sort [-옵션] 파일\*



- sort +2 -3 you.txt : 3번째 단어 기준으로 sort

3) split(파일 자르기) : 하나의 파일을 일정한 크기의 여러 개의 파일로 분할

-기본 format: split [-옵션] 입력파일 [출력파일]

- split –l 10 you.txt

ls -l

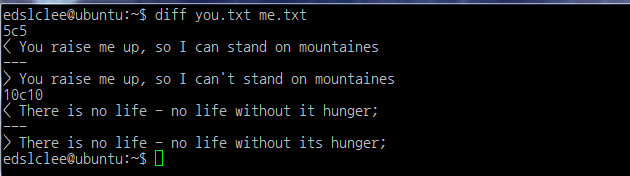


4) 파일비교

- cmp : cmp 파일1 파일2



- diff : diff 파일1 파일2



5) 파일찾기

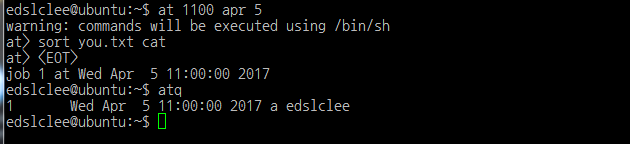
-format : find directory [-옵션]

6) 명령어 스케쥴링

- **$crontab 파일** : crontab파일을 cron시스템에 등록한다.

crontab –l : 등록된 crontab파일 list, -e: 수정 혹은 생성, -r: 삭제

- **$at [옵션] 시간**

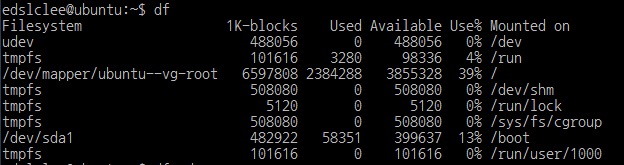
 $at –r jobnumber : 해당 at작업번호를 삭제

7) 디스크 및 아카이브

- **디스크 사용**

$ df 파일시스템\* : 파일명이 있을 경우 그 파일만, 파일명이 없을 경우 모든

파일 시스템에 대한 정보를 나타냄



$du [-s] 파일명 : 파일의 디스크 사용량을 나타냄

- **아카이브**

tar : 백업 또는 다른 장소로의 이동을 위해 파일을 묶어 놓은 묶음을 말하며,

tar(tape arcive)유틸리티를 사용하여 만들거나 푼다

$tar –[option] c(create), v(vervose, x(extract), t(table of contents), f(file)

UNIX에서는 압축을 할 경우 먼저 tar로 여러 파일을 묶은 후에 compress

또는 gzip으로 압축한다.

- **압축**

Compress : 유닉스에서 기본기본으로 제공하는 압축프로그램으로

. $compress 파일\*

. $uncompress 파일.Z

gzip: 윈도즈의 zip프로그램과 유사

. gzip 파일\*

. gzip –d 파일.gz

8) AWK

11. nano Editor사용법



^G: Get Help ^O: Write Out ^W :Where is ^K cut Text ^J: Justify ^C :Cur Pos ^Y: Prev Page

^X: Exit ^R: read file ^\:replace ^U un cut ^T: To spell

ctrl+^                         블럭지정하기 (흰색만 선택한 것임)    
alt-^     alt-shift-6      선택 종료후 컷버퍼에 복사, 선택 없으면 현재 라인을 복사  
^U                              붙여넣기  
^K                              잘라내기  
alt-R                           바꾸기  
alt-G                          지정한 라인, 컬럼으로 이동  
alt-W                         마지막 검색 반복  
^W                            원하는 문자열 찾기  
^G                             도움말   
^O                             새로운 파일 생성  
^X                              종료  
^R                              파일을 읽어오기  
alt-T                           커서부터 파일 끝까지 잘라내기  
alt-+                           화면을 줄 단위로 이동  
alt--                            화면을 줄 단위로 이동

12. Package Manager

LINUX의 package manager에는 apt와 yam이 있음.

1) sudo apt-get update; 로 update대상 catalog를 읽음

2) sudo apt-cache search htop

3) sudo apt-get install htop

1) ~ 3)의 순으로 package를 install.

4) sudo apt-get upgrade htop

5) sudo apt-get remove htop : 삭제

6) sudo apt-get purge apache : 더욱 강력함.

\* htop은 sudo htop을 하는 것이 좋다.

\* Bitnami LAMP는 /otc/lampstack~/uninstall

13. file을 다운로드 받을경우

1) wget을 사용

wget url/.\*

2) git을 활용

git clone https://www.github/edslclee/\*.git \* directory명

14. IO redirection \* http://slideplayer.com/slide/5117573/ 참고필요 (shell script)

1) stdout의 redirection

ls -l > result.text : ls -l의 출력 결과를 result.txt에

cat result.txt : 출력하기

- rm test.txt > log.txt명령어를 사용 할 경우 test.txt가 존재하지 않으면

screen상으로 error message가 출력됨. 이는 rm test.txt > log.txt는

rm test.txt 1 > log.txt이기 때문 즉 stdout임. file로 error message를 저장하려면

rm test.txt 2 > log.txt하면 stderr 형식이 되어 화일로 출력이 가능함.

따라서,

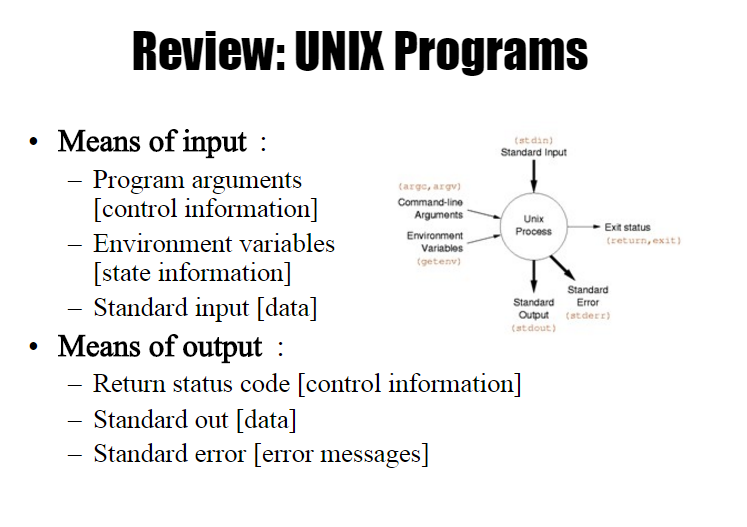
rm test.txt 1> result.txt 2>error.log 로 사용이 가능하다.

