



Kiwi Syslog Daemon

A Freeware Syslog Daemon for Windows

訳：ジュピターテクノロジー株式会社

平成16年5月24日

Program copyright 1998 - 2004 by Kiwi Enterprises.

Latest version available from: www.kiwisyslog.com, www.jtc-i.co.jp

Support: support@kiwisyslog.com, support@jtc-i.co.jp

目次

Kiwi Syslog Daemon	6
Kiwi Syslog Daemon.....	6
フリーウェア版の機能.....	6
正規登録版の機能.....	7
正規登録版の購入.....	8
フィードバック - コメントやバグ	8
ソフトウェアライセンスアグリーメント.....	8
否認.....	9
感謝.....	9
メイン表示ウィンドウ	9
メイン表示ウィンドウ.....	9
Fileメニュー.....	10
Setup (Ctrl-P、設定).....	10
Send Test message to local host (Ctrl-T、テストメッセージ送信)	10
Purge (パージ)	10
Debug options (デバッグ オプション).....	11
Copy display to clipboard (表示をクリップボードにコピー).....	11
Export settings to INI file (設定情報をINIファイルにエクスポート).....	11
Exit (終了).....	11
View (ビュー)メニュー	11
View syslog statistics (Syslog統計の表示).....	11
View e-mail log file (e-mailログファイル表示).....	11
View error log file (エラーログファイルを表示)	11
Adjust width to fit screen (画面幅の自動調節).....	12
Clear display (画面消去)	12
Choose font (表示フォント選択)	12
Manage (管理)メニュー.....	12
Manage (管理)メニュー	12
Install the Syslogd service (Syslogdサービスのインストール)	12
Uninstall the Syslogd service (Syslogdサービスのアンインストール).....	12
Start the Syslogd service (Syslogdサービスの開始)	12
Stop the Syslogd service (Syslogdサービスの停止).....	12
Ping the Syslogd service (SyslogdサービスにPing).....	13
Show the Syslogd service state (Syslogdサービス状態の表示).....	13
Debug options - Display the Service version (デバッグオプション-サービスバージョン表示).....	13
Debug options - Get diagnostic information (デバッグオプション-診断情報入手).....	13
Debug options - Reset the Syslogd service (デバッグオプション-Syslogdサービスリセット).....	13
Debug options - Clear the service DNS Cache (デバッグオプション-DNSキャッシュのクリア).....	13
Debug options - Apply new settings (デバッグオプション-新しい設定の適用)	13
Debug options - Retrieve last messages (デバッグオプション-最終メッセージの取得).....	13
Debug options - Send keep alive (デバッグオプション-Keep alive送信)-- (?)	14
Help (ヘルプ)メニュー.....	14
Kiwi Syslog Help (ヘルプ、F1).....	14
Help Topics (ヘルプトピックス).....	14
Online FAQ (オンラインFAQ)	14
Purchase the registered version (登録版購入).....	14
Enter the registration details (ライセンスの登録、F2).....	14
Make a suggestion or report a bug (バグレポート作成).....	14
Join the mailing list (メーリングリストへの参加).....	14
About Kiwi Syslog (Kiwi Syslogについて).....	15
Syslog プロパティの設定.....	15
最初のSyslog Daemon設定ガイド	15
キーボードの使用方法.....	15
Rules / Filters / Actions (ルール/フィルター/アクション)	15
ルールエンジンの動作	15

ルールの変更	16
Filter Type (フィルタータイプ)	16
Action - Display (アクション - 表示)	26
Action - Log to file (アクション - ファイル記録)	26
Action - Forward to another host (アクション - 他のホストへ転送)	32
Action - Play a sound (アクション - 音を鳴らす)	32
Action - Run external program (アクション - 外部プログラム実行)	32
Action - E-mail message (アクション - E-mailメッセージ送信)	32
Action - Send Syslog message (アクション - Syslogメッセージ送信)	35
Action - Log to ODBC database (アクション - ODBCデータベース記録)	35
Action - Log to NT Event log (アクション - NT Event log記録)	38
Action - Send pager or SMS message via NotePage Pro (アクション - NotePage Pro経由でポケットベルやSMS メッセージを送信)	39
Action - Send ICQ instant message (アクション - ICQインスタントメッセージ送信)	40
Action - Send SNMP Trap (アクション - SNMPトラップ送信)	41
Action - Run Script (アクション - スクリプト実行)	42
Setup - Archiving (設定 - アーカイビング)	53
Setup - Archiving (設定 - アーカイビング)	53
ログファイルアーカイビング動作	53
アーカイブレポートの例	54
アーカイブ時刻オプション	54
Setup - Formatting (設定 - フォーマット)	55
Custom file formats (カスタムファイルフォーマット)	55
Custom DB formats (カスタムDBフォーマット)	55
Setup - DNS Resolution (設定 - DNS解決)	56
Resolve the address of the sending device (送信デバイスアドレス解決)	56
Remove the domain name (ドメイン名を消去- ホスト名の表示のみ)	56
Resolve IP addresses found within the syslog message text (SyslogメッセージテキストのIPアドレス解決)	56
DNS query timeout (DNSクエリタイムアウト)	57
DNS resolver threads (DNSリゾルバースレッド)	57
Setup - DNS Cache (設定 - DNSキャッシュ)	58
local DNS cache (ローカルDNSキャッシュ)	58
Cache settings (キャッシュ設定)	58
Setup - Modifiers (設定 - モディファイア)	59
Syslog message modifiers (Syslogメッセージモディファイア)	59
Setup - Scripting (設定 - スクリプト作成)	59
Setup - Appearance (設定 - 概観)	60
Wallpaper (壁紙)	60
Setup - E-mail options (設定 - E-mailオプション)	60
E-mail setup options (設定 - E-mailオプション)	60
アラームメッセージの例	61
統計メッセージの例	62
Setup - Alarm thresholds (設定 - アラーム閾値)	62
Notify by Mail (メールで通知)	62
Audible Alarm (音で通知)	62
Run Program (プログラム実行)	63
Setup - Input options (設定 - 入力オプション)	63
Setup - Input options (設定 - 入力オプション)	63
Inputs - UDP (入力 - UDP)	63
Inputs - TCP (入力 - TCP)	64
Inputs - SNMP (入力 - SNMP)	64
Beep on every message received (メッセージ受信時ビーブ音)	65
Cisco PIX ファイアウォール(TCP)	66
Inputs - Keep-alive (入力 - Keep alive)	66
Setup - Display (設定 - 表示)	67
Always on top (常時トップ)	67
Rows of scrolling display (スクロール表示の行数)	67

Minimize to System Tray on start-up (スタートアップでシステムトレイを最小化)	67
Use 3D titles (3Dタイトルを使用)	67
Use dd-mm-yyyy date format (dd-mm-yyフォーマット使用、非US フォーマット)	67
Show messages per hour in title bar (タイトルバーに1時間の受信メッセージ数を表示)	68
Blink System Tray Icon when receiving messages (メッセージ受信によるシステムトレイアイコンの点滅)	68
Word wrap (ワードラップ)	68
Adjust column widths automatically (表示画面幅の自動調整)	68
Syslog statistics window (Syslog 統計ウィンドウ)	68
Syslog statistics window (Syslog 統計ウィンドウ)	68
1 Hour history (1時間表示)	69
24 Hour history (24時間表示)	69
Severity (セベリティ)	69
Top 20 Hosts (上位20送信ホスト表示)	69
Counters (カウンター表示)	69
Kiwi Syslog Daemon サービス版	70
Kiwi Syslog Daemon サービス版	70
Installing the Service edition (サービス版をインストールする)	70
サービス版を管理する	71
サービス版の問題解決	71
Kiwi Syslog Daemon NT サービスのアップグレード	71
Kiwi Syslog Daemon NT サービスのアップグレード	71
既存バージョンの削除	72
新バージョンのインストレーション	72
Syslog 送信デバイスを設定	72
Syslog 送信デバイスを設定	72
Cisco ルータ	72
Cisco PIX	73
Cisco Catalyst スイッチ	73
Cisco VPN コンセントレータ	73
Cisco ワイヤレスデバイス(Aironet)	74
Unix マシン	74
Extreme Summit スイッチ	75
Alliant セルラーゲートウェイ	75
DLink DL-840V ルータ	76
Pack X IDScenter	76
SonicWall ファイアーウォール	76
FREESCO ルータ/ファイアーウォール	77
FW-1 ファイアーウォール	77
3Com トータルコントロールシャーシ	77
3Com NetServer	78
Linksys ファイアーウォール	78
Linksys ワイヤレスVPN ルータ	79
Symantec ファイアーウォール/VPN 200	79
SnapGear SOHO+	79
BuffaloTech AirStation ルータ	80
Intertex ADSL ルータ	80
Lucent ルータ	80
Allied Telesyn ルータ	81
Arris ケーブルモデムターミネーションシステム	81
WatchGuard SOHO ファイアーウォール	81
Watchguard Firebox がDshieldと動くようにする	82
Bay Networks デバイス	82
Nortel Networks ルータ	84
ZyXEL ZyWALL 10	84
Netgear / ZyXEL RT311/RT314	85
Netgear RP114 ルータ	85
FVS318 VPN ファイアーウォール	86
HP JetDirect プリンタ	86

W-Linx MB ブロードバンドルータ	86
NetScreen ファイアーウォール	87
Bintech アクセスルータ.....	87
Syslogd エラーとe-mail ログ	88
エラーログ.....	88
エラーログファイルを見る	88
SMTP メールのログ	88
e-mail ログファイルを見る.....	88
Syslog プロトコル.....	88
Syslog ファシリティ	88
Syslog レベル	89
Syslog プライオリティ	90
転送.....	90
Syslog RFC 3164 ヘッダーフォーマット	90
問題解決.....	90
問題解決	90
上級者用の情報.....	91
Kiwi Syslog Daemonのレジストリー設定	91
送信e-mail メッセージの制限	91
統計メール配信時刻.....	91
サービス - スタート/ストップ タイムアウト.....	92
サービス - プロパティ更新タイムアウト.....	92
DNS - ビジー時にwaitをディセーブルにする	92
DNS - 最大キャッシュサイズ.....	93
メッセージバッファサイズ.....	93
E-mail 追加件名テキスト	93
E-mail 追加本文テキスト	94
サービス - Inter-App 通信ポート.....	95
ファイル書き込みキャッシュ	95
アーカイブ置き換え文字	96
アーカイブ分離文字.....	97
コマンドライン引数	97
コマンドライン引数.....	97
デバッグ開始	97
サービスインストール.....	97
サービスアンインストール.....	98
設定にINI ファイルを使用	98
Syslog 関連ソフトウェア	98
Kiwi SyslogGen	98
Kiwi Logfile Viewer	99

Kiwi Syslog Daemon

Kiwi Syslog Daemon

Kiwi Syslog Daemon はSyslogメッセージをネットワークデバイスから受け取り、それらをリアルタイムに表示します。

Syslog メッセージはさらに下記のようなイベント処理を行います：

- メッセージをスクロールウィンドウに表示
- メッセージをテキストファイルに記録
- 他のSyslog サーバーへのメッセージフォワーディング
- ODBCデータベースへの記録
- NTアプリケーションイベントログへの書き込み
- SMTP経由でメッセージをE-mail送信
- 音による警告
- ポケットベルシステムなどの外部プログラムの実行
- SNMPトラップメッセージの送信
- NotePager Proによる通知

受信メッセージにアクションを実行します。メッセージはホスト名、ホストIPアドレス、プライオリティ本文あるいは時刻でフィルターされます。

Kiwi Syslog Daemonには2つの製品があります

- Windows NT4/2K/XP/2K3用サービス版
- Windows 95/98/ME/NT4/2K/XP/2K3用スタンダード版

スタンダード版はインタラクティブに実行され、ユーザーがログインしている間だけ操作できます。

サービス版はNTサービスとして自動的に実行されます。操作のためにログオンする必要はありません。

Kiwi Syslog Service Manager はNTサービスを構成し、管理するインターフェイスを提供します。

BSD SyslogプロトコルはRFC3164で定義されています。

<http://community.roxen.com/developers/idoocs/rfc/rfc3164.html>

Syslogプロトコルについては下記を参照してください：

www.sans.org/infosecFAQ/unix/syslog.htm

フリーウェア版の機能

Kiwi Syslog Daemonフリーウェア版は下記の機能を含みます：

- GUIベースSyslogマネージャ
- 受信時にメッセージをリアルタイム表示
- 10種類のパーチャル表示
- 全てあるいはプライオリティ、日時フィルター後のメッセージを記録もしくはフォワーディング
- プライオリティ、日時によりログファイルを自動分割
- UDP, TCP またはSNMP経由でメッセージを受信
- UDPあるいはTCP経由でメッセージのフォワーディング
- 指定されたスケジュールでログファイルの自動アーカイビング
- 音やe-mailで単位時間のメッセージ数を警告
- 音やe-mailでログファイル容量を警告
- Syslogトラフィック統計を毎日 e-mailで連絡
- システムトレイを最小化
- 他のSyslogホストへのフォワーディング時送信元アドレスを保持
- Syslogトレンドグラフ機能 (直近24時間/1時間)
- 高負荷時でもメッセージ損失の無いバッファリング機能
- 送信元ホストIP の名前解決
- 100エントリーのDNSキャッシング
- 10スレッドまでの先行DNS ルックアップ
- プログラム概観変更の5種のクールスキン
- 表示フォント、表示色、背景の選択
- NTサービス
- RFC3164送受信オプション
- ヘルプ

- 無料（再販禁止）

正規登録版には多数の追加機能があります。

変更、バグ、新バージョンを通知するメーリングリストへの登録は：www.kiwisyslog.com/feedback.htm

正規登録版の機能

フリーウェア版の機能に加え、多くの柔軟性を提供します：

ログファイルの自動分割機能

- ホスト名
- ホストIPアドレス
- ドメイン名
- WELFフォーマットタグサポート

追加フィルターオプション

IPアドレス、ホスト名、テキスト本文によるフィルター
不要なホストメッセージの除去あるいはホスト名に依存する記録動作
特定キーワードを含むメッセージの処理

追加アクション

- フィルタリング、文脈解析、特別な統計と実行などの強力なスクリプトエンジン
- ODBCデータベースへのロギング（Access/SQL/Oracle/MySQL/Informix等）
- WindowsNTアプリケーションイベントログへの書き込み
- フィルター条件に合致したときの任意の音声ファイルによる警告
- e-mailによるSyslogメッセージのフォワーディング
- フィルター条件に合致したときのSyslogメッセージの他ホストへのフォワーディング
- SNMPトラップ送信（Version 1 又は Version 2）
- ICQインスタントメッセージ送信
- NotePager ProによるポケットベルやSMSメッセージ送信
- フィルター条件に合致したときに任意の外部プログラムを実行
- 受信Syslogメッセージの値を外部プログラム、e-mail又はSyslogへ送信：
 - メッセージテキスト
 - メッセージ時刻
 - メッセージ日付
 - ホスト名
 - ファシリティ
 - レベル
 - 警告閾値
 - 現在のSyslog統計

追加バッファリング機能

20,000のSyslogメッセージバッファにより高負荷時でのメッセージロスがありません。
1,000のe-mailメッセージバッファにより高負荷時やメールサーバーの一時的な停止でのe-mailメッセージロスがありません。
20,000エントリーのDNSキャッシュ
200スレッドの先行DNS ルックアップ

追加警告オプション

- 警告時に任意の音声ファイルの実行
- 警告時に任意の外部プログラムの実行。ポケットベルやSMS など

正規登録版におけるその他の長所

正規登録版：

- Kiwi Syslog Daemonで作成したログファイルの管理や調査の柔軟性に優れています。特に大規模なネットワークでは効果的です。拡張されたログファイルの自動分割機能は受信メッセージを容易に分類しそれぞれのログファイルに記録します。特定のデバイス、イベント、条件、あるいは興味に従ったレポートを作成するのに適しています。
- 拡張されたフィルター機能で必要なアクションコントロールを完全にかつ容易に行えます。
- 多数の拡張アクションは受信メッセージ、フィルター、ルールで自動的に実行されます。特に多くのアラート機能はモバイル環境の増加に適しています。
- 大容量バッファ機能。大規模なネットワークに対応でき、一時的なメッセージの大量発生時などでも信頼できるメッセージ処理が可能です。
- 拡張アラートオプション。
- e-mailの優先処理サポート。

その他の長所

- 'help about' ウィンドウに名前が表示され、Kiwi Syslog Daemonの正規ユーザーであることを表示します。
- 無料バージョンアップ(7.0.0 から7.9.9まで)。メジャーバージョンアップの割引提供(7.x.x から8.x.xへ)。

正規登録版の購入

フリーウェア版は無期限に使用できます。日本語資料、代理店による日本語サポート、追加機能が必要な場合は正規登録版を購入してください。

Kiwi Syslog Daemon正規登録版の購入はジュピターテクノロジー株式会社までご連絡ください。

フィードバック – コメントやバグ

プログラムについてのコメントや改良提案はe-mail support@kiwisyslog.com; support@jtc-i.co.jp までお願いします。

ソフトウェアライセンスアグリーメント

使用にあてっての遵守事項：

=====

Kiwi Syslog Daemonフリーウェア版は登録せずに任意の期間使用できます。しかしKiwi Softwareメーリングリストに参加することをお勧めします。バグレポート、使用アドバイス、ニュースリリースが連絡されます。

Kiwi Syslog Daemon (ソフトウェア製品)フリーウェア版を正規登録することにより、フリーウェア製品を超える追加拡張機能が使えます。登録コードは1台のマシンでインストールされる1つのソフトウェア製品で有効です。すべての機能を使用するためにはプログラムコピーごとにユニークなシリアル番号と登録コードが必要です。

ソフトウェアのインストールや使用にあたって、下記に違反しないこと：

=====

- (a) ソフトウェア製品や文書の全部または一部をデコンパイル、リバースエンジニアリング、ディスアセンブル、変更、これらを基本とする派生品を作成すること。
- (b) Kiwi Enterprises社の著作権や資産注意書きを削除すること。
- (c) ソフトウェア製品の登録キーを正規に登録されたエンドユーザー以外に配布すること。
- (d) このソフトウェア製品を他の第三者に貸出すこと。
- (e) Kiwi Enterprisesから直接入手しない登録コードやシリアル番号を使用すること。

ライセンス停止：

=====

使用者がこのライセンスアグリーメントの使用条件に違反した場合、Kiwi Enterprises は他のいかなる権利を損なうことなくライセンスアグリーメントを終了することができます。そのような場合、すべてのソフトウェア製品とコンポーネント、すべての登録コードを破壊しなければなりません。

所有権：

=====

Kiwi Enterprises webサイトのソフトウェア製品と情報は、著作権で保護されたKiwi Enterprises社の資産であり、Kiwi Enterprises社の事前の書面による了解なしではコピー、再作成、変更、出版、アップロード、郵送、転送、配布はどのような方法でもできません。

Kiwi Enterprises社の許可はメールでsupport@kiwisyslog.comまで申し込んでください。

ソフトウェア製品ライセンス：

=====

ソフトウェア製品は著作権法と著作権条約、他の知的財産法や条約で保護されます。ソフトウェア製品はライセンスされますが販売されません。

免責：

=====

ソフトウェア製品は現状で提供され、明示的あるいは暗黙の商行為の保障、特定の目的への適合あるいは非侵害の保障はありません。裁判権は暗黙の保障を認めておらず、前述の除外は完全には適用されません。

ソフトウェア製品は技術的な厳密さや印刷上のエラーを含むことがありますので予告なく変更や更新を行うことができます。

Kiwi Enterprises は予告なくソフトウェア製品を改良し、変更することができます。

ハイリスクアクティビティに使用しないこと：

=====

このソフトウェア製品は耐障害性がなく、そのように設計も、製造もされておられませんから、耐障害機能が要求される危険な環境での使用や、再販売は行わないでください。そのような環境やシステムは、核施設、航空運行、航空通信システム、飛行管理、生命維持装置、武器や、ソフトウェア製品の障害が直接あるいは間接に死、傷害、重大な物理的や環境的損傷をもたらすシステムです。

Kiwi Enterprises社は、ハイリスクアクティビティでのソフトウェア製品の使用に対する明示的あるいは暗黙の適合の保障に、責任はありません。

重大な障害に対する免責：

=====

Kiwi Enterprises がそのような損害賠償の可能性を指摘されていても、Kiwi Enterprises 製品の使用、あるいは使用できないことで生じる、どのような損害賠償(仕事上の利益喪失の被害、ビジネスの妨害、仕事上の情報の喪失、その他の金銭喪失を無制限に含み)もKiwi Enterprises や作者に責任はありません。

否認

このプログラムは無料で提供され保障もありません。この製品や製品の使用や誤用によるどのような障害も著者に責任はありません。

このソフトウェアの著作権は1998 – 2004までKiwi Enterprisesにあります。

このプログラム(Kiwi Syslog Daemon) の使用にあたってはこの否認に同意するものとします。

感謝

Kiwi Syslog Daemonのユーザーで激励のメールをいただいた方に感謝します。フィードバックや提案に感謝し、ユーザーのニーズに合う改良を行います。

正規登録版を購入していただいた、製品の改良をサポートしていただいたすべてのユーザーに感謝します

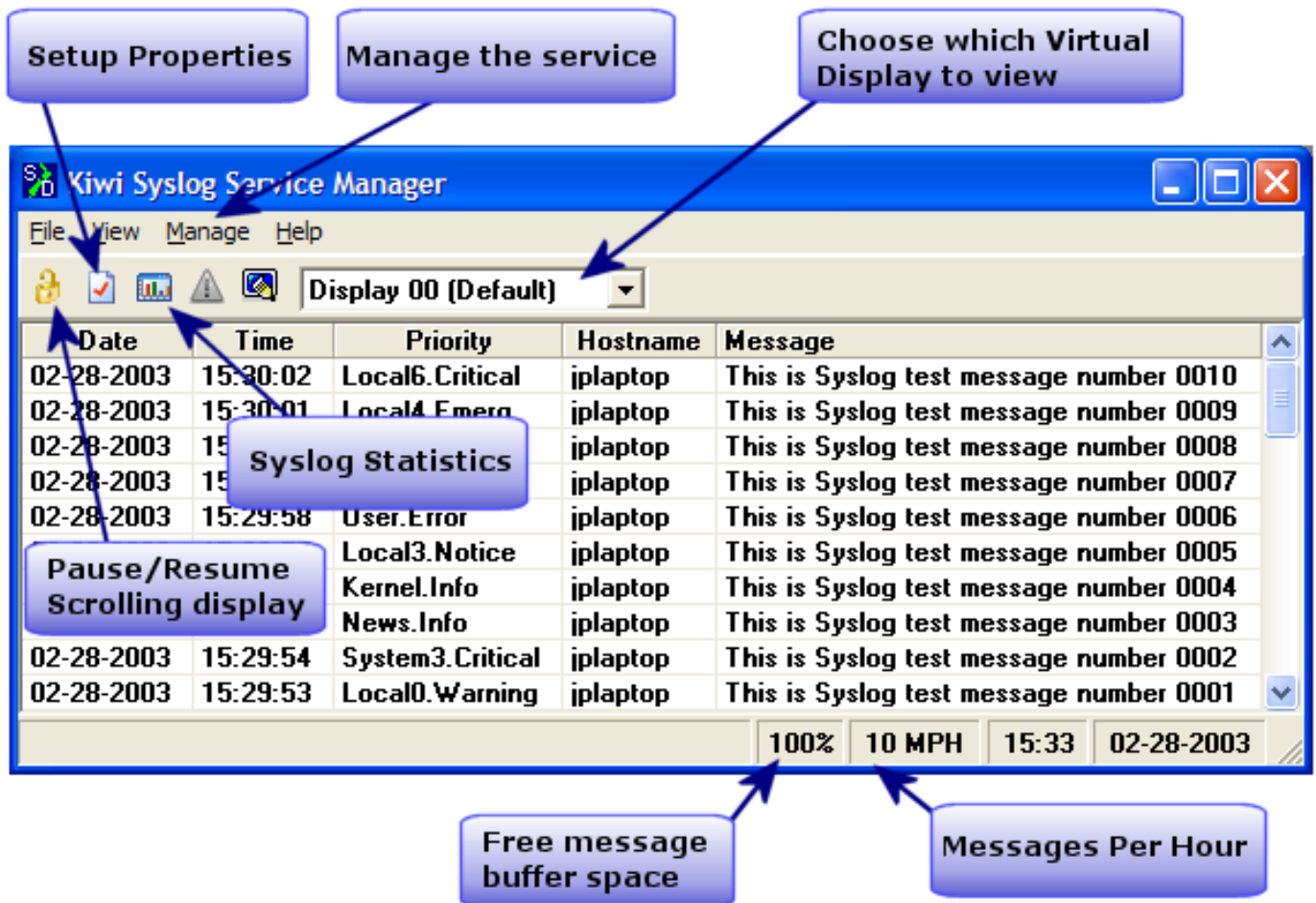
Kiwi Enterprisesチーム

support@kiwisyslog.com

メイン表示ウィンドウ

メイン表示ウィンドウ

スタート直後、Kiwi Syslog Daemonメイン表示ウィンドウが表示されます：



Fileメニュー

Setup (Ctrl-P、設定)

Syslog Setup ダイアログを開きます。 Syslog コンフィグレーションを設定します。

Send Test message to local host (Ctrl-T、テストメッセージ送信)

Localhost(127.0.0.1)にUDP Syslog メッセージを送信し、機能的に正常であることを確認します。 Syslogが待ち受けているポートに送られます。 プログラムのTCP設定の確認にはwww.kiwisyslog.comの SyslogGenソフトをお使いください。

テストメッセージはこのように送られます：

Kiwi Syslog Daemon - Test message number 0001

末尾の番号はテストごとに増加します。

Purge (パージ)

内容をクリアします：

- e-mailログ(InstallPath¥SendMailLog.txt)
- errorログ(InstallPath¥Errorlog.txt)
- 内部Syslogメッセージキュー(1000メッセージまで)

- 内部e-mailキュー(1000メッセージまで)

Debug options (デバッグ オプション)

下記のオプションが可能です：

- Enable Syslog Debug (全受信データをInstallPath¥Syslogd-debug.txtに記録します)
- Reset Syslog socket (待ち受けソケットをクローズし、データをクリアし再びソケットをオープンします)
- View the message buffer (キューのメッセージを表示します)
- View mail buffer (キューのメッセージを表示します)

Copy display to clipboard (表示をクリップボードにコピー)

現在表示中のSyslogメッセージまたはその一部をクリップボードにコピーします。

選択するには表示を中断し、メッセージセルをハイライトさせ Ctrl-Cを押します。

Export settings to INI file (設定情報をINIファイルにエクスポート)

INIファイルにプログラムの構成をセーブします。

このファイルを他のシステムに転送し、その設定をSetup | Defaults/Import/Export オプションで取り込むことができます。

Exit (終了)

プログラムをクローズします。スタンダード版ではプログラムをクローズするとメッセージの受信もロギングも停止します。システムをログオフしても受信、ロギング、メッセージ処理が必要ならばサービス版をインストールしてください。

Displayオプション"**Minimize to system tray on [X] close button**" がチェックされていると、フォーム右上の通常のX ボタンでプログラムをクローズできません。プログラムはシステムトレイポップアップメニューの**File | Exit** でクローズします。

View (ビュー)メニュー

View syslog statistics (Syslog統計の表示)

メッセージカウンターとトレンドグラフを含むSyslog統計ウインドウを表示します。

View e-mail log file (e-mailログファイル表示)

Windowsノートパッドで送信済みメールメッセージログファイルを表示します。
メールログファイルは： InstallPath¥SendMailLog.txtです。

View error log file (エラーログファイルを表示)

Windowsノートパッドでログエラーのログファイルを表示します。
エラーログファイルは： InstallPath¥Errorlog.txtです。

Adjust width to fit screen (画面幅の自動調節)

メインSyslogウィンドウをスクリーン幅に合わせて調節します。

Clear display (画面消去)

選択したスクロール表示の全メッセージを削除します。

Choose font (表示フォント選択)

メッセージ表示のフォント名、スタイル、カラー等を選択します。

Manage (管理)メニュー

Manage (管理)メニュー

サービス版でのみ表示されます。

Kiwi Syslog Daemon サービスマネージャからプログラムのサービス部分の管理とコントロールができます。

Install the Syslogd service (Syslogdサービスのインストール)

Kiwi Syslog DaemonをNT4/Win2K/XPのサービスとしてインストールします。

サービスは一度インストールするだけです。

インストール後、開始を選択すれば実行します。

Uninstall the Syslogd service (Syslogdサービスのアンインストール)

Kiwi Syslog Daemonサービスをアンインストールします。

アンインストール前にサービスを停止してください。

アンインストール後、スタート | 設定 | コントロールパネル | アプリケーションの追加と削除アプレットでアプリケーションを削除できます。

Start the Syslogd service (Syslogdサービスの開始)

Syslogdサービスを開始します。

サービスが開始されたら (実行中) ログの受信、書き込み、フォワードができます。

サービスが実行中かどうかは**Manage | Ping the Syslog service** メニューで確認できます。

Stop the Syslogd service (Syslogdサービスの停止)

Syslogdサービスを停止します。

サービスを停止するとプログラムの実行は止まります。メッセージログは止まり、表示されません。

サービスはManagerからの'Pings'またはどのような通信にも応答しません。

注意：サービス停止まで20秒かかります。

Ping the Syslogd service (SyslogdサービスにPing)

Syslogdサービスにテストメッセージを送り応答を待ちます。5秒以内に応答が無いことはサービスが停止中かインストールされていないことを示します。

結果はメインウィンドウの下部のステータスバーに表示されます。

Ping応答があれば "The Syslogd Service is Alive!" と表示されます。

Show the Syslogd service state (Syslogdサービス状態の表示)

現在のサービスの状態をチェックします。

可能な結果は：インストールされていない、実行中、停止中あるいは無応答です。

Debug options - Display the Service version (デバッグオプション-サービスバージョン表示)

バージョンがService Manager バージョンと同じか確認します。サービスのバージョン番号を確認することができます。

バージョン番号はステータスバーウィンドウに表示されます。

Debug options - Get diagnostic information (デバッグオプション-診断情報入手)

サービスの障害回復が必要ないろいろな段階で、このオプションはサービスマネージャに情報を送ります。データはクリップボードにストアされますのでe-mailやノードパッドに貼り付けることができます。

Syslog Daemon サービスに問題があったら、このオプションで得られる検査情報をチェックするのが良い方法です。

Debug options - Reset the Syslogd service (デバッグオプション-Syslogdサービスリセット)

プログラムやOSに問題は無いがサービスが停止し、分からない問題が発生することがあります。このオプションで再起動し、再インストール状態にします。

オプションが問題を起こすことはありませんが、サービスリスタート時の2,3のメッセージロスがあることに注意してください。

このオプションの実行に3秒必要です。

受信ソケット、つまりサービスのWinsockがリセットされます。

Debug options - Clear the service DNS Cache (デバッグオプション-DNSキャッシュのクリア)

サービスはIPアドレスのホスト名への名前解決を行いますので、DNSキャッシュはネットワークトラフィックを減少させます。

サービスマネージャのDNSキャッシュをクリアするとサービスのキャッシュもクリアします。

このオプションは手動で強制的にサービスキャッシュをクリアするためのものです。

Debug options - Apply new settings (デバッグオプション-新しい設定の適用)

サービスがレジストリーから現在のSyslog設定を読みその条件で再スタートさせます。

新しい設定を適用したことを確認したい場合使用できます。

サービスが新しい設定になったことはステータスバーの表示が示しています。

Debug options - Retrieve last messages (デバッグオプション-最終メッセージの取得)

バーチャルディスプレイの現在の全メッセージを送信するよう要求します。これはサービスマネージャがスタートしたとき自動的に行われます。

Debug options - Send keep alive (デバッグオプション-Keep alive送信)--- (?)

