

로그 분석 툴 (Graylog) 사용 실습

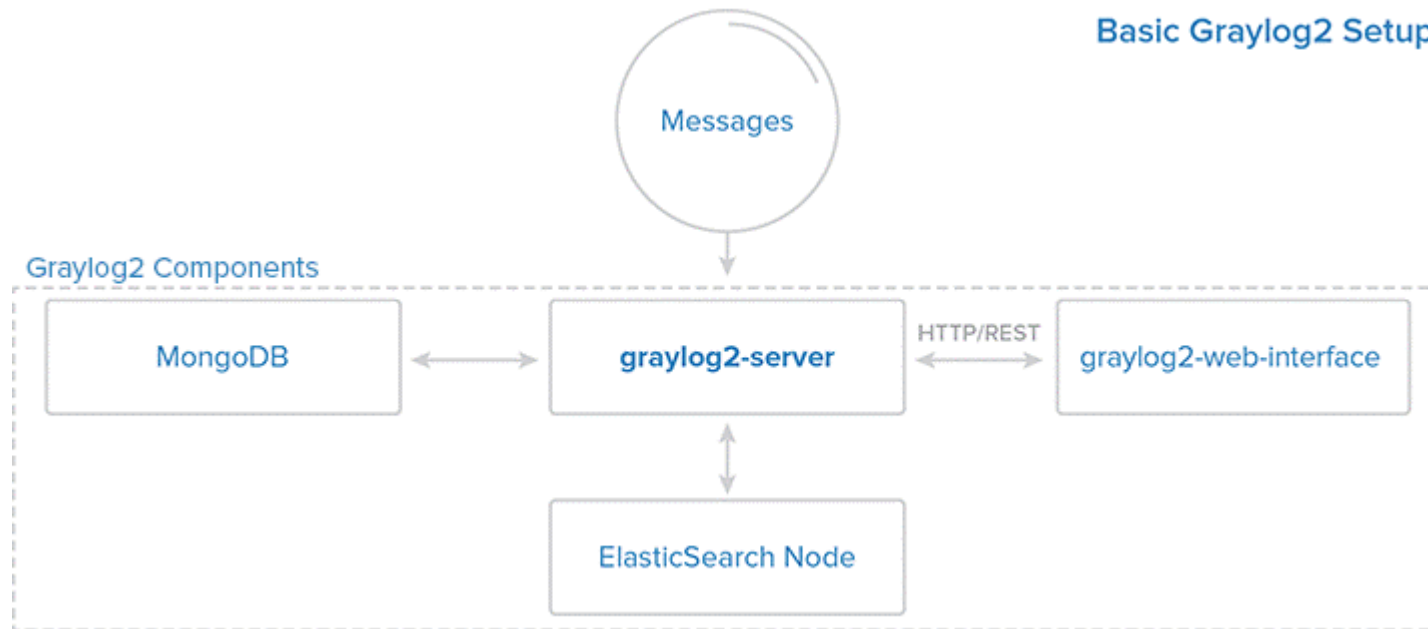
발표자: 양유진

링크: <https://youtu.be/9qRTk4YyAB0>

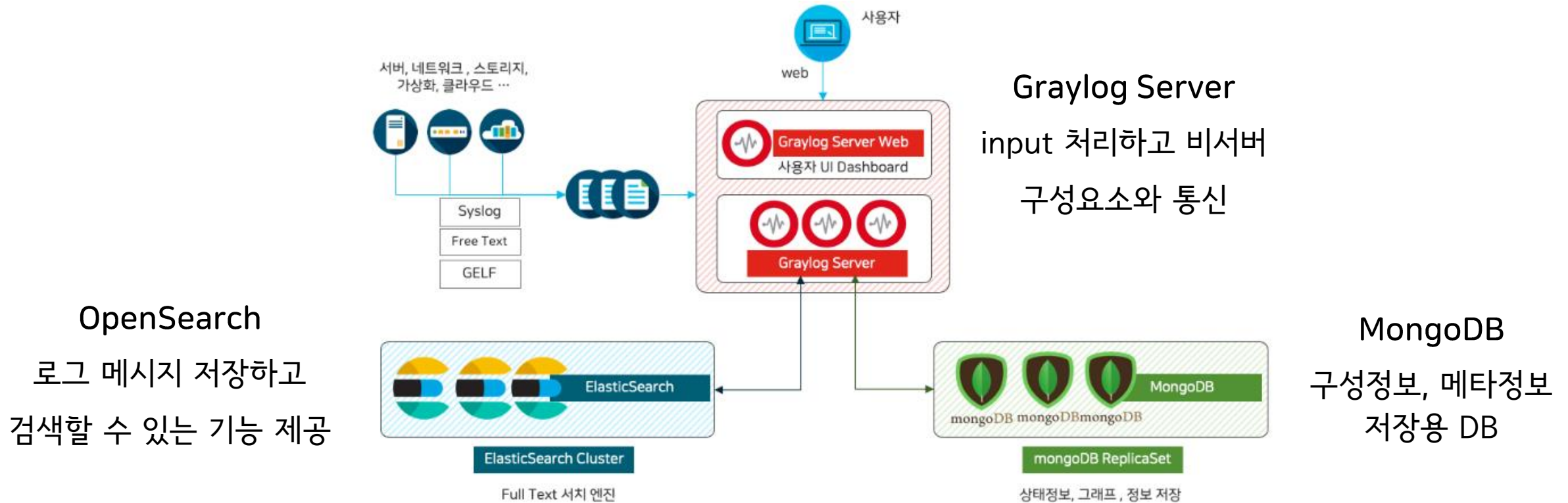
1. Graylog란?



