

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

```
270 client R5{
271   ipaddr=172.16.10.1
272   secret=1234
273 }
274
275 client SW1{
276   ipaddr=172.16.10.2
277   secret=1234
278 }
279
280 client SW2{
281   ipaddr=172.16.10.6
282   secret=1234
283 }
284
285 client SW3{
286   ipaddr=192.168.10.250
287   secret=1234
288 }
289
290 client SW4{
291   ipaddr=192.168.30.250
292   secret=1234
293 }
294
295 client SW5{
296   ipaddr=192.168.20.250
297   secret=1234
298 }
```

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 Analyzer 설치

- 1) `sudo apt install lamp-server^`
- 2) `sudo apt-get install rsyslog-mysql` (아래창 No 선택)

Configuring rsyslog-mysql

The rsyslog-mysql package must have a database installed and configured before it can be used. This can be optionally handled with dbconfig-common.

If you are an advanced database administrator and know that you want to perform this configuration manually, or if your database has already been installed and configured, you should refuse this option. Details on what needs to be done should most likely be provided in /usr/share/doc/rsyslog-mysql.

Otherwise, you should probably choose this option.

Configure database for rsyslog-mysql with dbconfig-common?

<Yes>

<No>

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 -xzf 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

LibreNMS Overview Devices Services Ports Health Routing Alerts librenms Global Search

Add Device

Devices will be checked for Ping/SNMP reachability before being probed.

Hostname or IP: 192.168.20.250

SNMP: ON

SNMP Version: v2c 161 udp

Port Association Mode: ifIndex

SNMPv1/2c Configuration

Community: cloud_sw4

Force add (No ICMP or SNMP checks performed): OFF

Add Device

2) 장비 로그 확인

LibreNMS Overview Devices Services Ports Health Routing Alerts librenms Global Search

192.168.30.250 CISCO

Memory Usage CPU Usage Device Traffic

Overview Graphs Health Ports VLANs Neighbours STP Inventory Logs Alerts Alert Stats Latency Notes

Logging » Outages | Event Log | Syslog

Syslog

All Programs ▾ All Priorities ▾ 2022-06-07 12:43 2022-06-08 12:43 Filter Search 50 ▾ ▮ ▾

| Timestamp | Level ▾ | Hostname | Program | Message | Priority |
|---------------------|---------|----------------|---------|---|----------|
| 2022-06-08 12:43:17 | 5 | 192.168.30.250 | 34 | 01:39:09: %SYS-5-CONFIG_I: Configured from console by console | 5 |

Showing 1 to 1 of 1 entries

Lists: [Basic](#) | [Detail](#) |
 Graphs: [Bits](#) | [CPU](#) | [Load](#) | [Memory](#) | [Uptime](#) | [Storage](#) | [Disk I/O](#) | [Poller](#) | [Ping](#) | [Temperature](#)

Agent ▼ [Remove Search](#) | [Remove Header](#)

Refresh [50](#) [List](#)

Search All All OS All Versions All Platforms All Featuresets All Locations All Device Types [Search](#) [Update URL](#) [Reset](#)

| S. | Id | M. | Vendor | Device | Metrics | Platform | Operating System | Up/Down Time | Location | Actions |
|----|----|----|---|-----------------------|---|-----------------------------------|---|--------------|----------|--|
| | 7 | |  | 172.16.10.2 sw1 |  31  5 | Catalyst 3550 (WS-C3550-24-EMI) | Cisco IOS 12.2(50)SE (IPSERVICESK9) | 23h 34m 3s | |       |
| | 2 | |  | 172.16.10.6 sw2 |  36  3 | Cat37xx Stacking | Cisco IOS 12.2(53)SE2 (IPSERVICESK9) | 23h 33m 26s | |       |
| | 3 | |  | 172.16.10.9 r5 |  7  27 | Cisco 2911 (CISCO2911/K9) | Cisco IOS 15.1(4)M1, RELEASE SOFTWARE (fc1) (UNIVERSALK9) | 23h 34m 59s | |       |
| | 4 | |  | 192.168.10.250 sw3 |  27  3 | Catalyst 2950 (WS-C2950-24) | Cisco IOS 12.1(22)EA12 (I6Q4L2) | 23h 34m 17s | |       |
| | 6 | |  | 192.168.20.250 sw5 |  27  2 | Catalyst 2960G (WS-C2960G-24TC-L) | Cisco IOS 12.2(25)SEE4 (LANBASEK9) | 23h 34m 42s | |       |
| | 5 | |  | 192.168.30.250 sw4 |  27  3 | Catalyst 2950 (WS-C2950-24) | Cisco IOS 12.1(22)EA13 (I6K2L2Q4) | 23h 35m 53s | |       |
| | 1 | |  | localhost librenms |  3 | innotek GmbH VirtualBox | Linux 5.4.0-97-generic (Ubuntu 20.04) | 4m 26s | Unknown |       |

« < 1 > »

Showing 1 to 7 of 7 entries

<Radius Server AAA인증 확인>

<SSH 인증>