サービスマネージャは1分に1回“ 現在動作中である ”メッセージをサービスに送ります。これでサービスはメッセージを活動中のサービスマネージャに送らなければいけないことが分かります。サービスが3分間“ 現在動作中である ”メッセージを受信しない場合、サービスマネージャへのメッセージ送信を停止します。サービスマネージャが実行していない時のCPU使用とネットワークトラフィックを減少させます。

このオプションはサービスにキープアライブメッセージを送信します。この機能はデバッグ用です。

Help (ヘルプ)メニュー

Kiwi Syslog Help (ヘルプ、F1)

helpファイル (英文) を開きます。

Help Topics (ヘルプトピックス)

目次を開きます。

Online FAQ (オンラインFAQ)

Webブラウザで www.kiwisyslog.comのFAQを開きます。

Purchase the registered version (登録版購入)

登録正規版ライセンスをwww.kiwisyslog.com/register.htm からオンライン購入できます。

注：日本語でのサポートは提供されません。

Enter the registration details (ライセンスの登録、F2)

現在の登録状況を表示し、ライセンスコードを登録します。

Make a suggestion or report a bug (バグレポート作成)

Kiwi Enterprisesへの示唆や障害報告を行うダイアログを開きます。SMTPメールサーバーアドレス、e-mailアドレス、名前が必要です。E-mailが作成されsupport@kiwisyslog.comに送られます。

あるいはWebサイトwww.kiwisyslog.com/feedback.htmのフィードバックフォームを使うこともできます。

Join the mailing list (メーリングリストへの参加)

メーリングリストに参加するフィードバックフォームを開きます。SMTPメールサーバーアドレス、e-mailアドレス、名前が必要です。E-mailが作成されsupport@kiwisyslog.comに送られます。

あるいはWebサイトwww.kiwisyslog.com/feedback.htmのフィードバックフォームを使うこともできます。

About Kiwi Syslog (Kiwi Syslogについて)

About Kiwi Syslog Daemon ダイアログを開きます。

バージョン、登録、プログラムの実行累積時間などが表示されます。

Syslog プロパティの設定

最初のSyslog Daemon設定ガイド

Kiwi Syslog Daemon の最初の実行時、デフォルト設定が使われます。全メッセージが表示され、ログファイルに書かれることを確認して下さい。

File | Setup メニューあるいはCtrl-P でこれらの設定を変更します。

Defaults/Import/Export プロパティオプションの**Load default Rules and Settings** ボタンでいつでもデフォルト設定に戻すことができます。

キーボードの使用法

Delete	選択したルール、フィルター、アクション、アーカイブスケジュールの削除
Insert	新しいルール、フィルター、アクション、アーカイブスケジュールの追加 (選択アイテムはルール、フィルター、アクション、アーカイブのみ)
Ctrl-V	ルール、フィルター、アクション、アーカイブスケジュールの貼り付け (選択アイテムはルール、フィルター、アクション、アーカイブのみ)
Ctrl-C	ルール、フィルター、アクション、アーカイブスケジュールのコピー
F2	ルール、フィルター、アクション、アーカイブスケジュールの名前変更
F4	フィルター、アクション、アーカイブスケジュールに自動的に名前付け
Home	ツリー先頭にカーソル移動
End	ツリー末尾にカーソル移動
Enter	現在の選択位置にツリーを展開もしくは圧縮(マウスダブルクリックと同じ)
Space bar	選択したルール、フィルター、アクション、アーカイブスケジュールをイネーブル又はディセーブルにする
Shift + Up Arrow	選択したルール、フィルター、アクション、アーカイブスケジュールを上に移動
Shift + Dn Arrow	選択したルール、フィルター、アクション、アーカイブスケジュールを下に移動

Rules / Filters / Actions (ルール/フィルター/アクション)

ルールエンジンの動作

最大100のルールを定義できます。各ルールは最大100のフィルターと最大100のアクションまで定義することができます。

受信したsyslogメッセージはルールで処理されます。上位から下位のルールに向かいます。ルールの順序はツールバーのボタンで上または下に調整できます。

各ルールでメッセージは特定のフィルターでチェックされます。上位から下位に向かってフィルターされます。全てのフィルターに合致しない場合、ルール処理をストップし次のルールに移ります。フィルター条件に合致すると指定された1つもしくは複数のアクションを実行します。上位から下位のアクションに向かいます。

ルールの全アクションが完了後、リストの次のルールを処理します。全てのルール処理を終了すると次のsyslogメッセージの受信を待ち、新しいメッセージ処理を最も上位のルールから行います。

各ルール、フィルター、アクションには分かり易い名称が付けられます。名称を編集するにはF2をクリックするかメニューを右クリックします。名称はユニークである必要はありませんが機能を表現すべきです。名称は最大25文字です。

ルールにフィルターが定義されていない場合全てのメッセージが合致します。

デフォルト初期設定ではDefault名称のルールが一つ定義されていますがフィルターは含まれません。全てのメッセージが合致します。二つのデフォルトアクションDisplayとLog to fileが使われます。デフォルトでは全てのメッセージが表示されファイルにロギングされます。

ルール、フィルター、アクションの追加/削除/名称変更はキーボードの使用方法を参照してください。

ルールの変更

新規ルール、フィルター、アクション、アーカイブスケジュールの追加

項目を選びツールバーのCreate new itemをクリックします。もしくは項目を右クリックしAdd...で追加します。追加するとカーソルがその項目に移動します。

ルール、フィルター、アクション、アーカイブスケジュールの削除

削除する項目を選びツールバーのDelete the itemをクリックします。もしくは項目を右クリックしDelete...で削除します。あるいはDeleteキーで削除します。

ルール、フィルター、アクション、アーカイブスケジュールのコピー

コピーする項目を選びツールバーのCopy the itemをクリックします。もしくはCtrl-C かメニューを右クリックします。

コピーしたルール、フィルター、アクション、アーカイブスケジュールのペースト

ツールバー、Ctrl-Vあるいはメニューを右クリックします。追加するとカーソルがその項目に移動します。

ルールのインポートとエクスポート

ルールをImportやExportするにはメニューを右クリックします。カーソルはImportするルールまたはExportするルールに移動します。Exportファイル名もしくはどこからImportするかを聞かれます。デフォルトファイル拡張子は.ksr (Kiwi Syslog Rule)です。

エクスポートされたルールファイルは後日の使用に備え、また他のsyslogサーバーで使うため、e-mailで送信することが可能です。

効果的なフィルター/アクション設定を作成し、それを他のユーザーを共有する気持ちがありましたら.ksr ファイルのコピーをsupport@kiwisyslog.comまで送ってください。

ルールファイルを他のシステムからインポートする時、アクション設定が正しいかチェックしてください。もとのシステムではドライブ名が異なる場合があります。正しく変更しなければなりません。例えばC:をD:もしくは逆の場合もあります。

Filter Type (フィルタータイプ)

Simple filer (シンプルフィルター)

概要

簡単な1行のフィルターです。メッセージのテキストの文字やIPアドレスのマッチングに有効です。複数の引用検索文字を含むと文字Aまたは文字Bのようなマッチングが可能です。

含む: "link up" "link down"

一致する: "link up" もしくは "link down"

詳細

simple filterは1行の文字やテキストを指定できます。各検索文字は" "で区切られます。複数の引用検索文字は同じ行に記述できます。フィルターは指定された文字のいずれかのマッチングを行います。これはORの関係です。

[C] ボタンは文字検索で大小文字を区別するかどうかを選択します。

[S] ボタンは一部分検索あるいは全体検索かどうかを選択します。 .

例:



The image shows a graphical user interface for configuring a filter. It features a text input field labeled "Include:" containing the string "POP3" "SMTP" "MAPI". To the right of the input field are two buttons: one labeled "C" and one labeled "S".

メッセージテキストがどこかにいずれかを含んでいれば結果は真です。

注意 [S] ボタンが押されると部分文字列検索になります。検索文字がテキストのどこかに現れることを意味します。

全ての文字は引用符でくくられます。項目を隣り合わせにできます。それらはORになります。

上のフィルターの意味は：

POP3、SMTP、MAPIが大文字か小文字でテキストに含まれていればフィルターは真です。

Include: "The link is down"	C	S
-----------------------------	---	---

メッセージテキストが指定文字と完全に一致していれば結果は真です。

注意 [S] ボタンが押されていないと選択文字はメッセージテキストに一文字ごとに完全に一致しなければなりません。

[C]ボタンが押されると大小文字を正確に指定します。

上のフィルターの意味は：

メッセージテキストがThe link is downであればフィルターは真です。

Complex filter (コンプレックスフィルター)

概要

複数行にわたる複雑なフィルターです。テキストとIPアドレスの複雑な 含む/含まない のマッチングをします。引用符でくくられた複数の、引用符でくくられた文字列を検索文字としてブール演算します。

AND, OR, NOT-OR, NOT-AND とエクスクルージョンが可能です。

詳細

コンプレックスフィルターでは複合検索文字列が指定できます。検索文字列は[(A または B) および (C または D)] しかし[(E または F) および(G または H)]のように相互を結合できます。

各検索文字列は“ ”で囲まれます。複数の検索文字列を同一行に書くことができます。フィルターは指定された文字列のマッチングを行います。ORの関係です。

[C]ボタンは文字検索で大小文字を区別するかどうかを選択します。

[S]ボタンは一部分検索あるいは全体検索かどうかを選択します。

フィルターマッチングでは空白フィールドは無視されます。

最初の2つのフィールドがブランクで、3,4番目でテキストを指定するとエクスクルージョンマッチングを実行します。テキストが一致しない場合が真です。

例：

Include: "fox" "quick" "hello"	C	S
And: "over" "the"	C	S
Exclude: "hello"	C	S
And: "brown"	C	S

注意 [S] ボタンが押されていると部分文字列検索になります。これは検索文字列がテキストのどこかに現れていることを意味します。

全ての文字は“ ”でくくられます。項目を隣り合わせにできます。それらはORになります。

上のフィルターの意味は：

メッセージテキストがfox あるいは quickあるいは helloを含み、over あるいはtheを含むが、hello および brown(大文字でも小文字でも良い)を含まない時フィルターは真である。

Include:	<input type="text"/>	<input type="button" value="C"/>	<input type="button" value="S"/>
And:	<input type="text"/>	<input type="button" value="C"/>	<input type="button" value="S"/>
Exclude:	<input "^the""="" type="text" value='"chicken" "duck""/></td> <td><input type="button" value="C"/></td> <td><input type="button" value="S"/></td> </tr> <tr> <td>And:</td> <td><input type="text"/></td> <td><input type="button" value="C"/></td> <td><input type="button" value="S"/></td> </tr> </table> </div> <div data-bbox="57 250 340 263" data-label="Text"> <p>エクスクルーションフィルターの例です：</p> </div> <div data-bbox="57 273 950 299" data-label="Text"> <p>テキストがchicken あるいは duck を含まない時、結果は真です。最初の2つのフィールドが空白であることに注意してください。これらのフィールドはフィルター処理で無視されます。</p> </div> <div data-bbox="57 309 85 322" data-label="Text"> <p>注：</p> </div> <div data-bbox="57 333 382 346" data-label="Text"> <p>And: フィールドは不要ならば空白のままが良い。</p> </div> <div data-bbox="57 356 666 370" data-label="Text"> <p>And: フィールドが値を持っている場合、その上のフィールドはデータを含んでいなければならない。</p> </div> <div data-bbox="65 405 513 423" data-label="Section-Header"> <h2><u>Regular Expression filter (正規表現フィルター)</u></h2> </div> <div data-bbox="57 450 90 463" data-label="Section-Header"> <h3>概要</h3> </div> <div data-bbox="57 462 950 488" data-label="Text"> <p>Unixタイプの標準表現一致を使います。テキストの数字の範囲、文字やシンボルで合致条件を作るのに有効です。テキストの検索で最も自由が利きます。例えばテキスト中の位置の指定なども含みます。</p> </div> <div data-bbox="57 500 497 511" data-label="Text"> <p>AND, OR, NOT OR, NOT AND やエクスクルージョン合致に有効です。</p> </div> <div data-bbox="57 534 90 547" data-label="Section-Header"> <h3>詳細</h3> </div> <div data-bbox="57 547 759 560" data-label="Text"> <p>正規表現フィルターではUnixタイプの正規表現引数でテキストの“どこ”で“何”を厳密にコントロールできます。</p> </div> <div data-bbox="57 569 950 595" data-label="Text"> <p>各検索文字列はダブルクォーテーションに含まれなければなりません。複数検索文字列を同じ行に並べることができます。フィルターは指定文字列のいずれかに合致するかを検索します。これはORになります。</p> </div> <div data-bbox="57 605 406 619" data-label="Text"> <p>[C] ボタンで大小文字の区別をするか否かを選択します。</p> </div> <div data-bbox="57 630 418 643" data-label="Text"> <p>フィルターマッチプロセスは空白フィールドを無視します。</p> </div> <div data-bbox="57 653 950 679" data-label="Text"> <p>最初の2つのフィールドを空白にし、3,4番目のフィールドを指定するとエクスクルージョンマッチングを行います。この場合、テキストが合致しないと結果は真です。</p> </div> <div data-bbox="57 690 85 703" data-label="Text"> <p>例：</p> </div> <div data-bbox="58 733 912 909" data-label="Form"> <table border="1"> <tr> <td>Include:</td> <td><input type="text" value='/>	<input type="button" value="C"/>	
And:	<input "chicken""="" type="text" value='"dog\$""/></td> <td><input type="button" value="C"/></td> </tr> <tr> <td>Exclude:</td> <td><input type="text" value='/>	<input type="button" value="C"/>	
And:			

全文字列はダブルクォートで区切ります。隣り合うアイテムはORになります。

上のフィルターの意味です：

メッセージテキストがThe（大文字区別有り）で始まり、dog で終わるがchicken やDuck を含まない時、結果は真です。

Include:	<input type="text"/>	<input type="button" value="C"/>
And:	<input type="text"/>	<input type="button" value="C"/>
Exclude:	<input type="text" value="'^The'"/>	<input type="button" value="C"/>
And:	<input "="" type="text" value='"dog\$'/>	<input type="button" value="C"/>

これはエクスクルージョンフィルターの例です：

メッセージテキストの先頭にThe が含まれず、終わりにdog が含まれなければ真です。
先頭の2つのフィールドが空白であることに注意してください。これらのフィールドはフィルター処理では無視されます。

注:

And: フィールドは不要なら空白で良い。

And: フィールドに値があれば、その上のフィールドにもデータが必要。

表現構文:

フィルターで認識される正規表現構文は次の特殊文字がベースです：

Char Description

^ 文字列の始まり

\$ 文字列の終わり

.

[list] リスト中の任意の文字。例、[AEIOU]は任意の大文字1字

[^list] リスト中不在任意の文字。例、[^]スペース以外の任意の文字

[A-Z] A~Zの1文字。例、[0-9]は任意の数字1文字

? 前の文字を0又は1回繰り返す。例、10?は1と10

* 前の文字を0又は1回以上繰り返す。例、10* は1、10、1000など

+ 前の文字を1回以上繰り返す。例、10+ は10、1000など

¥ 次の文字をエスケープ。文脈中の特殊文字に必要。例、¥.¥*¥+¥¥ は.*+¥" に合致。特殊な非印刷文字(タブなど)のエンコードにも必要。

上記の文字に加え、バックスラッシュでエンコードされる下記の7種類の特殊文字がある：

コード 説明

¥a ベル又はASCII 7

¥b バックスペース又はASCII 8

¥f 改行又はASCII 12

¥n 新行またはASCII 10

¥r キャリッジリターン又はASCII 13

¥t 水平タブ又はASCII 9

¥v 垂直タブ又はASCII 11

¥q 引用符又はASCII 34

例:

```
"^stuff"      ' stuffで始まる任意の文字列"  
"stuff$"     ' stuffで終わる任意の文字列"  
"o.d"       ' old, odd, ord等  
"o[ld]d"    ' old又はoddのみ  
"o[^l]d"    ' odd, ord, ではあるがoldではない  
"od?"      ' o 又は od  
"od*"     ' o, od, odd  
"od+"    ' od, odd, 等  
"¥."     ' 小数点(エスケープ文字が必要)  
"[A-Z][a-z]*" ' 任意の大文字語  
"[0-9]+"  ' 任意の数字列  
"[1-9]+[1-9]*" ' 0で始まらない任意の数字列  
"[+¥-]?[0-9]*[¥.]?[0-9]*" ' 符号と小数点付きの任意の数字  
                               '(2つのエスケープ文字が必要)  
"dst=¥qLOCAL MACHINE¥q" ' dst=LOCAL MACHINEが見つかる
```

IP Address Range filter (アドレス範囲フィルター)

概要

IPアドレス範囲の一致を見ます。ホストアドレスの範囲を含むか含まないかを判断します。

詳細

含むあるいは含まないIPアドレスの範囲を指定できます。

IncludeあるいはExcludeの範囲は空白でもかまいませんが両方はだめです。

Include範囲が空白であればフィルターはエクスクルージョンモードになります。IPアドレスがExclude値の範囲であれば結果は真です。

例:

Include range start:	<input type="text" value="203"/>	.	<input type="text" value="185"/>	.	<input type="text" value="100"/>	.	<input type="text" value="0"/>
Include range end:	<input type="text" value="203"/>	.	<input type="text" value="185"/>	.	<input type="text" value="100"/>	.	<input type="text" value="255"/>
Exclude range start:	<input type="text" value="203"/>	.	<input type="text" value="185"/>	.	<input type="text" value="100"/>	.	<input type="text" value="10"/>
Exclude range end:	<input type="text" value="203"/>	.	<input type="text" value="185"/>	.	<input type="text" value="100"/>	.	<input type="text" value="20"/>

上のフィルターの意味は:

IPアドレスが203.185.100.0 ~ 203.185.100.255であり、203.185.100.10 ~ 203.185.100.20の範囲でなければ結果は真です。

Include range start:	<input type="text"/>	.	<input type="text"/>	.	<input type="text"/>	.	<input type="text"/>
Include range end:	<input type="text"/>	.	<input type="text"/>	.	<input type="text"/>	.	<input type="text"/>
Exclude range start:	<input type="text" value="203"/>	.	<input type="text" value="185"/>	.	<input type="text" value="100"/>	.	<input type="text" value="10"/>
Exclude range end:	<input type="text" value="203"/>	.	<input type="text" value="185"/>	.	<input type="text" value="100"/>	.	<input type="text" value="20"/>

エクスクルージョンフィルター例です：

IPアドレスが203.185.100.10 ~ 203.185.100.20でなければ結果は真です。

IP Subnet Mask filter (サブネットマスクフィルター)

概要

ホストアドレスのInclude/Excludeの定義にサブネットマスクを使用できます。

詳細

IPサブネットマスクフィルターでマスクマッチングベースでIPアドレスのInclude・Excludeを指定できます。

IncludeあるいはExcludeの範囲は空白でもかまいませんが両方はだめです。

Include範囲が空白であればフィルターはエクスクルージョンモードになります。IPアドレスがExclude値の範囲であれば結果は真です。

例：

Include IP Address:	<input type="text" value="203"/>	.	<input type="text" value="185"/>	.	<input type="text" value="100"/>	.	<input type="text" value="0"/>
Mask:	<input type="text" value="255"/>	.	<input type="text" value="255"/>	.	<input type="text" value="255"/>	.	<input type="text" value="0"/>
Exclude IP Address:	<input type="text"/>	.	<input type="text"/>	.	<input type="text"/>	.	<input type="text"/>
Mask:	<input type="text"/>	.	<input type="text"/>	.	<input type="text"/>	.	<input type="text"/>

指定されたIPアドレスは指定のマスクとAND演算されメッセージのホストIPと比較されます。2つのアドレスが同一サブネットであれば結果は真です。

上のフィルターの意味は：

IPアドレスが203.185.100.0 ~ 203.185.100.255であれば結果は真。

Include IP Address:	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Mask:	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Exclude IP Address:	<input type="text" value="203"/>	<input type="text" value="185"/>	<input type="text" value="100"/>	<input type="text" value="0"/>
Mask:	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="0"/>

これはエクスクルージョンフィルターの例です：

IPアドレスが203.185.100.0 ~ 203.185.100.255でなければ、結果は真です。

Priority filer (プライオリティフィルター)

概要

選択プライオリティが受信メッセージプライオリティと比較されます。

詳細

各受信メッセージにはプライオリティが含まれています。この値はファシリティとレベルで構成されています。どのプライオリティでフィルター結果を真にするかを指定できます。

プライオリティを選択するにはファシリティとレベルの格子をダブルクリックします。緑の球はフィルター結果を真にするプライオリティであることを示します。

ポップアップメニューオプションを表示するにはマウスで行又は列を選び右クリックします。

	Emerg	Alert	Crit	Error	Warn	Notice	Info	Debug
Kernel	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
User	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
Mail	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
Daemon	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
Auth	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
Syslog	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
Lpr								
News								
UUCP								

Toggle to ON
 Toggle to OFF
 Select All
 Inverse

全てのプライオリティに緑の球を設定すると、メッセージのプライオリティ値の如何にかかわらず一致することになります。全てのプライオリティを一致させたいのであればフィルターを使用する必要はありません。プライオリティフィルターが無いということはすべてのプライオリティをパスさせることです。

Inverseは現在イネーブルのボックスをブランクにし逆の操作もします(イネーブルのボックスを逆にすることはエクスクルージョンフィルターを作成することです)。

Select All で全てのプライオリティを選びます。次にToggle to OFF or ON で緑の球を逆にします。

例：

	Emerg	Alert	Crit	Error	Warn	Notice	Info	Debug
Kernel	✓	✓	✓	✓	✓			
User	✓	✓	✓	✓	✓			
Mail	✓	✓	✓	✓	✓			
Daemon	✓	✓	✓	✓	✓			
Auth	✓	✓	✓	✓	✓			
Syslog	✓	✓	✓	✓	✓			

上のフィルターの意味は：

Warnigより高いレベルの全ファシリティのメッセージは結果が真です。

	Emerg	Alert	Crit	Error	Warn	Notice	Info	Debug
Kernel								
User	✓	✓	✓	✓	✓	✓	✓	✓
Mail								
Daemon								
Auth								
Syslog								

上のフィルターの意味は：

User ファシリティを持つ全てのメッセージは結果が真です。

	Emerg	Alert	Crit	Error	Warn	Notice	Info	Debug
Kernel	✓	✓	✓	✓	✓	✓	✓	✓
User								
Mail	✓	✓	✓	✓	✓	✓	✓	✓
Daemon	✓	✓	✓	✓	✓	✓	✓	✓
Auth	✓	✓	✓	✓	✓	✓	✓	✓
Syslog	✓	✓	✓	✓	✓	✓	✓	✓

上のフィルターはエクスクルーションフィルターでありその意味は：

Userファシリティ以外の全てのメッセージは結果が真である。

Time of day filter (時刻フィルター)

概要

現在の日時とマトリック中に設定された時刻を比較しアクションの許可、拒否が決まります。

詳細

ある時刻を含んでも含まなくても良い。

時刻（1/4時間単位）を選択するには時刻と日付の交差場所をダブルクリックする。緑の球は日時に一致したらフィルターの結果が真。

行、列の選択はマウスを使い、ポップアップオプションを右クリックで表示する。

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
00:00	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
00:15	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
00:30	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
00:45	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
01:00	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
01:15							
01:30							

Toggle to ON
 Toggle to OFF
 Select All
 Inverse

全時刻をイネーブルにすると、どのような時刻のメッセージが到着しても合致することになる。時刻を何も設定しないと、全時刻のメッセージがパスします。

Inverseは現在の全設定を逆にします（イネーブルボックスを逆にすることはエクスクルーションフィルターを作成することです）。

Select Allメニューは全タイムセグメントを選びます。次にToggle to OFF or ONで逆にします。

例：

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
07:45							
08:00		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
08:15		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
08:30		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
08:45		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
09:00		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
09:15		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

上のフィルターの意味は：

月曜日午前8時から金曜日午前9時までの全メッセージの結果は真である。

就業時間フィルターは月曜日から金曜日、午前8時から午後5時を選んで作成します。特別な構成のinverse オプションはエクスクルーションフィルターになります。例えば、月曜から金曜の午前8時から午後5時ではない。

Time interval filter (時間インターバルフィルター)

概要

1回のトリガーから次のトリガーまで設定した時間待ちます。

ルールのフィルターの後必要なFlags/Counters フィルターが置かれます。他のフィルターが先に処理されます。

詳細

タイムインターバルフィルターは特別なメッセージテキストが見つかった時のsend e-mail messageのような通知アクションで効果的です（例えば"link down"）。1分間に接続、切断が何度も繰り返すと回線切断メッセージを何度も受信します。タイムインターバルフィルターは1回実行すると次の実行までX分待ちます。

タイムインターバルフィルター使用での回線切断通知例：

```
Rule: Link down notify
Filters
  Filter: Field=Hostname, Type=Simple.
```

Include: "central-router.company.com" [S]

Filter: Field=Msg Text, Type=Simple.