MongoDB와 Elasticsearch(OpenSearch)를 기반으로 동작하는
오픈소스 로그 수집 및 분석 도구



1. Graylog란?



2. 실습 환경 구성 - 우분투 환경 구성

1) 우분투 환경 구성

- Ubuntu Linux 22.04 LTS
- 가상머신 Oracle Virtual box / VMware

[링크](#)

* 모든 설치를 마치고 우분투를 실행했을 때, 화면이 계속 멈춰 있는 문제가 발생할 경우

→ [링크](#)

- 그래픽 컨트롤러의 문제일 수도 있음. ([링크](#))

* Virtual box를 이용할 경우 중간 중간 Snapshot 기능을 이용하여 상태 저장을 권장함.

2. 실습 환경 구성 - MongoDB 설치

2) MongoDB 설치 (우분투 22.04 기준)

(1) GnUPG 설치 `sudo apt-get install gnupg`

- 통신상에서 혹은 데이터를 저장할 때 보안을 지키는 도구
- 공개키 암호화 기법을 사용하기 때문에 더욱 안전하게 통신 가능

(2) MongoDB 다운로드 및 파일 바로 등록

`wget -qO - https://www.mongodb.org/static/pgp/server-6.0.asc | sudo apt-key add -`

웹 서버에서 파일 다운로드를 도와주는 프로그램

- 파일에서 키를 불러와 키 리스트에 새로운 키 추가
- 키를 사용하여 패키지를 인증함으로써, 신뢰할 수 있는 패키지로 간주됨
- 표준 입력의 경우 파일 이름을 '-'로 대체
- sudo 암호 입력하면 됨

2. 실습 환경 구성 - MongoDB 설치

(3) MongoDB를 위한 list file 생성

```
echo "deb [ arch=amd64,arm64 ] https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/6.0 multiverse"  
| sudo tee /etc/apt/sources.list.d/mongodb-org-6.0.list
```

- apt repository에 MongoDB 6.0 추가
- echo: 출력 명령어
- jammy: Ubuntu 22.04 = Jammy Jellyfish
- multiverse: 지원되지 않는 폐쇄형 소스 소프트웨어 혹은 특허권이 부여된 소프트웨어 저장소
- tee: 출력한 값을 읽어 들여 지정한 파일에 출력함

(4) 설치된 로컬 패키지 최신으로 업데이트 `sudo apt-get update`

2. 실습 환경 구성 - MongoDB 설치

(5) MongoDB 최신 버전 설치 `sudo apt-get install -y mongodb-org`

설치 중간에 나오는 모든 물음에 yes를 사용하겠다는 옵션

(6) 서비스 등록

`sudo systemctl daemon-reload`

`sudo systemctl enable mongod.service`

`sudo systemctl restart mongod.service`

`sudo systemctl --type=service --state=active | grep mongod`

systemd(system daemon)를 관리하기 위한 도구로,
root 권한으로만 실행이 가능

- `systemctl daemon-reload`: 서비스 설정 반영
- `systemctl enable [서비스명]`: 부팅시 활성화
- `systemctl restart [서비스명]`: 서비스 재시작
- `systemctl --type=service --state=active | grep mongod`: 서비스 목록에서 상태가 활성화(active)인 목록 중 mongod 출력

2. 실습 환경 구성 - OpenSearch 설치 및 설정

3) OpenSearch 설치 및 설정

(1) OpenSearch 설치 전, Transparent Huge Pages(THP) 기능 비활성화

`sudo su` root 권한으로 전환 (`su [계정명]` : 다른 계정으로 전환하는 명령어)

`cat > /etc/systemd/system/disable-transparent-huge-pages.service <<EOF` 파일 생성/저장