2) stdin의 redrection

cat < hello.txt : hello.txt의 내용을 입력으로 받는다.

head -n1 test.txt : test.text 1줄

head -n1 < test.txt > one.txt



3) etc

. ls -l >> result.txt : stdout redirection 결과를 Append

. mail edslclee@gmail.com << eot

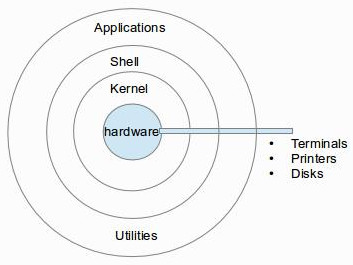
>hi

>djsjdsf

>eot

. ls -al > /dev/null : 쓰레기통으로

**15. Shell과 Kernel**



ls -l, ls;pwd등과 같이 입력한 명령을 shell이 받아서 kernel에게 전달. Kernel은

이 명령을 H/W에 전달 결과를 실행.

**16. bash vs zsh**

1) echo

echo $0 : bash

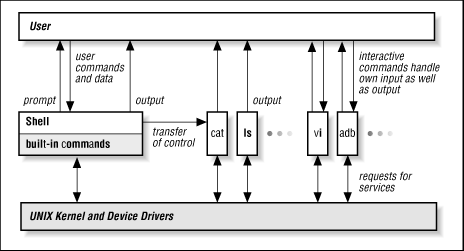
cd + tabkey : 숨긴 directory도 표시

2) zsh

echo $0 : zsh

cd + tabkey :

같은 kernel에 대해 다양한 shell이 존재할 수 있음.



ZSH에서 bash로 돌아 올 경우 : bash만 치면 됨.

**17. Shell Script**

여러 개의 shell명령어를 순서대로 실행할 수 있도록 하는 기능(Batch)

<script사용 전>

$mkdir script

$cd script

$touch a.log b.log c.log

$mkdir bak; cp \*.log bak

<Script사용>

$nano backup

#!/bin/bash : #! bin/bash를 통해서 실행된다는 것을 정의

if ! [ -d bak ]; then

mkdir bak

fi

cp \*.log bak

<실행을 하려면>

$./backup : permission denied

**$chmod +x backup : ls -l을 해보면 -rw-rw-r-- 1 backup이 -rwxrwxr-x로 바뀜 :권한 획득**

$./backup

<서버의 상태를 확인>

$ ~/script/serverstat

|  |
| --- |
| #!/bin/bash  sudo /opt/lampstack-5.6.30-1/ctlscript status |

**18. Directory**

google에서 linux directory structure 검색

http://www.thegeekstuff.com/2010/09/linux-file-system-structure/?utm\_source=tuicool

1. / – Root

* Every single file and directory starts from the root directory.
* Only root user has write privilege under this directory.
* Please note that /root is root user’s home directory, which is not same as /.

2. /bin – User Binaries 사용자가 사용하는 실행 프로그램들

* Contains binary executables.
* Common linux commands you need to use in single-user modes are located under this directory.
* Commands used by all the users of the system are located here.
* For example: ps, ls, ping, grep, cp.



3. /sbin – System Binaries

* Just like /bin, /sbin also contains binary executables.
* But, the linux commands located under this directory are used typically by system aministrator, for system maintenance purpose.
* For example: iptables, reboot, fdisk, ifconfig, swapon

4. /etc – Configuration Files

* Contains configuration files required by all programs.
* This also contains startup and shutdown shell scripts used to start/stop individual programs.
* For example: /etc/resolv.conf, /etc/logrotate.conf

5. /dev – Device Files

* Contains device files.
* These include terminal devices, usb, or any device attached to the system.
* For example: /dev/tty1, /dev/usbmon0

6. /proc – Process Information

* Contains information about system process.
* This is a pseudo filesystem contains information about running process. For example: /proc/{pid} directory contains information about the process with that particular pid.
* This is a virtual filesystem with text information about system resources. For example: /proc/uptime

7. /var – Variable Files

* var stands for variable files.
* Content of the files that are expected to grow can be found under this directory.
* This includes — system log files (/var/log); packages and database files (/var/lib); emails (/var/mail); print queues (/var/spool); lock files (/var/lock); temp files needed across reboots (/var/tmp);

8. /tmp – Temporary Files

* Directory that contains temporary files created by system and users.
* Files under this directory are deleted when system is rebooted.

9. /usr – User Programs

* Contains binaries, libraries, documentation, and source-code for second level programs.
* /usr/bin contains binary files for user programs. If you can’t find a user binary under /bin, look under /usr/bin. For example: at, awk, cc, less, scp
* /usr/sbin contains binary files for system administrators. If you can’t find a system binary under /sbin, look under /usr/sbin. For example: atd, cron, sshd, useradd, userdel
* /usr/lib contains libraries for /usr/bin and /usr/sbin
* /usr/local contains users programs that you install from source. For example, when you install apache from source, it goes under /usr/local/apache2

10. /home – Home Directories

* Home directories for all users to store their personal files.
* For example: /home/john, /home/nikita

11. /boot – Boot Loader Files

* Contains boot loader related files.
* Kernel initrd, vmlinux, grub files are located under /boot
* For example: initrd.img-2.6.32-24-generic, vmlinuz-2.6.32-24-generic

12. /lib – System Libraries

* Contains library files that supports the binaries located under /bin and /sbin
* Library filenames are either ld\* or lib\*.so.\*
* For example: ld-2.11.1.so, libncurses.so.5.7

13. /opt – Optional add-on Applications

* opt stands for optional.
* Contains add-on applications from individual vendors.
* add-on applications should be installed under either /opt/ or /opt/ sub-directory.

14. /mnt – Mount Directory

* Temporary mount directory where sysadmins can mount filesystems.

15. /media – Removable Media Devices

* Temporary mount directory for removable devices.
* For examples, /media/cdrom for CD-ROM; /media/floppy for floppy drives; /media/cdrecorder for CD writer

16. /srv – Service Data

* srv stands for service.
* Contains server specific services related data.
* For example, /srv/cvs contains CVS related data.

**19. Process**

processor : process를 실행

Memory : Memory에 적재

Storage : program이 저장

Process Monitoring :

1) ps

ps -aux

ps aux | grep apache

sudo kill 21222

2) sudo top or htop

**20. file을 찾는법**

1) file의 위치를 찾는 방법

- $locate \*.log

- sudo updatedb

\* **http://www.tecmint.com/35-practical-examples-of-linux-find-command/**

- $find --help | head

- $find ~ -name \*.log : 본인의 directory 하위의 모든 directory를 검색

\*.log를 찾아라

$find / -name \*.log : 시스템 전체에서 찾아라 sudo를 붙여야 함.