Include: "link down" [S]

Filter: Field=Flags/Counters, Type=Time interval

Fire this event once, then wait for 15 minutes before firing again.

Actions

Action: Send E-mail message

E-mail body: **The link has gone down, please call the helpdesk.**

Alert - %MsgText

ホストcentral-router.company.com からテキストにlink down を含むメッセージが来たら最初のフィルター(Message text) は真です。次にタイムインターバルフィルターが処理されます。最初の処理は真で次のアクションを実行します。指定された時間のカウントダウンが始まります。上の例では15分です。同じホストからlink down を含むメッセージが来ると最初のフィルター(Message text) は再び真になります。カウントダウンタイマーがゼロになるとタイムインターバルフィルターは偽になり次のアクションは実行されません。

このフィルターはアタック時のe-mail送信回数を減少させるために使われます。例えば、port scan detected テキストを受信したことを知りたいが、毎回ではなく1時間に1回で良いような場合です。タイムインターバルフィルターを1回実行し次の実行を60分待ちます。

Threshold filter (閾値フィルター)

概要

このフィルターは前のフィルターがY秒にX回の条件を満たすと実行されます。

ルール中の他の全タイプのフィルターの後にFlags/Counters フィルターが必要です。他のフィルターが先に処理されます。

詳細

Threshold フィルターはあるレベルに達したイベントについてのみ知りたい時有効です。例えば、port scan detectedを含むメッセージを1分間に5回以上受信した時だけアラートが必要な場合です。これは誰かが明らかにネットワークをスキャンしているからです。

他の例はログイン試行失敗監視です。テキストに30秒に5回以上login failed が含まれるとbrute force 攻撃の可能性があります。タイムインターバルフィルターを使ったlink down 通知の例です：

Rule: Failed login

Filters

Filter: Field=Hostname, Type=Simple.

Include: "unixhost.company.com" [S]

Filter: Field=Msg Text, Type=Simple.

Include: "login failed" [S]

Filter: Field=Flags/Counters, Type=Threshold

Filter is true if event occurs 10 times in 120 seconds.

Actions

Action: Send E-mail message

E-mail body: **Intruder Alert – Login failed 10 times in 2 minutes.**

Alert - %MsgText

ホストcentral-router.company.com から120秒に10メッセージがlogin failed テキストを含むとフィルターは真です。この時、下のアクションを実行します。

このフィルターはe-mail送信回数を減らすためにも使われます。通知されたい閾値を設定するために使うことが出来ます

Timeout filter (タイムアウトフィルター)

概要

このフィルターは前のフィルターがY分にX回の条件を満たすと実行されます。

ルール中の他の全タイプのフィルターの後にFlags/Counters フィルターが必要です。他のフィルターが先に処理されます。

詳細

タイムアウトフィルターはSyslogデバイスを監視しているが何も起きないとき有効です。例えば、ファイアーウォールは通常1時間に200メッセージ以上を生成します。メッセージ量が1時間に10メッセージ以下になった時、あるいはメッセージがなくなった時、e-mailで通知されます。

このフィルターは他のflags/countersのように入力メッセージで終わるものと異なります。メッセージが無いことによるカウントダウンタイマーで終わります。そこでこのフィルターが終わる時はイベントに伴うメッセージがありません。フィルターの下のアクションに渡すインフォメーションメッセージが作られます。メッセージは次のフォーマットです。

優先度: Local7.Debug (191)
ホストIP: 127.0.0.1 (localhost)
MsgText: ルールRule name hereがY分にX回一致したので閾値はZ回に設定されました。

Rule: Firewall Monitor
Filters
Filter: Field=Hostname, Type=Simple.
Include: **"firewall.company.com" [S]**
Filter: Field=Flags/Counters, Type=Timeout
Filter is true if event doesn't occur **1** times in **5** minutes.
Filter: Field=Time of Day, Type= Time of Day
Monday to Friday 8:00 a.m. to 6:00 p.m.

Actions
Action: Send E-mail message
E-mail body: Firewall is not alive
Alert - %MsgText

%MsgText will read:
Firewall Monitorルールは5分で1度も一致しませんので閾値は1回になりました。

firewall.company.com から5分間メッセージがこなければカウントダウン時間がなくなります。通すかどうかは続くTimeout フィルターがテストされ (時間は8:00 a.m. ~ 6:00 p.m.),アクションを実行します。このフィルターは他のフィルターの様に特別なメッセージがトリガーにはなりません。カウントダウンタイマーがなくなったときに限られます。現在のメッセージとしてインフォメーションメッセージが作成されます。アクションがアラートなどにこのメッセージを使います。

フィルター定義のインポートとエクスポート

後日あるいは他のユーザーと共有するためフィルター定義をファイルにエクスポートすることができます。ImportとExportを使います。

フィルターをインポートするにはImportボタンを選びます。KSDファイルをインポートするダイアログが聞かれます。

選択したフィルターをファイルにセーブするにはExportボタンを選びます。フィルターファイルの拡張子は**KSR** です。

他のユーザーにとっても有効なフィルター定義を作成したらエクスポートフィルター定義をsupport@kiwisyslog.comまでe-mailで送ってください。

Action - Display (アクション - 表示)

メッセージを画面に表示します。
メッセージ送信先として10個の仮想画面の一つを選びます。メインSyslog daemon表示のドロップダウンリストからどの画面を表示するかを選びます。

Action - Log to file (アクション - ファイル記録)

Action - Log to file (アクション - ファイル記録)

選択したファイルフォーマットに従いメッセージを指定のファイルに記録する。

Log file name フィールドにログ記録の完全なパス名とファイル名を入力、または[...]ボタンでファイルをブラウズする。

デフォルトログファイル名は"SyslogCatchAll.txt"。
デフォルトパスは"InstallPath¥Logs¥"、InstallPath はKiwi Syslog Daemonをインストールしたフォルダーです。

AutoSplit values (オートスプリット値)

AutoSplit値を使えば受信メッセージを複数ログファイルに分ける時、フィルターやアクションの必要がなくなります。

AutoSplit値を使うには、カーソルを挿入したい新しい値に置き、Insert AutoSplit valueリンクをクリックしメニューから選びます。新しい変数は現在のカーソルの位置に置き換えられます。

メッセージを受信すると変数はメッセージの値に置き換えられます。例えば、%PriLevAA はメッセージのプライオリティレベルに置き換えられます。

AutoSplit値は結果が正しいファイル名になるのであれば、パスやログファイル名のどこでも使用可能です。

例：

メッセージを日付でファイルに分割する。

C:¥Logs¥MyLogFile¥DateD2.txt

%DateD2 は現在の日付に置き換わります。23日であれば次のファイルに記録されます：

C:¥Logs¥MyLogFile23.txt

パスやファイル名で任意の数のAutoSplit values を使えます。

プライオリティレベルと現在の日付を基本にメッセージを分けるには：

C:¥Logs¥%PriLevAA¥MyLogFile-%DateISO.txt

パスやファイル名は次のようになります：

C:¥Logs¥Debug¥MyLogFile-2002-04-09.txt

あるいは送信ホストを基本にメッセージを分け、次に各ホストをプライオリティレベルに分けます。

C:¥Logs¥%HostName.%HostDomain¥MyLogFile-%PriLevAA.txt

その結果パスやファイル名は次のようになります：

C:¥Logs¥myhost.mycompany.com¥MyLogFile-Debug.txt

Run Script アクションを使えば、任意のVarCustom あるいはVarGlobalフィールドをautosplitアイテムとして使用できます。

%variable 名を思い出すより、メニューアイテムを使って値を挿入してください。

現在可能なAutoSplit 値の全リストです：

Date 値

メニュー名: ISO Date (YYYY-MM-DD)

パラメータ: %DateISO

説明: 国際日付形式 YYYY-MM-DD。先頭0付き、常に10文字。

例: 2002-10-15

メニュー名: Year (YYYY)

パラメータ: %DateY4

説明: 4桁の年、常に4文字。

例: 2002

メニュー名: Year (YY)

パラメータ: %DateY2

説明: 2桁の年、常に2文字です

例: 02

メニュー名: 先頭0つきMonth (MM)

パラメータ: %DateM2

説明: 2桁の月、常に2文字。

例: 12

メニュー名: 英語のMonth (MMM)

パラメータ: %DateM3

説明: 英語3文字の月、常に3文字。先頭は大文字。(Jan, Feb, Mar, Apr...)

例: Nov

メニュー名: 先頭0つきDate (DD)

パラメータ: %DateD2

説明: 2桁の日、常に2文字。

例: 05

メニュー名: 英語のDay (DDD)
パラメータ: %DateD3
説明: 英語3文字の曜日、常に3文字。先頭は大文字。(Sun, Mon, Tue...)
例: Fri

Time 値

メニュー名: 先頭0つきHour (HH)
パラメータ: %TimeHH
説明: 2桁の時間、常に2文字。24時間表示。 3 p.m. = 15
例: 14

メニュー名: 先頭0つきMinute (MM)
パラメータ: %TimeMM
説明: 2桁の分、常に2文字。
例: 59

メニュー名: AM/PM indicator (AM または PM)
パラメータ: "%TimeAMPM
説明: 2文字の時刻、常に2文字。00:00 ~ 11:59 = AM. 12:00 ~ 23:59 = PM
例: AM

Priority 値

メニュー名: Level (アルファベット)
パラメータ: %PriLevAA
説明: 言葉でのプライオリティレベル。Debug, Notice, Info等...
例: Critical

メニュー名: Facility (アルファベット)
パラメータ: %PriFacAA
説明: メッセージプライオリティfacility語。Local1, News, Cron...
例: User

メニュー名: Level (2桁数字)
パラメータ: %PriLev00
説明: 2桁のメッセージプライオリティレベル。00~07
例: 05

メニュー名: Facility (2桁数字)
パラメータ: %PriFac00
説明: 2桁のメッセージプライオリティfacility。00~23
例: 23

メニュー名: Priority (3桁数字)
パラメータ: %Pri000
説明: 3桁のメッセージプライオリティ。000~191
例: 016

IP Address 値 (登録正規版のみ)

メニュー名: IP Address (4桁8進数, ゼロパディング)
パラメータ: %IPAdd4
説明: メッセージ送信デバイスのIPアドレス。ゼロパディング。常に15文字。
例: 192.168.001.024

メニュー名: IP Address (3桁8進数, ゼロパディング)
パラメータ: %IPAdd3
説明: メッセージ送信デバイスのIPアドレスの先頭3オクテット。ゼロパディング。常に11文字。
例: 192.168.001

メニュー名: IP Address (2桁8進数, ゼロパディング)
パラメータ: %IPAdd2
説明: メッセージ送信デバイスのIPアドレスの先頭2オクテット。ゼロパディング。常に7文字。
例: 203.056

Host name 値 (登録正規版のみ)

メニュー名: Hostname (ドメイン無し)
パラメータ: %HostName
説明: メッセージ送信デバイスのホスト名。ドメイン名は含まない。
例: sales-router

メニュー名: Domain (ホスト無し)
パラメータ: %HostDomain
説明: メッセージ送信デバイスのドメイン名。ホスト名は含まない。
例: mycompany.co.nz

メニュー名: Reversed domain (ホスト無し)
パラメータ: %HostDomRev
説明: メッセージ送信デバイスのドメイン名の逆順序。ホスト名は含まない。
例: nz.co.mycompany

Message Text - WELF フォーマット (登録正規版のみ)

WELF フォーマットはWebTrends拡張ロギングフォーマットです。このフォーマットはGNATBox, SonicWall, CyberWallPlus, NetScreen 等を含む多くのファイアーウォールで使われています。メッセージテキストの各フィールドにはタグがプレフィックスされています。例えばfw= ファイアーウォール名称、src= パケット送信元 などです。もっと多くのフィールドが後でAutoSplitリストに追加されます。追加が必要な場合 support@kiwisyslog.comまで連絡してください。

メニュー名: Firewall name (WELFフォーマット)
パラメータ: %TextFW
説明: メッセージを生成したファイアーウォール名
例: protector

メニュー名: Source address (WELFフォーマット)
パラメータ: %TextSrc
説明: ファイアーウォールでロギングされたパケットの送信元IPアドレス。ゼロパディング無し。
例: 192.168.1.6

メニュー名: Destination address (WELFフォーマット)
パラメータ: %TextDst
説明: ファイアーウォールでロギングされたパケットの宛先IPアドレス。ゼロパディング無し。
例: 203.57.12.1

メニュー名: Protocol (WELFフォーマット)
パラメータ: %TextProto
説明: ファイアーウォールでロギングされたパケットのプロトコル。
例: http

Input Source 値 (登録正規版のみ)

メニュー名: Input Source (UDP/TCP/SNMP)
パラメータ: %InpSrc
説明: メッセージの入力ID(メッセージ待ち方法)
例: UDP

Custom/Global script フィールド (登録正規版のみ)

メニュー名: VarCustom01 ~ VarCustom16
パラメータ: %VarCustom01 ~ %VarCustom16
説明: Run Script アクションで変更される16カスタムフィールドがあります。これらのフィールドがスクリプトで変更されない時は、空白になります。空白autosplit値は不正なファイル名の結果であるかもしれません。新しいメッセージが到着するとカスタムフィールドの値はクリアされます。それらは現在のメッセージについてののみ正しい値です。単一メッセージ以上の値をストアするにはVarGlobal フィールドを使ってください。
例: スクリプトが生成する任意の値

メニュー名: VarGlobal01 ~ VarGlobal16
パラメータ: %VarGlobal01 ~ %VarGlobal16
説明: Run Script アクションで変更される16グローバルフィールドがあります。これらのフィールドがスクリプトで変更されない時は、空白になります。空白autosplit値は不正なファイル名の結果であるかもしれません。グローバルフィールドにはメッセージ間の値が保たれます。
例: スクリプトが生成する任意の値

ログファイルフォーマット

指定のファイルにロギングするフィールドとメッセージを変更する種々の標準フォーマットがドロップダウンリストにあります。使いたいファイルフォーマットが含まれていない場合自分のフォーマットを作成できます。Formatsオプションの下でのadd a new Custom File Formatで希望するフィールドを設定します。次にLog to file アクションでこの新しいフィールドフォーマットをドロップダウンリストから選びます (カスタムフォーマットはリストの最後に表示されます)。

次の標準ファイルフォーマットはプログラムに含まれます :

Kiwi format ISO yyyy-mm-dd (タブ区切り)

フォーマット : DateTime (YYYY-MM-DD HH:MM:SS) [TAB] Priority (Facility.Level) [TAB] Host name [TAB] Message text

例: 2002-07-22 12:34:56 [TAB] Local5.Debug [TAB] firewall-inside [TAB] prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64

Kiwi format ISO UTC yyyy-mm-dd (タブ区切り)

フォーマット : UTC DateTime (YYYY-MM-DD HH:MM:SS) [TAB] Priority (Facility.Level) [TAB] Host name [TAB] Message text

例: 2002-07-22 12:34:56 [TAB] Local5.Debug [TAB] firewall-inside [TAB] prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64

Kiwi format mm-dd-yyyy (タブ区切り)

フォーマット : Date (MM-DD-YYYY) [TAB] Time (HH:MM:SS) [TAB] Priority (Facility.Level) [TAB] Host name [TAB] Message text

例: 07-22-2002 [TAB] 12:34:56 [TAB] Local5.Debug [TAB] firewall-inside [TAB] prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64

Kiwi format dd-mm-yyyy (タブ区切り)

フォーマット : Date (DD-MM-YYYY) [TAB] Time (HH:MM:SS) [TAB] Priority (Facility.Level) [TAB] Host name [TAB] Message text

例: 22-07-2002 [TAB] 12:34:56 [TAB] Local5.Debug [TAB] firewall-inside [TAB] prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64

Kiwi format UTC mm-dd-yyyy (タブ区切り)

フォーマット : UTC Date (MM-DD-YYYY) [TAB] UTC Time (HH:MM:SS) [TAB] Priority (Facility.Level) [TAB] Host name [TAB] Message text

例: 07-22-2002 [TAB] 12:34:56 [TAB] Local5.Debug [TAB] firewall-inside [TAB] prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64

Kiwi format UTC dd-mm-yyyy (タブ区切り)

フォーマット : UTC Date (DD-MM-YYYY) [TAB] UTC Time (HH:MM:SS) [TAB] Priority (Facility.Level) [TAB] Host name [TAB] Message text

例: 22-07-2002 [TAB] 12:34:56 [TAB] Local5.Debug [TAB] firewall-inside [TAB] prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64

Comma Separated Values yyyy-mm-dd (CSV)

フォーマット : Format: DateTime (YYYY-MM-DD HH:MM:SS),Priority (Facility.Level),Host name,Message text

例: 2002-07-22 12:34:56,Local5.Debug,firewall-inside,"prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64"

Comma Separated Values UTC yyyy-mm-dd (CSV)

フォーマット : UTC DateTime (YYYY-MM-DD HH:MM:SS),Priority (Facility.Level),Host name,Message text

例: 2002-07-22 12:34:56,Local5.Debug,firewall-inside,"prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64"

BSD Unix syslog フォーマット

フォーマット: DateTime (Mmm DD HH:MM:SS) [SPACE] Host name [SPACE] Message text (PID tag followed by message content)

例: Jul 22 12:34:56 [SPACE] firewall-inside [SPACE] amd[308]: key sys: No value component in "rw,intr"

XML タグ付きフォーマット

フォーマット: Format: <Message><DateTime> DateTime (YYYY-MM-DD HH:MM:SS) </DateTime><Priority> Priority (Facility.Level) </Priority><Source_Host> Host name </Source_Host><MessageText> Message Text </MessageText></Message>

例: <Message><DateTime>2002-07-23 21:53:35</DateTime><Priority>Local7.Debug</Priority><Source_Host>firewall-inside</Source_Host><MessageText> prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64</MessageText></Message>

RnRsoft ReportGen フォーマット

フォーマット: Format: rnrsoft [TAB] Date (YYYY-MM-DD) [TAB] Time (HH:MM:SS) [TAB] Host name [TAB] Level (numeric 0-7) [TAB] Message text

例: rnrsoft [TAB] 2002-07-23 [TAB] 22:02:51 [TAB] firewall-inside [TAB] 7 [TAB] prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64

ReportGen for SonicWall, PIX, GNATbox and Netscreen に関しては: www.jtc-i.co.jp

WebTrends フォーマット

フォーマット: Format: WTsyslog[2001-11-12 12:44:45 ip=192.168.168.1 pri=6] <134>id=firewall time="2001-11-15 08:43:42" fw=192.168.1.1 pri=6 src=192.168.1.34 proto=http

例: WTsyslog[2001-11-12 12:44:45 ip=192.168.168.1 pri=6] <134>id=firewall time="2001-11-15 08:43:42" fw=192.168.1.1 pri=6 src=192.168.1.34 proto=http

Webtrends firewall suite に関しては: <http://www.netiq.com/products/fwr>

Cisco PIX PFSS format (ローログ)

フォーマット: Format: <Priority value (0-191)>Message text

例: <191>Built outbound TCP connection 12004 for faddr grc.com/80 gaddr 192.168.2.2/4120 laddr 192.168.1.1/4391

3Com 3CDeamon format (BSD スペース区切り)

フォーマット: Format: DateTime (Mmm DD HH:MM:SS) [SPACE] Host address [SPACE] Message text

例: Jul 22 12:34:56 [SPACE] 192.168.1.1 [SPACE] key sys: No value component in "rw,intr"

Raw - Message text only (優先値なし)

フォーマット: Format: Message text only

例: Built outbound TCP connection 12004 for faddr grc.com/80 gaddr 192.168.2.2/4120 laddr 192.168.1.1/4391

Sawmill format ISO yyyy-mm-dd (タブ区切り)

フォーマット: DateTime (YYYY-MM-DD HH:MM:SS) [TAB] Priority (Facility.Level) [TAB] Host name [TAB] Message text

例: 2002-07-22 12:34:56 [TAB] Local5.Debug [TAB] firewall-inside [TAB] prot=UDP port=53 dst=203.25.36.47 src=192.168.1.2 bytes=64

Sawmill ログ処理ソフトウェアに関しては: www.sawmill.net

Action - Forward to another host (アクション - 他のホストへ転送)

他のSyslogホストに受信メッセージをフォワーディングします。

送信元ホストIPアドレスはメッセージテキストに含まれますので本来の送信元がわかります。

メッセージをフォワードするホストのホスト名かIPアドレスを**Hostname or IP address** フィールドに入力してください。

複数ホストにメッセージフォワーディング出来ます。

各ホスト名やIPアドレスはカンマで区切ります。

例: l.e. Myhost.com, SecondHost.net, 203.75.21.3

フォワーディングメッセージで異なるFacilityやLevelを使うには**New facility** と**New level** リストから選びます。

[Test] ボタンで指定ホストへの送信テストが出来ます。

Action - Play a sound (アクション - 音を鳴らす)

登録正規版のみで有効

フィルターセットにメッセージが合致した場合、指定の音を鳴らすことが出来ます。

Sound file name フィールドに音声ファイル名を指定するか"..." browseボタンでファイルを選んでください。

¥sounds フォルダにサンプル音声ファイルがあります。[Test] ボタンで音を聞いてください。

Action - Run external program (アクション - 外部プログラム実行)

登録正規版のみで有効

フィルターセットにメッセージが合致した場合、外部プログラムを実行できます。コマンドライン引数としてメッセージとSyslog統計の詳細を外部プログラムに渡すことが出来ます。**Program file name** フィールドに外部プログラム名を入力するか、"..." browseボタンで選んでください。

Command line options フィールドでプログラムに渡すコマンドラインオプションを指定してください。外部プログラムへ渡すメッセージの詳細やSyslog統計のシンタックスは? ボタンで見ることが出来ます。

Insert message content or counter

外部プログラムにプログラム変数、カウンター、スクリプトフィールド、統計を渡すにはthe Insert message content or counter link をクリックしポップアップメニューからオプションを選びます。値の詳細はここで見る事が出来ます。

変数をポップアップメニューから選べます。変数はプログラムの実行前に現在値に置き換えられます。たとえば%MsgText は現在のSyslogメッセージに置き換えられます。カーソルをcommand line options textライン に置きハイパーリンクをクリックします。ポップアップメニューが表示されますので変数を選びます。

command line オプション例:

"555-1234", "Syslog - A link has gone down - %MsgAll"

または: "Warning, message received from host %MsgHost at %MsgTime"!

Action - E-mail message (アクション - E-mailメッセージ送信)

登録正規版のみで有効

フィルター設定に合致したSyslogメッセージを受信したらe-mailメッセージを送信する。

受信したSyslogメッセージの詳細やSyslog統計をe-mail件名やメッセージ本体に含むことが出来ます。Syslogからe-mail へのコンバータとして使うことが出来ます。

最初にe-mailオプションでSMTPサーバーオプションの設定が必要です。

E-mail recipient フィールドで受信者アドレスを指定します。複数アドレスの指定が可能であり、各アドレスはカンマで区切ります。

E-mail subject フィールドで件名を指定できます（1行のみ）。件名の送信文字数は**Max subject length** オプションで指定できます。

E-mail message フィールドでメッセージを指定できます（複数行可能）もしこのメッセージをポケットベルに送るのであればメッセージ本体は使うべきではありません。この場合ブランクにできます。多くのポケットベルシステムは限られたスペースしかなく、メッセージ件名のみを使うべきです。メッセージ本体の送信データ文字数を制限するために**Max message length** オプションを使えます。メッセージ本体で変数%MsgText を使っており大きなSyslogメッセージを受信すれば、e-mailで送信するには大きすぎます。メッセージ本体を管理可能な長さに制限することが可能です。

Test ボタンは指定された受信者にテストe-mailを送信します。テストメッセージ内容は**Test Setup** ボタンで変更できます。

Insert message content or counter

プログラム変数、カウンター、スクリプトフィールド、統計をメッセージや件名に渡すにはInsert message content またはcounter link をクリックしポップアップメニューからオプションを選びます。値の詳細はここで見る事が出来ます。

ポップアップメニューから変数を選びます。変数はメッセージの送信前に現在値に置き換えられます。例えば%MsgText は現在のSyslogメッセージテキストに置き換えられます。カーソルを件名やメッセージテキスト行に置き、hyperlink をクリックします。ポップアップメニューが表示されますので変数を選びます。

例 subject欄: Syslog Alert from %MsgHost

例 メッセージ本体欄:

Message from Host %MsgHost at %MsgTime on %MsgDate Message: %MsgText

Kiwi Syslog Daemon をSyslogのe-mailコンバータとして使うにはメッセージ本体テキストの%MsgAll キーワードで受信Syslogメッセージ情報をe-mailメッセージに渡します。

大量のメッセージを受け取る時、e-mailサーバーで渋滞が発生することに注意してください。E-mailバッファは最大1,000です。大量のSyslogメッセージを一度に受信しメールサーバーがビジーのとき助かります。

E-mail は送信前短時間キューに入ります。メッセージ送信の都度メールサーバーに接続するより効率的です。キューに入ったメッセージはバッチ送信されます。

メッセージの <013><010> を展開

<013> や <010>に置き換えられたキャリッジリターンやラインフィードを展開します。replace non printable characters with ASCII value オプションが設定されるとSyslogメッセージのCR、LFは置き換えられます。テキストを読み易くしますのでe-mailでフォワードする時展開するのは効果的です。

Insert message content or counter (メッセージ内容やカウンターの挿入)

変数をポップアップメニューから選びます。変数はメッセージ送信前に現在値に置き換えられます。たとえば%MsgText は現在のSyslogメッセージに置き換えられます。ポップアップメニュー項目をクリックすると現在のカーソル位置が%variable になります。

subject 欄の例: Syslog Alert from %MsgHost

変数とファンクションリスト

メニュー名: All of the message

パラメータ: %MsgAll

説明: メッセージ全体が画面と同様に表示されます。時刻、日付、プライオリティ、メッセージテキストがスペースで区切られます。

例: 2002-10-10 11:28:04 Local7.Debug host.company.com This is a test message

メニュー名: Date

パラメータ: %MsgDate

説明: メッセージ受信日。フォーマットはYYYY-MM-DD

例: 2002-02-18

メニュー名: Time

パラメータ: %MsgTime

説明: メッセージ受信時刻。フォーマットはHH:MM:SS

例: 22:30:16

メニュー名: Facility

パラメータ: %MsgFacility

説明: メッセージのfacility。テキストフォーマット。

例: Local7, Mail

メニュー名: Level

パラメータ: %MsgLevel

説明: メッセージのlevel。テキストフォーマット。

例: Debug, Info

メニュー名: Host address of sender

パラメータ: %MsgHost

説明: 送信デバイスのホストIPアドレス

例: 192.168.1.1

メニュー名: The message text

パラメータ: %MsgText

説明: syslogメッセージのメッセージテキスト

例: This is a test message

メニュー名: Alarm min msg threshold

パラメータ: %MsgAlarmMin

説明: 警告の最小メッセージ数アラートの閾値レベル設定

例: 100 (1時間あたりの最小メッセージ)

メニュー名: Alarm max msg threshold

パラメータ: %MsgAlarmMax

説明: 警告の最大メッセージ数アラートの閾値レベル設定

例: 5000 (1時間あたりの最大メッセージ)

メニュー名: Alarm disk space threshold

パラメータ: %MsgAlarmDisk

説明: MB単位のディスク残量の最小閾値レベル設定

例: 90 (MB)

メニュー名: Message count this hour

パラメータ: %MsgThisHour

説明: この時間での受信メッセージ数

例: 254

メニュー名: Message count last hour

パラメータ: %MsgLastHour

説明: 直前1時間の受信メッセージ数

例: 254

Custom/Global/Statistics フィールド (登録正規版でのみ有効)

メニュー名: VarCustom01 ~ VarCustom16

パラメータ: %VarCustom01 ~ %VarCustom16

説明: Run Script アクションで変更できる16カスタムフィールドがあります。これらのフィールドがスクリプトで変更されない時は、ブランクになります。ブランクautosplit値は不正なファイル名になる可能性があります。新しいメッセージが到着するとカスタムフィールドの値はクリアされます。それらは現在のメッセージについてのみ正しい値です。単一メッセージ以上の値をストアするにはVarGlobal フィールドを使ってください

例: スクリプトが生成する任意の値

メニュー名: VarGlobal01 ~ VarGlobal16

パラメータ: %VarGlobal01 ~ %VarGlobal16

説明: Run Script アクションで変更される16グローバルフィールドがあります。これらのフィールドがスクリプトで変更されない時は、ブランクになります。ブランクautosplit値は不正なファイル名になる可能性があります。グローバルフィールドは複数メッセージ間でその値が保たれます。

