



**syslog-ng Premium Edition  
Version 7**

**UDP による  
ログメッセージ収集**

Rev.1.1

2023.9.20

## 目次

1	UDP メッセージの喪失問題.....	1
2	UDP メッセージの喪失問題を解決.....	2
	ログの送信側(ログソース)の近くでログを収集.....	2
	適切なネットワークカードとネットワークドライバを使用.....	2
	仮想マシンではなく物理マシンを使用.....	3
	カーネル内の大きなバッファを使用.....	3
	UDP 用に syslog-ng をチューニング.....	3

## 変更履歴

版	発行日	変更内容
Rev. 1.0	2020/10/19	新規作成
Rev.1.1	2023/9/20	お問合せ先追加

## お問合せ先、およびカスタマーポータル

ジュピターテクノロジー株式会社 (Jupiter Technology Corp.)

住所: 〒183-0023 東京都府中市宮町一丁目 40 番地 KDX 府中ビル 6F

URL: <https://www.jtc-i.co.jp/>

TEL: 042-358-1250(代表) FAX: 042-360-6221

ご購入のお問い合わせ:

    お問い合わせフォーム <https://www.jtc-i.co.jp/contact/scontact.php>

製品サポートのお問い合わせ:

    カスタマーポータル <https://www.jtc-i.co.jp/support/customerportal/>

評価版のダウンロード:

<https://www.jtc-i.co.jp/support/download/>

---

## 1 UDP メッセージの喪失問題

ログの集中管理は、ほとんどの場合、TCP 接続(または暗号化した TCP 接続)をベースにしています。これは、UDPには無い幾つかの信頼性のある特徴を有しているからです。勿論、UDP を使用せざるを得ない状況もまだあります。1つの例では、企業のサーバの標準的なシスログ構成が、宛先が単一の共通の UDP になっており、IT ポリシーのためそれを変更できない場合があります。他の例では、ルータやスイッチやファイアウォールのようなネットワークデバイスが、ログ転送に UDP を使用して送信している場合です。これらのデバイスは、シスログ用に TCP が実装されていないことがほとんどです。幾つかの例では、TCP は実装されていますが、きちんと動作しないため、ユーザにより利用が避けられています。

TCPと比較すると、UDPは軽量でコンピューティングリソースの消費がより少ないです。しかしながら、ログメッセージの転送に関しては、これが UDP の唯一の良い特徴と言えます。送信側では UDP はパケットを送りっぱなし (fire and forget) 方式で送信し、パケットが受信されたか確実ではないことを意味しています。エラー処理、応答、再送、タイムアウトがないため、メッセージを喪失することがあります。

UDP を使用した場合、送信中にメッセージを喪失するいくつかのポイントがあります：

- 複数のホップがある場合、バースト(急激にログ量増大)時にログメッセージを喪失することがあります。
- カーネルのネットワークカードドライバのレベル： 仮想化が問題になるかもしれません。また、あるドライバやカードは、高速転送に追いついて行けず、メッセージを喪失することがあります。
- カーネルバッファサイズ： syslog-ng がカーネルから十分な速さで読み出せない場合、バッファが一杯になり、メッセージを喪失することがあります。
- syslog-ng で転送先が十分な速さでなくバッファが一杯になった場合です。例えば、ディスクIOが他の幾つかのアプリで使用されている場合、メッセージを syslog-ng で書き込むことができません。たとえ専用サーバであっても、格納されたログを閲覧するだけで、この原因になります。

これらの課題は軽減することができますが、覚えておいてほしいのは、UDP は信頼性のあるプロトコルではないということです。

---

## 2 UDP メッセージの喪失問題を解決

UDP は信頼性のあるプロトコルではないため、メッセージの喪失は完全に避けることはできません。状況を改善するために沢山の方法があります。受信する UDP メッセージが少ない場合、安全対策は必要ないかもしれませんが。しかしながら、UDP の高速転送やバーストが予想される場合、これらをすぐに実装する価値はあります。

### udp-balancer()ソースの使用

udp-balancer()ソースを使用すると、複数の CPU コアを使用して、使用可能なハードウェアリソース、受信メッセージサイズ、syslog-ng Premium Edition (syslog-ng PE) の設定に応じて、非常に高いメッセージレートで UDP の受信メッセージを処理できます。

**注意:** この機能には、SO\_REUSEPORT カーネルオプションをサポートする Linux カーネルが必要であるため、それをサポートしたプラットフォームでのみサポートされます。

udp-balancer()ソース、その制限と推奨される使用例、宣言と構成の例、および udp-balancer()ソースオプションの詳細については、[syslog-ng PE の管理者ガイド](#)の”udp-balancer: 超高速での UDP メッセージの受信”を参照してください。

### ログの送信側(ログソース)の近くでログを収集

UDP パケットはスイッチやルータを通るだけで簡単に喪失します。こういう種類の喪失の検出は、メッセージ数を送信側と受信側の両方でカウントしない限り難しいです。メッセージ喪失を避けるには、syslog-ng リレーをログの送信側(ログソース)にできるだけ近いところにインストールします。理想的には、同じスイッチまたは少なくとも同じサブネットにします。ログをより信頼性の高い TCP や ALTP プロトコルを使用して中央のログサーバに転送します。