2) 실행파일을 찾는 whereis, $PATH로 명령어가 어디에 위치하는가를 지정

- $whereis rm

- $echo $PATH : 환경변수

**21. Background 실행**

1) 두 개의 Program을 전환하는 방법

- $nano 로 edit하고 있다가 file을 save하되 종료하지 않고 ctr+Z를 누르면

다른 작업이 가능

- $fg를 누르면 foreground 인 nano로 전환

- $jobs : background에서 실행되는 file들을 볼 수 있음

- $vim : vi tool

- $Ctr-Z; $jobs : 2개의 shell nano와 vim이 stopped되어 있다

- $fg %2

-$kill %4 or kill -9 %4

2) 실행하면서 background로 작업을 수행

. ls -alR / > result.txt 2>error.log &

**22. Daemon, Service**

1) Daemon : 항상 실행이 되고 있다.

$sudo apt-get install apache2

$cd /etc/init.d/ : demon들이 위치하는 directory임

2) Demon용 서비스를 키고,끌 경우

$sudo service apache2 start :

$ps aux | grep apache2

$sudo service apache2 stop : 끄는 명령어

3) $cd \etc ; $rc.tabkey

cd rc3.d/ : S02apache2-> ../init.d/apache2

$./S02apache2

**23. cron : Time based job schedule**

1) 정기적으로 어떠한 작업을 실행하여야 하는 경우

$crontab -e : google에서 crotab exp로 검색

1/\* \* \* \* \* date >> date.log

$date >> date.log

$cat date.log

$crontab -l

$cd ~ ; ls

$tail -f date.log

$cron -e

\*/1 \* \* \* \* date 1>> date.log 2>&1: 표준 error를 표준 출력으로

2) 10000명에게 -mail을 보내는 경우 사용자가 전송하고 서버에서는 저장 후

전송자에게 response를 주고 서버 side에서 background로 전송을 하는 경우

cron을 사용함

**24 shell을 시작할 때 특정한 명령어를 실행하는 방법**

1) alias - https://www.cyberciti.biz/tips/bash-aliases-mac-centos-linux-unix.html

alias l ='ls -al'

alias .. = 'cd..'

2) shell을 열었을때 이러한 기능을 사용하려면

$echo $SHELL : /bin/bash

$cd ~

$nano .bashrc

echo 'Hi bash'

$

**25. 다중 사용자**

1) id : 나는 누구인가?

$id

2) who : 누가 접속해 있는가?

**26 관리자와 일반 사용자**

1) Root user (Super user)

일시적으로 권한을 위임 : $sudo apt-get update;

~$ : 일반유저, #: superuser

$su - root : 변경

Password:

root@ubunu:~# id : super user로 변경된 것임

root@ubunu:~# exit

$sudo passwd -u root : root password를 unlock

$su - root : super user 권한

$sudo passwd -l root : root password을 lock

$su - root

2) 일반사용자의 추가 : unix add user google검색

$sudo useradd -m duru

$su - duru

$sudo passwd duru

<sudo 권한을 줄려면>

$sudo adduser hduser sudo 또는

$sudo usermod -a -G sudo duru

**Steps to create a new sudo user on Ubuntu**

1. First add the user, run: sudo adduser <UserNameHere>
2. Add the user to sudo group by typing the command in terminal for Ubuntu version 12.04 and above: sudo adduser <UserNameHere> sudo
3. In older version of Ubuntu (version 12.04 and older), run: sudo adduser <UserNameHere> admin
4. Verify it: id <UserNameHere>

https://www.cyberciti.biz/faq/how-to-add-delete-grant-sudo-privileges-to-users-on-freebsd-unix-server/

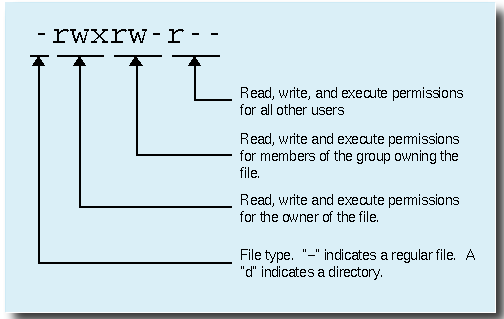
**Linux: Delete / Remove User Account**

userdel userName  
userdel [options] userName  
userdel -r userName

**27 권한(Permission)**

\* https://help.ubuntu.com/community/FilePermissions

\* https://en.wikipedia.org/wiki/Chmod

****

Here are a few examples of chmod usage with letters (try these out on your system).

First create some empty files:

user@host:/home/user$ touch file1 file2 file3 file4

user@host:/home/user$ ls -l

total 0

-rw-r--r-- 1 user user 0 Nov 19 20:13 file1

-rw-r--r-- 1 user user 0 Nov 19 20:13 file2

-rw-r--r-- 1 user user 0 Nov 19 20:13 file3

-rw-r--r-- 1 user user 0 Nov 19 20:13 file4

Add owner execute bit:

user@host:/home/user$ chmod u+x file1

user@host:/home/user$ ls -l file1

-rwxr--r-- 1 user user 0 Nov 19 20:13 file1

Add other write & execute bit:

user@host:/home/user$ chmod o+wx file2

user@host:/home/user$ ls -l file2

-rw-r--rwx 1 user user 0 Nov 19 20:13 file2

Remove group read bit:

user@host:/home/user$ chmod g-r file3

user@host:/home/user$ ls -l file3

-rw----r-- 1 user user 0 Nov 19 20:13 file3

Add read, write and execute to everyone:

user@host:/home/user$ chmod ugo+rwx file4

user@host:/home/user$ ls -l file4

-rwxrwxrwx 1 user user 0 Nov 19 20:13 file4

user@host:/home/user$

chmod with Numbers

Usage: chmod {options} filename

|  |  |
| --- | --- |
| **Options** | **Definition** |
| #-- | owner |
| -#- | group |
| --# | other |
| 1 | execute |
| 2 | write |
| 4 | read |

**Numerical permissions**

|  |  |  |
| --- | --- | --- |
| **#** | **Permission** | **rwx** |
| 7 | read, write and execute | rwx |
| 6 | read and write | rw- |
| 5 | read and execute | r-x |
| 4 | read only | r-- |
| 3 | write and execute | -wx |
| 2 | write only | -w- |
| 1 | execute only | --x |
| 0 | none | --- |

Here are a few examples of chmod usage with numbers (try these out on your system).