`Description=Disable Transparent Huge Pages (THP)`

`DefaultDependencies=no`

`After=sysinit.target local-fs.target`

`[Service]`

`Type=oneshot`

`ExecStart=/bin/sh -c 'echo never | tee /sys/kernel/mm/transparent_hugepage/enabled > /dev/null'`

`[Install]`

`WantedBy=basic.target`

`EOF`

2. 실습 환경 구성 - OpenSearch 설치 및 설정

(2) THP 비활성화 서비스 등록

```
sudo systemctl daemon-reload
```

```
sudo systemctl enable disable-transparent-huge-pages.service
```

```
sudo systemctl start disable-transparent-huge-pages.service
```

(3) 공개 PGP키 가져와 APT 저장소 서명 확인

```
curl -o- https://artifacts.opensearch.org/publickeys/opensearch.pgp | sudo apt-key add -
```

- curl (Client URL): URL를 이용하여 서버에 데이터를 보내거나 가져오는 명령어
- -o: 명령의 결과를 저장하는 옵션
- pgp키를 가져와 키 리스트에 새롭게 추가

2. 실습 환경 구성 - OpenSearch 설치 및 설정

(4) OpenSearch의 APT repository 생성

```
echo "deb https://artifacts.opensearch.org/releases/bundle/opensearch/2.x/apt stable main" |  
sudo tee -a /etc/apt/sources.list.d/opensearch-2.x.list
```

(5) 설치된 로컬 패키지 최신으로 업데이트 `sudo apt-get update`

(6) OpenSearch 설치 `sudo apt-get install opensearch`

2. 실습 환경 구성 - OpenSearch 설치 및 설정

(7) 설정파일 수정

`sudo nano /etc/opensearch/opensearch.yml`

GNU nano 6.2 /etc/opensearch/opensearch.yml *

```
# ----- Cluster -----  
#  
# Use a descriptive name for your cluster:  
#  
cluster.name: graylog  
#  
# ----- Node -----
```

End OpenSearch Security Demo Configuration

add

```
action.auto_create_index: false  
plugins.security.disabled: true  
discovery.type: single-node
```

GNU nano 6.2 /etc/opensearch/opensearch.yml *

```
# ----- Network -----  
#  
# Set the bind address to a specific IP (IPv4 or IPv6):  
#  
#network.host: 192.168.0.1  
network.host: 0.0.0.0  
Ubuntu Software
```

- ctrl + W : 검색
- ctrl + X → Y → Enter: 저장

(8) OpenSearch 서비스 등록

`sudo systemctl daemon-reload`

`sudo systemctl enable opensearch`

`sudo systemctl start opensearch`

`sudo systemctl status opensearch`

2. 실습 환경 구성 - Graylog 설치 및 설정

4) Graylog 설치 및 설정

(1) Graylog 패키지 다운로드

```
wget https://packages.graylog2.org/repo/packages/graylog-5.0-repository_latest.deb
```

(2) 다운받은 패키지 설치

```
sudo dpkg -i graylog-5.0-repository_latest.deb
```

(3) 패키지 업데이트 및 Graylog 설치

```
sudo apt-get update && sudo apt-get install graylog-server
```

(4) pwgen 설치 `sudo apt-get install pwgen`

무작위로 비밀번호를 생성해주는 명령어

2. 실습 환경 구성 - Graylog 설치 및 설정

(5) 구성 파일 편집 `sudo nano /etc/graylog/server/server.conf`

```
# The default root user is named 'admin'
root_username = admin

# The time zone setting of the root user. See http://www.joda.org/joda-time/ti>
# Default is UTC
root_timezone = Asia/Seoul

# If the port is omitted, Graylog will use port 9000 by default.
#
# Default: 127.0.0.1:9000
http_bind_address = 0.0.0.0:9000
```

(5-1) 관리자 패스워드 설정 `echo -n [비밀번호] | sha256sum | cut -d" " -f1`

```
# modify it in this file.
# Create one by using for example: echo -n yourpassword | shasum -a 256
# and put the resulting hash value into the following line
root_password_sha2 = | 출력 복사-붙여넣기
```

