### sendsyslog-tcp

入力されたレコードをSyslog（シスログ）形式に変換し、TCP通信を通じて宛先サーバーへ送信します。

#### 構文

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

必須パラメータ

**dst=IP\_ADDR**

SyslogサーバーのIPアドレス

オプションパラメータ

**format=json|txt**

送信するログのフォーマットをjsonまたはtxtから選択します（デフォルト：txt）。

* json: 入力データ全体をJSON形式に変換して送信
* txt: **line**フィールドの文字列値をそのまま送信

**framing=lf|rfc6587**

Syslogメッセージの区切り方法を指定します（デフォルト：lf）。Syslogを受信するサーバーに適した方式を選択してください。

* lf: Syslogメッセージの末尾に改行文字（LF）を使用
* rfc6587: [RFC 6587](https://datatracker.ietf.org/doc/html/rfc6587)に準拠し、各メッセージの先頭にバイト単位のメッセージ長を明記

**port=INT**

Syslogサーバーのリスニングポート番号（デフォルト：514）。1～65535の整数を指定可能です。

**pri=INT**

[RFC 5424](https://datatracker.ietf.org/doc/html/rfc5424)で定義されたPRI定数値（デフォルト：134）。これはlocal0かつINFOレベルに該当します。

PRI定数値はFacility値の8倍にSeverity値を加算した値です。下記の表を参照し、計算した値を使用してください。

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 / daemon | 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**（デフォルト） | 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 |

#### 説明

本コマンドはTCP経由でSyslogメッセージを送信するため、UDP方式と異なりIPパケットの断片化問題がなく、信頼性の高いメッセージ送信が可能です。ただし、Syslogサーバーとの接続が切断されたり遅延が発生した場合、送信待ちのSyslogメッセージキューが滞留することがあります。sendsyslog-tcpコマンドは、メッセージキューの滞留を防ぐため、30秒以内に送信できなかったメッセージは破棄します。メッセージ送信キューを管理するため、ログプレッソ・シェルでは以下のようなシステムスイッチを提供しています。

|  |  |  |
| --- | --- | --- |
| スイッチ | 説明 | 値 |
| logpresso.tcp\_sender.idle\_timeout | サーバーから応答がない場合に送信を中断する基準 | 1～86400秒、デフォルト300秒 |
| logpresso.tcp\_sender.max\_queue\_time | 送信に時間がかかる場合に送信を中断する基準 | 1～600秒、デフォルト30秒 |
| logpresso.tcp\_sender.max\_queue\_chars | 滞留した文字列が多すぎる場合に送信を中断する基準 | 1,000,000～1,000,000,000文字、デフォルト100,000,000（約10MB） |

スイッチを適用するには、ログプレッソ・シェルで以下のコマンドを実行してください。

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

環境設定ファイルconfig.shまたはlogpresso.shに、以下のようにシステムスイッチを適用できます。

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"