First create some empty files:

user@host:/home/user$ touch file1 file2 file3 file4

user@host:/home/user$ ls -l

total 0

-rw-r--r-- 1 user user 0 Nov 19 20:13 file1

-rw-r--r-- 1 user user 0 Nov 19 20:13 file2

-rw-r--r-- 1 user user 0 Nov 19 20:13 file3

-rw-r--r-- 1 user user 0 Nov 19 20:13 file4

Add owner execute bit:

user@host:/home/user$ chmod 744 file1

user@host:/home/user$ ls -l file1

-rwxr--r-- 1 user user 0 Nov 19 20:13 file1

Add other write & execute bit:

user@host:/home/user$ chmod 647 file2

user@host:/home/user$ ls -l file2

-rw-r--rwx 1 user user 0 Nov 19 20:13 file2

Remove group read bit:

user@host:/home/user$ chmod 604 file3

user@host:/home/user$ ls -l file3

-rw----r-- 1 user user 0 Nov 19 20:13 file3

Add read, write and execute to everyone:

user@host:/home/user$ chmod 777 file4

user@host:/home/user$ ls -l file4

-rwxrwxrwx 1 user user 0 Nov 19 20:13 file4

user@host:/home/user$

**chmod with sudo**

Changing permissions on files that you do not have ownership of: (**Note** that changing permissions the wrong way on the wrong files can quickly mess up your system a great deal! Please be careful when using **sudo**!)

user@host:/home/user$ ls -l /usr/local/bin/somefile

-rw-r--r-- 1 root root 550 2005-11-13 19:45 /usr/local/bin/somefile

user@host:/home/user$

user@host:/home/user$ sudo chmod o+x /usr/local/bin/somefile

user@host:/home/user$ ls -l /usr/local/bin/somefile

-rw-r--r-x 1 root root 550 2005-11-13 19:45 /usr/local/bin/somefile

user@host:/home/user$

**28. 그룹**

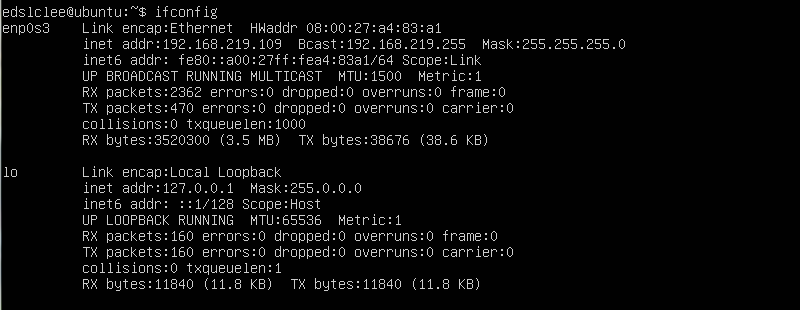
**29. 인터넷, 네트워크,서버**

1) 자신의 IP Address를 알 수 있는 방법

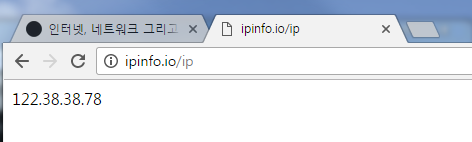
**- $ip addr**



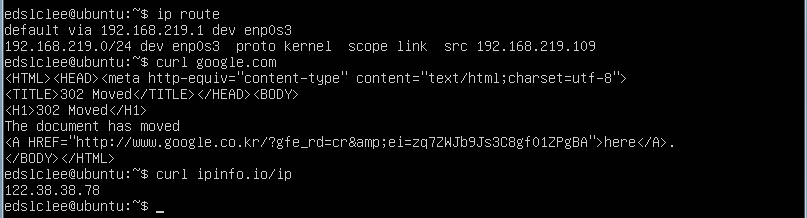
**- $ifconfig**



**- ipinfo.io/ip**

**susucd /**

**linux : $curl google.com; curl ipinfo.io/ip**

****

**- default IP address : $ip route**

****

2) 외부 IP(ipinfo.io/ip)는 122.38.38.78이고 내부 IP의 default gateway(ip route)는 192.168.219.1 서버가 설치된 내부 IP(ifconfig)는 192.168.219.109임

****

122.38.38.78:9000

192.168.219.1

9000-> 192.168.219.109:80

Private Address

Public Address

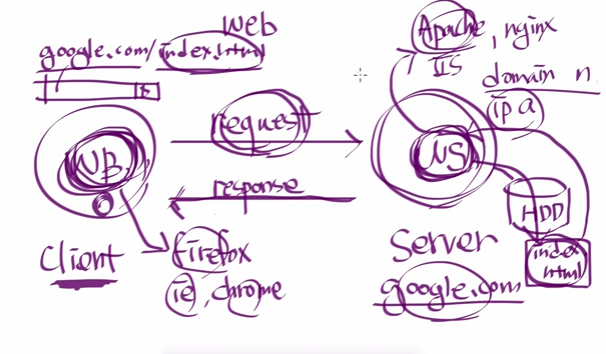
192.168.219.104

192.168.219.106

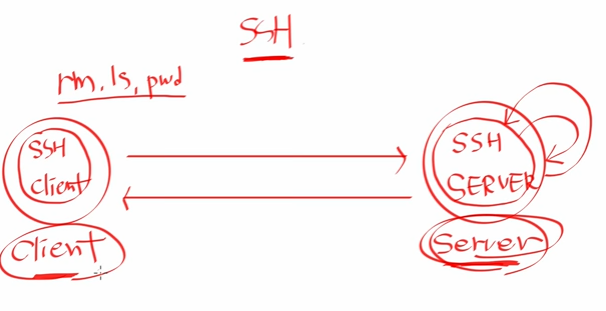
122.38.38.78

192.168.219.109

**30. 웹서버(Apache)**



**31. 원격제어(ssh)**

****

1) Sever설치

- $sudo apt-get install openssh-server

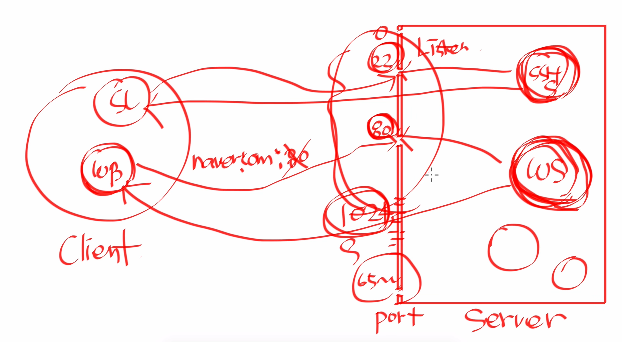
- $sudo service ssh start

- $sudo aux | grep ssh

2) client

windows Putty설치

**32. port**

**nan**

1) Port개요

$sudo nano /etc/ssh/sshd\_config

port 22 -> 2222

$sudo service ssh restart

client에서 2222로 접속해야 함.

2) port forwading



**33. Domain**

**34. 서버간 동기화(rsync)**

$mkdir rsync

$cd rsync

$mkdir source dest

$cd source

$touch test{1..10} : 한꺼번에 10개의 파일을 생성함 test1 ~ test10까지

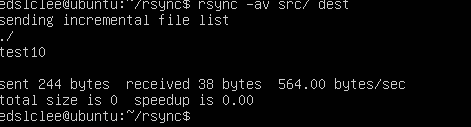
$cd ..