2. 실습 환경 구성 - Graylog 설치 및 설정

(5-2) password_secret 생성 `pwgen -N 1 -s 96`

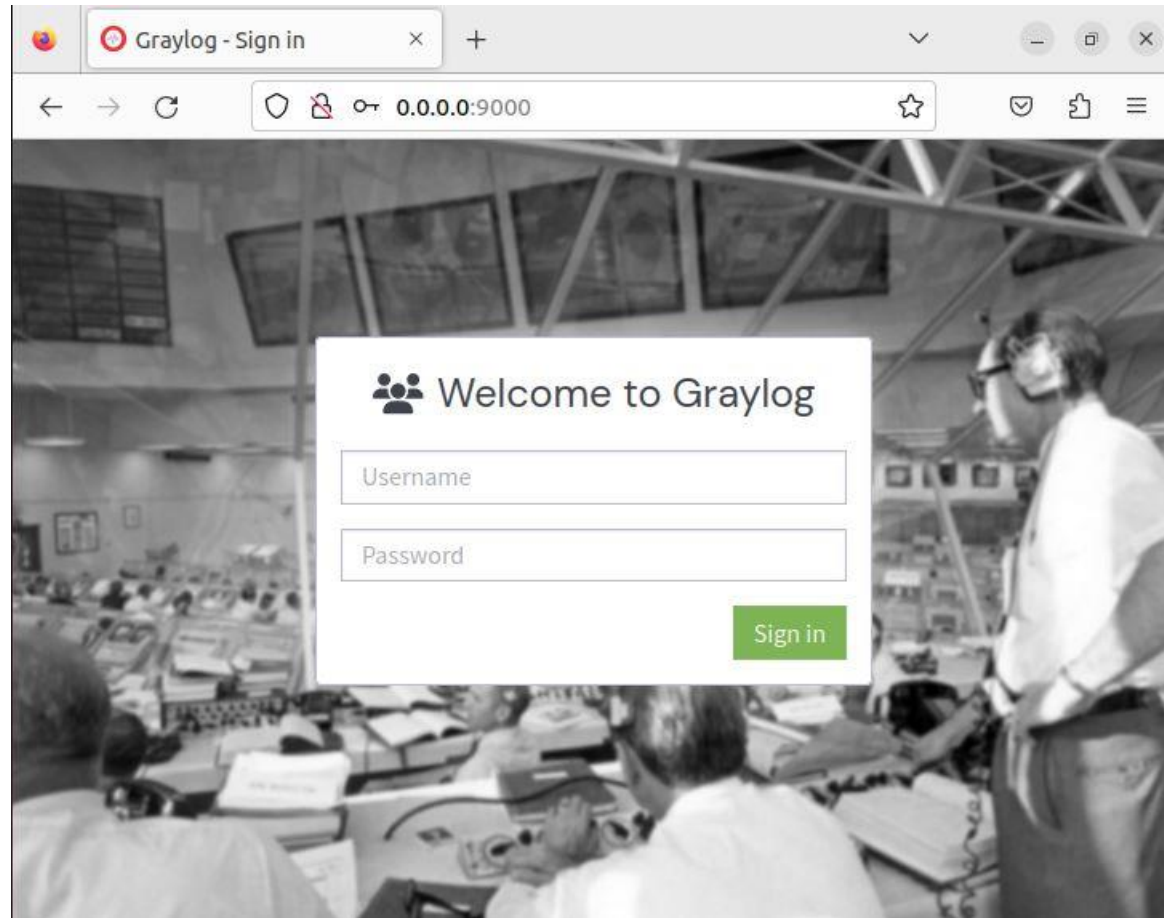
```
# You MUST set a secret to secure/pepper the stored user passwords here. Use a  
# Generate one by using for example: pwgen -N 1 -s 96  
# ATTENTION: This value must be the same on all Graylog nodes in the cluster.  
# Changing this value after installation will render all user sessions and enc  
password_secret = 출력 복사-붙여넣기
```

(6) Graylog 서비스 등록

- `sudo systemctl daemon-reload`
- `sudo systemctl enable graylog-server.service`
- `sudo systemctl start graylog-server.service`
- `sudo systemctl status graylog-server.service`

2. 실습 환경 구성 - Graylog 설치 및 설정

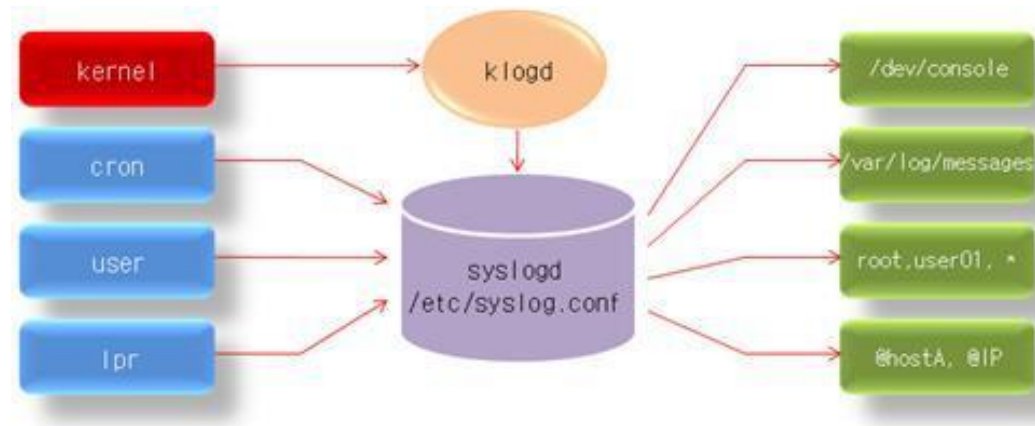
(7) Graylog 서버 접속 및 로그인 시도



3. syslog 수집

syslog란?

