Radius Server, NMS Server, SSO(통합인증 관리자)

1. Radius Server(SSO)

1) <라우터 및 스위치 인증 절차>

/etc/freeradius/3.0$ sudo vim clients.conf

```
client R5{
ipaddr=172.16.10.1
secret=1234
}

client SW1{
ipaddr=172.16.10.2
secret=1234
}

client SW2{
ipaddr=172.16.10.6
secret=1234
}

client SW3{
ipaddr=192.168.10.250
secret=1234
}

client SW4{
ipaddr=192.168.30.250
secret=1234
}

client SW5{
ipaddr=192.168.20.250
secret=1234
}
```

2) /etc/freeradius/3.0$ sudo vim users

radius Cleartext-Password := “radius”입력하여 변경

```
216 ##########################################################
217 # You should add test accounts to the TOP of this file! #
218 # See the example user "bob" above.                      #
219 ##########################################################
220 radius Cleartext-Password := "radius"
221
```

<Radius 서버 서비스 시작 및 상태 확인>

sudo service freeradius restart

sudo service freeradius status

2. NMS Server & rsyslog

1. rsyslog 설정

1) sudo vim /etc/rsyslog.conf 아래와 같이 수정 및 내용 추가

```
16 # provides UDP syslog reception
17 module(load="imudp")
18 input(type="imudp" port="514")
19
20 # provides TCP syslog reception
21 module(load="imtcp")
22 input(type="imtcp" port="514")
23
24 # provides kernel logging support and enable non-kernel klog messages
25 module(load="imklog" permitnonkernelfacility="on")
```

```
59 $IncludeConfig /etc/rsyslog.d/*.conf
60 $template remote-incoming-logs,"/var/log/%FROMHOST-IP%.log"
61 *.* ?remote-incoming-logs
```

