syslog-ngの検証

長岡技術科学大学
数理工学・宇宙物理学研究室
佐々木 幸次,高橋 弘毅

目次

- 導入方法
- 設定方法
- 検証結果
- 比較

導入方法

- yum syslo-ngでインストール(依存関係にあるパッケージ等もインストール)
- OSの再起動をすると、rsyslogdが起動する点に注意(設定を変更する事で対処可能)
- syslogやrsyslogと競合するので、stopする

設定方法

出典:http://www.atmarkit.co.jp/ait/articles/0808/21/news120_3.html

設定方法(source)

internal	syslog-ng内部で生成されるメッセージを出力
unix-stream	SOCK_STREAMモードで指定したUNIXソケットを開き、ログメッセージを受信（Linux場合）
file	指定されたファイルを開き、メッセージを読む
pipe、fifo	指定した名前パイプをオープンして、ログメッセージを読む
udp	UDPポートを待機しログメッセージを受信
tcp	TCPポートを待機しログメッセージを受信

```
source s_input {
    pipe("/var/log/input1.log");
    pipe("/var/log/input2.log");
};
```

設定方法(filter)

facility	指定したfacilityに合致するログメッセージが対象となる。facility（faciliy[,facility]）の形式で指定する。
level	指定したpriorityに合致するログメッセージが対象となる。priority（）level（pri[,pri1..pri2[,pri3]]）の形式で指定する。
host	指定したホスト名（正規表現可）に合致するログメッセージが対象となる。host（ホスト名）の形式で指定する。
match	指定した正規表現そのものに合致するログメッセージが対象となる。

```
filter f_input {
    facility(user);
};
```

設定方法(destinations)

file	指定したファイルにログを出力
fifo、pipe	指定したFIFOやパイプにログを出力
unix-stream	UNIXドメインソケットのSOCK_STREAM形式でメッセージを送信（Linux syslog）
host	udp指定したホストとUDPポートにログを送信
usertty	ログイン中のユーザーにログを出力
program	外部プログラムにログを出力

```
destination d_input {
    file("/var/log/output.log");
};
```

検証結果

- log { source(s_input); filter(f_input); destination(d_input); };

- echo “input_test1” > input1.log
- echo “input_test2” > input2.log
- tail -f output.log

May 25 02:51:12 ip-172-31-3-167 input_test1

May 25 02:51:18 ip-172-31-3-167 input_test2

検証結果

- rmdir dir1 > file3 2>> input1.log

- May 28 00:38:32 ip-172-31-3-167

rmdir: failed to remove ‘dir1’: No such file or directory

検証結果

- fprintf(stderr,”error”)
- ./error.exe 2>> input1.log

- May 28 00:48:34 ip-172-31-3-167 error

比較

	syslog-ng	rsyslog	fluentd
ログ出力形式	自由	自由	json
インストール	yumでのインストールが必要	インストール済み	Gemでのインストールが必要
設定方法	他のファシリティなども設定	他のファシリティなども設定	ログを取りたいものだけ設定
設定項目	未検証	local0～local7まで(デフォルト設定では)	ログを取るアプリケーションだけ