네트워크

로그 아날라이저 설치
어댑터 1 - 네트워크 연결(NAT-고급-케이블연결) - 스냅샷 찍기 - 시작(user/user) - ping 8.8.8.8 확인

 - 웹 기반 : Apache(WAS), mysql(or mariadb), php => AMP

```
user@cloud:~$ sudo apt install lamp-server^    //lamp=리눅스 AMP
......
Creating config file /etc/php/7.2/apache2/php.ini with new version
Module mpm_event disabled.
Enabling module mpm_prefork.
apache2_switch_mpm Switch to prefork
apache2_invoke: Enable module php7.2
Setting up php-mysql (1:7.2+60ubuntu1) ...
Setting up mysql-server (5.7.37-0ubuntu0.18.04.1) ...
Setting up libapache2-mod-php (1:7.2+60ubuntu1) ...
Processing triggers for libc-bin (2.27-3ubuntu1.5) ...
Processing triggers for systemd (237-3ubuntu10.53) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for ufw (0.36-0ubuntu0.18.04.2) ...
Processing triggers for ureadahead (0.100.0-21) ...
```

```
user@cloud:~$ sudo apt-get install rsyslog-mysql       //자동화 no 선택
Creating config file /etc/rsyslog.d/mysql.conf with new version
dbconfig-common: flushing administrative password
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for libc-bin (2.27-3ubuntu1.5) ...
```

```
user@cloud:~$ sudo mysql -u root -p
Enter password:                              //입력하지 않고 엔터만 치기
mysql> CREATE DATABASE Syslog;
Query OK, 1 row affected (0.00 sec)
```

※ 에러날때
mysql> show database; => 목록에 syslog가 있는지 확인

```
mysql> drop database Syslog;
Query OK, 1 row affected (0.00 sec)

mysql> show database; => 목록에 syslog가 없어야 한다.

mysql> CREATE DATABASE Syslog;
Query OK, 1 row affected (0.00 sec)
```

```
mysql> GRANT ALL ON Syslog.* TO 'rsyslog'@'localhost' IDENTIFIED BY 'Password';
Query OK, 0 rows affected, 1 warning (0.00 sec)

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)

mysql> exit
Bye

user@cloud:~$ sudo mysql -u rsyslog -D Syslog -p < /usr/share/dbconfig-common/data/rsyslog-mysql/install/mysql
Enter password:Password

user@cloud:~$ sudo mysql -u root -p
Enter password:

mysql> CREATE DATABASE loganalyzer;
Query OK, 1 row affected (0.00 sec)

mysql> GRANT ALL ON loganalyzer.* TO 'loganalyzer'@'localhost' IDENTIFIED BY 'Password';
Query OK, 0 rows affected, 1 warning (0.00 sec)

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)

mysql> exit
Bye
user@cloud:~$ sudo vim /etc/rsyslog.conf
 17 module(load="imudp")                    //#풀려있어야 함(17,18,21,22)
 18 input(type="imudp" port="514")          //514 = syslog 포트번호
 module(load="imtcp")
 input(type="imtcp" port="514")

user@cloud:~$ sudo vim /etc/rsyslog.d/mysql.conf
  *.* action(type="ommysql" server="localhost" db="Syslog" uid="rsyslog" pwd="Password")
      //pwd(패스워드) 입력하기

user@cloud:~$ sudo systemctl restart rsyslog.service  //오류가 나면 오타가 발생한것
user@cloud:~$ cd /tmp
user@cloud:/tmp$ wget https://download.adiscon.com/loganalyzer/loganalyzer-4.1.12.tar.gz
......
2022-04-26 10:13:19 (1.83 MB/s) - ‘loganalyzer-4.1.12.tar.gz’ saved [5028816/5028816]

user@cloud:/tmp$ ls
loganalyzer-4.1.12.tar.gz     //압축파일
user@cloud:/tmp$ tar -xzvf loganalyzer-4.1.12.tar.gz
user@cloud:/tmp$ ls
loganalyzer-4.1.12            //압축해제 후 디렉토리
loganalyzer-4.1.12.tar.gz
user@cloud:/tmp$ sudo mkdir /var/www/html/loganalyzer     //디렉토리 생성
user@cloud:/tmp$ sudo cp -r /tmp/loganalyzer-4.1.12/src/* /var/www/html/loganalyzer/
user@cloud:/tmp$ cd /var/www/html/loganalyzer/
user@cloud:/var/www/html/loganalyzer$ ls
admin                 convert.php   favicon.ico   js                      search.php
asktheoracle.php      cron          images        lang                    statistics.php
BitstreamVeraFonts    css           include       login.php               templates
chartgenerator.php    details.php   index.php     reportgenerator.php     themes
classes               export.php    install.php   reports.php             userchange.php
user@cloud:/var/www/html/loganalyzer$ sudo touch config.php      //설정을 저장하는 파일
user@cloud:/var/www/html/loganalyzer$ sudo chown www-data:www-data config.php
user@cloud:/var/www/html/loganalyzer$ sudo chmod 666 config.php
user@cloud:/var/www/html/loganalyzer$ sudo chown www-data:www-data -R
/var/www/html/loganalyzer/
```