<rsyslog 서비스 재시작 및 상태 확인>

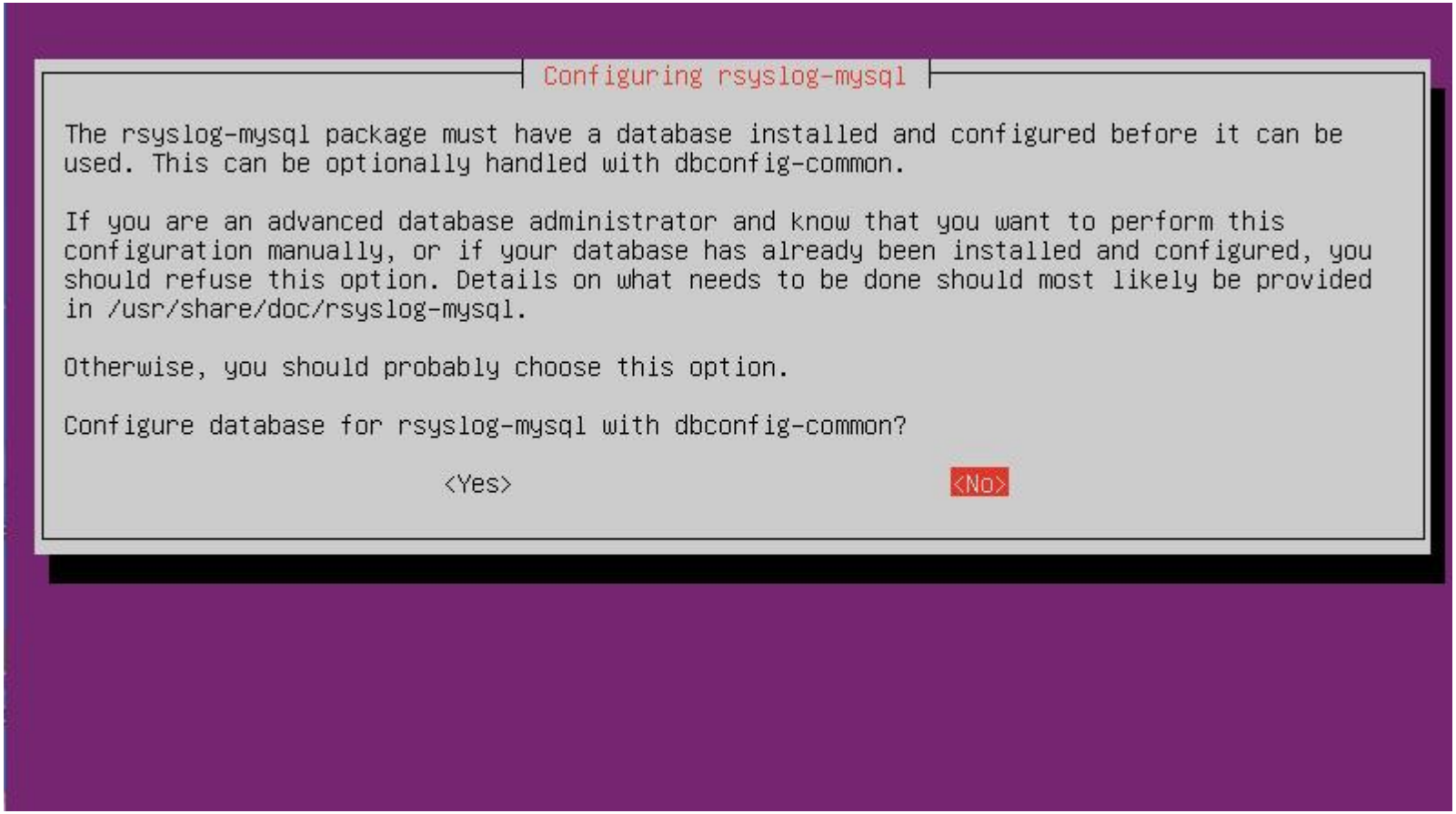
sudo service rsyslog restart

sudo service rsyslog status

2. Log Analayzer 설치

1) sudo apt install lamp-server^

2) sudo apt-get install rsyslog-mysql (아래창 No 선택)



3) sudo mysql -u root –p로 접속하기(root권한 접속이기 때문에 비번이 필요없이 접속)

3-1) CREATE DATABASE Syslog;

3-2) show databases; - Syslog 생성되어 있는지 확인하기

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| Syslog             |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
5 rows in set (0.00 sec)
```

3-3) PRIVILEGES 권한 주고 그 권한을 적용합니다.

```
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)
```

3-4) 다시 sudo mysql -u root –p로 접속 아래와 같이 진행(loganalyzer 생성, 권한 주고 권한 적용하기)

```
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 (0.01 sec)
```

3-5) sudo vim /etc/rsyslog.d/mysql.conf

. action(type="ommysql" server="localhost" db="Syslog" uid="rsyslog" pwd="Password")으로 수정