$rsync source\ dest : source밑의 도든 파일을 des로 Rsync한다

이 상태에서 dest의 test10 파일을 삭제하고

$rsync -av source\ dest를 하면

test10만 복사한다 : 즉 증분된(incremental) 부분만 복사함



원본과 복사본이 같으면 아무것도 안한다.

rsync -a : archive mode로 동작한다.

- remote

$rsync -aZP ~/rsync/src/ k8805@192.168.0.65:~/rsync/dest/

password:

### [Apache2 설치 (Ubuntu 16.04)](http://lng1982.tistory.com/288)

nklee 2017.09.15 10:47

**설치**

ubuntu 기본 소프트웨어 저장소에 사용할 수 있는 apache가 있다.

1. root 로그인

2. 패키지 관리 툴인 apt-get을 이용하여 apache2를 설치한다. (apache2 설치와 함께 의존하는 프로그램도 함께 설치된다.)

 > apt-get update

 > apt-get install apache2

3. 설치 후 Apache 상태 확인

 > systemctl status apache2

4. Apache 접속

 > sername -I  명령어를 통해 IP를 알아낸 후 웹 브라우저를 이용하여 http://{IP} 로 접속해보자.

**Apache Configuration**

/etc/apache2/

아파치 설정 디렉토리

/etc/apache2/apache2.conf

아파치 기본 설정 파일

/etc/apache2/ports.conf

아파치 포트 설정 파일

/etc/apache2/sites-available/

virtual host 관리 디렉토리 (아파치에서는 해당 디렉토리를 직접 참조하지는 않는다.)

/etc/apache2/sites-enabled/

virtual host를 이용하기 위한 설정 디렉토리

000-default.conf -> ../sites-available/000-default.conf 와 같이 심볼릭 링크를 이용하여 sites-available 디렉토리 파일을 참조하는 방식으로 사용되어진다.

/etc/apache2/mods-available/, /etc/apache2/mods-enabled/

모듈 설정 디렉토리

**로그**

/var/log/apache2 디렉토리

**시작,중지**

root 로그인

service apache2 start

service apache2 stop

**버전 확인**

apachectl -version

**모듈 사용 설정 확인**

apachectl -M

**Reverse Proxy 설정**

mod\_proxy 모듈을 이용해 Reverse Proxy 설정을 하겠다.

root로 로그인

a2enmod 명령어를 통해 아래 모듈 활성화

|  |  |  |
| --- | --- | --- |
| 1  2  3  4 | a2enmod proxy  a2enmod proxy\_http  a2enmod proxy\_balancer  a2enmod lbmethod\_byrequests | [cs](http://colorscripter.com/info#e) |

활성화를 한다고 해서 모듈을 다운로드 받고 설치하는 작업을 하는게 아니다.

단지 mods-available 디렉토리에 존재하는 모듈을 사용 가능한 상태로 만들기 위해 mods-enabled 하위에 심볼릭 링크를 생성한다.

Apache 서버 재시작 하자.

root로 로그인

service apache2 restart

**궁금**

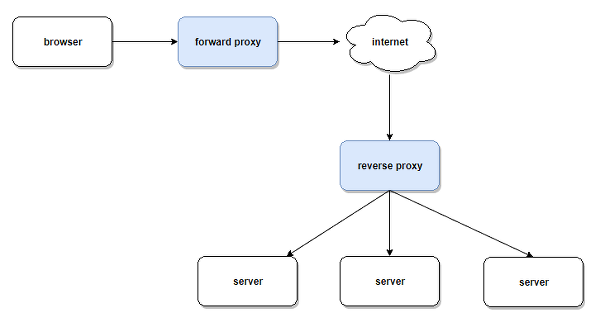
**1. reverse proxy와 forward proxy 차이**

대게 인터넷에 떠도는 정보를 얻기 위해서는 브라우저를 키고 도메인을 입력한 후 접속하여 내가 원하는 정보를 취득한다.

여기에 브라우저는 요청자가 되고 정보를 제공하는 웹 서버는 응답자가 된다.

forward proxy는 요청자 앞단에 위치하고 있는 서버를 말하는 것이고 reverse proxy는 응답자 앞단에 위치한다.

여기서 궁금한 것은 reverse라는 단어가 왜 붙었냐는 것인데.. 이유는 아래 흐름을 보면 쉽게 알 수 있다.



server의 전면에 위치하고 있는 reverse proxy는 요청자의 요청을 받아서 서버로 보내주기 때문에 reverse라는 단어가 붙은 것으로 이해하면 되겠다.

L4, L7 스위치도 어찌보면 reverse proxy라고 할 수 있겠다.

**2. reverse proxy의 장점**

로드 밸런싱 가능

proxy서버에만 방화벽 설정 가능

보안 강화 - 웹 서버가 뚫리면 DB까지 털리지만 proxy서버가 있기 때문에 보안이 강화된다.

요청이 한 곳으로 집중되기 때문에 확장 가능성 (트래픽 감시, 로그 기록)

**참고**

설치

<https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-ubuntu-16-04>

모듈 추가

<https://www.digitalocean.com/community/tutorials/how-to-use-apache-as-a-reverse-proxy-with-mod_proxy-on-ubuntu-16-04>

<http://manpages.ubuntu.com/manpages/trusty/man8/a2enmod.8.html>

**버추얼박스 우분투 Apache MySQL PHP설치 및 제거**

<https://help.ubuntu.com/community/ApacheMySQLPHP>

※ 우분투서버의 apache2 는 **/var/www** 를 DocumentRoot 디렉토리로 기본 설정하고 있다.

/etc/apache2/sites-available/default 에서 DocumentRoot 를 수정하면 해당 디렉토리를 변경 할 수 있다.

php 도 제대로 설치되어있는지 확인해보려면, /var/www/phpinfo.php 파일을 만들어서 <? phpifno(); ?> 내용으로 저장하고 브라우저로 확인해보면 php configuration 내용이 나오면 php 설치 성공.

**Apache 설정**

일반적인 아파치 설정은 원래 httpd.conf 파일이지만, 우분투에서는 아파치 설정파일이 세분화 되어있다. 아래참고.

/etc/apache2/apache2.conf : 기본설정

/etc/apache2/ports.conf : 포트설정

/etc/apache2/mods-enabled/dir.conf : index 파일설정

/etc/apache2/mods-available/userdir.conf : 사용자계정설정

/etc/apache2/mods-enabled/autoindex.conf : 언어셋 관련설정

/etc/apache2/mods-enabled/mime.conf : 파일타입설정

/etc/apache2/sites-enabled/default : 웹서비스설정

먼버 서버네임부터 등록한다. 이거 안해두면 자꾸 등록하라고 귀찮게 한다;

$ sudo vi /etc/apache2/apache2.conf

....