### 適切なネットワークカードとネットワークドライバを使用

あるネットワークカードは、他ネットワークより高い負荷をよりよく処理します。高速転送の環境では、サーバークラスのオフロード機能を持つネットワークカードを使用する価値があります。同じハードウェアに対して異なるドライバを使用できる場合があるため、要件に合う最適なドライバを選択します。

ストレステスト用にシスログを生成するには、syslog-ng に含まれている loggen を使用することができます。ハードウェアレベルでドロップしたパケットをチェックするには、ifconfig または ethtool を使用できます。

---

## 仮想マシンではなく物理マシンを使用

VMware のようなハードウェアの仮想化では、性能が低下します。特に高速ネットワーキングのようなハードウェアにアクセスする場合です。ある状況では、仮想マシン内で適切なネットワークドライバを使用することでこの問題を解決することもできます。負荷の掛かったホストの場合、適切なネットワークドライバでもこれらの問題を解決できないでしょう。それゆえ、物理マシンにログ収集を移動するのが良いです。

## カーネル内の大きなバッファを使用

もし `syslog-ng` が UDP ソケットから十分な速さでメッセージを読み出すことができない場合、カーネルのバッファは一杯になり始め、設定した制限に達すると、カーネルはメッセージを捨て始めます。このような場合、バッファサイズをそれに応じて調整する必要があります。カーネルの受信バッファを大きくするには、`sysctl` コマンドを使用し `net.core.rmem_max` パラメータを調整します。次に `syslog-ng` のソース定義の `so_rcvbuf` オプションのサイズを大きくします。これにより、`syslog-ng` は、大きなカーネル受信バッファを利用できるようになります。高いトラフィックの環境では、256MB くらいの大きさが必要かもしれません。

```
sysctl -w net.core.rmem_max=268435456
```

値はバイトで入力します。上記は、 $256 * 1024 * 1024 = 268,435,456$  バイトです。実用上このバッファサイズで十分な筈です。ピーク時の受信メッセージを少なくとも 1 秒間保持できます。



### 注意:

大きなバッファの場合、バッファの内容を喪失させるような問題が発生すると、より大きなメッセージ喪失になります。リスクを小さくするには、本当に必要なサイズ以上のバッファを使用せず、要求されたバッファサイズを決めることが重要です。

パケットロスをモニターするには、下記のコマンドを使用してください。

```
netstat -su | grep "receive errors"
```

## UDP 用に syslog-ng をチューニング

UDP プロトコルの関連では、`syslog-ng` は幾つかの設定をすることが可能です。メッセージのバーストを処理するには、`log_fifo_size()` オプションの値を大きくします。上述した `net.core.rmem_max` の値と整合するように、`so_rcvbuff()` の値を大きくします。

---

syslog-ng のフロー制御は、何かの理由で転送先がスローダウンした場合、メッセージの受信をスローダウンさせます。これは、送信側(ソース)が TCP でメッセージを送っている場合に良く機能します。送信側は受信側が遅くなっていることに気付くので、低速でメッセージを送信します。UDP のようなステートレス(状態を持たない)プロトコルでは、こういう状況に対応できません。送信側は、受信側がスローダウンしていることに気付かないため、メッセージを喪失することになります。それゆえ、UDP ソースの場合は、転送先用のフロー制御は有効にしないようにします。

syslog-ng Store Box (SSB)を中央で集中管理するログサーバとして使用する場合、フロー制御は、メッセージの喪失を避けるため、メッセージをログスペースに書き込むログパスに、常に適用されています。それゆえ、ログの処理は、ログが多くのユーザから大量に検索される場合、スローダウンするかもしれません。柔軟に設定することができる syslog-ng PE とは反対に、SSB の管理アプリ下の OS レベルのバッファは、細かくチューニングする機能がありません。それゆえ、メッセージの転送レートがすでに低い場合、UDP ベースのログ収集を TCP ベースに変更するのが良いでしょう。

syslog-ng の UDP のソースドライバは、マルチスレッドではありません。1つの UDP ソースは、シングル CPU コア上でシングルスレッドとして動作します。メッセージの転送レートが高く複数の CPU コアを有している場合、複数の UDP ソースを syslog-ng の config ファイルに定義することができます。この方法により、複数の CPU コアに負荷が分散され、CPU がボトルネックになるのを避けることができます。また、メッセージをいくつかの UDP ソースから受信し同じファイルに書き込む場合、転送先がボトルネックになることがあります。

結果として、UDP ベースのログ収集はメッセージ喪失のリスクを常に伴います。メッセージの喪失の可能性は環境により異なります。そのため、メッセージ喪失のリスクを除去する正しい安全策を選択するため、周囲の全状況を調査する必要があります。

---

日本語マニュアル発行日 2023 年 9 月 20 日  
本書の原文は 『syslog-ng PE Collecting log messages from UDP sources  
July 2020』 です  
ジュピターテクノロジー株式会社 技術グループ