목차

rsyslog send to remote server 3
rsyslog 서버로 설정 3
rsyslog를 전송할 클라이언트 3
Apache 로그를 원격 rsyslog로 전송 3
참조링크 4

rsyslog send to remote server

syslog 및 rsyslog 데몬을 이용하여 대상 서버로 로컬에서 발생한 syslog를 전송할 수 있습니다. 예를들어 로그 통합 서버를 구축하여 syslog 및 rsyslog 데몬을 이용하여 로그 통합 서버로 보내 관리를 할 수 있습니다.

Fedora 10 이후에는 rsyslog가 기본 데몬으로 설치되기 때문에 Linux OS 에서는 rsyslog를 많이 볼 수 있습니다. Unix OS에는 syslog를 이용 할 수 있습니다.

기본적으로 rsyslog의 설정파일 경로는 /etc/rsyslog.conf 에 위치하고, syslog의 설정파일 경로는 /etc/syslog.conf 에 위치합니다. 포트는 514번 포트를 사용하며 UDP, TCP 방식으로 전송이 가능합니다.

rsyslog 서버로 설정

로그를 전송받을 서버에는 접속을 허용하도록 모듈과 포트를 활성화 해줍니다.

/etc/rsyslog.conf

```
# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514

# Provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514
```

rsyslog를 전송할 클라이언트

/etc/rsyslog.conf

```
# UDP 전송
*.info       @로그 통합 서버 IP
*.info       @로그 통합 서버 IP:포트번호

# TCP 전송
*.info       @@로그 통합 서버 IP
*.info       @@로그 통합 서버 IP:포트번호
```

Apache 로그를 원격 rsyslog로 전송

가장 간단한 방법은 ErrorLog, CustomLog 설정을 syslog출력으로 바꿔주는것이다. 기본적으로

local7 카테고리로 출력이 되지만 별도로 설정해줄 수도 있다.

```
# 기본값
ErrorLog logs/error_log
# rsyslog 로 local0 카테고리 출력
ErrorLog syslog:local0
```

이렇게 설정한 로그를 원격 로그 서버로 전송하기 위해 아래와 같이 추가한다. /etc/rsyslog.conf

```
local0.*  @syslog.example.com
# 아래줄은 로컬파일에 같이 출력되는것을 방지한다.
& ~
```

이후 아파치와 로깅 서비스를 재시작한다.

```
systemctl restart rsyslog
systemctl restart httpd
```

참조링크

- https://access.redhat.com/solutions/20745
- https://access.redhat.com/articles/2318351
- https://m.blog.naver.com/scvpark/221017723884

From:
https://atl.kr/dokuwiki/ - **AllThatLinux!**

Permanent link:
https://atl.kr/dokuwiki/doku.php/rsyslog_send_to_remote_server

Last update: **2020/12/15 02:03**