# Global configuration

ServerName "서버이름"

....

// 파일 저장 후 아파치 재시작

$ sudo /etc/init.d/apache2 restart

**PHP 설정**

우선 php5 가 적용되는 파일 확장자를 아파치설정에 추가해준다.

$ sudo vi /etc/apache2/mods-enabled/mime.conf

.....

AddType application/x-bzip2 .bz2

AddType application/x-httpd-php .php .php .php4 .php3 .inc .phtml .html .htm .xhtml // 추가

AddType application/x-httpd-php-source .phps // 추가

.....

// 파일 저장 후 아파치 재시작

$ sudo /etc/init.d/apache2 restart

**PhpMyAdmin 설치**

shell 에서 직접 mysql 을 관리하는 불편함을 덜고, 웹에서 편리하게 관리할수 있도록 phpmyadmin 을 설치한다.

// phpmyadmin 패키지 설치

$ sudo apt-get install phpmyadmin

// 아파치 설정파일을 열고 맨 마직막줄에 아래 구문 두줄을 추가한다

$ sudo vi /etc/apache2/apache2.conf

......

# Enable PhpMyAdmin

Include /etc/phpmyadmin/apache.conf

// 파일 저장후 아파치 재시작

$ sudo /etc/init.d/apache2 restart

브라우저에서 PhpMyAdmin 접속해서 우분투 설치때 입력한 mysql root password 와 함께 root 로 로그인해본다.

*ex) http://192.168.219.199/phpmyadmin*

**※ 외부 GUI 툴에서 Mysql 접근 가능하도록 하는 방법**

Mysql Workbench 와 같은 외부 툴에서도 mysql 접근이 가능하도록 하려면 약간의 설정이 필요하다.

우선 localhost(127.0.0.1) 이외에서도 접근 가능하도록 my.conf 의 bind-address 부분을 주석처리한다.

$ sudo vi /etc/mysql/my.cnf

....

#bind-address           = localhost // 주석(#) 처리

....

// 파일 저장후 mysql 재시작

$ sudo /etc/init.d/mysql restart

그리고 mysql 권한 설정을 통해 접근 권한을 준다.

$ mysql -u root -p // mysql 에 root 로 접속

$ mysql> use mysql; // database 'mysql' 선택

// root 사용자에게 어디서라도(%) 모든데이터베이스.모든테이블(\*.\*) 에 접근 가능한 권한을 준다.

$ mysql> GRANT ALL PRIVILEGES ON \*.\* to 'root'@'%' IDENTIFIED BY '패스워드';

$ mysql> flush privileges; // 권한 변경을 즉시 반영

**FTP 설치**

작성한 소스코드를 외부에서 쉽게 서버로 업로드 할수 있도록 ftp 가 필요하다.

우분투에서 가장 인기있는 vsftp 를 설치해보자.

// vsftpd 설치

$ sudo apt-get install vsftpd

// vsftpd 설정

$ sudo vi /etc/vsftpd.conf

....

anonymous\_enable=NO // YES 에서 NO 로 변경

local\_enable=YES // 주석(#) 제거

write\_enable=YES // 주석(#) 제거

local\_umask=022 // 주석(#) 제거

....

// vsftpd 재시작

$ sudo /etc/init.d/vsftpd restart

※ 참고: vsftpd 포트를 변경하려면 vsftpd.conf 에 아래처럼 추가해주면 된다  
listen=YES  
listen\_port=5020

그리고 DocumentRoot 인 /var/www 디렉토리의 소유자를 root 에서 자신의 관리자ID 로 변경하고,

자신의 계정 디렉토리에 /var/www 를 바라보는 심볼릭 링크를 만들어주면 ftp 를 통해서 홈디렉토리로 파일전송이 가능해진다.

$ sudo chown -R 관리자ID /var/www

$ cd

$ ln -s /var/www www

이제 filezilla 와 같은 외부 ftp 클라이언트를 통해서 ID/password 로 접속하고,

심볼릭 링크를 걸어둔 www 를 통해 홈디렉토리로 이동한 후 파일전송까지 잘되는것을 확인한다.

**※ 사용자계정 디렉토리를 설정해서 사용자별로 웹페이지 접근이 가능하도록 설정하는 방법**

우분투에서는 기본적으로 /var/www 를 통해서 웹서버로 접근하도록 구성되어 있지만,  
각 사용자 계정에 부여되는 공간에는 웹서버로 접근되지 않도록 디폴트로 설정 되어있다.

사용자 계정별로 웹페이지 접근이 가능하기 위해서 아파치 설정에서 해당 설정파일을 심볼릭링크로 추가해 주면 된다.

$ cd /etc/apache2/mods-enabled

$ sudo ln -s ../mods-available/userdir.conf userdir.conf

$ sudo ln -s ../mods-available/userdir.load userdir.load

$ sudo /etc/init.d/apache2 restart // 파일 저장 후 아파치 재시작

각 사용자 계정의 공간에 웹서버로 접근되도록 php 설정을 변경해준다.

$ sudo vi /etc/apache2/mods-enabled/php5.conf

// 아래 볼드처리된 부분을 주석처리 한다

...

    # Running PHP scripts in user directories is disabled by default

    #

    # To re-enable PHP in user directories comment the following lines

    # (from <IfModule ...> to </IfModule>.) Do NOT set it to On as it

    # prevents .htaccess files from disabling it.

**#<IfModule mod\_userdir.c>**

**#    <Directory /home/\*/public\_html>**

**#        php\_admin\_value engine Off**

**#    </Directory>**

**#</IfModule>**

...

$ sudo /etc/init.d/apache2 restart // 파일 저장 후 아파치 재시작

다음은 사용자 계정을 추가하여 각 사용자들에게 웹서버로 사용할 수 있는 공간을 만들어 보자.

참고로 각 사용자 계정의 홈디렉토리는 **사용자ID/public\_html/** 이다.

$ sudo adduser 사용자ID

// ... 패스워드 및 기타 정보를 입력하면 사용자계정이 추가된다

$ su - 사용자ID // 해당 사용자ID 로 전환

$ cd

$ mkdir public\_html // 홈디렉토리 생성

$ cp /var/www/index.html ./public\_html/

Mysql 에도 아래처럼 각 사용자별로 database 접근을 제한허용해 두면, 외부 mysql 클라이언트에서 각 사용자계정으로  접근시 사용자아이디와 같은 이름으로 된 데이터베이스에만 접근이 가능하게 된다.

$ mysql -u root -p // mysql 에 root 로 접속

$ mysql> create database 사용자ID; // 사용자ID 같은 이름으로된 database 생성

$ mysql> use mysql; // database 'mysql' 선택

// 사용자에게 어디서라도(%) 사용자ID와 같은 이름의 데이터베이스.모든테이블(\*.\*) 에 접근 가능한 권한을 준다.