例: スクリプトが生成する任意の値

メニュー名: VarStats01 ~ VarStats16

パラメータ: %VarStats01 ~ %VarStats16

説明: Run Script アクションで変更される16スタティクスフィールドがあります。スタティクスフィールドには複数メッセージ間でその値が変わりません。スタティクスに伴う名前を変更でき、その初期値は設定ウィンドウのScript optionsから決まります。カスタムスタティクス値はスタティクス表示やデイリー統計e-mailで見ることが出来ます。

例: スクリプトが生成する任意の値

Action - Send Syslog message (アクション – Syslogメッセージ送信)

登録正規版でのみ有効

メッセージを受信し、フィルターを通過したSyslogメッセージは指定したホストに送られます。

受信メッセージの詳細とSyslogスタティクスが送信Syslogメッセージに含まれます。

選択したSyslogメッセージを他のホストに追加情報とともにあるいは自分自身のテキストを追加してリレーできます。

Hostname or IP address フィールドに宛先IPアドレス又はホスト名を指定します。

ホスト名文脈を見るには**Hostname or IP address** フィールドの横の ? ボタンを押します。

複数のホストがフォワードメッセージを受信できます。

各ホスト名またはIPアドレスはカンマで区切ります。

例. Myhost.com, SecondHost.net, 203.75.21.3

フォワードするメッセージの新しいfacilityとlevelを指定するには、**New facility** と **New level** リストから選択します (デフォルトは受信したfacilityとlevelですが変更することが出来ます)。

指定されたアドレスにSyslogメッセージを送信するため**Test** ボタンを押してください。

Insert message content or counter

新しいsyslogメッセージにプログラム変数、カウンター、スクリプトフィールドを渡すには、Insert message content or counter link をクリックしポップアップメニューからオプションを選びます。値の詳細はそこで見ることが出来ます。

ポップアップメニューから変数を選ぶことが出来ます。メッセージが送信される前に変数は現在の値で置き換えられます。例えば、%MsgText は現在のsyslogメッセージテキストで置き換えられます。カーソルをsyslogメッセージテキスト行に置き、ハイパーリンクをクリックします。ポップアップメニューが表示されますので変数を選びます。

メッセージテキストフィールド例: Syslog Alert from %MsgHost

または: Message from Host %MsgHost at %MsgTime on %MsgDate Message: %MsgText

Action - Log to ODBC database (アクション – ODBCデータベース記録)

Action - Log to ODBC database (アクション – ODBCデータベース記録)

登録正規版でのみ有効

メッセージをODBC Data Source Name (DSN)で指定したテーブルに記録します。

ODBC DSN connect string

DSN connect string field にデータベースDSN、ユーザーID、パスワードを入力します。

あるいは、browseボタンでマシンに構成されているODBC DSNから選びます。

DSN connect string は次の要素で構成されます:

Data Source Name

システムで構成されたODBC DSNを参照します。**Browse** ボタンを押してシステムのODBC Data Source Names リストから選びます。

UID=UserID; データベースがパスワードで保護されている時に限り必要です。データベースのユーザー名を入力します。

PWD=Password; データベースがパスワードで保護されている時に限り必要です。データベースのパスワードを入力します。

例. DSN=Syslogd;UID=Admin;PWD=Password;

各要素はセミコロンで区切ります。UserID や Password が不要の時、接続文字列はDSNのみで構成されます。

デフォルトDSN 接続文字列は DSN=Syslogdです;

多くの場合,DSN名の前にテキストDSN=を指定しなければなりません。

Database Table name

正しいデータベーステーブル名を指定します。指定したテーブルは選択したデータベースフォーマットに合致するフィールド名を含まなければなりません。フィールドサイズが短すぎると、データがデータベースに記録される時、打ち切られます。

デフォルトテーブル名はSyslogdです。

ODBCデータベースのログアクションをテストするにはTest ボタンを押します。メッセージがアクションの成功・不成功の詳細を表示します。

Database type/field format

デフォルトデータベースタイプリストから選ぶか、**Edit custom format** ボタンをクリックし自分のフォーマットを生成します。

デフォルトデータベースタイプ：

- Access
- SQL
- MySQL
- Oracle

デフォルトデータベーステーブルデザイン：

Microsoft Access database

Field	Name	Type	Size
Date	MSGDATE	Date	10
Time	MSGTIME	Time	8
Priority	MSGPRIORITY	Text	30
Hostname	MSGHOSTNAME	Text	255
Message text	MSGTEXT	Memo	1024

SQL database (Microsoft SQL とgeneric SQL)

Field	Name	Type	Size
Date	MSGDATE	DateTime	10
Time	MSGTIME	DateTime	8
Priority	MSGPRIORITY	VarChar	30
Hostname	MSGHOSTNAME	VarChar	255
Message text	MSGTEXT	VarChar	1024

MySQL database

Field	Name	Type	Size
Date	MSGDATE	Date	10
Time	MSGTIME	Time	8
Priority	MSGPRIORITY	VarChar	30
Hostname	MSGHOSTNAME	VarChar	255
Message text	MSGTEXT	Text	1024

Oracle database

Field	Name	Type	Size
Date	MSGDATE	Date	10
Time	MSGTIME	Time	8
Priority	MSGPRIORITY	VarChar2	30
Hostname	MSGHOSTNAME	VarChar2	255
Message text	MSGTEXT	VarChar2	1024

注：

ODBC データソースに記録するにはMDAC (Microsoft Data Access Components) ドライバーが必要です。バージョン2.50以上をお奨めします。このパッケージは次のURLからダウンロードできます：

<http://www.microsoft.com/data/>

データベースが他のプロセスで排他的にオープン中Kiwi Syslog Daemon はデータベースへの新しいレコードの記録ができません。

ODBC データベースのいくつかの例を下記からダウンロードできます。
http://www.kiwitools.com/downloads/Syslog_ODBC_Samples.zip

Zipファイルには情報とサンプルデータベースが含まれており、自分のシステムでODBCロギング設定のガイドになります。

ODBC Control Panel ボタン

Control Panel ODBC applet を開きますのでSystem DSN の構築や可能なODBCオプションのチェックが可能です。

Create table ボタン

DSNで参照されたデータベースに指定されたテーブルを作成します。既存のテーブルは削除され内容が失われます。選んだデータベースタイプで指定されたフィールド名とタイプの新しいテーブルが作成されます。すべてうまく行き、新しいテーブルが作成されると確認メッセージが表示されます。テーブル作成で問題があると、メッセージが表示されますので問題の訂正が出来ます。

Query table ボタン

指定されたテーブルの最終5エンタリをリトリブします。ダイナミックアクセスができるようDSNタイプを指定します。フォワードのみのデータベースはデータベースにMove previous コマンドが出されていますので正しく読めません。

得られたデータはノートパッドで読めます。最後の5フィールドのテーブルストラクチャとデータから情報を得ることが出来ます。

クエリーで得られた情報の例：

Field name	Type	Size	Data
MsgDate	adDBTimeStamp	16	28/07/2002
MsgTime	adDBTimeStamp	16	14:45:16
MsgPriority	adVarChar	30	Local7.Debug
MsgHostname	adVarChar	255	host.company.com
MsgText	adLongVarChar	1024	This is a test message from Kiwi Syslog Daemon

Edit custom format ボタン

データベースタイプのドロップダウンリストからカスタムフォーマットを選んで、このボタンを押すとカスタムフォーマットを選択できます。カスタムフォーマットを選ばない場合、Custom DB formats オプションで新しいフォーマットを生成できます。

Show SQL commands ボタン

選択したテーブルにデータを生成し挿入するSQLコマンドを生成します。生成されるコマンドはどのデータベースが選ばれたかによります。これらのコマンドを使ってデータベースアプリケーションでデータベーステーブルスキーマを生成できます。もしくは、Create table ボタンでテーブルを生成することも出来ます。

生成されたSQLコマンドの例：

Database type: Access database
Database name: Kiwi Access format ISO yyyy-mm-dd

テーブル生成のSQLコマンド：

```
CREATE TABLE Syslogd (MsgDate DATE,MsgTime TIME,MsgPriority TEXT(30),MsgHostname TEXT(255),MsgText MEMO)
```

SQL INSERT コマンド例：

```
INSERT INTO Syslogd (MsgDate,MsgTime,MsgPriority,MsgHostname,MsgText) VALUES ('2002-07-28','14:58:04','Local7.Debug','host.company.com','This is a test message from Kiwi Syslog Daemon')
```

Connection Inactivity timeout

最終メッセージの送信からどのくらいデータベース接続をオープンするかをコントロールします。接続のオープンとクローズはデータベースのロギングにおいて最も遅い処理です。そのためデータのロギング中は継続してオープンにします。タイムアウト前にログデータが無い場合、データベース接続はクローズされます。新しいメッセージが到着すると接続がオープンされます。

Run debug command button

データベースへのロギングの問題はこのボタンで診断します。データベースで実行するSQLコマンドを入力する別のウィンドウが開かれます。コマンドが失敗すると結果のフィールドに詳細なエラーメッセージが表示されます。デフォルトでは選択されたデータベースタイプの現在のINSERT文がqueryフィールドに表示されます。この文を変更し文のバリエーションをテストします。

このオプションはデータベースでqueryを実行するのには使われません。エラー情報だけが結果のフィールドに返されます。たとえばSelect From statement を実行し結果を得ることは出来ません。分かるのは文が正しく実行されたか否かだけです。

Show SQL commands でデバッグでの正しい文脈が得られます。

Custom fields

Custom fields はスクリプト実行アクションで使います。パーススクリプトを作成すると、syslog メッセージテキストをいくつかのサブフィールドに分離できます。値は16のカスタムフィールドにアサインされデータベースに記録されます。各デバイスメーカーは異なるフォーマットで syslogメッセージを生成しますので、メッセージテキストを別々のフィールドに分離する一般的なパーサーを作成するのは不可能です。メッセージテキストをパースし、カスタムデータベースフィールドに置くためのカスタムスクリプトを作成しなければなりません。パーススクリプトの例が¥Scripts サブフォルダーにあります。

To configure an ODBC database DSN (ODBCデータベースDSNの構築)

設定 | コントロールパネル | ODBC Data Sources (32bit)アプレット を開きます。

System DSN タブの**Add** ボタンをクリックします (サービスとしてKiwi Syslog Daemon を実行する場合は、System DSN の生成が必要です)。

使用するドライバーを選びます (例のデータベースでは、Microsoft Access driverです)

ユニークなData Source Nameをピックし1番上の欄に入力します (**Syslogd** からスタートすると良いでしょう)。

Select ボタンをクリックし、希望のデータベースファイル名を指します。

OKをクリックしData Source Names リストにDSNが追加されているか確認します。

Log to ODBC database アクション設定で、DSN connect string フィールドにこの新しいDSN名を使います。

Problems logging when running as a Service (サービス実行中の記録の問題)

Service Manager からのODBC記録のテストで、プログラムは現在のユーザーで実行しています (通常Administrator)。

サービスがログをODBCデータベースに記録する時、デフォルトではLocal Systemユーザーとして実行します。

テストメッセージは正しく動作するが、サービスが正しく実行しない場合、Serviceログオン名をLocal System からAdministratorに変えてください。

コントロールパネル | サービスで変更できます。

プログラムをデスクトップから操作できるようボックスをチェックできます。

Action - Log to NT Event log (アクション - NT Event log記録)

Action - Log to NT Event log (アクション - NT Event log記録)

登録正規版でのみ有効

メッセージを受信し設定したフィルターに合致した時syslogメッセージをNT イベントログに書きます。

NTイベントログには5種類のログレベルがあります : Error, Warning, Information, Success および Failure

ドロップダウンリストからログレベルを選びます。メッセージはこのレベルでNTイベントログに書かれます。

ログ挿入タイプを設定

メッセージがイベントログに挿入される時は、3つの方法があります。

メッセージは次のように書かれます :

1文字挿入

%1 is replaced with:

Date – Tab – Time – Priority – Tab – Hostname – Tab – Message

タブ区切り5文字挿入

%1 Tab %2 Tab %3 Tab %4 Tab %5

%1 = Date

%2 = Time

%3 = Priority

%4 = Hostname

%5 = Message

スペース区切り5文字挿入

%1 Space %2 Space %3 Space %4 Space %5

%1 = Date

%2 = Time

%3 = Priority

%4 = Hostname

%5 = Message

Test ボタンを押してNTイベントログをテストしてください。Windows 95/98のようなNT以外のシステムではメッセージは書き込まれずエラーメッセージが表示されます。

注: デフォルトではNTイベントログビューワでNTイベントログを見るとログタイプはSystemイベントを見るように設定されています。アプリケーションイベントを見るにはNTイベントビューワのログメニューでアプリケーションをチェックしてください。

Action - Send pager or SMS message via NotePage Pro (アクション - NotePage Pro経由でポケットベルやSMSメッセージを送信)

登録正規版でのみ有効

このアクションはNotePagerProアプリケーション経由でポケットベル、SMSあるいはor e-mailメッセージを送信します。動くようにするにはまず<http://www.notepager.com>からNotePagerを購入し、インストールしてください。NotePager Pro は低価格ですが非常に強力なポケットベルとSMSゲートウェイのアプリケーションです。

NotePager Proを使用するメリット:

- グループメッセージ送信機能
- 携帯電話とポケットベル通信会社を含む複数通信会社をサポート
- SNPP, WCTP とSMTPを含むインターネットポケットベルプロトコルサポート
- スケジュールメッセージ、繰り返しメッセージ、事前プログラムメッセージのサポート

メッセージがNotePager Proに渡ると、メッセージが送信キューに入ります。NotePager Pro は周期的にキューをチェックし、指定された方法でそれらを送信します。それらはSNPP, e-mail, modem, TAPI, あるいは設定したポケットベルインターフェイスです。

"Insert message content or counter" リンクで、送信されるポケットベルメッセージに含まれる受信Syslog メッセージとSyslog 統計の詳細を見てください。

Send Page To:

ドロップダウンリストから受信者を選択します。このリストはNotePager Pro Recipients と Groupsから自動的に蓄積されます。ドロップダウンリストに名前がない場合は、NotePager Proが正しくインストールされていません。受信者1人を選択するか、受信者グループを選択します。例えば: Send to: Joe、またはSend To: All-Network-Staff.

Message From:

どんな名前での大丈夫です。NotePager Pro で設定した受信者がe-mail経由で受信する場合、指定するFrom nameが設定したデフォルトドメインの前に追加されます。例えば、NotePager Pro がデフォルトドメイン"company.com"で設定されると"Syslog"からメッセージを送信すると、Syslog@company.comからメッセージが送られたように見えます。

Message:

ポケットベルやSMSメッセージに入れるメッセージです。通常これは%MsgTextと設定します。これはオリジナルメッセージで置き換えられます。他の変数をメッセージで使うこともできます。"Insert message content or counter" ハイパーリンクをクリックして可能な変数のポップアップメニューを表示してください。Max message length オプションでメッセージ送信するデータを制限できます。変数 %MsgText をメッセージ本体で使い、大きなsyslog メッセージを受けると、ポケットベルで送信するには大きすぎます。メッセージ本体の長さを管理可能な長さに制限する必要があります。

ポケットベルが数字メッセージのみを受信するのであれば、%MsgTextの代わりにメッセージフィールドで番号を指定します。その番号は例えば、1=link up, 2=link down, 9=Router unreachable などです。

Test Button:

Test ボタンで受信者に対してテストポケットベルメッセージを送信します。その内容は**Test Setup** ボタンを押して変更します。

Insert message content or counter

変数、カウンター、スクリプトフィールド、統計をポケットベルメッセージに渡すには、Insert message content やcounter リンクをクリックしてポップアップメニューからオプションを選択します。値の詳細はここで見ることができます。

このオプションでポップアップメニューから変数を選択します。変数はメッセージが送信される前に現在値で置き換えられます。例えば、%MsgText は現在のsyslogメッセージで置き換えられます。カーソルを件名やメッセージテキストに置きハイパーリンクをクリックします。ポップアップメニューが表示されますので変数を選びます。

メッセージフィールド例:

Message from Host %MsgHost at %MsgTime on %MsgDate Message: %MsgText

Action - Send ICQ instant message (アクション - ICQインスタントメッセージ送信)

登録正規版でのみ有効

*****この機能はICQ WWWページングシステムへの変更中であり無効になっています。まもなく変更が完了します。*****

フィルターに合致したSyslogメッセージを受信すると指定したICQ番号にICQインスタントメッセージを送信します。

ICQに警告がWWPagerメッセージとして表示されます。ユーザーは読んだ後ICQ警告をクローズします。

メッセージはICQ Webベースインターフェイスで送られます。現在は無料のサービスです。ICQクライアントは<http://www.icq.com> から無料でダウンロードできます。

メッセージの配信は保証されずベストエフォートベースです。ICQはポケットベルメッセージを2秒に1回に制限されます。これより早いメッセージは失われます。

この機能を使うには標準httpでICQ Webサーバーのポート80に接続します。Proxyは問題になりません。この機能はポート80をブロックするファイアウォール経由では動作しません。宛先Webサイトアドレスは<http://www.icq.com> です。このアドレスをファイアウォールのアクセスリストに追加します。

メッセージ件名あるいは本文に受信Syslog受信メッセージやSyslog統計の詳細が含まれます。

ICQ number:

正しいICQ番号を入れてください。

From name:

わかりやすい説明です。ICQメッセージのニックネームとして表示されます。

From e-mail address:

正しい返送アドレスを入れてください。ICQメッセージのE-mail欄に示されます。

Subject:

メッセージ主題を示します。通常%MsgHost に設定します。本来のsyslogメッセージを送信したホスト名やデバイスに置き換えられます。他の変数を件名行に使えます。Insert message content or counter ハイパーリンクをクリックし、可能な変数のポップアップメニューを表示してください。Max subject length オプションは件名で送信する文字数を制限します。

Message:

ICQメッセージに表示するメッセージテキストです。通常%MsgText に設定します。本来のSyslogメッセージで置き換えられます。他の変数をメッセージ本文に使えます。Insert message content or counterハイパーリンクをクリックし、可能な変数のポップアップメニューを表示してください。

Max message length オプションは本文で送信する文字数を制限します。メッセージ本文で変数%MsgText を使うと、それより長いメッセージが到着するとICQで送れません。メッセージ本文長を管理できる長さに制限することができます。

Expand <013><010> in message

<013> と <010>で置き換えられたキャリッジリターンやラインフィードを展開します。replace non printable characters with ASCII value オプションを設定するとsyslogメッセージのCRやLF文字は置き換えられます。テキストを読み易くするためICQでフォワードされた時展開するのは有効です。

例:

下記はICQポケットベルメッセージの表示例です。

Nickname: Syslog Daemon
E-mail: syslog@company.com
Sender IP: xxx.xxx.xxx.xxx
Subject: firewall.company.com
Firewall Alert - Unauthorized login attempt: User=Administrator

TestボタンはテストICQメッセージを指定のICQ番号に送信します。メッセージ内容はTest Setupボタンで変更できます。

Insert message content or counter

ICQポケットベルメッセージにカウンター、スクリプトフィールド、統計を渡せます。Insert message content or counterリンクをクリックしポップアップメニューからオプションを選びます。値の詳細はここで見る事が出来ます。

ポップアップメニューから変数を選びます。変数はメッセージ送信前に現在値に置き換えられます。例えば %MsgText は現在のSyslogメッセージに置き換えられます。カーソルを件名かメッセージテキストに置きハイパーリンクをクリックしてください。ポップアップメニューが表示されるので変数を選びます。

subject欄の例: Syslog Alert from %MsgHost

message 欄の例:

Message from Host %MsgHost at %MsgTime on %MsgDate Message: %MsgText

Action - Send SNMP Trap (アクション - SNMPトラップ送信)

登録正規版でのみ有効

このアクションは受信Syslog メッセージがフィルターセットに一致すると、指定のIPアドレスにSNMPトラップを送信します。

File | Properties | Action を右クリック、または選択した後**Add New item**をクリックすると新しいアクションを作成することができます。

次のパラメータを**"Send SNMP trap"**オプションで使います:

Destination IP address

SNMP トラップを受信するシステムのIPアドレス

Message text

フォワードするSNMP トラップの内容。このフィールドは全ての標準メッセージ変数を含むことができ、**Insert message content or counters** リンク(**Message text** フィールドのすぐ上)をクリックして選択します。

Agent IP address

SNMP トラップ送信元として表示されるIPアドレス。デフォルトでは"The original sender"に設定されるが "From this machine" (つまりKiwi Syslog Daemonを実行するマシンアドレス)として設定することもできます。

Generic type

送信されるトラップタイプを示す 0 ~ 6の値。version 1 トラップのみ有効です。

値は:

- 0 コールドスタート
- 1 ウォームスタート
- 2 リンクダウン
- 3 リンクアップ
- 4 認証失敗
- 5 EGP ネイバース

6 Enterprise Specific

ドロップダウンメニューから選択できます。

Version

Kiwi Syslog DaemonからSNMPトラップを受信するシステムがサポートするSNMPバージョン（v1あるいはv2）。

Enterprise OID

SNMP トラップのMIB エンタープライズを表す値(たとえば1.3.6.1.x.x.x.x)。バージョン1トラップ専用フィールド。バージョン2トラップのエンタープライズ値はメッセージの2番目の変数の値です。

Generic Type を6に設定すると、エンタープライズタイプトラップです。この場合特定のトラップ値を考慮しなければなりません。

Variable OID

バージョン2 SNMP トラップのMIB変数を表す値 (たとえば1.3.6.1.x.x.x.x)。

Community

トラップメッセージのパスワードのようなものです。通常この値は"public", "private" または "monitor"に設定されます。

Specific type

トラップ送信の原因を示します。バージョン2 トラップでは、特定のトラップ(またはsyslog メッセージ)を送信するデバイスのために定義されたMIBに固有の条件。

Remote port

SNMPトラップを送信するポート。 デフォルトは162。

この設定を変更すると、SNMPトラップ受信デバイスのポートも同じ番号にします。

Action - Run Script (アクション – スクリプト実行)

登録正規版でのみ有効

(フリーウェア版はアクションのテストだけが可能です)

このアクションは指定のスクリプトを実行し現在のメッセージのフィルターや解析ができます。

スクリプトの作成と使用の手順が説明されています。

スクリプトファイルの規則

スクリプトは関数Main()を含まなければなりません。パラメータは関数にわかりませんが成功したことを示すOKを返します。OK以外が返された場合はエラーの発生を示しエラーログにエントリーが残ります。スクリプト関数から返された値は後の診断用にエラーログに入ります。

例:

```
Function Main()
```

```
' Your code goes here
```

```
' Set the return value
```

```
Main = "OK"
```

```
End Function
```

スクリプト変数の値はFieldオブジェクトからアクセスできます。

Script file name

スクリプトファイルはVBスクリプトやJスクリプトを含む標準テキストファイルです。ファイルの拡張子は任意ですがデフォルトはノートパッドで編集し易いように.txtを使います。

Script description

この欄には任意の記述文が含まれます。スクリプトの機能を説明する目的で使われます。

Script Language

現在2つのスクリプト言語がサポートされています:

VBスクリプト - MS Word と Excel で使われるVisual Basic や VBA (Visual Basic for Applications) の一種です。易しく豊富な機能があります

Jスクリプト - Webで使われるJavaスクリプトの一種です。Javaスクリプトになれているなら選択してください。

どちらの言語も似た機能と性能です。選択は好みによります。

PerlやTCLなどのスクリプト言語は後日追加します。興味がありましたらsupport@kiwisyslog.com に連絡してください。

VBスクリプトに関しては:

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/script56/html/vtoriVBScript.asp>

Jスクリプトに関しては:

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/script56/html/js56jsoriJScript.asp>

Edit script ボタン

ノートパッドでスクリプトファイルを開き参照や変更が出来ます。コードを変更したら保存してください。Testボタンでテストできます。

Test ボタン

指定のスクリプトを実行します。スクリプトはファンクション名Main()を含まなければなりません。Syslogからコールされる唯一のファンクションです。Main()からOKが返されるとスクリプトは成功したことになります。

エラーが起こるとメッセージボックスにエラーの説明とその行番号が表示されます。スクリプト実行が成功しshow test results ボタンがチェックされていると実行前と後の変数が表示されます。スクリプトにより変数が変化したことがわかります。

Properties ウィンドウからスクリプトをテストすると(Test ボタンを押す) キャッシュに保存されません。各スクリプトは実行前に新しくロードされます。

Show test results オプション

スクリプトが正しく実行されshow test results オプションがチェックされていると実行前と後の変数が表示されます。スクリプトにより変数が変化したことがわかります。

Script file caching

通常の実行ではスクリプトファイルがディスクから読まれるとキャッシュに入ります。プログラム実行速度が上がり余分なディスクアクセスが減ります。スクリプトを変更しディスクにセーブしてもプログラムを再起動しなければ効果はありません。しかしFile | Debug options | Clear the script file script file cache メニューでスクリプトファイルキャッシュをフラッシュし、ディスクからファイルをリロードすることが出来ます。あるいはメインSyslogウィンドウからCtrl-F8 を押します。キャッシュをフラッシュするたびディスクから新しいスクリプトファイルが読み込まれることを覚えておいてください。

Field Read/Write permissions

セキュリティとスピードの面で、メッセージとスクリプト変数のアクセスを制限することが出来ます。スクリプトが実行されると、メッセージフィールドがスクリプト変数にコピーされ、スクリプトが完了すると戻されます。コピーは時間とCPUサイクルを消費しますので、Read/Writeアクセスを使用する変数に制限すると、実行速度が上がります。

フィールドグループのReadアクセスをイネーブルにすると、値がスクリプト変数に書かれますのでスクリプト中で読むことが出来ます。

フィールドグループのWriteアクセスをイネーブルにすると、値がスクリプト変数から読まれ等価のプログラムフィールドが置き換わります。

フィールドはスクリプト中での似た使用方法にグループ化できます。

フィールドの詳細はここで分かります。

共通フィールド

VarFacility
VarLevel
VarInputSource
VarPeerAddress
VarPeerName
VarPeerDomain
VarCleanMessageText

その他のフィールド

VarDate
VarTime
VarMilliseconds
VarSocketPeerAddress
VarPeerAddressHex
VarPeerPort
VarLocalAddress

VarLocalPort
VarPriority
VarRawMessageText

カスタムフィールド

VarCustom01 から VarCustom16

下記のスクリプト変数はスクリプトからのRead/Writeアクセスが常に可能です。

スクリプト間フィールド

VarGlobal01 から VarGlobal16

カスタム統計フィールド

VarStats01 から VarStats16

コントロールとカウンターフィールド

ActionQuit
SecondsSinceMidnight
SecondsSinceStartup

定期的にスクリプトをトリガーにする

Keep-alive入力ファンクションをイネーブルにすると、メッセージが等間隔で挿入されます。このメッセージをスクリプトアクションのトリガーとして使えます。

練習 – 最初のスクリプトの作成

この練習はどのようにスクリプトを作成し、それを使ってSyslogメッセージのテキストを検索し置き換えるかを示します。

スクリプトアクションは登録正規版のみです。フリーウェア版ではスクリプトアクションのテストは出来ませんが、通常に使用することはできません。

Step 1. スクリプトアクションの作成...

Create a new rule called "Replace text"
Add a new Run Script action.
Set the script file name to: ReplaceText.txt
Set the script description to: Replaces occurrences of "cat" with "dog".
Set the script language to VBScript
Set the field read/write permissions to:
Common fields: Read=Yes, Write=Yes
Other fields: Read=No, Write=No
Custom fields: Read=No, Write=No

Edit Script ボタンを押してノートパッドにファイルを開いてください。ファイルが存在しませんので、新規を選びます。ノートパッドに下記のスクリプトをコピー/貼り付けし、ノートパッドのFile | Saveをクリックします。

```
Function Main()  
  
' Replace cat with dog within the message text field  
Fields.VarCleanMessageText = Replace(Fields.VarCleanMessageText, "cat", "dog")  
  
' Return OK to tell syslog that the script ran correctly.  
Main = "OK"  
  
End Function
```

Step 2. アクションの作成...