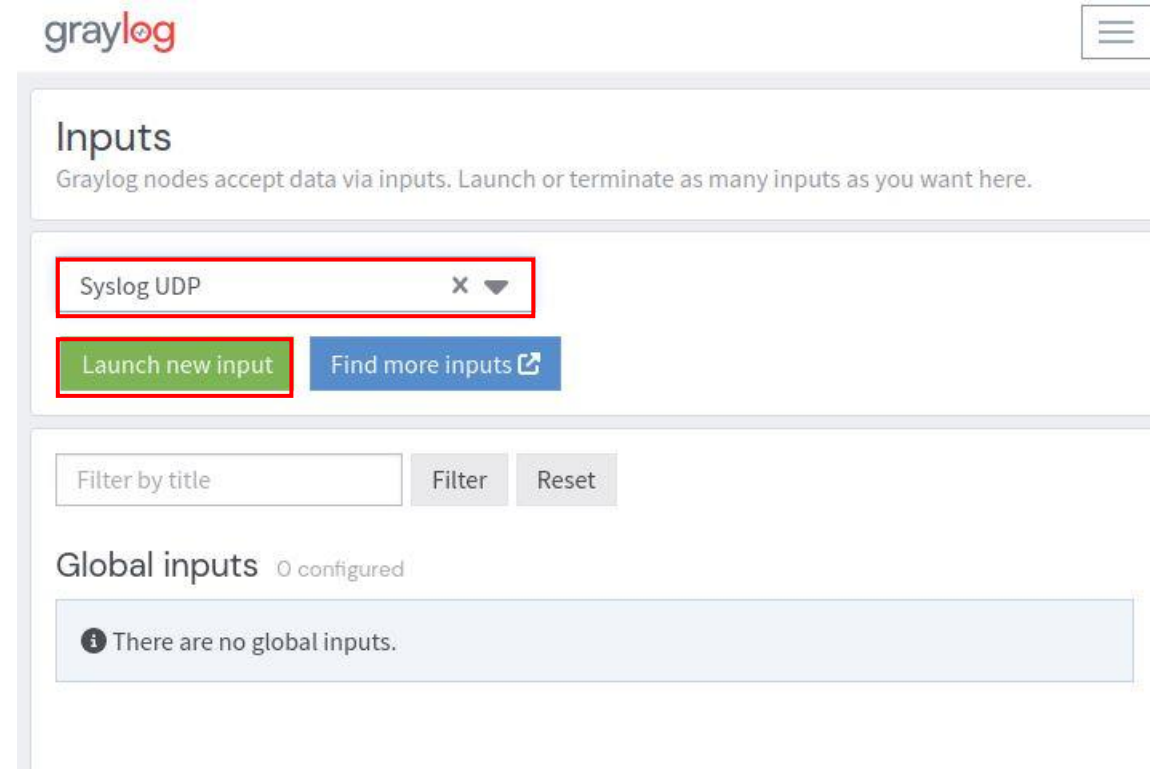
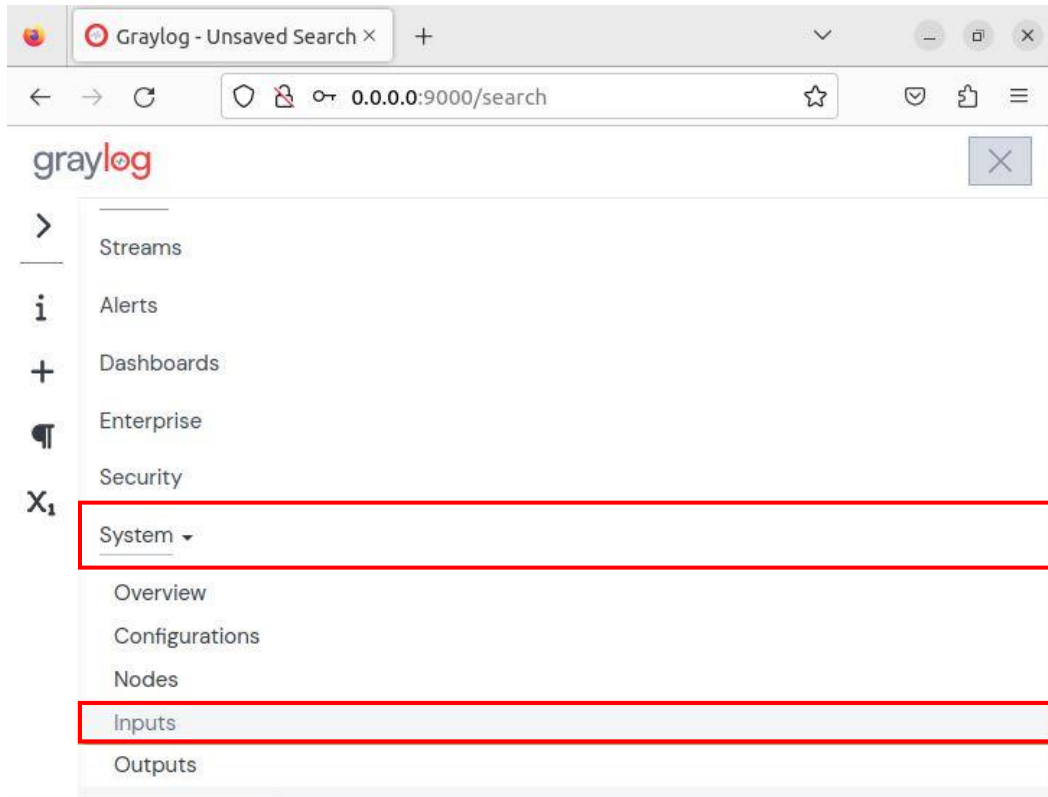
- (system log) 리눅스에서 사용하는 로그 생성/관리 도구
- 커널 및 응용프로그램이 syslog API를 통해 로그를 생성하면 syslogd 데몬 프로세스가 규칙이 적힌 syslog.conf 설정 파일을 참조하여 로그를 기록함.
- 리눅스에서는 /var/log 디렉토리에 시스템의 모든 로그를 기록, 관리함.