$ mysql> GRANT ALL PRIVILEGES ON 사용자ID.\* to '사용자ID'@'%' IDENTIFIED BY '사용자패스워드';

$ mysql> flush privileges; // 권한 변경을 즉시 반영

각 사용자계정으로 FTP를 통해서 계정공간으로 파일 전송도 가능하다.

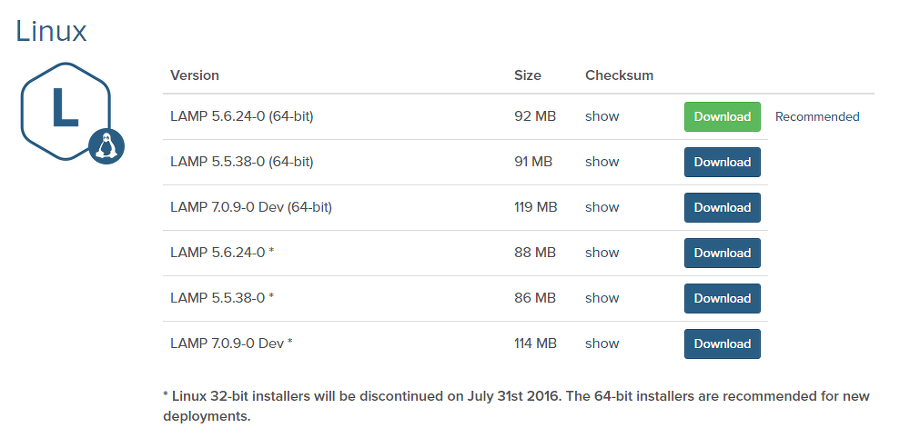
이제 브라우저를 통해서 http://서버IP주소/~사용자ID/ 로 접속해보면 **It Works!** 라는 문구를 확인할 수 있다.

*ex) http://192.168.219.199/~userid/*

출처: <http://www.overfloweb.com/32> [overfloweblog]

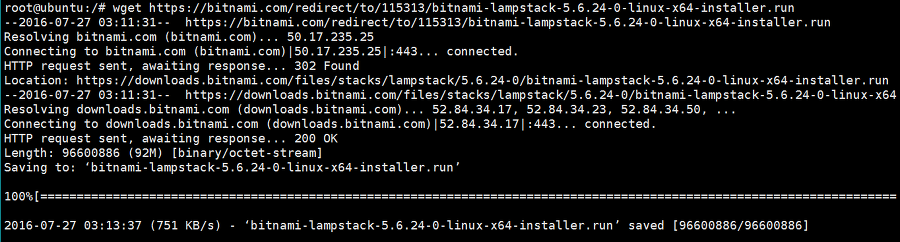
**35. Bitmnami설치**

https://bitnami.com/stack/lamp/installer



다운 받을 파일의 버튼을 오른쪽 클릭한 다음 링크 주소 복사를 한다. 터미널 창으로 들어가 wget 명령어를 사용하여 다운받는다.wget 복사한 링크 주소 붙여넣기

wget https://bitnami.com/redirect/to/115313/bitnami-lampstack-5.6.24-0-linux-x64-installer.run



chmod 명령어를 사용하여 권한을 변경해 준다.

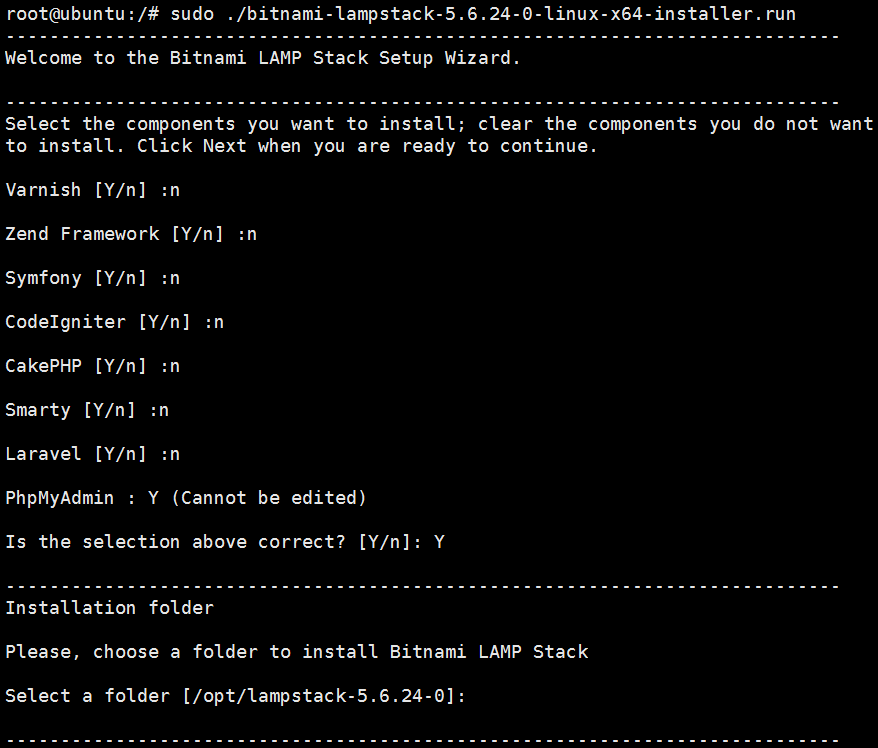
sudo chmod 755 bitnami-lampstack-5.6.24-0-linux-x64-installer.run

lamp를 설치 한다.

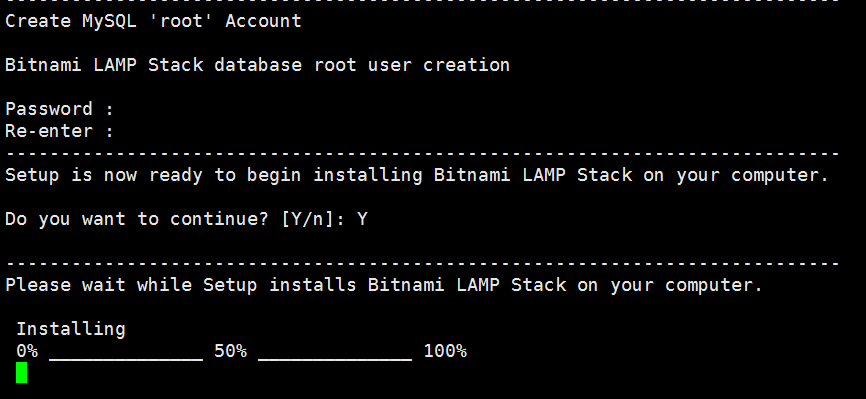
sudo ./bitnami-lampstack-5.6.24-0-linux-x64-installer.run

설치할 때 PhpMyAdmin을 제외한 나머지는 설치 하지 않는다. 전부 n 를 해준다.