Add a new Log to file action
Set the file name to "MyCustomLog.txt" in the folder of your choice.
Leave the file format as default.
Click the action and then press F4 to auto name the action "Log to file"
Add a new Display action
Leave the display number as default.
Click the action and then press F4 to auto name the action "Display"

Run script アクションはdisplay and log to file アクションの上になります。そうでない場合、アクションを選びツールボタンで上へ動かします。

ルールはこのようになります：

Rules

Rule: Replace Text

Filters

Actions

Run Script

Display

Log to file

Step 3. スクリプトのテスト...

Select the Run Script action.

Click the Test Setup button.

Change the message text to read: The cat sat on the mat.

Click the Show action button

Check the Show test results check box

Press the Test button

スクリプトを実行すると結果がノートパッドに開かれます。そこでは全てのスクリプト変数を見ることが出来ます。VarCleanMessageText フィールドをチェックしてください。Catがdogに代わっていることが分かります。

Step 4. SyslogGen でスクリプトをテスト

Apply the new rule changes by clicking OK on the Properties window. You will then have just the main syslog window showing.

Download SyslogGen from www.kiwisyslog.com

Install it on the same machine as the Syslog Daemon

Set the send options to "send message once"

Set the destination to localhost (127.0.0.1).

Set the message text to be: This is a test. The cat sat on the mat.

Press the Send button

ディスプレイにThis is a test. The dog sat on the mat .と表示されます。

スクリプト変数

いくつかの変数がスクリプトへ、またスクリプトから渡されます。アクションに設定したRead/Writeパーミッションに従い、変数が変わり、Syslog プログラムで使うために返されます。

変数とファンクションはグローバルにアクセスできるオブジェクト名Fields で渡されます。変数やファンクションをアクセスするには変数やファンクション名の前にFields.を付けます。

Common フィールド

Fields.VarFacility

詳細: メッセージのfacility値

タイプ: 整数 (0-32767)

範囲: 0 ~ 23. facilityのリストは[ここをクリック](#)

Fields.VarLevel

詳細: メッセージのlevel値

タイプ: 整数 (0-32767)

範囲: 0 ~ 7. Levelのリストは[ここをクリック](#)

Fields.VarInputSource

詳細: メッセージの入力元

タイプ: 整数 (0-32767)

範囲: 0 to 2. 0=UDP, 1=TCP, 2=SNMP, 3 = KeepAlive, 4 = NT Event Log, 5 = Log file, 6 = Comm port
(4, 5 と6 は未使用)

Fields.VarPeerAddress

詳細:

nnn.nnn.nnn.nnn フォーマットの送信デバイスIPアドレス。メッセージが他のSyslogコレクタからフォワーディングされても、この値は本来の送信元アドレスです。

Case A.

ファイアーウォールデバイス (192.168.1.1) ---> 最初のSyslogコレクタ (192.168.1.2) ---> このSyslogコレクタ (192.168.1.3)
フィールドの値は 192.168.1.1です。

Case B.

ファイアーウォールデバイス (192.168.1.1) ---> このSyslogコレクタ (192.168.1.3)
フィールドの値は 192.168.1.1です。

タイプ: 文字列

フォーマット: nnn.nnn.nnn.nnn ゼロパディングされない

例: 192.168.1.67

Fields.VarPeerName

詳細:
送信デバイスのホスト名。DNSルックアップオプションがイネーブルでルックアップが成功した時に限り値が入る。それ以外はVarPeerAddress
と同一の値。フォーマットはnnn.nnn.nnn.nnn。FQDNのホスト名だけでありドメインサフィックスは含まない。

タイプ: 文字列

フォーマット: myhost

Fields.VarPeerDomain

詳細:
FQDN 解決のドメイン名部分。ドメインサフィックスでありホスト名を含まない。DNSルックアップオプションがイネーブルでルックアップが成
功した時に限り値が入る。それ以外は空白。

タイプ: 文字列

フォーマット: mydomain.com

Fields.VarCleanMessageText

詳細:
変更後の文字列(ヘッダー削除, DNS ルックアップ, 元のアドレス削除, Cisco 日付削除 など)。

タイプ: 文字列

例:
%SEC-6-IPACCESSLOGP: list 101 denied udp 10.0.0.3 (firewall) (137) -> 216.7.14.105 (webserver.company.com) (137), 1
packet

その他のフィールド

Fields.VarDate

詳細: メッセージ受信日付

タイプ: 文字列(10バイト)

フォーマット: YYYY-MM-DD

例: 2002-03-17

Fields.VarTime

詳細: メッセージ受信時刻

タイプ: 文字列(8バイト)

フォーマット: HH:MM:SS

例: 23:10:04

Fields.VarMilliSeconds

詳細: 1/1000秒単位のメッセージ受信時刻

タイプ: 文字列 (3バイト)

範囲: 000 から 999

フォーマット: nnn (3バイト, ゼロパディング)

Fields.VarSocketPeerAddress

詳細: メッセージ送信デバイス又は最も近いコレクターのIPアドレス

Case A.

ファイアーウォール (192.168.1.1) ---> 最初のSyslogコレクタ (192.168.1.2) ---> このsyslog コレクタ (192.168.1.3)
値は 192.168.1.2.

Case B.

ファイアーウォール (192.168.1.1) ---> このsyslog コレクタ (192.168.1.3)
値は 192.168.1.3.

タイプ: 文字列

フォーマット: nnn.nnn.nnn.nnn. 値のゼロパディングなし

例: 192.168.1.67

Fields.VarPeerAddressHex

詳細:

メッセージを送信したIPアドレスを8文字16進数に変換。

16進アドレスはIPマスクとIPレンジフィルターに使われます。VarPeerIPAddress を変更しIPマスクやIPレンジフィルターを使うにはVarPeerAddressHex フィールドも変更します。

タイプ: 文字列 (8バイト)

範囲: 00000000 から FFFFFFFF

例: C0A80102 (192.168.1.2 を2バイト16進数に変換)

Fields.VarPeerPort

詳細: メッセージを送信した UDP/TCP ポート

タイプ: 整数 (0-65535)

範囲: 0 から 65535

通常: 1023以上

Fields.VarLocalAddress

詳細: このマシンにメッセージを送信したIPアドレス

タイプ: 文字列

例: 127.0.0.1, 192.168.1.2

Fields.VarLocalPort

詳細: メッセージを受信したローカルマシンのUDP/TCP ポート

タイプ: 整数 (0-65535)

範囲: 0 から 65535

通常: UDP では514, TCPでは1468, SNMPでは162

Fields.VarPriority

詳細: メッセージプライオリティ値

タイプ: 整数 (0-32767)

範囲: 0 から191

Fields.VarRawMessageText

詳細:

変更前の受信メッセージ (<pri> タグ, 元のアドレスなどを含む)。

このフィールドは読むだけです。スクリプトのフィールドを変更しても相当するプログラム変数を変更しません。

カスタムフィールド

これらのフィールドは動的であり、新しいメッセージでクリアされます。これらのフィールドはスクリプトの結果が入るためLog to file や Log to Databaseアクションに使われます。このフィールドは%VarCustom01 **Insert message content or counter** オプションかAutoSplit 文でアクションにパラメータとして渡されます。メッセージをスクリプトで分割し分離したフィールドのファイルやデータベースに保存するのに適しています。

16個のカスタムフィールドがあります。1~9はゼロがパディングされます(VarCustom1ではなくVarCustom01です)。

[Fields.VarCustom01](#) から [Fields.VarCustom16](#)

スクリプト間フィールド

各メッセージで固定されており変化しません。他のスクリプトへの値の受け渡し、同一スクリプトで後に利用するために値を維持するためのものです。%VarGlobal01 **Insert message content or counter** オプションあるいはAutoSplit文で値をアクションに渡します。

16個のグローバル フィールドがあります。1~9はゼロがパディングされます(VarGlobal1ではなくVarGlobal01です)。

[Fields.VarGlobal01](#) から [Fields.VarGlobal16](#)

カスタムスクリプトフィールド

各メッセージで固定されており変化しません。自分のカスタム統計とカウンター用に使われます。%VarStats01 **Insert message content or counter** オプションで値がアクションに渡されます。

Counters タブのStatistics ビューウィンドウで現在のフィールド値を見ることが出来ます。カスタムStaticsはデیلیーstatistics e-mail に含まれます。

Statistics フィールドの名前と初期値はScriptingオプションから設定します。

16個のカスタムstatistics フィールドがあります。1~9はゼロがパディングされます(VarStats1ではなくVarStats01です)。

[Fields.VarStats01](#) から [Fields.VarStats16](#)

コントロールとタイミングフィールド

Fields.ActionQuit

詳細:
スクリプト実行後何をするかを設定します。0はルールの次のアクションを続けます。1~99はルール中のアクションスキップ数です(1=1アクションスキップ、3=3アクションスキップ)。100は次のルールへのジャンプです。1000は全てのルールをスキップしメッセージ処理を終了します。値が無い場合は0とみなします。
タイプ: 整数 (0-32767)
範囲: 0 から 1000
指示: 0=スキップしない, 1-99=アクションスキップ数, 100=次のルールまでスキップ, 1000=メッセージ処理終了

Fields.SecondsSinceMidnight

詳細: 真夜中からの経過時間(秒)
タイプ: 倍長 (0-20億)
範囲: 0 ~ 86400

Fields.SecondsSinceStartup

詳細: プログラムスタートからの経過時間(秒)
タイプ: 倍長 (0-20億)

スクリプトファンクション

Fields オブジェクトからいくつかのビルトインファンクションを利用できます。今後のリリースではさらに追加される予定です。

ビルトインファンクションはFields オブジェクトの前に名前を付ければアクセスできます。必要なパラメータを渡し、結果が戻ります。

"Fields" オブジェクトの組み込み関数

Fields.IsValidIPAddress(IPAddress as string) as Boolean

機能: 渡された文字列をチェックし正しいIPアドレスフォーマットであれば真を返す
入力パラメータ: IPAddress文字列
結果: 論理値 (真/偽)

使用例:
If Fields.IsValidIPAddress(Fields.VarPeerAddress) = True then
 Fields.VarCustom01 = Fields.VarPeerAddress
End if

Fields.ConvertIPToHex(IPAddress As String) As String

機能: IP address を8バイトの16進数に変換
入力パラメータ: IPAddress 文字列
結果: 8 バイト16進数

使用例:
If Fields.IsValidIPAddress(Fields.VarPeerAddress) = True then
 Fields.VarCustom01 = Fields.ConvertIPToHex(Fields.VarPeerAddress)
End if

Fields.ConvertPriorityToText(PriorityValue)

機能: メッセージプライオリティ値をfacility.levelのテキスト表現に変換する
入力パラメータ: プライオリティ値
範囲: 0 ~ 191
結果: 文字列Facility.Level
例: 191は"Local7.Debug"を返す

使用例:
Filename = "C:¥Program files¥Syslogd¥Logs¥TestLog.txt"
' Use the date and time from the current message
With Fields
 MsgDate = .VarDate & " " & .VarTime
 MsgText = "This is a test message from the scripting action"
 Data = MsgDate & vtab & .ConvertPriorityToText(.VarPriority) & vtab & _
 .VarPeerAddress & vtab & MsgText
 Call .ActionLogToFile(Filename, Data)
End with

Fields.ActionPlaySound(SoundFilename As String, RepeatCount as Long)

機能: 音を鳴らす、あるいは指定したwav ファイルを実行。X回もしくはキャンセルされるまで繰り返す。
入力パラメータ: 文字列SoundFilename, 倍長RepeatCount
結果: 無

SoundFilename が無い場合はシステムビープ音を鳴らす。

RepeatCountオプション:

0 = キャンセルされるまで繰り返し(メイン表示ウィンドウで点滅するベルを押してキャンセルします)
1 ~ 100 = 繰り返し数

繰り返し数が1以上の時、5秒間隔になります。

使用例:

```
' Play the squeak sound 5 times  
Call Fields.ActionPlaySound("C:¥Program Files¥Syslogd¥Sounds¥Squeak.wav", 5)
```

```
' Play the squeak sound until cancelled  
Call Fields.ActionPlaySound("C:¥Program Files¥Syslogd¥Sounds¥Squeak.wav", 0)
```

```
' Play the system beep sound 10 times  
Call Fields.ActionPlaySound("", 10)
```

```
' Play the system beep sound until cancelled  
Call Fields.ActionPlaySound("", 0)
```

Fields.ActionSendEmail(MailTo, MailFrom, MailSubject, MailMessage)

機能: 指定のアドレスにe-mailを送信

結果: 無

複数アドレスの場合は各アドレスをカンマで区切ります。

例

```
MailTo = "user1@company.com,user2@company.com,user3@company.com"
```

使用例:

```
MailTo = "joe@company.com"  
MailFrom = "server@company.com"  
MailSubject = "This is a test of the scripting action"  
MailMessage = "This is a test mail message" & vbCrLf & "Multiple lines."
```

```
Call Fields.ActionSendEmail(MailTo, MailFrom, MailSubject, MailMessage)
```

Fields.ActionLogToFile(Filename, Data)

機能: 指定のログファイルの終わりにデータを追加します

結果: 無

ファイルへのメッセージログを独自フォーマットで書きます。

ファイル名にAutoSplit 値が使えます。

現在の日時をファイル名に現在の日時を含むには%TimeHHを使います。

```
例: Filename = "C:¥Program files¥Syslogd¥Logs¥TestLog%TimeHH.txt"
```

使用例:

```
Filename = "C:¥Program files¥Syslogd¥Logs¥TestLog.txt"  
MsgPriority = "Local7.Info"  
MsgHostAddress = Fields.VarPeerAddress  
' Use the date and time from the current message  
MsgDate = Fields.VarDate & " " & Fields.VarTime  
MsgText = "This is a test message from the scripting action"  
Data = MsgDate & vbtabs & MsgPriority & vbtabs & MsgHostAddress & vbtabs & MsgText
```

```
Call Fields.ActionLogToFile(Filename, Data)
```

注: この例ではOther fieldsのRead権限が必要です。VarDate とVarTime変数にscript read accessを与えます。

Fields.ActionLogToFileWithCache(Filename, Data)

機能: 指定のログファイルにデータを書きます。キャッシュは100メッセージまたは5秒ごとにフラッシュされます。キャッシュの設定はレジストリーで行います。この機能はActionLogToFileが書き込みキャッシュを使うこと以外は同じです。毎秒10メッセージ以上を受信する場合書き込みキャッシュ機能を使ってください。

結果: 無

ファイルへのメッセージログを独自フォーマットで書きます。

ファイル名にAutoSplit 値が使えます。

現在の日時をファイル名に現在の日時を含むには%TimeHHを使います。

例 : Filename = "C:¥Program files¥Syslogd¥Logs¥TestLog%TimeHH.txt"

使用例 :

```
Filename = "C:¥Program files¥Syslogd¥Logs¥TestLog.txt"
```

```
MsgPriority = "Local7.Info"
```

```
MsgHostAddress = Fields.VarPeerAddress
```

```
' Use the date and time from the current message
```

```
MsgDate = Fields.VarDate & " " & Fields.VarTime
```

```
MsgText = "This is a test message from the scripting action"
```

```
Data = MsgDate & vtab & MsgPriority & vtab & MsgHostAddress & vtab & MsgText
```

```
Call Fields.ActionLogToFileWithCache(Filename, Data)
```

注:この例ではOther fieldsのRead権限が必要です。VarDate とVarTime変数にscript read accessを与えます。

Fields.ActionDeleteFile(Filename)

機能 : 指定ファイルを削除

結果 : 無

ログファイルを削除し完全なスタート状態にします。

ワイルドカードを使用できませんので、具体的なファイル名の指定が必要です。確認の必要がありませんので使う場合は注意が必要です。

使用例 :

```
Filename = "C:¥Program files¥Syslogd¥Logs¥TestLog.txt"
```

```
Call Fields.ActionDeleteFile(Filename)
```

Fields.ActionDisplay(DisplayNumber, TabDelimitedMessage)

機能 : パーチャル表示番号にメッセージを表示

結果 :

画面に独自フォーマットメッセージを表示するための機能です。

TabDelimitedMessageは5個のタブ区切りフィールドが必要です。各フィールドの内容は何でもかまいません。標準の表示フィールドは : 日付
タブ 時刻 タブ プライオリティ タブ ホスト名 タブ メッセージ

使用例 : With Fields

```
MsgPriority = ConvertPriorityToText(.VarPriority)
```

```
MsgHostAddress = .VarPeerAddress
```

```
' Use the date and time from the current message
```

```
MsgDate = .VarDate & " " & .VarTime
```

```
MsgText = "This is a test message from the scripting action"
```

```
Display = MsgDate & vtab & MsgTime & vtab & MsgPriority & vtab & _
```

```
MsgHostAddress & vtab & MsgText
```

```
Call .ActionDisplay(0, Display)
```

```
End with
```

スクリプト例

ヘルプファイルのスクリプトで最初に勉強ができます。今後さらに www.kiwisyslog.com に追加されます。

サンプルスクリプトを含むプログラムは音を鳴らす、e-mailを送信する、ファイルにログを記録などを含みます。インストールフォルダーの ¥Scripts サブフォルダーにあります。

他のユーザにとっても効果的なスクリプトを作ったらsupport@kiwisyslog.comまで送ってください。Webサイトに追加します。

PIX メッセージの検査

下記のファンクションは特定のPIXメッセージ数を調べカスタムメッセージフィールドに説明を送ります。カスタムフィールドはSend e-mail アクションで使います。

このスクリプトの値はCisco Webサイトで見ることが出来ます：
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v53/syslog/pixmsgs.htm

スクリプトアクション設定

Common fields: Read=yes

Custom fields: Write=yes

ルール設定

```
Rules
  Rule: Lookup PIX msg
    Filters
      Filter: Host IP address: Simple: Match PIX firewall address
    Actions
      Action: Run Script: Lookup PIX msg
      Action: Send e-mail
        To: helpdesk@company.com:
        Subject: Problem with PIX
        Body: %MsgText%
        Explanation: %VarCustom01
        Action to take: %VarCustom02

Function Main()

' Set the return value to OK
Main = "OK"

' By default, skip to the next rule, don't take the actions that follow
' If we exit the function before we get to the end, the default 'skip to next rule'
' will be used.
Fields.ActionQuit = 100

' Example of a PIX message
' %PIX-4-209004: Invalid IP fragment...

Dim M ' Message
Dim E ' Explanation
Dim A ' Action

' Copy message to local variable for speed
M = Fields.VarCleanMessageText

' If message length is too short, exit function
If Len(M) < 15 then exit function

' Grab the first 15 chrs
M = Left(M,15)

' Check the message is a valid PIX message
If Mid(M,1,5) <> "%PIX-" then exit function

' Add any additional checks you want to perform here

' Grab the important part ("4-209004")
M = Mid(M,6,8)

E = ""
A = ""

' Now lookup the values and create an explanation and action for each match
Select Case M
  Case "4-209004"
    E = "An IP fragment is malformed. The total size of the reassembled IP packet exceeds the maximum possible size of 65,535 bytes"
    A = "A possible intrusion event may be in progress. If this message persists, contact the remote peer's administrator or upstream provider."
  Case "2-106012"
    E = "This is a connection-related message. A IP packet was seen with IP options. Because IP options are considered a security risk, the packet was discarded."
    A = "A security breach was probably attempted. Check the local site for loose source or strict source routing."

' Insert other values to lookup here
```

End Select

' Exit if we don't have any values to pass

If len(E) = 0 then exit function

If len(A) = 0 then exit function

' Pass the Explanation and Action to take to the custom variables

Fields.VarCustom01 = E

Fields.VarCustom02 = A

' Since we have a valid match, we want to execute the send e-mail action which follows.

' Setting ActionQuit to 0 means we won't skip any actions.

Fields.ActionQuit = 0

End function

全ての変数 - (Info機能)

下記のファンクションで全フィールド変数を表示します。参考のため自分のスクリプトに貼り付けてください。

注: 全ての変数はコメントでありファンクションをコールしても実行されません。

Function Info()

' // Common fields

' VarFacility

' VarLevel

' VarInputSource

' VarPeerAddress

' VarPeerName

' VarPeerDomain

' VarCleanMessageText

' // Other fields

' VarDate

' VarTime

' VarMilliSeconds

' VarSocketPeerAddress

' VarPeerAddressHex

' VarPeerPort

' VarLocalAddress

' VarLocalPort

' VarPriority

' VarRawMessageText (Read only)

' // Custom fields

' VarCustom01 to VarCustom16

' // Inter-Script fields

' VarGlobal01 to VarGlobal16

' // Custom Stats fields

' VarStats01 to VarStats16

' // Control and timing fields

' ActionQuit

' 0=No skip, 1-99=skip next n actions within rule,

' 100=skip to next rule, 1000=stop processing message

'

' SecondsSinceMidnight

' SecondsSinceStartup

' // Functions and Actions

' IsValidIPAddress(IPAddress as string) as boolean

' ConvertIPtoHex(IPAddress as string) as string

' ActionPlaySound(SoundFilename as string, RepeatCount as long)

' RepeatCount 0=until cancelled, 1-100=repeat x times

' Soundfilename ""=system beep, "wav file name"=play wav file

' ActionSendEmail(MailTo as String, MailFrom as string, MailSubject as string, MailMessage as string)

' Sends an e-mail message to the addresses specified in MailTo

End function

Setup – Archiving (設定 – アーカイピング)

Setup – Archiving (設定 – アーカイピング)

ログのアーカイブをイネーブルにするにはArchivingオプションをクリック後右クリックしadd a new custom scheduleをクリックします。もしくは Archiving オプションのクリック後にツールバーの[New]ボタンを選びます。

リストに最大100のカスタムアーカイブスケジュールを登録できます。それぞれ連続して実行されます。同時刻に2つのスケジュールがセットされたらリストの上位のスケジュールから実行されます。

スケジュール名の左のチェックボックスでいつでもスケジュールのイネーブル、ディセーブルが可能です。

カスタムスケジュールの名称は任意です。ユニークでなくてもかまいませんが内容あるいは実行時間が分かるよう命名してください。

ログファイルアーカイピング動作

リストにアーカイピングスケジュールが無い場合アーカイピングは実行されません。 Rules/Filters/Actions で定義されたログファイルがメッセージの受信に伴って大きくなります。

新しいアーカイブスケジュールの追加にはArchivingオプションを右クリック後、右クリックしポップアップメニューから**Add new archive schedule**を選択します。

アーカイブスケジュールのリストは上位から下位に実行されます。アーカイブがイネーブルで設定時刻に一致するとアーカイブが実行されます。ソースフォルダーのログファイルのファイル仕様と容量が一致した全てのログファイルは全て宛先アーカイブフォルダーに移動します。

作成される宛先アーカイブフォルダーには現在の日時が追加されます。

Example: "C:¥Program Files¥Syslogd¥Dated Syslogs¥2002-02-23¥"

日付スタンプフォーマットは YYYY-MM-DDです。

注意: 個々のログファイルは新しい一つのフォルダーに移されますのでログファイルには固有の名前が必要です。

さもなければ移動するファイルの名前を変更します。新しい名前にはその一部に現在の日付を入れてください。

Example: "C:¥Program Files¥Syslogd¥Dated Syslogs¥MyLogFile2002-02-23.txt"

日付スタンプフォーマットは YYYY-MM-DDです

ArchiveオプションがHourlyの時は、ファイル名に追加される日付スタンプの一部にはアーカイブ作成時刻01から24が含まれます。

Example: "C:¥Program Files¥Syslogd¥Dated Syslogs¥MyLogFile2002-02-27-24.txt"

日付スタンプフォーマットは YYYY-MM-DD-HHです。HH は01から24です

同一名のアーカイブファイルが存在する場合、ファイルまたはフォルダー名に 001から 099 が追加されます。複数のアーカイブスケジュールで送信ファイルやフォルダーが使われる場合、既存のアーカイブに上書きされるのを防止します。Test Archiveボタンを押すと一日に複数のアーカイブファイルやフォルダーを作ります。

登録正規版ではアーカイブフォルダーやファイルの圧縮がサポートされます。ファイルを移動した時やアーカイブが完了した時、外部プログラムを実行することもできます。ファイル名やアーカイブフォルダーを外部プログラムに渡せます。アーカイブ実行時アーカイブしたログファイルをBLATのような外部e-mailプログラムで送信できます。

アーカイブ終了の連絡はNotify by e-mailチェックボックスで可能です。E-mailオプションで指定した、Statistics 連絡アドレスに送られます。各通知メッセージには移動と圧縮されたファイルの全リストが含まれます。

コマンドラインe-mailプログラム"BLAT for windows"の情報は次のWebサイトにあります：

<http://www.interlog.com/~tcharron/blat.html>

外部プログラムコマンドラインオプション実行

外部プログラムにパラメータとしてプログラム変数を渡すことができます。全ての%parameter オプションを思い出すよりも、青色の**Variable options** リンクをクリックし、ポップアップメニューからパラメータを選択してください。選択したオプションがコマンドラインに置かれます：現在のカーソル位置のテキストボックスです。

可能な変数：

%Folder = Dest folder inc date stamp

例: C:¥Program Files¥Syslogd¥Dated logs¥2004-02-27¥

%FileLong = Dest file name inc path

例: C:¥Program Files¥Syslogd¥Dated logs¥2004-02-27-001¥SyslogCatchAll.txt

%FileShort = Dest file name (no path or extn)

例: SyslogCatchAll

%DateStamp = Date Stamp

例: 2004-02-27

%FileZipLong = Dest zip file inc path

例: C:¥Program Files¥Syslogd¥Dated logs¥2004-02-27-006¥2004-02-27.zip

%FileZipShort = Dest zip file name (no path)

例(全てのファイルをひとつのzipファイルに): 2004-02-27

例(それぞれのzipファイルに): SyslogCatchAll

アーカイブレポートの例

各アーカイブ完了後、e-mailでレポートが送られます。下はアーカイブレポートの例です。

```
///                Archive Status Report                ///
```

```
Date and Time:      Fri, 26 Jul 2002 00:00:01
Schedule name:      Daily
Source Folder:      C:¥Program Files¥Syslogd¥Logs¥
Destination Folder: C:¥Program Files¥Syslogd¥Dated logs¥2002-07-26¥
+-----+-----+-----+-----+
| File name:          | File size | Move | Zip |
+-----+-----+-----+-----+
| pix.txt             | 6582642 | OK  | OK  |
+-----+-----+-----+-----+
```

End of report.