(출처: <https://itragdoll.tistory.com/79>)

3. syslog 수집

1) Graylog Input 설정



3. syslog 수집

1) Graylog Input 설정

Title
syslogudp

Bind address
0.0.0.0
Address to listen on. For example 0.0.0.0 or 127.0.0.1.

Port
5140
Port to listen on.

Receive Buffer Size (optional)
262144
The size in bytes of the recvBufferSize for network connections to this input.

No. of worker threads (optional)
2

graylog

Show received messages Manage extractors **Start input** More actions ▾

```
allow_override_date: true
bind_address: 0.0.0.0
charset_name: UTF-8
expand_structured_data: false
force_rdns: false
number_worker_threads: 2
override_source: <empty>
port: 5140
recv_buffer_size: 262144
store_full_message: false
```

Throughput / Metrics
No metrics available for this input

3. syslog 수집

2) 방화벽 설정 (Graylog서버 Redirection)

(1) firewalld 설치 `sudo apt install firewalld -y`

(2) UDP 5140 방화벽 허용 설정

`sudo firewall-cmd --add-masquerade --permanent`

리눅스의 NAT(Network Address Translation)기능으로,
리눅스 서버를 통해 다른 네트워크에 접속할 수 있게 해줌.

`sudo firewall-cmd --add-forward-port=port=514:proto=udp:toport=5140 --permanent`

