### sendsyslog-tcp

입력되는 레코드를 시스로그(syslog) 형식으로 변환한 다음 TCP 통신을 통해 목적지로 전송합니다.

#### 문법

sendsyslog-tcp dst=IP\_ADDR port=INT [framing=lf|rfc6587] [format=json|txt] [pri=INT]

필수 매개변수

**dst=IP\_ADDR**

Syslog 서버의 IP 주소

**port=INT**

Syslog 서버의 리스닝 포트 번호(기본값: 514). 1 ~ 65535 사이의 정수를 입력할 수 있습니다.

선택 매개변수

**format=json|txt**

전송할 로그의 형식을 json, txt 중에서 선택해 지정(기본값: txt).

* json: 입력으로 받는 데이터를 모두 JSON 형식으로 변환해 전송
* txt: **line** 필드의 문자열 값을 그대로 전송

**framing=lf|rfc6587**

시스로그 메시지의 경계를 식별하는 방법(기본값: lf). 시스로그를 수신하는 서버에 적합한 방식을 선택

* lf: 시스로그 메시지의 끝을 나타내는 문자로 줄바꿈 문자(LF)를 이용
* rfc6587: [RFC 6587](https://www.rfc-editor.org/rfc/rfc6587)에 따라 각 메시지의 시작 부분에 메시지의 길이를 바이트로 명시

**pri=INT**

rfc 5424 (https://tools.ietf.org/html/rfc5424)에 정의된 PRI 상수값(기본값: 134). 이는 local0와 INFO 수준에 해당됩니다.

PRI 상수값은 Facility 값의 8배수에 Severity 값을 더한 값입니다. 다음 표를 참조해서 계산된 값을 사용하세요.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Facility(↓)<br />Severity(→) | 0/Emer | 1/Alert | 2/Crit | 3/Error | 4/Warn | 5/Notice | 6/Info | 7/Debug |
| 0 / kern | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 / user | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 2 / mail | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| 3 / deamon | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| 4 / auth | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 |
| 5 / syslog | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 |
| 6 / lpr | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 |
| 7 / news | 56 | 57 | 58 | 59 | 60 | 61 | 62 | 63 |
| 8 / uucp | 64 | 65 | 66 | 67 | 68 | 69 | 70 | 71 |
| 9 / clock | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 |
| 10 / authpriv | 80 | 81 | 82 | 83 | 84 | 85 | 86 | 87 |
| 11 / ftp | 88 | 89 | 90 | 91 | 92 | 93 | 94 | 95 |
| 12 / ntp | 96 | 97 | 98 | 99 | 100 | 101 | 102 | 103 |
| 13 / audit | 104 | 105 | 106 | 107 | 108 | 109 | 110 | 111 |
| 14 / alert | 112 | 113 | 114 | 115 | 116 | 117 | 118 | 119 |
| 15 / solaris-cron | 120 | 121 | 122 | 123 | 124 | 125 | 126 | 127 |
| 16 / local0 | 128 | 129 | 130 | 131 | 132 | 133 | **134** (기본값) | 135 |
| 17 / local1 | 136 | 137 | 138 | 139 | 140 | 141 | 142 | 143 |
| 18 / local2 | 144 | 145 | 146 | 147 | 148 | 149 | 150 | 151 |
| 19 / local3 | 152 | 153 | 154 | 155 | 156 | 157 | 158 | 159 |
| 20 / local4 | 160 | 161 | 162 | 163 | 164 | 165 | 166 | 167 |
| 21 / local5 | 168 | 169 | 170 | 171 | 172 | 173 | 174 | 175 |
| 22 / local6 | 176 | 177 | 178 | 179 | 180 | 181 | 182 | 183 |
| 23 / local7 | 184 | 185 | 186 | 187 | 188 | 189 | 190 | 191 |

#### 설명

이 명령어는 TCP를 통해 시스로그 메시지를 전송하므로 UDP 방식과 달리 IP 패킷 단편화 문제 없이 안정적인 메시지 송신이 가능하게 해줍니다. 그러나 시스로그 서버와 연결이 끊기거나, 지연이 발생하면 전송할 시스로그 메시지 큐가 적체될 수 있습니다. sendsyslog-tcp 명령은 메시지 큐 적체를 방지하기 위해 메시지가 30초 이내에 전송되지 않으면 메시지를 버립니다. 메시지 전송 큐를 관리할 수 있도록 로그프레소 셸에서 다음과 같은 시스템 스위치를 제공합니다.

|  |  |  |
| --- | --- | --- |
| 스위치 | 설명 | 값 |
| logpresso.tcp\_sender.idle\_timeout | 서버에서 응답이 없으면 전송을 중단할 기준 | 1 ~ 86400초, 기본값 300 초 |
| logpresso.tcp\_sender.max\_queue\_time | 전송 시간이 오래 걸리면 전송을 중단할 기준 | 1 ~ 600초, 기본값 30 초 |
| logpresso.tcp\_sender.max\_queue\_chars | 적체된 문자열이 너무 많으면 전송을 중단할 기준 | 1,000,000 ~ 1,000,000,000 문자, 기본값 100,000,000(약 10MB) |

스위치를 적용하려면 로그프레소 셸에서 다음과 같은 명령을 실행하세요.

set logpresso.tcp\_sender.idle\_timeout=300set logpresso.tcp\_sender.max\_queue\_time=30set logpresso.tcp\_sender.max\_queue\_chars=100000000

환경 설정 파일 config.sh 또는 logpresso.sh에 다음과 같이 시스템 스위치를 적용할 수 있습니다.

JAVA\_OPTS="$JAVA\_OPTS -Dlogpresso.tcp\_sender.idle\_timeout=300"JAVA\_OPTS="$JAVA\_OPTS -Dlogpresso.tcp\_sender.max\_queue\_time=30"JAVA\_OPTS="$JAVA\_OPTS -Dlogpresso.tcp\_sender.max\_queue\_chars=100000000"