アーカイブ時刻オプション

可能なarchive timeオプションリストです。

Custom	任意の設定時間に実行
Monthly	毎月末の真夜中に実行
Weekly	毎日曜日の真夜中に実行
Daily	真夜中に実行
Hourly	毎正時に実行

UTCオプションをセットするとUTC時刻での実行を試験できます。

真夜中とは

真夜中は00:00であり翌日の始まりです。日付スタンプでは前日になります。一日分がアーカイブファイルに入ることになります。

Hourlyアーカイブオプションではファイル名に含まれる日付スタンプの一部には01から24が追加されますがアーカイブが作成された時間となります。

Example "C:¥Program Files¥Syslogd¥Dated Syslogs¥MyLogFile2002-02-27-24.txt"

日付スタンプフォーマットは YYYY-MM-DD-HHです。HHは01から24です。

Setup – Formatting (設定 – フォーマット)

Custom file formats (カスタムファイルフォーマット)

準備中

Custom DB formats (カスタムDBフォーマット)

新しいカスタムフォーマットの作成

新しいカスタムフォーマットの作成にはCustom DB formatsを選択し、右クリック後add new custom DB formatを選びます。もしくは、フォームトップのツールバーのNewツールバーボタンを使います。最初にデータベースタイプAccess databaseが表示されますので、ドロップダウンリストからデータベースタイプを選びます。データベースタイプが不明の時はUnknown formatを選び、データベースタイプに合うようフィールドを変更します。

フィールド順序の変更

データベースに作成されたフィールド順序を変更するにはフィールドファンクションセルを他のセルの上下にドラッグ&ドロップします。マウスを灰色のファンクションセルの上まで動かすとマウスカーソルはドラッグ&ドロップカーソルに変わります。順序を変更するにはドラッグそしてドロップをクリックしてください。表示された順序でデータベーステーブルが作成されテーブルにデータが挿入されます。

Field Function

データベースのフィールドファンクションは最初の列です。次の列はフィールドのイネーブル、ディセーブルのチェックボックスです。フィールドのチェックが無い場合は、データベースINSERT文が含まれないかデータベーステーブルの作成時使用されません。

Field names

フィールド名は編集可能です。適切な名前を付けてください。デフォルトフィールド名が全てのデータベースに付いています。たとえばフィールド名としてDATEを選択するとあるデータベースでは予約名となっておりますので問題が発生します。フィールド名の最初にMSGを使えば予約名を避けることができます。

Field size

データベースの作成にあたり、フィールドに最大のデータが入るようにサイズを指定することが重要です。いくつかのフィールドではフィールドタイプでサイズが決まりますので指定する必要がありません。たとえばTimeは常に8バイトとみなされます。サイズはまたプログラムでログをデータベースに書く時必要です。データはINSERT文で渡されますので、指定されたフィールドサイズにトリムされます。フィールドに大きすぎるデータが入ることを避けるためです。例えば、メッセージテキストフィールドに255バイトを指定し、メッセージが300バイトの時、ログの前に255バイトにトリムされます。

Field type

フィールドタイプはログデータのタイプに一致しなければなりません。正しいデータタイプが不明な時は、安全のため多くの場合VarCharとすれば大丈夫です。データタイプセルの編集時、ドロップダウンリストが表示されますので選択してください。リストから選ぶ代わりに、値をセルにタイプすることもできます。リストのデータタイプは選択したデータベースタイプに特有のもので、例えばAccessでのTextはSQLではVarCharです。

Custom fields

カスタムフィールドはスクリプト実行アクションで使えます。解析スクリプトを書く時、Syslogメッセージテキストをサブフィールドに分割できます。値は16のカスタムフィールドにアサインし、データベースに記録されます。デバイス製造業者は異なるフォーマットのSyslogメッセージを生成しますので、メッセージテキストを独立したフィールドに分離する一般的な解析文を作成することはできません。カスタムスクリプトでテキストを解析し、カスタムデータベースフィールドに記録します。解析スクリプト例は¥Scriptsにあります。

Example of data format being logged:

Field name	Type	Size	Data
MsgUnique	adInteger	4	1
MsgDate	adDBTimeStamp	16	28/07/2002
MsgTime	adDBTimeStamp	16	16:12:54
MsgDateTime	adDBTimeStamp	16	28/07/2002 16:12:54
MsgUTCDate	adDBTimeStamp	16	28/07/2002
MsgUTCTime	adDBTimeStamp	16	04:12:54
MsgUTCDateTime	adDBTimeStamp	16	28/07/2002 04:12:54
MsgTimeMS	adInteger	4	0
MsgPriorityNum	adInteger	4	191
MsgFacilityNum	adInteger	4	23
MsgLevelNum	adInteger	4	7
MsgPriority	adVarChar	30	Local7.Debug
MsgFacility	adVarChar	15	Local7
MsgLevel	adVarChar	15	Debug
MsgHostAddress	adVarChar	15	192.168.0.1
MsgHostname	adVarChar	255	host.company.com
MsgInputSource	adVarChar	10	UDP
MsgText	adLongVarChar	1024	This is a test message from Kiwi Syslog Daemon

Field format

データフォーマットを各データフィールドで指定できます。多くの場合は不要です。日付フィールドでは多くのフォーマットが可能で、その独自の内部フォーマットに変換します。問合せ時、記録と異なるフォーマットで表示されます。HostAddressフィールドフォーマットはアドレスに0パッドできますので表示されると先頭に0が現れます。これはアドレスが常に15バイトでありIPアドレスによるソートを容易にするためです。

フォーマットセルを空白にすると、データは変更されず、受信したとおり追加されます。

Show SQL commands button

このボタンを押すとテーブルを作成し、データを挿入するために使われるコマンドリストが表示されます。これらのコマンドで自分自身のテーブルを自分のデータベースアプリケーションに作成できます。コマンドを発生する時デフォルトテーブル名はSyslogdになります。

SQL コマンド例:

Database type: MySQL database
Database name: New Format

SQL command to create the table:
CREATE TABLE Syslogd (MsgDate DATE,MsgTime TIME,MsgPriority VARCHAR(30),MsgHostname VARCHAR(255),MsgText TEXT)

SQL INSERT command example:
INSERT INTO Syslogd (MsgDate,MsgTime,MsgPriority,MsgHostname,MsgText) VALUES
('2002-07-28', '16: 22: 44', 'Local7.Debug', 'host.company.com', 'This is a test message from Kiwi Syslog Daemon')

Setup - DNS Resolution (設定 - DNS解決)

Resolve the address of the sending device (送信デバイスアドレス解決)

送信デバイスのIPアドレスをホスト名に変換します。203.50.23.4に代えてsales-router.company.comのような表示になります。

解決されたホスト名は表示や他の操作に使われます。

ホスト名はまたHostnameタイプフィルターでも使われます。

希望するなら、Remove the domain name オプションで、表示からドメイン名セクションを削除することが可能です。

Remove the domain name (ドメイン名を消去- ホスト名の表示のみ)

Resolve the IP address of the sending device オプションをチェックした時、このオプションで解決したホスト名の後ろのドメイン名を削除できます。この場合、sales-router.company.comではなくsales-routerとなります。

同一ドメインからのみメッセージを受信する場合や、スクロール表示のホスト名表示スペースを節約する時、効果的です。

このオプションは全てのロギング操作で使われるホスト名フィールドで有効です。

Resolve IP addresses found within the syslog message text (SyslogメッセージテキストのIPアドレス解決)

この機能は登録正規版でのみ有効です。

Webブラウザやファイアーウォールからのデータのロギング時、メッセージテキストはIPアドレスを含みます。このオプションをイネーブルにして、IPアドレスをホスト名やWebサイト名に変換します。プログラムはテキストのIPアドレスをサーチします。解決した名前の表示方法を指定できます。IPアドレスを名前に置き換え、あるいはIPアドレスの後に名前を追加することができます。

* NetBIOS名解決はDNSエン트리解決より時間がかかります。NetBIOS名解決する時はDNSタイムアウトを20ないし30秒にしてください。

例:
Test user connected to website http://192.168.1.2/index.html. src=192.168.5.100 rxbytes=64
With **replace IP address with host name** option, the message becomes...
Test user connected to website http://website.company.com/index.html. src=userpc.company.com rxbytes=64

With **place host name next to IP address** option, the message becomes...

```
Test user connected to website http://192.168.1.2 (website.company.com) /index.html. src=192.168.5.100  
(userpc.company.com) rxbytes=64
```

Remove the domain nameオプションは解決した名前からドメイン名を削除します。
フィルター一致条件から選択的に含んだり、削除したりするには **If domain name contains**チェックボックスをチェックしてください。

削除するドメイン名を引用符で囲みます。複数ドメインをフィルターするには引用符で囲んだ文字列をスペースかカンマで区切ってください。
".companyabc.com", ".companyxyz.co.uk"

mypc.company.co.uk と解決されたIPアドレスは"mypc"になります。 .

Hostname tagging:

place host name next to IP address オプションを選択するとホスト名には [] とスペースタグが付きます。解決したホスト名に任意のタグをつけることができます。例えばhostname=[] サフィックスを付けられます。プレフィックス、サフィックスをメッセージに合わせ変更できます。

WELFフォーマットメッセージでの推奨タグフォーマットは、プレフィックスがresolved_host= サフィックスはスペースです。

DNS query timeout (DNSクエリータイムアウト)

DNSサーバーのテーブル参照のタイムアウトを指定します。デフォルトは8秒です。遅いDNSサーバーやネットワークリンクが低速であれば大きな値に変更できます。

この値はNetBIOS (Windows用コンピュータ名) の名前解決をする場合のみ大きくすべきです。ユニキャストによる名前解決には20秒かかることがあります。

DNSサーバーがローカルで内部アドレス変換だけの場合安心して3秒以下にできます。

タイムアウト時間を大きくしすぎると名前解決終了までメッセージがキューにたまるのが分かります。キューが1,000以上になるとメッセージが失われます。メッセージバッファのフリースペースはメインSyslog画面で分かります。

DNS resolver threads (DNSリゾルバースレッド)

このオプションは送信ホストあるいはメッセージテキスト中のIPアドレス解決にいくつのDNS名前解決スレッドを使用するかを指定します。ブリエンプティブDNSルックアップを有効にすると、受信メッセージの全てのIPアドレスがDNS解決キューにロードされます。一度に最大200IPアドレスの名前解決ができます。

フリーウェア版では1,2または10スレッドが可能です。

登録正規版では最大200スレッドまで可能です。

25スレッド以上にするとシステム性能に影響します。

注意:

このオプションを**only take effect after a program restart**に変更、またはサービス版ではサービスをストップしたあと、再起動すると有効になります。

送信ホストIPアドレスの解決だけであれば、通常10スレッドが適切です。

メッセージテキストのIPアドレスの解決では、50-100スレッドが適切です。

リアルタイムDNS解決できないほどの大量受信メッセージの場合、DNSオプションを無効にしてください。その代わりに、レポータリングツールで興味のあるログエントリーのサブセットを取り出してください。次にレポータリングツールでIPアドレスをホスト名に変換してください。例えば、全てをリアルタイムに実行する代わりに上位20IPアドレスをレポータリングツールで解決します。多くのユーザーはログファイルエントリーのサブセットに興味があるための、これは有効です。リアルタイムに全IPアドレス解決をすることは資源の無駄使いです。

Setup - DNS Cache (設定 - DNSキャッシュ)

local DNS cache (ローカルDNSキャッシュ)

IPアドレスのホスト名への解決要求の都度DNSサーバーへの問合せが発生します。これは多数のメッセージを受信した時、プログラム、ネットワーク、DNSサーバーへ大きな負荷をかけます。

DNSトラフィックを減少させ、名前解決時間を短縮するにはDNS キャッシュ が使われます。一度ホスト名解決するとその結果が残ります。次のそのアドレスの解決には他のDNSリクエストを出さずに結果をキャッシュから貰います。

フリーウェアライセンスではローカルDNSキャッシュは100エントリー、登録正規版では20,000エントリーです。

View ボタン:

現在のキャッシュエントリーをファイルに出力しノートパッドでその内容を見ます。キャッシュ性能も表示します。

Refresh ボタン:

キャッシュ中の正しいエントリー数を計算します。

Clear ボタン:

ダイナミックなエントリー(DNS参照の結果) を削除します。ファイルからロードされたスタティックエントリーはクリアしません。

Clear Allボタン:

全DNSエントリーをクリアします。スタティックエントリーファイルを読むにはプログラムのリスタートが必要です。

Cache settings (キャッシュ設定)

Flush entries after X seconds:

指定時間後キャッシュから古いエントリーを消去します。デフォルトは1440分(1日)です。1日キャッシュエントリーに残りますが、その後キャッシュから消去されルックアップから再度作られます。

Enable pre-emptive lookup of IP addresses:

各アドレスをシークエンシャルに解決する代わりに、メッセージをプロセスキューに追加する前にIPアドレスを抽出します。アドレス解決を非同期に実行し結果をキャッシュに残します。メッセージが処理される時にはアドレスはすでにキャッシュにあります。DNS解決はマルチスレッドルックアップシステムで同時に100個(フリーウェアモードでは10個)実行します。大量の受信メッセージがあり、そのIPアドレス解決を実行する場合、このオプションをイネーブルにしてください。

Pre-load the cache with static entries from a hosts file:

スタートアップ時、静的ホストエントリーをプログラムがロードします。リストにはタブで区切ったIPアドレスとホスト名が含まれていなければなりません。アドレスはキャッシュにロードされ、スタティックマークがつけられます。有効期限の無いことを意味し、ダイナミックなエントリーの様に消去されません。

サンプルhostsファイルがインストールフォルダーにあります。名前はStaticHosts.txtです。

Hostファイルの例

```
# Static DNS host file
# Each entry must consist of an IP address, a tab, then a host name
# The IP address is in the format aaa.bbb.ccc.ddd
# The host name can be any text value that you like up to 63 characters in length
#
# Comments can be on a separate line and must start with a # character
#
# Example:
# 192.168.1.1 myhost.mycompany.com
#
# NOTE: The IP address and host name MUST be separated with a tab (ASCII chr 9)
#       Spaces will not be recognised as a valid separator

# Default value for localhost
127.0.0.1 localhost

# local machines
192.168.1.2myfunny.valentine.com
192.168.1.5flyme2.themoon.com
```

Setup – Modifiers (設定 – モディファイアー)

メッセージを受信すると、各種の修正が行われます。メッセージは短縮、不正な優先度は修正され、さらにCR/LFコードは削除されます。

Syslog message modifiers (Syslogメッセージモディファイアー)

Remove imbedded date and time from Cisco messages

Ciscoデバイスはメッセージに自分の時刻スタンプを追加します。これらの余分な時刻スタンプを削除し、スペースの節約と読みやすいログファイルにすることができます。

このオプションは特定のCiscoメッセージフォーマットをさがして動作します。将来はCisco PIXファイアウォールメッセージを含む全てのCisco時刻フォーマットに対応します。

Allow messages with no priority (use default priority)

ルータやホストはメッセージにプライオリティを含まない場合があります。このような場合メッセージにデフォルトプライオリティを設定することができます。このボックスをチェックしドロップダウンリストからデフォルトプライオリティを設定してください。

正常なSyslogメッセージテキストでは先頭にプライオリティが入ります。

例. <100>This is a test message

標準Unixプライオリティコードでのプライオリティは0~191です。

Maximum message length (bytes)

受信メッセージの最大メッセージ長を制限します。短いメッセージにしたい場合この値をデフォルトの4096より小さくできます。

ハッカーから送られる、あるいはエラーで送られる大きなメッセージを拒否することができます。

あるSyslog Daemonは大きなパケットを受信するとクラッシュします。このオプションはプログラムが受信し処理するパケットのサイズを制限します。

Syslog RFC 3164 は正常なメッセージ長は1024バイトを超えないことを定義しています (パケットヘッダーは除く)

Allow messages with priority > 191 (use default priority)

Syslogメッセージの先頭にプライオリティがついています。通常Unixやルータでは0~191です。時にはデバイスが191以上の値を送ります。191以上ではプライオリティの標準定義はありません。

このオプションでデフォルトプライオリティに加え191以上のプライオリティを追加します。

Remove CR/LF from end of messages

あるルータやホストはメッセージの終わりがCR/LFであり、ログファイルに2行の空白行ができます。

このオプションで全てのCR/LFを除きます。

Replace non-printable characters with <ASCII value>

ルータやホストは制御文字を含むメッセージを送ります。マルチラインメッセージはCRおよびLFを含みます。このオプションで制御文字の代わり、同等のASCII文字を表示します。

例えば、CRの代わり、<013>で置き換えます。

Parse RFC 3164 headers and use imbedded time and date

Setup – Scripting (設定 – スクリプト作成)

カスタム統計フィールドに名称と初期値を設定しスクリプトファイルと統計レポート内で使います。

スクリプト用に16のカスタム統計フィールドがあります。これらの値は固定されており他のスクリプトフィールドの様に消去できません。

カスタム統計値はCounterタブのStatisticsウィンドウで見ることができます。指定したフィールド名は統計ウィンドウとデイリー統計e-mailで使われます。

統計カウンターの初期値は任意の値にできます。デフォルトは0です。例えばデクレメントカウンターとして初期値を1000にしスクリプトアクション実行毎にデクレメントすることができます。

名称と初期値はプログラムのスタート時に適用されます。プログラムでフィールドをこれらの値で再初期値化するにはFile|Debug options|Initialize custom statistics メニューを使います。あるいはメインsyslogウィンドウからCtrl-F9を押します。

Setup – Appearance (設定 – 概観)

Wallpaper (壁紙)

表示の背景イメージです。サンプルとしてペーパースタイルイメージが提供されます。

Setup - E-mail options (設定 – E-mailオプション)

E-mail setup options (設定 – E-mailオプション)

Send syslog alarm messages to:

アラーム閾値を超えるとe-mailでアラームメッセージが送信されます(アラーム閾値はAlarmで設定します)。

アラームが発生した場合に通知すべきe-mailアドレス(複数可)を入力します。E-mailアドレスはカンマで区切ります。

例 noc@company.com, helpdesk@company.com, pager123@company.com

テキスト左側のチェックボックスで警告e-mail送信のイネーブル、ディセーブルを決定します。

Testをクリックしアラームメッセージ送信をテストできます。

Send syslog statistics to:

毎晩、真夜中に毎日の統計情報がメールで送られます。ここにはログファイル容量、アーカイブドライブのディスク空き容量、メッセージ総数、送信元のブレイクダウン、FacilityとLevelなどが含まれます。

Courier new フォントを固定するのが最も適しています。

Short alarm messages (for pagers)

チェックすると、サブジェクト行だけが送信されます。メッセージ本体は使われません。メッセージをポケットベルで送信する時や限られた表示スペースの時有効です。

Keep a log file of e-mail activity

e-mailで警告や統計を送信する場合、どのメッセージを誰に送ったかというログを残すことができます。

ログファイル名はSendMailLog.txt でありプログラがインストールされたところと同じディレクトリにあります。

このファイルをノートパッドで見るにはView logボタンを使います。

既存のログファイルを消去し、新しいログファイルでスタートするにはdelete log ボタンを使います。

Enable verbose logging

メールが正常に送られない時有効です。プログラムからメールサーバーへの送信情報がログファイルとして残ります(メッセージ内容はありません)

注: 多数のメッセージが送信される時、このオプションを使うと多くのディスクスペースが使われます。

Hostname or IP address of SMTP mail server:

SMTPサーバーのホスト名かIPアドレスです。ローカルサーバーもしくはISPのサーバーです。

メールサーバーのホスト名は通常mail.company.com 又は smtp.company.comのような名称です。

ローカルSMTPサーバーが無い場合はhttp://www.ocloudsoft.com で可能なMail Directを使うことをお奨めします。

Valid 'from' e-mail address on SMTP server:

このフィールドでは有効な応答アドレスを使ってください。メールの送信エラー時SMTPサーバーはここにメッセージを送ります。

あるSMTPサーバーはドメイン名を終わりに要求しますが、他のものは要求しません。

ここで使うアドレスは受信e-mailのmessage from表示と同じでなくてはなりません。

アドレスの後ろにもっと馴染み深い名前を()で指定してもかまいません。これはメールクライアントのFromに表示されます。

例 noc@company.com (Syslog Server)

上の例で名前のSyslog Serverは受信メッセージのFromフィールドに現れます。あるSMTPサーバーはこのフォーマットをサポートしませんので、e-mailアドレスのみを使います。

SMTP port:

SMTPサーバーの受信ポートが非標準であればここにそのポート番号を指定します。普通SMTPサーバーはポート25です。ある会社はセキュリティ上の理由でこの数字を変更します。数字は1~65535です。

Timeout:

プログラムがSMTPサーバーの応答を待つ時間です。SMTPがダイヤルアップが非常に混んでいる場合、デフォルトの30秒より大きくします。値は1~240までです。

SMTP Username and Password:

SMTPサーバーがe-mail受付前に認証が必要な場合に使います。多くのSMTPサーバーではこのオプションは不要です。

左のチェックボックスをチェックし、SMTPのユーザー名とパスワードを入力すると認証が可能になります。この値はネットワーク管理者、SMTPサーバープロバイダ、ISPから提供されます。

認証でPOP before SMTP オプションを使わなければならない時、フリーウェアのPOPメールボックスチェッカーをダウンロードし使ってください。新しいメッセージを5分ごとにチェックしその後SMTPメールが送られます。POP before SMTP 認証は将来のバージョンに追加されます。

アラームメッセージの例

Syslog Alarm: 2198 messages received this hour.
The current maximum threshold is set at 3 messages per hour.
This could indicate a problem, please check the log files and syslog statistics below.

```
///      Kiwi Syslog Daemon Statistics      ///
```

```
24 hour period ending on: Fri, 26 Jul 2002 15:39:16 +1200
Syslog Daemon started on: Wed, 17 Jul 2002 11:39:53
Syslog Daemon uptime:    9 days, 3 hours, 59 minutes
-----
```

```
+ Messages received - Total:          361965
+ Messages received - Last 24 hours:  37964
+ Messages received - Since Midnight: 26530
+ Messages received - Last hour:      2821
+ Messages received - This hour:      2198
+ Messages per hour - Average:       1582

+ Messages forwarded:                 3063
+ Messages logged to disk:            26530

+ Errors - Logging to disk:           0
+ Errors - Invalid priority tag:      0
+ Errors - No priority tag:           0
+ Errors - Oversize message:          0

+ Disk space remaining on drive C:    59505 MB
-----
```

Breakdown of Syslog messages by sending host

```
+-----+
| Top 20 Hosts      | Messages | Percentage |
+-----+-----+-----+
| pix_firewall_inside|    26530 |    100.00% |
+-----+-----+-----+
```

Breakdown of Syslog messages by severity

```
+-----+
| Message Level    | Messages | Percentage |
+-----+-----+-----+
| 0 - Emerg        |         0 |    0.00%   |
| 1 - Alert        |         0 |    0.00%   |
| 2 - Critical     |         0 |    0.00%   |
| 3 - Error        |        123 |    0.46%   |
| 4 - Warning      |         0 |    0.00%   |
| 5 - Notice       |        715 |    2.70%   |
| 6 - Info         |       25692 |   96.84%   |
| 7 - Debug        |         0 |    0.00%   |
+-----+-----+-----+
```

End of Report.

統計メッセージの例

```
///      Kiwi Syslog Daemon Statistics      ///
```

```
24 hour period ending on: Fri, 26 Jul 2002 00:00:01 +1200
Syslog Daemon started on: Wed, 17 Jul 2002 11:39:53
Syslog Daemon uptime:      8 days, 12 hours, 19 minutes
-----
+ Messages received - Total:          335435
+ Messages received - Last 24 hours: 35206
+ Messages received - Since Midnight: 35967
+ Messages received - Last hour:      1149
+ Messages received - This hour:      366
+ Messages per hour - Average:        1467
+ Messages forwarded:                  0
+ Messages logged to disk:             35967
+ Errors - Logging to disk:            0
+ Errors - Invalid priority tag:       0
+ Errors - No priority tag:            0
+ Errors - Oversize message:          0
+ Disk space remaining on drive C:     59573 MB
-----
```

Breakdown of Syslog messages by sending host

Top 20 Hosts	Messages	Percentage
pix_firewall_inside	35967	100.00%

Breakdown of Syslog messages by severity

Message Level	Messages	Percentage
0 - Emerg	0	0.00%
1 - Alert	0	0.00%
2 - Critical	0	0.00%
3 - Error	69	0.19%
4 - Warning	0	0.00%
5 - Notice	731	2.03%
6 - Info	35167	97.78%
7 - Debug	0	0.00%

End of Report.

Setup - Alarm thresholds (設定 - アラーム閾値)

Notify by Mail (メールで通知)

最低もしくは最高の閾値を超えるとアラーム連絡リストの受信者にe-mailが送られます (e-mailオプションからセットされる)。

e-mailメッセージはアラームメッセージの説明であり、閾値を超えたことや、現在の閾値などを説明します。

最終時間の統計にはさらに情報が含まれます。

Audible Alarm (音で通知)

正規登録版でのみ可能です。

最低もしくは最高閾値を超えるとSyslogはメインSyslog Daemonのステータスバーの赤く点滅する警告ベルをダブルクリックして警告をキャンセルするまで1秒に1回警告音を鳴らします。

Play sound file をイネーブルにするとキャンセルされるまで5秒に1回鳴ります。

警告音をキャンセルするには赤く点滅する警告ベルアイコンをダブルクリックしてください。

Run Program (プログラム実行)

正規登録版でのみ可能です。

最低もしくは最高閾値を超えると任意の外部プログラムを実行します。コマンドラインパラメータで実行するプログラムに情報を渡すことができます。

外部プログラムには次の値を渡すことが可能です。

%Min = 1時間あたりの最小メッセージ警告閾値
%Max = 1時間あたりの最大メッセージ警告閾値
%LogMax = ログファイル最大容量警告閾値
%LogSize = ログファイルの現在の容量
%MsgCount = 直前1時間の受信メッセージ

例

Pager.exe "555-1234" ,"Syslog - Warning, lots of messages received, Max set at %Max but received %MsgCount (log files size=%LogSize)"

または

EmailProg.exe "To:admin@company.com", "Subject:Time to archive the logs (Now %LogSize)"

外部プログラムが期待通りに実行されたか確認するためTestボタンを使ってください。

スペースを含むファイル名やパスは"で囲んでください。

Setup - Input options (設定 - 入力オプション)

Setup - Input options (設定 - 入力オプション)

プログラムはsyslogメッセージをUDPまたはTCPで受信できさらにSNMP Version1又は2cトラップの受信もできます。

デフォルトではUDP514がイネーブルです。これはsyslog配信の最も普通の方法です。

あるファイウォール (Cisco PIX) や他のsyslogコレクタはTCPでsyslogを送信します。Cisco PIXはTCP1468を使います。TCP受信はデフォルトではイネーブルではありません。

SNMP Version1と2cの受信とデコーディングもサポートされますがデフォルトではイネーブルではありません。普通のSNMPトラップ受信ポートはUDP162です。

3種類のリスソケット、UDP、TCPおよびSNMPがあります。

さらにkeep aliveメッセージを受信ストリームに挿入しトラフィックのシミュレートが可能です。

Inputs - UDP (入力 - UDP)

通常Syslog Daemon はUDPポート514でsyslogメッセージを受信します。他のポートで受信する場合は1~65535の任意の数値を入力出来ます。ポートを514から変更するとsyslogメッセージを送信するデバイスもポート番号を変えなければなりません。

Syslog Daemon でUDP syslogメッセージ受信を停止するにはListen for UDP Syslog messages チェックボックスのチェックをはずしてください。Kiwi Syslog Daemon は一度に一つのUDPポートのみ受信します。将来は複数UDPポート受信が可能になります。

Bind to Address:

デフォルトでは、UDP ソケットは全ての接続されたインターフェイスのメッセージを受けます。特定のインターフェイスに限定するときは **Bind to address** フィールドでIPアドレスを指定することができます。そうでなければこのフィールドは空白にしてください。(**Bind to address** フィールドが空白であれば全てのインターフェイスから受信します。多くの場合これが最適です)。例えば、コンピュータにルーティングされていない二つのインターフェイス192.168.1.1 と192.168.2.1があれば192.168.1.1 インターフェイスにだけバインドすることができます。この場合他のインターフェイスへのsyslog メッセージは無視されます。

Inputs – TCP (入力 – TCP)

Syslog ロギングは伝統的にUDPポート514でおこなわれています。

UDPはコネクションレスプロトコルであり、不確実性が内在します。UDPでは応答、エラー検出、シーケンス管理、喪失パケット再送などは行いません。

Cisco PIX などはTCPによるsyslog プロトコルをサポートします。TCP はコネクション向きです。あて先ホストが存在することが保証されます。送信デバイスが初期化されると、あるいは最初のsyslogメッセージが送信される前に接続が確立されます。最初に3ウェイハンドシェイクを行い、全てのパケットはサーバーが受信し次の送信前に応答が返されますので、TCPを使うと遅くなります。TCPプロトコルは信頼性とエラー補正を提供します；メッセージがsyslog サーバーに確実に送信されたことが確認できます。

PIX ファイアーウォールサポートを参照してください。

Cisco PIX はポート1468を使います。デフォルト動作は、Its default behavior is that if it cannot connect to the syslog サーバーへの接続ができなかった場合、全てのネットワークトラフィックがブロックされます。

Cisco Pix ファイアーウォールについての情報は: www.cisco.com/univercd/cc/td/doc/product/iaabu/pix

Inputs – SNMP (入力 - SNMP)

このプログラムはSNMP v1とv2トラップを受信します。トラップはデコードされ正規syslogメッセージと同様に処理されます。

Listen for SNMP traps:

デフォルトは無効です。ボックスをチェックしてSNMP受信を有効にします。

UDP port:

SNMPトラップ受信のためのUDP ポートです。通常トラップは162ポートに送信されます。1から65535までの値を入力できます。162以外を選択した場合は、トラップ送信デバイスも同じポートを指定します。

Specified fields:

どのSNMPフィールドをデコードし入力メッセージに追加するかを選択します。フィールド横のボックスをチェックし有効にします。フィールド名の上をクリックしドラッグすることによりメッセージをデコードする順序を変更できます。

Community:

トラップメッセージに含まれるパスワードのようなものです。通常この値は"public", "private" あるいは"monitor"に設定されています。

Enterprise:

SNMPトラップのMIB企業を表す小数点付きの数値(1.3.6.1.x.x.x.x) です。このフィールドはv1トラップにのみ適用されます。v2トラップでは企業値はメッセージの2番目の変数です。

Uptime:

メッセージ送信デバイスのシステムアップタイムです。値はデバイスが再起動すると0にリセットされます。小さい値は最近デバイスがウォームあるいはコールドスタートされたことを示します。このフィールドはv1トラップにのみ適用されます。v2トラップではメッセージの最初の変数がシステムアップタイムです。

Agent address:

送信デバイスのIPアドレスです。

Trap type:

2種類のトラップタイプです。Generic タイプとSpecific タイプです。これらのフィールドはv1トラップにのみ適用されます。6種類のGeneric タイプとトラップが定義されています。Generic タイプが6に設定されていると企業タイプとトラップであることを示します。この場合はSpecific トラップ値を考慮しなければなりません。

Version:

受信トラップのバージョンです。このプログラムはv1と2cをサポートします。

Message:

すべての変数で構成されます。多くのトラップは1以上の変数結合を含みます。変数が8進文字タイプであれば、平文としてみることができます。多くの変数はカウンターや整数値で表されます。この場合、その値をMIBシンタックスとしてチェックしてください。

Syslog priority to use:

各受信SNMP メッセージは内部で標準syslog メッセージに変換されます。標準syslog メッセージ同様フィルターできることになります。SNMP トラップはメッセージfacility やlevelがありませんのでデフォルト値を適用しなければなりません。この値をルールエンジンで使用することができます。たとえば、すべてのトラップをLocal0.Debugとすることができます。プライオリティフィルターでこのfacility とlevel を捕らえ、特定のアクションを実行するフィルターを作成することができます。

SNMP field tagging:

このドロップダウンリストでデコードされたフィールドをどのようにメッセージに変換するかを指定します。デフォルトでは、"fieldname=value" オプションが使われます。これは、この後のログの解析を容易にします。タノプションはXML、カンマ区切り、[] 区切りなどです。

fieldname=value オプションタグによるメッセージ例です。

```
community=public enterprise=1.3.6.1.2.1.1.1 enterprise_mib_name=sysDescr uptime=15161 agent_ip=192.168.0.1
generic_num=6 specific_num=0 version=Ver1 generic_name="Enterprise specific" var_count=01 var01_oid=1.3.6.1.2.1.1.1
var01_value="This is a test message from Kiwi Syslog Daemon" var01_mib_name=sysDescr
```

スペースのみを含む値は引用符 ("") で囲まれます。

Use LinkSys Display filter:

LinkSys Display フィルターは表示からすべてのPPP メッセージを除去します。PPP メッセージは通常通りファイルには記録されます。この機能はLinkSys ネットワークデバイスからのロギングでのみ有効です。

Perform MIB lookups:

この機能はversion 7.0.3 で追加され将来も開発を続けます。既知のオブジェクトIDとそのテキスト名がプログラム中のデータベースに含まれます。非常に一般的なCisco, 3Com, Allied Telesyn, SonicWall, Nokia, Checkpoint, BreezeCom, Nortel やSNMP MIB-IIを処理します。

MIB データベースファイルはファイル名: KiwiMIBDB.kmf のフォルダーInstallPath\MIBs にあります。

このデータベースは圧縮されたテキストファイルであり、35,000以上のMIB ツリーエントリーが含まれます。多くのMIB ファイルは使用できるトラップ情報の5%以下しか含まず、このプレコンパイル方法は標準MIBコンパイラー/パーサー利用において参照時間、ディスクスペースハッシュテーブルメモリーを大幅に節約します。

追加MIB 解決値を追加するのであれば、協力します。Zip圧縮したMIBファイルをsupport@kiwisyslog.comあるいはsupport@jtc-i.co.jpまで送ってください。新しいデータベースファイルをコンパイルし更新結果を返送します。すべてのOIDを参照できるようにUnknown_OID_list.txt ファイルも含んでください。

When creating the MIB データベースを作成するとき、MIBファイルからすべてのトラップ、注意書き、参照変数がパースされます。オブジェクトが正しく参照されないときは追加されません。この場合は、知るべきことはOID 値であり、それが含まれることを確認できます。詳細は次のセクションを参照してください。

Log failed lookups to debug file:

OID 値がデータベースに無く、"log failed lookups" オプションがチェックしてあれば、OID 値はデバッグファイルに記録されます。ファイルはInstallPath\MIBs にあり、その名前は Unknown_OID_list.txtです。このファイルをzip圧縮しsupport@kiwisyslog.comあるいはsupport@jtc-i.co.jpまで送ってください。次のデータベースリリースにこれらの値を追加します。

Beep on every message received (メッセージ受信時ピーブ音)

このオプションをイネーブルにするとsyslogメッセージ又はSNMPトラップ受信ごとにピーブ音が鳴ります。フィルターで表示やロギングをブロックしてもピーブが聞こえます。このオプションはデバッグ時メッセージを受信したことを知るのに有効です。

* 全てのメッセージが来るとピーブ音を聞くことになりませんがメッセージをディスクにロギングするのに問題があるかどうかはチェックしません。問題の詳細はエラーログをチェックしてください (Viewメニューから)。メッセージが指定されたログファイルに書かれていないと、ピーブは問題があることを教えます。

Cisco PIX ファイアーウォール(TCP)

Cisco PIX ファイアーウォールはUDPの代わりに、安全な接続向けのTCPを提供します。PIXのデフォルトTCP ポートは1468です。このポートは1 から65535の任意のもので、その場合Cisco PIX は設定が必要です。

TCP はコネクション向けであり、PIXはログデバイス(Kiwi Syslog Daemon) がメッセージを受信できないことを知ることができます。例えばディスクがフルの場合です。PIX にフィードバックするには、Syslog Daemon は接続をクローズしメッセージの受信ができませんようにします。Kiwi Syslog Daemon はログドライブの可能なディスクスペースをチェックし空きエリアの割合が閾値より低ければPIXへのTCP接続を切断します。Kiwi Syslog Daemon がPIXからの接続要求を再度受け付けるまでPIXはこれ以上トラフィックを送れません。空きディスクの割合が閾値より高くなれば、Kiwi Syslog Daemon はPIXからのログメッセージを受け付けトラフィックは再び流れ始めます。

警告: ディスクチェックを有効にし、ディスク使用量が閾値に達すると、全てのPIXトラフィックがストップします。ユーザーのインターネットアクセスができません。インターネットアクセスよりログの整合性が重要な場合だけこのオプションを有効にしてください。

Inputs - Keep-alive (入力 – Keep alive)

keep alive メッセージの動作

Keep alive メッセージは等間隔でsyslog受信ストリームに入ります。これらはスクリプトアクションのトリガーとして、または等間隔でログファイルにスタンプするために使われます。

keep alive メッセージは他の受信メッセージと同等に扱われruleエンジンで処理されます。Rule設定によりますが、メッセージはディスクに書かれ、表示され、他のsyslogサーバーにフォワードされます。

keep alive メッセージが他のsyslogサーバーにフォワードされる時、I am still alive and well メッセージとして他のサーバーに全て順調であることを告げます。リモートサーバーでkeep alive メッセージが失われたことを検出するフィルターを設定し警告をあげることが出来ます。

ファシリティ、レベル、ホストIPアドレスやテキスト値を指定しメッセージプロパティを変更できます。

keep-alive メッセージはスクリプトでvarInputSource フィールドをチェックし検出することができます。keep-aliveメッセージは "3"を使います。

Enable keep-alive messages:
デフォルトはディセーブルです。keep-aliveメッセージ を入れるにはボックスをチェックしてください。

Frequency:
入力ストリームに入れるkeep-aliveメッセージの頻度を設定します。デフォルトは60秒に1回ですが1から86400秒(1日)の範囲で指定できます。

Syslog facility:
keep-aliveメッセージのファシリティを設定します。このファシリティのみで動作するようルールのパライオリティフィルターを設定することが出来ます。通常このオプションはSyslogプログラムがメッセージを生成していることを示すSyslogに設定されます。

Syslog level:
keep-aliveメッセージのレベルを設定します。このファシリティ/レベルの組み合わせでのみで動作するようルールのパライオリティフィルターを設定することが出来ます。通常このオプションはinformationalメッセージであることを示すinfoに設定されます。

From IP Address:
keep-aliveメッセージの送信元IPアドレスを設定します。その範囲は1.1.1.1 ~ 255.255.255.255です。デフォルトは127.0.0.1にしてください。指定されたアドレスはルール設定でフィルターされます。

Message text:
keep-aliveメッセージのテキストです。任意の文字列が可能です。デフォルトはKeep-alive message です。

keep alive メッセージの使用法:

Scripting use.

ルール設定にRun script が含まれるとアクションはメッセージが到着した時とルールエンジンが処理する時だけ実行されます。時間でアクションを実行する時はkeep-aliveメッセージをルールエンジンのトリガーとして使えます。

```
Rules
Rule: MyScript
  Filters
  Priority: Match Syslog.Info only
  Actions
  Action: Run script
  Action: Stop processing (Exits the rule engine here)
Other Rules here...
```

keep-alive メッセージはスクリプトでvarInputSource フィールドをチェックし検出することができます。keep-aliveメッセージは "3"を使います。

ビーコンとして他のホストにフォワーディング

keep-aliveメッセージは全てOKであることを告げるために、他のホストにフォワードすることが出来ます。

Rules

Rule: Send keep alive message

Filters

Priority: Match Syslog.Info only

Actions

Action: Forward to host (send to another host via a syslog message)

Action: Stop processing (Exits the rule engine here)

Other Rules here...

Stop processing アクションを使用していますので、keep-aliveメッセージはこれ以降のルールには見えません。プライオリティフィルターは Syslog.infoに合致したらアクション(フォワードメッセージ)を実行、次にルールエンジンはメッセージを捨て次の到着を待ちます。

Setup – Display (設定 – 表示)

Always on top (常時トップ)

Kiwi Syslog Daemon は常に最も上のウィンドウであることを確認して下さい。

Rows of scrolling display (スクロール表示の行数)

スクロール画面の行数を設定します。

通常は40行に設定されます(メッセージが全画面表示されます)

フリーウェア版では10~50を選択できます。

正規登録版では5~1000を選択できます。

注 – スクロール画面の列数を多くすると画面アップデート時間がかかります。

新しいメッセージは表示された全てのメッセージをシャッフルし最後のメッセージを捨てます。このシャッフルにはCPUが使われますので多くの列のシャッフルにはよりCPUが消費されます。

Minimize to System Tray on start-up (スタートアップでシステムトレイを最小化)

Kiwi Syslog Daemon がスタート後にシステムトレイを最小化したい時チェックします。

Kiwi Syslog Daemon をWindowsスタートアップで実行し目障りにならないようシステムトレイに移すのに有効です。

Use 3D titles (3Dタイトルを使用)

メイン表示とプロパティ画面のタイトルに3Dテキスト(影付き)を使います。

Use dd-mm-yyyy date format (dd-mm-yyフォーマット使用、非US フォーマット)

通常Kiwi Syslog Daemon はUS日付フォーマットmm-dd-yyyyを使います。

ニュージーランド、オーストラリア、ヨーロッパ式日付フォーマットdd-mm-yyyyを使う時チェックしてください。

日付フォーマットは表示で有効です。ログファイルの日付フォーマットはログフォーマットの選択で選択されます。

Show messages per hour in title bar (タイトルバーに1時間の受信メッセージ数を表示)

アクティブになった時、タイトルバーに1時間の受信メッセージ数を表示します。

Blink System Tray Icon when receiving messages (メッセージ受信によるシステムトレイアイコンの点滅)

メッセージを受信すると最小化したシステムトレイアイコンが青と緑でブリンクします。

Word wrap (ワードラップ)

Syslogウィンドウサイズより大きなメッセージをラップし、スクローリング無しで内容を読めるようにします。

Adjust column widths automatically (表示画面幅の自動調整)

メッセージが到着するとテキストに合うように列数を自動的に調節します。

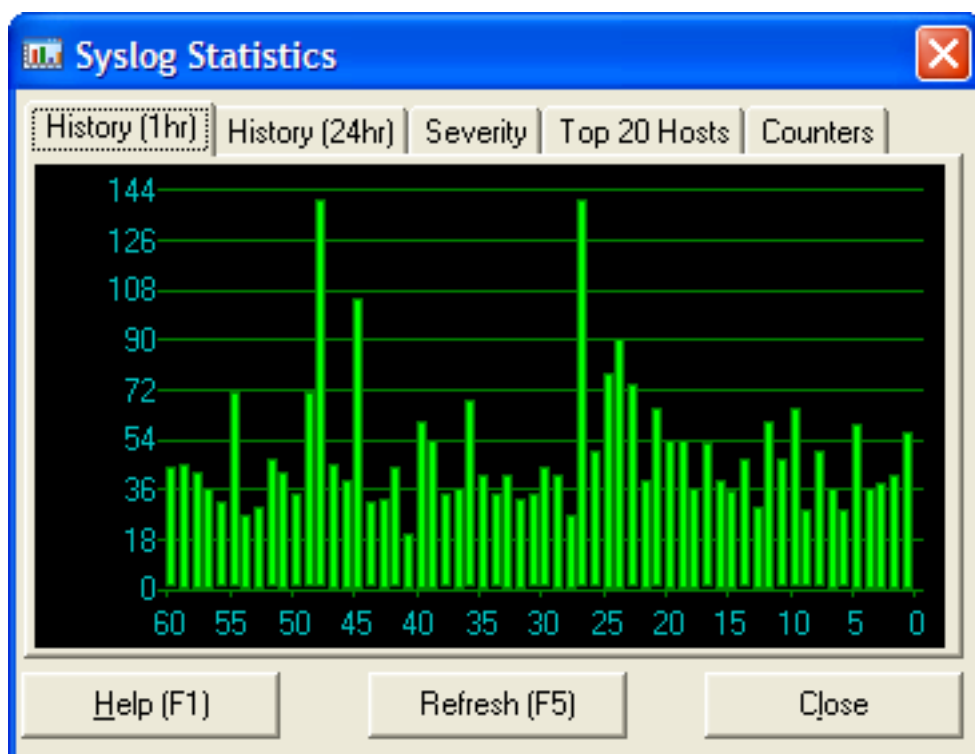
テキストが読み易くなります。多くのテキストを読むにはフォントサイズを小さくします。View | Choose font で行います。

Syslog statistics window (Syslog 統計ウィンドウ)

Syslog statistics window (Syslog 統計ウィンドウ)

メインKiwi Syslog Daemon 画面からView | View Syslog Statistics メニューを選択もしくは Ctrl-Sを押します。

Syslog Statistics 画面が開きます。



Syslog 統計は10秒ごとに更新されます。RefreshあるいはF5ボタンで、即座に更新できます。

1 Hour history (1時間表示)

直近60分間のトラフィックをバーチャートで表示します。各バーは1分間の受信メッセージ数です。チャートは右から左にスクロールします。チャートの左端に1時間前のトラフィックが表示されます。1番右のバーは現在のトラフィックです。

24 Hour history (24時間表示)

直近24時間のトラフィックをバーチャートで表示します。各バーは1時間ごとの受信メッセージ数です。チャートは右から左にスクロールします。チャートの左端に24時間前のトラフィックが表示されます。1番右のバーは現在のトラフィックです。

Severity (セベリティ)

Severity テーブルはプライオリティによるメッセージのブレイクダウンです。0-Emergency は最もseverityが高く、問題解決用の7-Debug タイプのメッセージは最も低くなっています。

テーブルにはメッセージ数と全トラフィックに対する割合が示されます。

ヘッダーをクリックするとその欄のソートを行います。もう一度クリックすると逆のソートを行います。

Top 20 Hosts (上位20送信ホスト表示)

送信ホストのメッセージのブレイクダウンです。ホストごとのメッセージ数と全体に対する割合が表示されます。

ヘッダーをクリックするとその欄のソートを行います。もう一度クリックすると逆のソートを行います。

特定ホストが大量のトラフィックを発生したり、パターンが変化することはそのデバイスに問題があることを示します。

Counters (カウンター表示)

トラフィックとエラーを示します。平均メッセージ数は警告を出す閾値の設定や、どのくらいのsyslogがあるのかを予測するのに役立ちます。

多くのカウンターは直近24時間 (現在の時刻からの)の値を表示します。他は深夜(0:00)からの値です。

1時間はプログラムスタートを0とし、実際のHH:MM:SS 時刻からではありません。プログラム実行時間はプログラムアップタイムカウンターをチェックしてください。

Messages - Total:

プログラムスタート時からの受信メッセージ数です。この値はプログラムかサービスのリスタートでリセットされます。

Messages - Last hour:

直近1時間の受信メッセージ数です。時間はプログラムスタート時からカウントされます。プログラム実行が60分以内であればこの値は0です。1時間経過していれば、値は最終1時間の受信メッセージ総数です。次の1時間が経過するまでその値が保たれます。

Messages - This hour:

直近1時間前からの受信メッセージ数です。時間はプログラムスタート時からカウントされます。この値は毎時0にリセットされ、新しいメッセージを受信すると増えます。

Messages - Last 24 hours:

直近24時間(現在を基準に)の受信メッセージです。この値は直近23時間の受信メッセージの合計および直近1時間の受信メッセージ数です。各時間のはじめに、最近23時間の値がシャッフルされますのでその値は捨てられます。この値は最近1時間に受信されたメッセージで再計算されます。その値の計算式は: 直近(1 ~ 23) + この時間のメッセージです。

Messages - Average:

過去24時間における1時間あたりの平均受信メッセージ数です。各時間のはじめに再計算されます。最初の1時間経過後、値は1時間に一度更新されます。

Messages - Forwarded:

"Forward message" アクションで他のsyslogコレクターにフォワードされたメッセージ数です。このカウンターはデイリー統計の送信後すぐリセットされます。デイリー統計は通常深夜に送信されるので、その値は深夜からのカウントになります。

Messages - logged to disk:

"Log to file" アクションでディスクに記録されたメッセージ数です。このカウンターはデイリー統計の送信後すぐリセットされます。デイリー統計は通常深夜に送信されるので、その値は深夜からのカウントになります。

Errors - logged to disk:

ディスクに記録されたプログラム内部エラー数です。エラーの原因はログファイルのアクセス不能あるいはプログラム内部エラーにあります。このカウンターはデイリー統計の送信後すぐリセットされます。デイリー統計は通常深夜に送信されるので、その値は深夜からのカウントになります。値が0でなければ、エラーログ(View | Error log メニュー) を見てください。

Disk space remaining:

ディスクスペースの残量をMBで示します。監視するドライブはAlarms | Disk space monitor 設定オプションで設定できます。デフォルトでは C がマウントされています。

CustomStats:

custom statistics 値はCounters タブから見るができます。これらの値は"Run Script" アクションで変更できます。このstatistics counters でどのような値の係数と表示でも可能です。

カウンター名を意味がわかるようにするには、Scripting 設定オプションでカウンター名と初期値を設定できます。

Kiwi Syslog Daemon サービス版

Kiwi Syslog Daemon サービス版

サービス版実行における推奨条件

Windows NT Version 4 (サーバー又はワークステーション)SP4 以上。 またはWindows 2000 プロフェッショナル又はサーバー
Microsoft Internet Explorer Version 5.x
Kiwi Syslog Daemon NT サービス版 6.3.2 以上
RAM 128MB 以上
画面解像度 800 x 600, 256 色 以上

Installing the Service edition (サービス版をインストールする)

NTサービスとしてKiwi Syslog Daemon をインストールするには注意が必要です

。新しいバージョンをインストールする前に既存バージョンをストップしアンインストールされていることを確認して下さい。

インストールにあたってはinstallation .exe をダブルクリックし実行します。

セットアッププログラムによりKiwi Syslog Daemon Service Manager がインストールされます。

インストール完了後、スタートメニューからプログラムを起動します。メインSyslog daemon 画面が表示されます。

Manage メニューでNTサービスをコントロールします。

サービスのインストールは**M**anage | **I**nstall the Syslogd Service で行います。

インストールが成功したか失敗したかを示すメッセージが表示されます

。失敗した場合、すでに他のバージョンがインストールされていた可能性があります。

スタート|実行 メニューまたはコマンドラインでサービスをインストールするには次のように入力します。

C:¥Program files¥Syslogd¥Syslogd_Service.exe -install

サービスのアンインストールは -uninstall スイッチを使います。

C:¥Program files¥Syslogd¥Syslogd_Service.exe -uninstall

サービスがインストールされたらスタートします。

サービスは次にNTをリブートすると自動的に立ち上がります。手動で立ち上げるには **Manage | Start the Syslogd service** メニューを使います。あるいは**Ctrl + F3** でも可能です。

サービスをコマンドラインでスタートさせるには次のように入力します。

```
C:¥>net start "Kiwi Syslog daemon"
```

下記の内容が表示されます。

```
The Kiwi Syslog Daemon service is starting.  
The Kiwi Syslog Daemon service was started successfully.
```

コマンドラインでサービスをストップさせるには次のように入力します。

```
C:¥>net stop "Kiwi Syslog Daemon"
```

下記の内容が表示されます。

```
The Kiwi Syslog Daemon service is stopping.  
The Kiwi Syslog Daemon service was stopped successfully.
```

注: サービスがストップするまで約20秒かかります。

NTコントロールパネルのサービスアプレットからNTサービスをコントロールができます。

サービスをインストールしスタートしたら、Pingでオペレーションのテストが可能です。

Manage | Ping the Syslogd service メニューを使います。

サービスがSyslogメッセージを受信するかは**Ctrl + T** でlocalhostにテストメッセージを送信することで確認できます。

次のような表示があります：

```
Kiwi Syslog Daemon - Test message number 0001
```

メッセージが表示されない場合、**File | Properties** メニューのDisplayで確認します。

サービス版を管理する

Kiwi Syslog Daemon Service Manager からSyslogdサービスの管理とコントロールができます。

Manageメニューの部分参照してください。

サービス版の問題解決

動かない時のチェック項目です-

1). サービスにPingできるか？

Manage | Ping Syslogd service メニューを使います

2). 自分自身へのテストメッセージ送信と受信はOKか？

Syslog Service Manager から**Ctrl + T** でテストメッセージをlocalhostに送信する。

3). ローカルマシンからメッセージ送信テストをする

www.kiwisyslog.com からKiwi Syslog Message Generator をダウンロードする

Kiwi Syslog Daemon NT サービスのアップグレード

Kiwi Syslog Daemon NT サービスのアップグレード

Kiwi Syslog Daemon の新バージョンがリリースされたら最新機能を入手しバグフィックスするためアップグレードしてください。

最新バージョンはwww.kiwisyslog.comあるいはwww.jtc-i.co.jpから入手できます。

アップグレード前に既存バージョンを削除してください。

既存バージョンの削除

- 1). Service Managerからサービスをストップする
Manage | Stop the Syslogd service メニューを使う
- 2). Service Managerでサービスをアンインストールする
Manage | Uninstall the Syslogd service メニューを使う
- 3). Service manager プログラムをクローズする
- 4). アプリケーションをアンインストールする (新バージョンをフルインストールする場合)。
新バージョンがパッチやアップグレードの場合アプリケーションの削除は実行しません(アップグレードやパッチは.exe だけでありフルセットアップではありません)。
コントロールパネルのアプリケーションの追加と削除を使います。

新バージョンのインストール

- 1). Kiwi Syslog Daemon の最新NTサービス版をダウンロードします。
- 2). 新バージョンをインストールします。
- 3). スタートメニューからSyslogd Service Manager を実行します。
スタート | プログラム | Kiwi Syslog Daemon | Kiwi Syslog Daemon Service Manager
- 4). デフォルトAction設定の使用でYesかNoを選びます。
以前の設定をそのまま使う時はNoを選びます。
- 5). Syslogd サービスをインストールします。
Manage | Install the Syslogd service メニューを使います。
- 6). Syslogd サービスをスタートします
Manage | Start the Syslogd service メニューを使います
- 7). Pingで新しいインストールをチェックします。
Manage | Ping the Syslog service メニューを使います。
- 8). メッセージ受信が正常かチェックします。
localhostにCtrl + T でテストメッセージを送信します。

Syslog 送信デバイスを設定

Syslog 送信デバイスを設定

ネットワークハードウェアでSyslogメッセージを利用するための設定方法を説明します。

Syslogメッセージを送信する他のデバイスをご存知でしたら詳細をsupport@kiwisyslog.comまでお願いします。

Cisco ルータ

ルータにTelnet でログインまたはコンソール経由で接続しイネーブルモードにします。

ルータのイネーブルプロンプトから次のコマンドを入力します。

```
Config term
Logging on
```

Logging Facility Local7 (またはこのルータにアロケートする他のfacility)
Logging [Kiwi Syslog Daemon実行マシンのIPアドレスまたはホスト名]
End

他の有用なコマンドはIOS v11.2で初めて現れた**logging source-interface** です。Ciscoによれば、Syslogメッセージにはルータの出力側IPアドレスを含みます。logging source-interface コマンドで、実際に出力されるアドレスと異なる、特定のインターフェイスのIPアドレスがSyslogに含まれるように出来ます。

*バグのため、あるIOSバージョンでは logging source-interface コマンドを必ず使用してください。このコマンドを使わないと送信されるSyslogメッセージのUDPチェックサムは不正であり、Syslog Daemon が受け取る前にWinsockで廃棄されます。

Ciscoロギングコマンドの詳細は:

www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/cs/csprtf/csprtf4/cstroubl.htm

Cisco PIX

Cisco PIX ファイアーウォールのSyslog メッセージ送信を可能にする...

Cisco Webサイトを開く:

www.cisco.com/warp/public/110/pixsyslog.html

PIX ログメッセージの情報は:

www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_63/63syslog/pixmsgs.htm

www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v53/syslog/pixmsgs.htm

または: www.cisco.com/cgi-bin/Support/Errordecoder/home.pl

または: www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/index.htm

セキュアVPNトンネル経由のPIX SNMPトラップ、Syslog メッセージ送信の情報は:

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_configuration_example09186a0080094469.shtml

Cisco Catalyst スイッチ

'set' コマンドタイプ CLIを使う Catalyst スイッチで動きます。古い2900シリーズや5000シリーズです。

スイッチへTelnetもしくはコンソールケーブルで接続しイネーブルモードにします。

スイッチのイネーブルプロンプトから次のコマンドを入力します。

Set logging enable

Set logging level all 7 default (this will set all facilities with a level of debug)

Set logging [IP Address or Hostname of machine running Kiwi Syslog Daemon]

新しい **IOS タイプCLIを使うCatalystスイッチ** は次のコマンドを使います。

Logging on

logging trap warnings (or whatever level you want)

Logging Facility Local7 (or any other facility you want to allocate for this router.)

Logging <IP Address or Hostname of machine running Kiwi Syslog Daemon>

Catalyst 6000 のロギング情報は:

www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_5_5/cnfg_gd/logging.htm

また:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_system_message_guide_chapter09186a008007e784.html

Cisco VPN コンセントレータ

Cisco VPN 3000 Series コンセントレータはSyslogメッセージとSNMPトラップの送信をサポートしています。Kiwi Syslog Daemon はどちらも受信できます。

設定手順に関してはCisco web サイトに情報がありません...

Cisco ワイヤレスデバイス(Aironet)

ワイヤレスアクセスポイントにTelnetあるいはConsole経由で接続しenableモードにします。

デバイスのenableプロンプトから次のコマンドを入力します。

Config terminal

Logging on

Logging Facility Local7 (or any other facility you want to allocate for this device.)