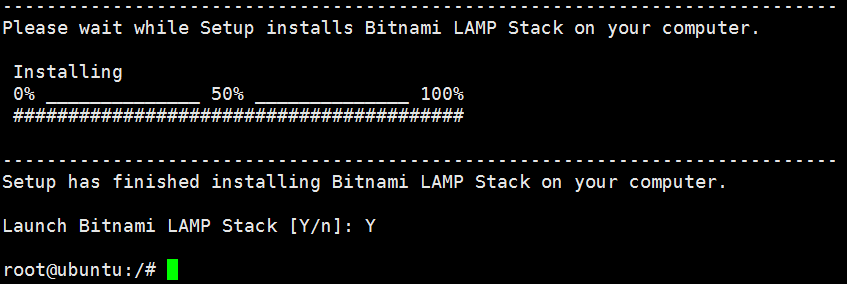
Bitnami의 설치 위치를 변경하지 않는다면 엔터 해준다. ( 기본은 /opt/lampstack-버전 )



MySQL의 root 사용자의 비밀번호를 설정해 준다.



설치 완료하면 실행 시켜 준다



apache 설정 파일 : Bitnami 설치경로/apache2/conf/httpd.conf

document root : Bitnami 설치경로/apache2/htdocs/

**36. server의 IP가 변동되는 경우**

1) IPv6로 변경되지 않도록 하는 방법

cd /etc/default

명령으로 해당 디렉토리로 이동. sudo vi grub  이나 sudo gedit grub , sudo nano grub  같은 명령으로 해당 파일을 수정. 수정해야 할 곳은

GRUB\_CMDLINE\_LINUX\_DEFAULT="quiet splash ipv6.disable=1"

다음, grub.cfg 를 생성해 준다.

sudo grub-mkconfig -o /boot/grub/grub.cfg

명령으로 해당 파일을 생성. 제대로 설정 되었는지 확인하려면, 재부팅시에 grub 이 실행되었을때 'e' 키를 눌러서 우리가 추가한 옵션이 잘 추가되어 있는지 확인 해 볼 수 있다.또한 ipv6 가 제대로 비활성화 되어있는지 확인해 보려면 부팅 후 에 '/proc/sys/net'  디렉토리를 확인해 보면 된다.원래는 여기에 'ipv6' 디렉토리가 있으나 위처럼 설정하고 확인해 보면 아예 ipv6 디렉토리가 존재하지 않는다.

2) 서버의 Ethernet IP가 변경될 경우 변경이 필요한 것들

2-1) Web Server의 주소: ifconfig, ip addr의 주소로

2-2) PhpMyadmin :

- putty의 접속변경 : 변경된 서버 IP로 변경

- http://127.0.0.1:8888/phpmyadmin/

**37. 서버제어**

1) Apache, MySQl 기동

sudo /opt/lampstack-5.6.30-1/ctlscript.sh start

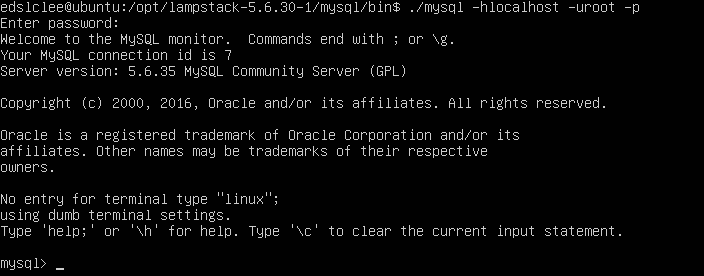
sudo /opt/lampstack-5.6.30-1/ctlscript.sh restart mysql

sudo /opt/lampstack-5.6.30-1/ctlscript.sh restart apache

Obtain current status of all services:

sudo /opt/lampstack-5.6.30-1/ctlscript.sh status

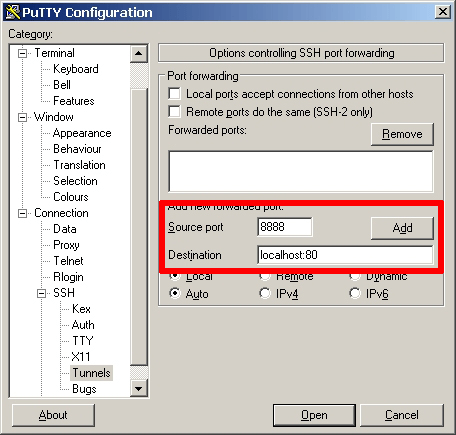
MYSQL



2) putty로 ssh session을 열고 phpmyadmin 접속

To access the application using your Web browser, create an SSH tunnel, as described below.

* Download PuTTY and make sure you can log in to the virtual machine console with it following the instructions in [the FAQ](https://docs.bitnami.com/virtual-machine/faq#how-to-connect-to-the-server-through-ssh). Once you have confirmed you are able to log in successfully, log back out.
* Reconnect to the virtual machine using PuTTY, this time adapting the steps to include an additional SSH tunnel. When configuring the new SSH session in PuTTY, additionally navigate to the "Connection -> SSH -> Tunnels" section and create a secure tunnel by forwarding port 80 on the virtual machine to port 8888 on the local host (127.0.0.1 or localhost).
* Click the "Add" button to add the secure tunnel configuration to the session. Here is an example:

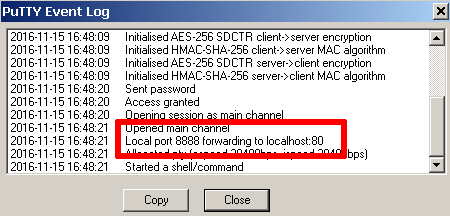
[](https://docs.bitnami.com/images/img/infrastructure/common/create-ssh-tunnel-8888-1822d77b.png)

* Go back to the "Session" section and save your changes by clicking the "Save" button.
* Click the "Open" button to open an SSH session to the virtual machine. The SSH session will now include a secure SSH tunnel between the two specified ports.

While the tunnel is active, you should be able to access the phpMyAdmin console through the secure SSH tunnel you created, by browsing to ㅊㅇ

To log in, use username root for MySQL. The default password is bitnami.

If you are unable to access phpMyAdmin, verify that the SSH tunnel was created by checking the PuTTY event log (accessible via the "Event Log" menu):

[](https://docs.bitnami.com/images/img/infrastructure/common/create-ssh-tunnel-log-409dee64.png)

3) web Browser에서 127.0.0.1:8888/phpmyadmin을 입력 연결됨.

**38. SSH Key를 이용하여 Git로 전송하기**

Git bash에서 ssh-keygen :

c:/user/.ssh/rsa-pub에서 Rsa-pub를 copy하여 github에 setup에서 등록