인터넷에서 192.168.56.101/loganalyzer 들어보기

step 1. here - next - step 2.녹색 불 떠야함 - next - step 3. 50 80 30 yes yes yes locahost 3306 loganalyzer logcon_ loganalyzer Password

- step 4. - next - step 5. - next - step 6. admin admin admin - next - step 7. source type MYSQL Native Syslog SystemEvents rsyslog Password

- next - step 8. - finish

어댑터 1 네트워크 연결하지 않음으로 변경 - gns 켜기
22.04.26 파일 생성

라우터와 스위치만 켜기(스위치의 e0/0, e0/1은 라우터로 되어있기 때문에 e1/0부터 스위치로 사용할 수 있다.)
라우터에 DHCP서버로 변경
컴퓨터 켜서 IP 받아지는지 확인 후 서버 오픈
서버 들어가서(ID user Pass user) IP 확인(enp0s3)
컴퓨터 10.100
서버 10.101

윈도우에서 인터넷을 통해 http://172.16.10.101/loganalyzer/ 에 들어가져야 한다.

```
R1(config)#logging on
R1(config)#logging buffered 4096(=4MB)
R1(config)#logging host 172.16.10.101 or logging 172.16.10.101
R1(config)#logging trap ?
  <0-7>          Logging severity level
  alerts         Immediate action needed           (severity=1)
  critical       Critical conditions               (severity=2)
  debugging      Debugging messages                (severity=7)
  emergencies    System is unusable                (severity=0)
  errors         Error conditions                  (severity=3)
  informational  Informational messages            (severity=6)
  notifications  Normal but significant conditions (severity=5)
  warnings       Warning conditions                (severity=4)
  <cr>
R1(config)#logging trap debugging or logging trap 7
R1(config)#logging origin-id string Cloud-502
R1(config)#end
R1#
*Mar  1 00:24:57.299: %SYS-5-CONFIG_I: Configured from console by console
R1#
*Mar  1 00:24:58.303: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 172.16.10.101 port 514 started - CLI initiated

ESW1(config)#int vlan 1
ESW1(config-if)#ip add dhcp(172.16.10.102)
ESW1(config-if)#no sh
```

logging 하기 -> 확인

```
R1(config)#logging on
R1(config)#logging buffered 4096(=4MB)
R1(config)#logging host 172.16.10.101
R1(config)#logging trap 7
R1(config)#logging origin-id string Cloud-502
R1(config)#end
```

※ 라우터에서 SSH 활성화

```
R1#sh control-plane host open-port            //열려있는 포트 확인
Active internet connections (servers and established)
Prot        Local Address       Foreign Address                 Service     State
 tcp                  *:23                  *:0                  Telnet    LISTEN
 udp              *:60128     172.16.10.101:514                   Syslog ESTABLIS
 udp                   *:67                  *:0            DHCPD Receive    LISTEN
R1#sh ip domain           //히든 명령어
R1(config)#ip domain-name 502.com
R1(config)#do sh ip domain
502.com
R1(config)#do sh crypto key mypubkey rsa
없음
R1(config)#crypto key generate rsa
The name for the keys will be: R1.502.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#
*Mar  1 01:00:36.559: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#username admin password admin
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#tran
R1(config-line)#transport input ssh
R1(config-line)#exit
R1(config)#ip ssh version 2       //ssh 버전을 2로 변경
R1#show ip ssh
SSH Enabled - version 2.0
```

```
Authentication timeout: 120 secs; Authentication retries: 3
```

※ 원격부분 access-list 하기

```
R1(config)#access-list 10 permit host 172.16.10.100
R1(config)#line vty 0 4
R1(config-line)#access-class 10 in
```

PC에서 PuTTY로 접속