`sudo firewall-cmd --permanent --add-port=5140/udp`

`sudo firewall-cmd --reload`

`sudo firewall-cmd --list-all`

3. syslog 수집

3) 외부 서버로 syslog 전송하도록 설정

`sudo nano /etc/rsyslog.conf`

```
GNU nano 6.2 /etc/rsyslog.conf
#####

module(load="imuxsock") # provides support for local system logging
#module(load="imark") # provides --MARK-- message capability

# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
#module(load="imtcp")
#input(type="imtcp" port="514")

# provides kernel logging support and enable non-kernel klog messages
module(load="imklog" permitnonkernelfacility="on")
```

```
GNU nano 6.2 /etc/rsyslog.conf
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog

#
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog

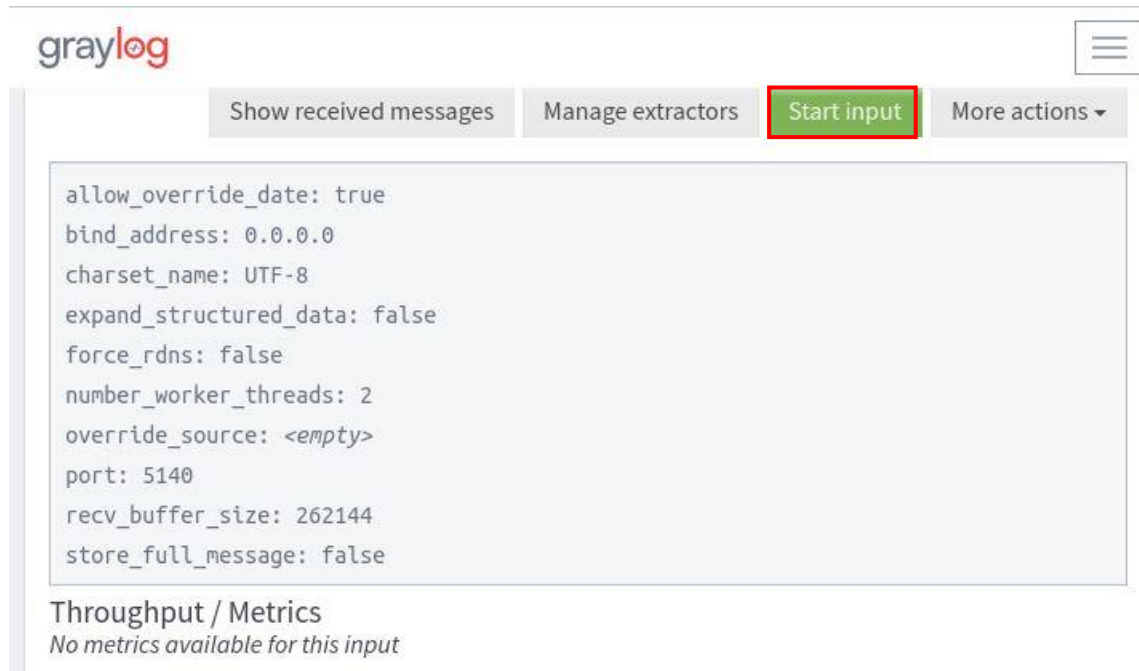
#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf
*.info;mail.none;cron.none @0.0.0.0:5140
```

forwarding rule 설정

`sudo systemctl restart rsyslog` rsyslog 서비스 재시작

3. syslog 수집

4) Graylog 웹에서 syslog 수집



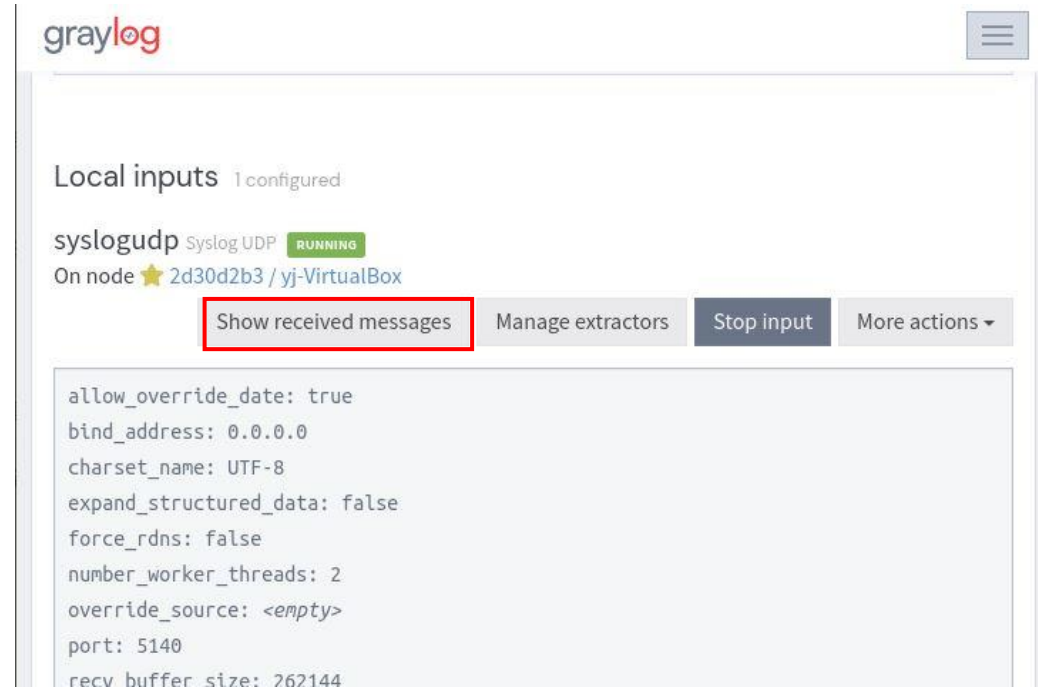
The screenshot shows the Graylog web interface for configuring a new input. The 'Start input' button is highlighted with a red box. Below the configuration fields, the 'Throughput / Metrics' section indicates that no metrics are available for this input.