```
### Configuration file for rsyslog-mysql
### Changes are preserved

module (load="ommysql")
*.* action(type="ommysql" server="localhost" db="Syslog" uid="rsyslog" pwd="Password")
```

3-6) sudo systemctl restart rsyslog.service

4. loganalyzer 페이지 구축

4-1) cd /tmp하여 디렉토리 변경 후 wget https://download.adiscon.com/loganalyzer/loganalyzer-4.1.12.tar.gz - 압축파일받기

4-2) tar -xzvf loganalyzer-4.1.12.tar.gz하여 압축 풀어주기

<loganalyzer 페이지 생성>

4-3) sudo mkdir /var/www/html/loganalyzer

4-4) sudo cp -r /tmp/loganalyzer-4.1.12/src/* /var/www/html/loganalyzer/

<loganalyzer 설정파일 만들어주고 소유권을 주기>

4-5) sudo touch config.php

4-6) sudo chown www-data:www-data config.php

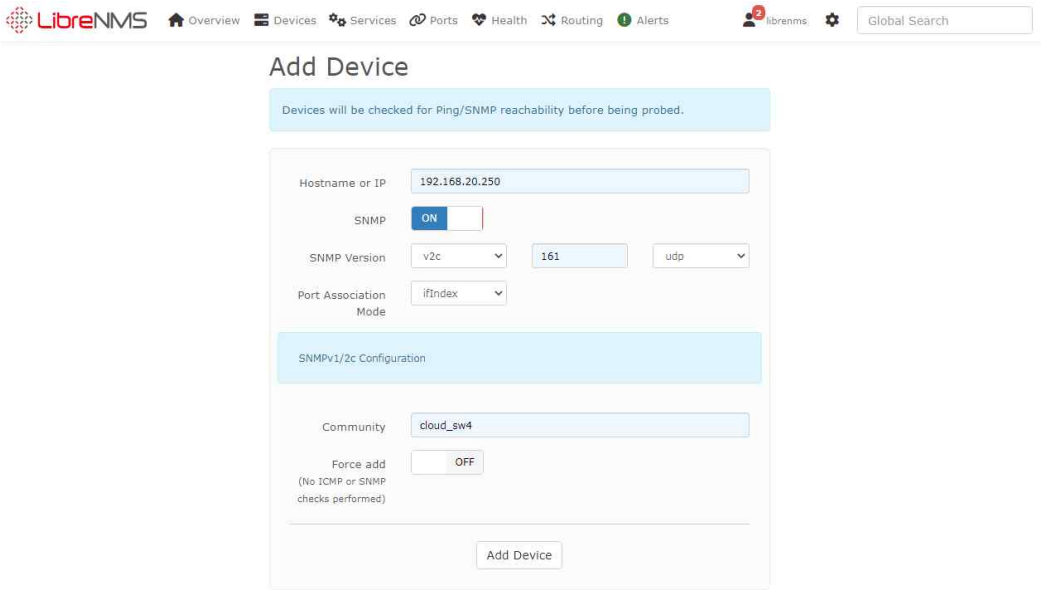
4-7) sudo chmod 666 config.php

4-8) sudo chown www-data:www-data -R /var/www/html/loganalyzer/

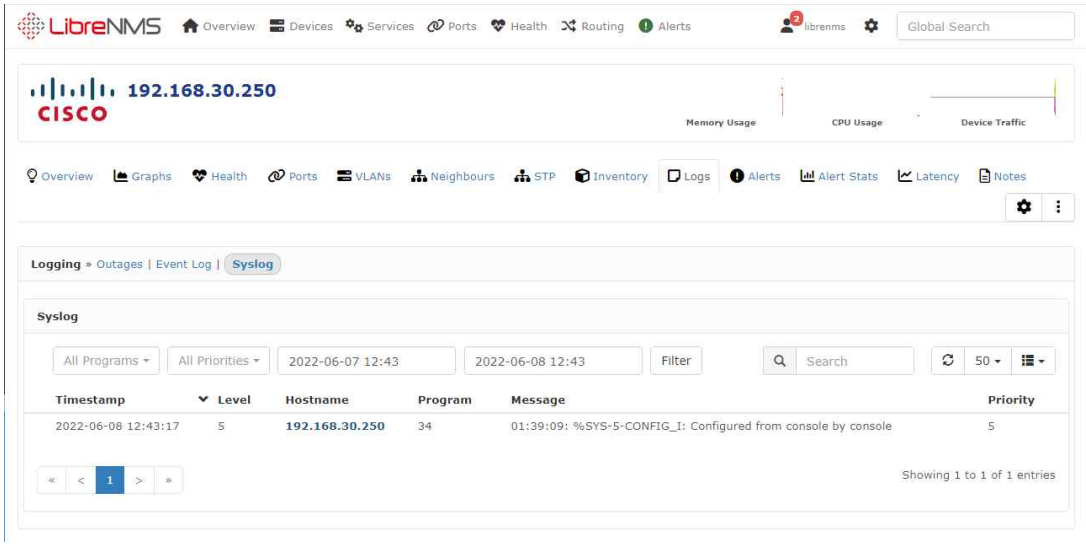
```
user@cloud1:/tmp$ sudo mkdir /var/www/html/loganalyzer
user@cloud1:/tmp$ sudo cp -r /tmp/loganalyzer-4.1.12/src/* /var/www/html/loganalyzer/
user@cloud1:/tmp$ sudo touch config.php
user@cloud1:/tmp$ sudo chown www-data:www-data config.php
user@cloud1:/tmp$ sudo chmod 666 config.php
user@cloud1:/tmp$ sudo chown www-data:www-data -R /var/www/html/loganalyzer/
user@cloud1:/tmp$ _
```

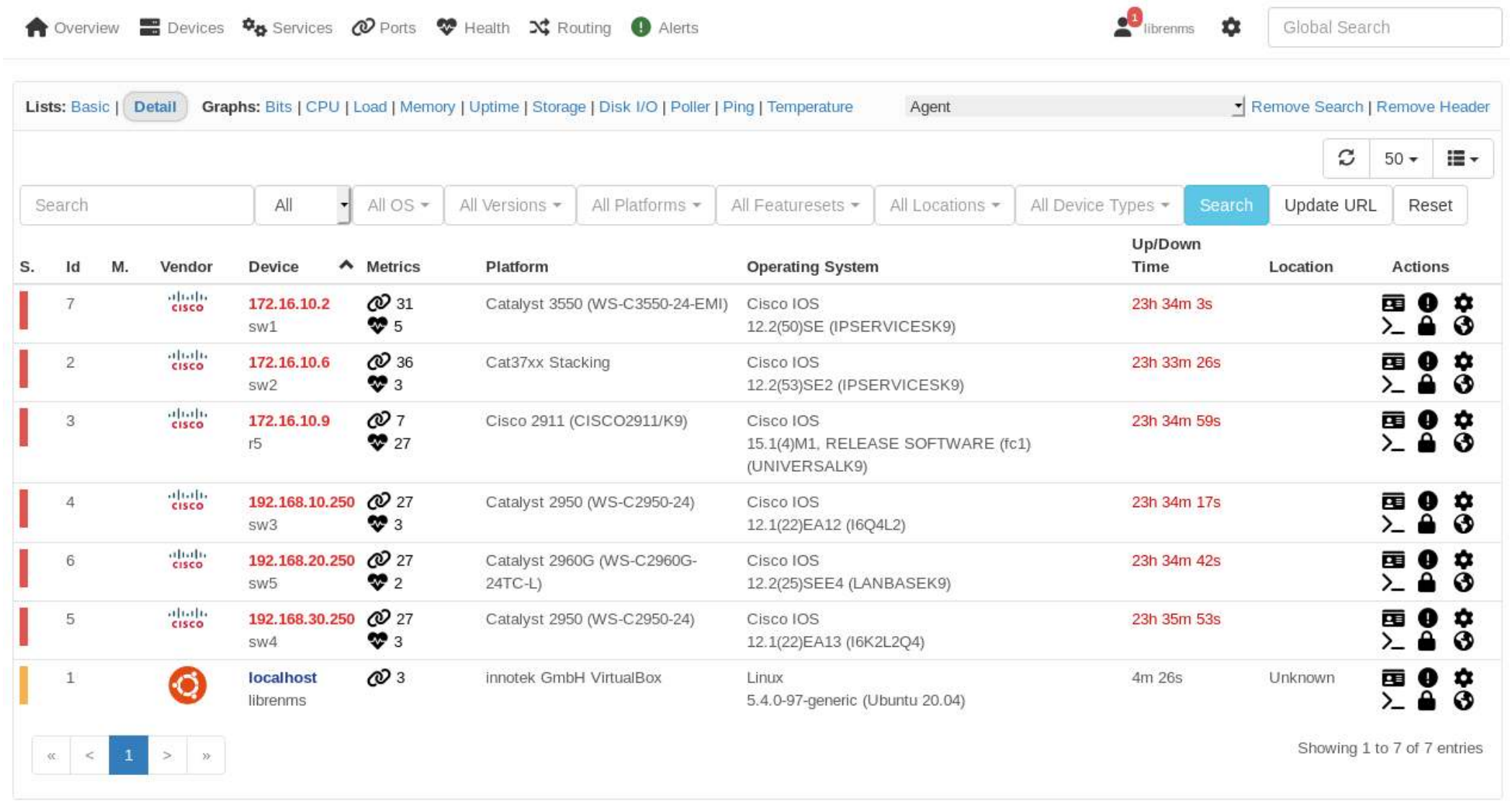
<NMS 작동 확인하기>

1) 장비 등록



2) 장비 로그 확인





<Radius Server AAA인증 확인>

<SSH 인증>