### sendsyslog

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

#### 문법

sendsyslog dst=DST\_IP [format=json|txt] [port=INT] [pri=INT] [src=IP\_ADDR]

필수 매개변수

**dst=IP\_ADDR**

Syslog 서버의 IP 주소

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

**port=INT**

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

**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 |

**src=IP\_ADDR**

출발지 IP 주소를 로그프레소 서버의 IP 주소가 아닌 임의의 IP 주소로 바꿔서 전송하려는 경우 설정

출발지 IP 주소를 변경해 전송하려면 운영체제에 libpcap이나 winpcap 라이브러리가 설치되어 있어야 합니다. 또한 araqne-pcap 라이브러리를 운영체제에 맞게 다시 컴파일해야 할 수 있습니다. 출발지 IP 주소를 지정하는 경우에만 PCAP을 사용하여 주소를 변경한 패킷을 생성하여 전송합니다. MTU를 넘는 패킷 크기는 전송에 실패하므로 주의해야 합니다.