graylog

Show received messages Manage extractors **Start input** More actions ▼

```
allow_override_date: true
bind_address: 0.0.0.0
charset_name: UTF-8
expand_structured_data: false
force_rdns: false
number_worker_threads: 2
override_source: <empty>
port: 5140
recv_buffer_size: 262144
store_full_message: false
```

Throughput / Metrics
No metrics available for this input



The screenshot shows the Graylog web interface for an existing 'syslogudp' input. The 'Show received messages' button is highlighted with a red box. The input is shown as 'RUNNING' and is located on node '2d30d2b3 / yj-VirtualBox'.

graylog

Local inputs 1 configured

syslogudp Syslog UDP **RUNNING**
On node ★ 2d30d2b3 / yj-VirtualBox

Show received messages Manage extractors Stop input More actions ▼

```
allow_override_date: true
bind_address: 0.0.0.0
charset_name: UTF-8
expand_structured_data: false
force_rdns: false
number_worker_threads: 2
override_source: <empty>
port: 5140
recv_buffer_size: 262144
```


3. syslog 수집

5) Graylog 웹에서 수집된 syslog 확인 vs 우분투에 저장된 syslog 확인

`sudo tail -f /var/log/syslog`



The screenshot shows the Graylog web interface. On the left, there is a sidebar with navigation icons: a magnifying glass, an 'i' icon, a plus sign, a speaker icon, and an 'X1' icon. The main area displays a list of log entries. Each entry has a timestamp, a source, and a message. The messages are warnings from a window manager about overwriting key bindings.

Timestamp	Source	Message
2023-05-01 16:40:44.000	yj-VirtualBox	yj-VirtualBox gnome-shell[1141]: Window manager warning: Overwriting existing binding of keysym 32 with keysym 32 (keycode b).
2023-05-01 16:40:44.000	yj-VirtualBox	yj-VirtualBox gnome-shell[1141]: Window manager warning: Overwriting existing binding of keysym 34 with keysym 34 (keycode d).
2023-05-01 16:40:44.000	yj-VirtualBox	yj-VirtualBox gnome-shell[1141]: Window manager warning: Overwriting existing binding of keysym 36 with keysym 36 (keycode f).
2023-05-01 16:40:44.000	yj-VirtualBox	yj-VirtualBox gnome-shell[1141]: Window manager warning: Overwriting existing binding of keysym 37 with keysym 37 (keycode 10).
2023-05-01 16:40:44.000	yj-VirtualBox	yj-VirtualBox gnome-shell[1141]: Window manager warning: Overwriting existing binding of keysym 39 with keysym 39 (keycode 12).
2023-05-01 16:40:44.000	yj-VirtualBox	yj-VirtualBox gnome-shell[53337]: > X11 cannot support keycodes above 255.

At the bottom of the log list, there is a pagination bar with buttons for navigating between pages: <<, <, 1, 2, 3, >, >>.

```
yj@yj-VirtualBox:~$ sudo tail -f /var/log/syslog
May  1 16:40:44 yj-VirtualBox gnome-shell[1141]: Window manager warning: Overwr
iting existing binding of keysym 34 with keysym 34 (keycode d).
May  1 16:40:44 yj-VirtualBox gnome-shell[1141]: Window manager warning: Overwr
iting existing binding of keysym 35 with keysym 35 (keycode e).
May  1 16:40:44 yj-VirtualBox gnome-shell[1141]: Window manager warning: Overwr
iting existing binding of keysym 36 with keysym 36 (keycode f).
May  1 16:40:44 yj-VirtualBox gnome-shell[1141]: Window manager warning: Overwr
iting existing binding of keysym 37 with keysym 37 (keycode 10).
May  1 16:40:44 yj-VirtualBox gnome-shell[1141]: Window manager warning: Overwr
iting existing binding of keysym 38 with keysym 38 (keycode 11).
May  1 16:40:44 yj-VirtualBox gnome-shell[1141]: Window manager warning: Overwr
iting existing binding of keysym 39 with keysym 39 (keycode 12).
May  1 16:40:44 yj-VirtualBox gnome-shell[53337]: The XKEYBOARD keymap compiler
(xkbcomp) reports:
May  1 16:40:44 yj-VirtualBox gnome-shell[53337]: > Warning:                Unsupport
ed maximum keycode 708, clipping.
May  1 16:40:44 yj-VirtualBox gnome-shell[53337]: >                               X11 canno
t support keycodes above 255.
May  1 16:40:44 yj-VirtualBox gnome-shell[53337]: Errors from xkbcomp are not f
```

감사합니다