Logging [IP Address or Hostname of machine running Kiwi Syslog Daemon]

End

その他の有効なコマンドはIOS v11.2で最初に現れる**logging source-interface** コマンドです。Ciscoによれば、syslogメッセージはデバイスから出力されるときインターフェイスのIPアドレスを含みます。logging source-interface コマンドを使うとsyslog パケットに、実際の出力インターフェイスと関係なく、特定のIPアドレスを含むことができます。

* logging source-interface コマンドはIOS のあるバージョンではバグがあるため必ず使わなければなりません。使わない場合、Syslog に不正なUDPチェックサムを含むことになり、Kiwi Syslog Daemonが受信する前にWinsockで廃棄します。

Cisco コマンドの詳細はCisco webサイトで確認してください:

http://www.cisco.com/en/US/products/hw/wireless/ps5279/products_configuration_guide_chapter09186a0080184b04.html#42426

Unix マシン

下記情報を提供してくれた Antonino Iannellaさんに感謝します。

Unix ホストではファイルを変更するためにはsuper user privileges が必要です -

```
/etc/syslog.conf  
/etc/hosts
```

Syslog Daemon をリスタートします。

Viあるいは他のテキストエディターで/etc/hostsファイルを変更します。

hosts ファイルの例

```
#  
# Internet host table  
#  
127.0.0.1    localhost  
192.168.230.23 loghost
```

メッセージのホスト名loghostになります。

LoghostのIPアドレスはKiwi Syslog Daemonを実行するマシンです。

Viあるいは他のテキストエディターで/etc/syslog.conf ファイルを変更します。

syslog.confファイルの例

```
# Syslog configuration file.  
#  
*.err;kern.notice;auth.notice      /dev/console  
*.err;kern.debug;daemon.notice;mail.crit /var/adm/messages  
  
*.alert;kern.err;daemon.err        operator  
*.alert                             root  
  
*.emerg                             @loghost  
mail.debug                          @loghost
```

emergレベルの全てのファシリティはlocalhost（hostsファイルで定義されている）にフォワーディングされ、そしてdebugレベルのメール警告も同様であることに気づきます。

一般的には **Facility.Level <TAB> @loghost**

編集後このファイルを保存しUnixのSyslog Daemonを再スタートすれば有効になります。syslog daemon プロセス ID を見つけSIGHUP信号を送ります。syslog server が**logger** コマンドでメッセージを書いていることをテストしてください。**logger -p user.emerg Unix test message**のように。

疑わしい時は**man syslog** を再ソートしてください。

The general idea is **Facility.Level <TAB> @loghost**

Extreme Summit スイッチ

スイッチにTelnetあるいは console経由で接続し、管理者（admin）レベルユーザーでログインします。

configにsyslogサーバーエントリーを追加します。次のようにします：

Configure syslog add <IP address of syslog server> <Facility name>

E.g. Configure syslog add 192.168.1.1 local0

configからsyslogサーバーエントリーを削除するのは次のコマンドです：

Configure syslog delete <IP address of syslog server> <Facility name>

E.g. Configure syslog delete 192.168.1.1 local0

CLI コンフィグレーションコマンドのロギングを有効にするのは、次のコマンドです。

enable cli-config-logging

Alliant セルラーゲートウェイ

この情報を提供してくれたMark Hamiltonに感謝します。

Alliant セルラーゲートウェイの詳細は、次を参照してください：

<http://www.alliantnetworks.com/>

SYSLOG メッセージを有効にしフィルタする

デフォルトは、SYSLOG メッセージ送信は無効です。SYSLOG サーバーの設定後、SYSLOG メッセージを有効にしなければなりません。出力するメッセージタイプを制限することによりフィルタすることができます。

次の情報が必要です：

- SYSLOG サーバーのIPアドレス
- ゲートウェイの管理者パスワード(デフォルトパスワードは: public)
- Telnet CLIを使うのであれば、ゲートウェイのIPアドレス
- シリアルCLIを使うのであれば、シリアルケーブルによるゲートウェイへの接続

次の手順でSYSLOG出力を有効にしフィルタしてください：

1. シリアルまたはTelnetでCLIをアクセス
2. 次のコマンドを入力：

```
CG> login <password>
CG# configure system
CG(sys)# configure syslog
CG(sys-sys)# set status on
```

3. コマンドの効果は、show log コマンドで表示して確認します。
SYSLOG configuration. The following is an example of show log output:
SYSLOG messages are enabled
First SYSLOG server's IP address: 10.0.1.2
Second SYSLOG server's IP address: 0.0.0.0
Severity threshold 6
CG(sys)#

4. severityでメッセージをフィルターすると有効です。次の例はerror以下のレベルのメッセージは全て除外し、errorイベント(severity は3) とそれ以上のみを含みます。

```
CG> login <password>
CG# configure system
Maintenance Onboard logging
CG(sys)# configure syslog
CG(sys-sys)# set status on
CG(sys-sys)# set severity 3
```

DLink DL-840V ルータ

この情報はwww.dshield.org 設定ガイドから入手しました。

詳細は: <http://www.dshield.org/clients/dlinkhelp>

- 1). ルータをインストールして動作させてください
- 2). コンフィグレーションパネル (<http://192.168.0.1>)で"Advanced Settings" タブをクリックします
- 3). 左のナビゲーションバーで"Administration Settings"を選択
- 4). 'SYSTEM Log'の下で "Enable System Log Function"をクリックしKiwi Syslog Daemon をインストールしたコンピュータのIPアドレスを入力します。

Pack X IDScenter

IDScenter はWindowsプラットフォーム用Snort IDSのコンフィグレーションと管理ツールです。

次のサイトからダウンロードできます:

<http://www.packx.net/packx/html/en/index-en.htm>
outputプラグインを使えばアラートをKiwi Syslog Daemon に送信できます。

コンフィグレーション:

IDScenter メインウィンドウから、左側のIDS Rules タブを選択します
左側のOutput プラグインアイコンを押します。
全ての設定済みoutputプラグインリストが表示されます。

新しいプラグインの追加は、-> **Add** ボタンを押しポップアップメニューから"**Syslog Alert Plugin**"を選択します。

ウィンドウの株にプラグインの設定画面が表示されます。

アラートメッセージを送信したいfacility とpriority (level) を選択します。

Facility: LOG_LOCAL7
Priority: LOG_ALERT

その後通知されるべきエラー状態をチェックします。

LOG_CONS, LOG_PERROR, LOG_NDELAY, LOG_PID

次に下右の**Add** ボタンを押します。syslog アラートoutput プラグインが上のリストに表示されます。

SonicWall ファイアウォール

SonicWALLファイアウォールはリモートSyslog daemonへのSyslogメッセージ送信をサポートします。2台のサーバーまで構成できます。

SonicWALLマネージメントインターフェイスにWebブラウザで接続し、ユーザー名とパスワードでログインします。

メニューの**Log**ボタンをクリックします。

メインディスプレイにタブ付きウィンドウが表示されます。

Log Settings タブをクリックします

Sending the Log でsyslog daemon実行マシンのIPアドレスをフィールド名: Syslog Server 1に入力してください。受信ポートが514以外の場合、フィールド名: Syslog server port 1にその番号を入力してください。

Automation で **Syslog Format** Webtrendsを選択してください。

Categories のLog subheadingで、Syslogメッセージとして受信する全てのイベントタイプをチェックしてください。

update ボタンを押してください。

新しい設定を有効にするにはSonicWALL のリポートが必要です。

SonicWALL syslog メッセージのレポート作成にはRnRSoft ReportGen for SonicWALL をご利用ください。www.reportgen.comからダウンロードできます。

FREESCO ルータ/ファイアーウォール

Bill Helyからいただいた情報です。

FreeSCO (<http://www.freesc0.org/>) は優れたフロッピーベースのLinux ファイアーウォール/ルータ O/S です。8Mb RAM 付の386sx 以上 (486 以上が望ましい)で動作します。オプションのHDD インストールでさらに大規模な利用が可能です。FreeSCO は syslogを出力しKiwi Syslog Daemonをサポートするには小さなファイルを編集するだけです。

- FreeSCO PC にrootでログイン
- [Linux] プロンプトで、edit /boot/etc/syslog.cfg と入力 (既存のsyslog.cfg ファイルが表示される。このファイルではNote that in this file a TAB が大文字の "I"のように垂直線として表示されていますので注意が必要です)。
- 既存ファイルの末尾行に、次のエントリを追加します: *.*[press the TAB key]@192.168.1.20 (IPアドレスはKiwi Syslog Daemonを実行するコンピュータです。"@ " はIPアドレスの直前です。)
- Enterキーを押してファイルの最後が空白行であることを確認してください。
- Alt-Sで変更したファイルを保存します。次にAlt-X でエディタを終了します。
- F1 を押せば他の使用できるコマンドキーがリストされます。
- FreeSCO コンピュータを再起動すると変更が有効になります。

FW-1 ファイアーウォール

この情報はLogAnalysis フォーラムからの投稿です。

<http://lists.jammed.com/loganalysis/2001/09/0006.html>

これはFirewall-1のUNIX版用です。

Checkpoint コマンド\$FWDIR/bin/fw log -f でCheckpoint 固有フォーマットから平文に変換できます。次にUNIX "logger" ユーティリティで平文をsyslogにします。しかし、"fw log -f" は全てのネットワーク接続ログを平文に変換しますので—毎回ファイアーウォールのストップ、リスタートが必要です。全ての接続ログをsyslogにするのは大変です。リスタート時には毎回ネットワーク接続ログをローテーションすることを薦めています。

またネットワーク接続ログや標準ホストOS syslogでは見ることのできないファイアーウォールの稼働状態の価値ある情報がたくさんあります。特に、ファイアーウォール管理にGUIを使うと管理者のGUIへのログインやログアウト、ファイアーウォールへの新しいポリシーの挿入などを見ることができます。集中ログサーバーにこれらの情報を記録するには、ファイル\$FWDIR/log/cpmgmt.audに上で述べた"logger" トリックが必要です。

3Com トータルコントロールシャーシ

Total Control Chassis からSyslog メッセージを送信する...

Telnet あるいはコンソールケーブルでHiPer Access Router Card (HiPer ARC) に接続します。
Add Syslog コマンドを使います...

ADD SYSLOG <IP Address> FACILITY <Facility> LOGLEVEL <logging level>

IP address はKiwi Syslog Daemon を実行するPCのアドレスです。

Facility は次の一つです...

LOG_AUTH
LOG_LOCAL0
LOG_LOCAL1
LOG_LOCAL2
LOG_LOCAL3
LOG_LOCAL4
LOG_LOCAL5
LOG_LOCAL6
LOG_LOCAL7

Logging level は次の一つです...

COMMON
CRITICAL
UNUSUAL
VERBOSE

例...

ADD SYSLOG 10.0.10.23 FACILITY LOG_LOCAL7 LOGLEVEL VERBOSE

LIST SYSLOGS でエントリーを表示しSyslogエントリーが追加されていることを確認します。

出力はこのようになります...

```
Console Prompt>LIST SYSLOGS
SYSLOG SINKS
SysLog      Log Level Msg Count Facility
192.168.203.203 COMMON    507     LOG_LOCAL7
192.168.203.230 COMMON    4551    LOG_AUTH
```

SAVE ALL コマンドで詳細をNVRAMにストアします。

3Com NetServer

NetServer 8 or NetServer 16からSyslogメッセージ送信を可能にする...

NetServerをTelnetかコンソールケーブルで接続します。
次のようにAdd Syslog コマンドを使います...

ADD SYSLOG <IP Address> LOGLEVEL <logging level>
IP address はKiwi Syslog Daemon を実行するPCです。

logging level は次のいずれかです。

COMMON
CRITICAL
DEBUG
UNUSUAL
VERBOSE

例...

ADD SYSLOG 10.0.10.23 LOGLEVEL VERBOSE

LIST SYSLOGS でエントリーを表示しSyslogエントリーが追加されていることを確認します。

出力はこのようになります...

```
Console Prompt>LIST SYSLOGS
SYSLOG SINKS
SysLog      Log Level Msg Count
192.168.203.203 COMMON    507
192.168.203.230 COMMON    4551
```

SAVE ALL コマンドで詳細をNVRAMにストアします。

Linksys ファイアウォール

Linksys ファイアウォールはSNMP経由でメッセージを送信します。Kiwi Syslog Daemon のポート162でSNMPトラップを受信します。

- メインKiwi Syslog Daemonウィンドウで File | Propertiesメニューを開く

- PropertiesページのInputs | SNMPオプションへ移動
- Listen for SNMP trapsをチェックします (デフォルトポートは162です)。

Use Linksys Display Filter...をチェックしてもかまいません。PPPとPPPoEメッセージの表示を削除しますがログファイルには残ります。Linksysファイアーウォールがこれらを大量に送信する時きわめて効果的です。

これらの変更後システムをリスタートしてください。

LinksysメッセージはSNMPトラップにエンコードされたテキストメッセージです。MIBはOIDを参照しますが、多くの有用な情報はテキストに含まれています。

Linksys ワイヤレスVPN ルータ

新しいLinksys Wireless-G VPN ブロードバンドルータでsyslogメッセージ送信が可能になりました。以前のLinksys ファームウェアはアラートはSNMP トラップ経由で送信しました。SNMPトラップの設定は Linksys ファイアーウォール設定を見てください。

- web ブラウザからLinksysルータへログインする
- Administration タブをクリック
- Log サブタブをクリック
- Syslog notification へ移動
- オプションをEnabledにする
- ログメッセージ識別のためDevice 名を入力、あるいは"Linksys"のままにする
- Kiwi Syslog Daemon (例: 192.168.1.100)を実行するマシンのIPアドレスを入力
- 送信するsyslog メッセージタイプを設定。 Informational がデフォルト。全てのメッセージはpriorityをdebugにする
- Alert Log の下で、通知されたいアラートに関するボックスをチェック
- General Log の下で、通知されたいメッセージに関するボックスをチェック
- ページ下部のSave Settings リンクをクリックして変更を保存
-

Symantec ファイアーウォール/VPN 200

この情報を提供していただいた David Masilottiに感謝します。

web ブラウザで、マネージメントコンソールに接続します。

左側の**Advanced** セクションの下で、**Log Settings** |リンクをクリックします。

Syslog Server フィールドにrunning Kiwi Syslog Daemon を実行するマシンのIPアドレスまたはホスト名を入力します。

異なるメッセージタイプの新を有効にするためにチェックボックスをチェックします: 必要に応じて**System, Debug, Blocked, Dropped** と **Attack** をチェックします。全てのメッセージタイプを有効にし、情報が多すぎたらチェックをはずしてください。

Save ボタンを押して変更を適用します。

これでsyslog logの全ての新しいイベントはKiwi Syslog Daemon サーバーに送信されます。

SnapGear SOHO+

web ブラウザで、SOHO+ マネージメントコンソールに接続します。

左の**SYSTEM** セクションの下の**Advanced** リンクをクリックします。

System Log セクションの下の**System Log** リンクをクリックします。

Address of remote machine フィールドにrunning Kiwi Syslog Daemon を実行するマシンのIPアドレスまたはホスト名を入力します。 .

Enable remote logging チェックボックスをチェックしてメッセージ送信を有効にします。

Submit ボタンを押して変更を適用します。

これでsyslog logの全ての新しいイベントはKiwi Syslog Daemon サーバーに送信されます。

BuffaloTech AirStation ルータ

この情報はBuffalo AirStation ユーザーマニュアルから入手しました。 .

詳細はオンラインマニュアルで確認してください:

<http://www.buffalotech.com/wireless/support/downloads.php?type=manuals>

コンフィグレーションガイド:

- CDからAirStation設定ソフトウェア"AirNavigator"をインストールします
- 管理するAirStation に接続します
- 左のメニューリストから、"Management" を選択します
- ツリーから"Syslog Transmitting"をクリックします
- syslogメッセージ送信を有効にするため"Use" を選択します
- Kiwi Syslog Daemonを実行するマシンのIPアドレスを入力します
- リモートsyslog daemonに記録するメッセージレベルを指定するためにError や Notify を選択します
- Log informationから、syslog daemonに送信する特定のレポートを選択します

Intertex ADSL ルータ

オンラインIG Manual ADSL ルータからのコピーです。

外部Syslog ServerへのSystem Logエクスポート

本製品のSyslogクライアントはシステムとセキュリティログをRFC3164準拠Syslogサーバーに送信できます。Syslogを有効にするにはSyslogサーバーが動いていなければなりません。多くのシェアウェアあるいはフリーウェアのSyslogサーバーがあります。Windows用のKiwi syslogもその一つです。

syslogスタート:

1. WebブラウザでInternet Gate Webページを開く (デフォルトIPアドレス: 192.168.0.1.)
2. ログイン
3. **Administration**をクリック
4. **Syslog server**フィールドでKiwi SyslogサーバーのIPアドレスを入力
5. **Save** をクリック

システムログの新しいイベントは指定したSyslogサーバーに送られます。

Lucent ルータ

Ethernet -> Mod Config --> Log...

```
Syslog=Yes
Log Host=10.23.45.111
Log Facility=Local5
```

MAX がSyslog daemon にメッセージ送信するように構成するにはEthernet Profile (Mod Config menu)のLogサブメニューを開き次の手順に従います:

Syslog をYesにする

ホストがMAXと同じサブネットに無い場合、Kiwi Syslog daemonを実行するホストのIPアドレスを指定します。 .

MAX はRIPまたは静的にホストへのルートが無ければなりません。

Table 12-3を参照. "System configuration and administration parameters."
"Location Parameters via RIP or a static route."
Chapter 10を参照."Configuring the MAX as an IP Router."

注: ダイアルアップ接続でのみ接続できるSyslogホストにレポートを送らないで下さい。MAXはログアクションの度にログホストにダイアルしハンクアップします。

Log Facility パラメータはMAXからのメッセージを識別するために使われます。log facility 番号を設定した後、Kiwi Syslog daemonを、特別なログファイル(MAXログファイル)への全てのメッセージにそのfacility番号を含むよう、設定します。

各facility用のログファイル設定にActionタブを使います。

詳細はMAX Reference Guide またはLucent webサイトを見てください。

Allied Telesyn ルータ

Allied Telesyn New ZealandのTaylor Wilkensから提供された情報です。

syslog daemon にログ出力を送信する定義を作成できます。そのコマンドは：

```
create log output=1 destination=syslog server=address
```

ここでaddressはsyslog daemonを実行するホストのIPアドレスです。

出力定義後、どんな種類のメッセージを送信するかを決めるフィルターを追加します。たとえば、IP traffic filterで生成されたメッセージを送信するにはコマンドは：

```
add log output=1 type=IPFILT
```

あるいは、ISDNコールの時間を記録するにはコマンドは：

```
add log output=1 mod=ICC type=CALL subtype=DOWN
```

すべてのイベント表示フィルターは：

```
add log output=1 filter=1 all
```

フレームアップ/ダウンのようなインターフェイスイベントやImi状態を記録するには

```
add log output=1 filter=1 type=vint  
add log output=1 filter=1 type=dlink
```

もっと多くのロギングコマンドは次のWebにあります：

<http://www.alliedtelesyn.co.nz/documentation/arrouter/241/pdf/log.pdf>

Arris ケーブルモデムターミネーションシステム

次の情報を頂いたDale Hutchinson に感謝します...

Kiwi Syslog daemon をArris CMTS1000 DOCSIS 1.0 Cable Modem Termination System とCMTS1500 DOCSIS 1.1 Cable Modem Termination Systemで使うコンソールコマンドです。

```
manage  
event-level  
syslog-ip-addr xxx.xxx.xxx.xxx //IP address of your Kiwi Syslog Daemon server  
admin-status-of-throttle unconstrained
```

WatchGuard SOHO ファイアーウォール

この情報は WatchGuard 知識ベースからのものです

SOHO 2.4.0以上ではネットワーク経由でSyslogサーバーにログ送信ができます。Syslogはログデータを Solaris, SCO Unix, BSD, Linuxその他のUnix-style OSから受け取るツールです。SOHOでは標準ログと同時にSyslog機能が働きます。

しかし若干の制約があります。SyslogサービスではUDP514でネットワークデータを送ります。SOHOやSyslogホストでは正確な配信を検証できません。Syslog仕様によれば暗号化されません。

設定手順を示します：

SOHO syslog configuration

SOHOコンフィグレーションインターフェイスを開く

System Administrationをクリック

Syslog Loggingをクリック

Enable Syslog output チェックボックスをチェック

syslogd サービス実行ホストのIPアドレスを入力

Syslog はログデータの暗号化をしません。Syslogを悪意のあるネットワーク経由で送信してはなりません。

Submitをクリック

SOHO をレポート

Watchguard Firebox がDshieldと動くようにする

詳しい情報は:

http://live.dshield.org/clients/watchguard_kiwi_setup.php

Bay Networks デバイス

この情報はBay Networks web ページからのコピーです:

<http://support.baynetworks.com/library/tpubs/html/switches/bstream/115412A/MARKER-2-455>

ルータのSyslog を設定

ルータのsyslogを設定するにはTechnician Interface コマンドが使えます。syslog をタスクシーケンスとして設定します。ここでタスクは1以上の番号つきのステップです。

ルータでsyslogを設定するのに必要なタスクの概要です:

1. ルータに接続したコンソール、またはルータにTelnetし、Technician Interface セッションを開く
2. ルータにSyslogをロードするためのスロットマスク (スロットマップ) を定義する
3. ルータにsyslog エンティティを生成
4. syslog グローバル属性を設定
5. syslog ホストテーブルにリモートホストを追加
6. syslog エンティティフィルターテーブルにエンティティフィルターを追加
7. 5と6を繰り返してリモートホストとエンティティフィルターを追加。終了後8へ行く
8. NVFS volumeのファイルに保存し、syslog 設定を追加する
9. Technician Interface からログアウト

以下でsyslog 設定シーケンスを詳しく説明します (タスクとステップレベル)。

設定手続きに続き、ここではsyslog 設定例とsyslog 属性定義を提供します。

Task 1: ルータに接続したコンソール、またはルータにTelnetし、Technician Interface セッションを開く

Bay Networks ルータのTechnician Interfaceセッションのオープンの詳細は1章を参照してください。

Task 2: ルータにSyslogをロードするためのスロットマスク (スロットマップ) を定義する

ルータにsyslog エンティティを生成する前に、syslogスロットマスクを定義します。スロットマスクはシステムがsyslog エンティティをロードし実行するスロットを特定します。Technician Interface プロンプトで、下記の入力を行います。

```
$: set wfProtocols.wfSYSLLoad.0 0x7FFE0000;commit
```

このコマンドはルータモデルに関係なく全てのsyslog 実行を有効にします。

次に、ルータのsyslog エンティティを作成します。

Task 3: ルータにsyslog エンティティを生成

次のようにルータ設定でsyslog エンティティを生成します:

```
set wfSyslog.wfSyslogDelete.0 1;commit
```

これはまたルータノsyslogを有効にします(システムはsyslog ベースレコードの属性wfSyslogDisable, OID = 1.3.6.1.4.1.18.3.3.2.15.1.2, を1にします)。

次に、syslog グローバル属性を設定します。

Task 4: syslog グローバル属性を設定

ルータのsyslog を生成し有効にすると、wfSyslogMaxHosts と wfSyslogPollTimer 属性のデフォルト値を受け取ることができます。またはカスタム化した値を設定することもできます。syslog グローバル属性でデフォルト値を希望するならタスク5へ、それ以外は次のステップへ進みます:

1. ルータのsyslogでサポートするアクティブホスト最大数を設定:

```
$: set wfSyslog.wfSyslogMaxHosts.0 <1 - 10>;commit
```

wfSyslogMaxHosts のデフォルトは5 ホストです。最大数以上にYou can add to the syslogホストテーブルを追加することができますが、but syslog フォワードメッセージは最初の"n" アクティブホストです。ここでn = wfSyslogMaxHostsの値

2. ルータのsyslog ポーリングサイクル間隔(秒) を設定:

```
$: set wfSyslog.wfSyslogPollTimer.0 <5 - 610000>;commit
```

wfSyslogPollTimer のデフォルトは5 秒

次に、syslog ホストテーブルにリモートホストを追加

Task 5: syslog ホストテーブルにリモートホストを追加

ネットワークのルータでsyslog メッセージを受信するリモートホストを定義する。

これがsyslog ホストテーブルへの最初の登録であればステップ1へ行きます。それ以外は、最初にルータにすでに設定されているホストリストを入力することができます。To list existing entries in the syslog ホストテーブルの既存リストは、Technician Interface プロンプトから次のコマンドで入手します:

list -i wfSyslogHostEntry

リストはsyslogホストテーブルに定義されている全てのインスタンスID (この場合はIPアドレス) を含みます。

1. 次のようにsyslog ホストテーブルに新しいホストエントリーを追加します:

```
$: set wfSyslogHostTable.wfSyslogHostDelete. <host_IP_address> 1
$: commit
```

このエントリーは指定したあて先IPアドレスのリモートホストのThis entry informs syslog 情報です。

ホスト属性wfSyslogHostLogFacility (184 = Local7)と wfSyslogHostTimeSeqEnableのデフォルト設定は (2 = disabled), タスク6へ行きます。それ以外はカスタマイズ設定をステップ2で行います。

2. ルータからsyslogメッセージを受信するUNIXシステムファシリティを定義するには、次のコマンドを使います:

```
$: set wfSyslogHostTable.wfSyslogHostLogFacility. <host_IP_address> <128/136/144/152/160/168/176/184>;commit
```

128 = local0	160 = local4
136 = local1	168 = local5
144 = local2	176 = local6
152 = local3	184 = local7

3. リモートホストのsyslog メッセージタイムシーケンシングを有効にするには、次のように入力します:

```
$: set wfSyslogHostTable.wfSyslogHostTimeSeqEnable.
<host_IP_address> 1;commit
```

注意: エントリーが有効で (wfSyslogHostDisable = 1) アクティブ (wfSyslogHostOperState = 1) なリモートホストのみがルータのsyslog からメッセージを受信します。

次に、追加したホストエントリーにエンティティフィルターを追加します。

Task 6: リモートホストにエンティティフィルターを追加

syslog ホストテーブルにホストを定義したら、ホストにエンティティ固有のメッセージフィルターを追加 (定義) します。

もしこれがエンティティとリモートホストペアの最初のフィルターで無ければ、次のようにしてフィルターインスタンスリストを入手します:

list -i wfSyslogEntFiltrEntry

インスタンスIDリスト(フォーマットは<host_IP_address>.<entity_code>.<filter_index>)から、与えられた

<host_IP_address>.<entity_code>ペアにアサインする新しいフィルター< filter_index>番号を決定します。新しいフィルター 番号はリストの最も大きな<filter_index>に+1された値です。

ステップ1に進みます。

1. エンティティとリモートホストペアに新しいフィルターを作成します:

```
$: set WfSyslogEntityFilterTable.WfSyslogEntFiltrDelete. <host_IP_address>.<entity_code>.<filter_index>
1;commit
```

<host_IP_address> リモートホスト (マネージメントワークステーション)のIPアドレス

<entity_code> <host_IP_address>のリモートホストへのイベントメッセージのフォワードをするソフトウェアエンティティ。

<filter_index>次のエンティティとリモートホストペアにフィルターをアサインできる番号

2. 特定のホストのエンティティフィルターの作成後、以下を定義します。

- イベント番号(または範囲) とスロット番号 (または範囲)

または:

- セベリティマスクとスロット番号 (または範囲)

注意: フィルターはイベントとスロット番号、またはセベリティマスクとスロット番号を定義するまで動作しません。

エンティティフィルター属性の設定:

a. イベント番号で定義しイベントメッセージをsyslog で選択し 特定のリモートホストに送信する:

```
$: set wfSyslogEntFiltrEntry.wfSyslogEntFiltrLogEvtLowBnd.
<host_IP_address>.<entity_code>.<filter_index> <0 - 255>
$: set wfSyslogEntFiltrEntry.wfSyslogEntFiltrLogEvtUppBnd.
<host_IP_address>.<entity_code>.<filter_index> <0 - 255>
$: commit
```

イベント番号でフィルター定義をしなくなければ、イベント番号の下限0と上限255を受け入れます (ステップ2bへ行く)。デフォルトを受け入れるとメッセージの選択とフォワーディング条件はセベリティとスロット番号が使われます。

b. まだイベント番号 (またはイベント番号範囲)を定義していないときに限りセベリティマスクを定義します。イベント番号や番号範囲を定義すると、syslog はこのフィルターのセベリティマスクを無視します。

syslog が選択し師弟のリモートホストにフォワーディングするイベントメッセージのセベリティレベルの定義方法:

```
$: set wfSyslogEntFiltrEntry.wfSyslogEntFiltrSevMask.
<host_IP_address>.<entity_code>.<filter_index> "<fwitd>"
$: commit
```

c. スロット番号で定義しイベントメッセージをsyslog で選択し 特定のリモートホストに送信する:

```
$: set wfSyslogEntFiltrEntry.wfSyslogEntFiltrSlotLowBnd.
<host_IP_address>.<entity_code>.<filter_index> <0 - 14>
$: set wfSyslogEntFiltrEntry.wfSyslogEntFiltrSlotLowUpp.
<host_IP_address>.<entity_code>.<filter_index> <0 - 14>
$: commit
```

注意: 正しいスロット番号の下限と上限はそれぞれ0と14ですが、設定しようとしているルータモデルの実際のスロット番号の範囲の値を指定します。そうでないとフィルターは実行状態になれません。

3. ルータイベントメッセージとUNIXシステムエラーレベルをマッピングする

大胡の場合、デフォルトマッピングを受け入れタスク7へ行きます。その他の場合メッセージのカスタムマッピングを次の手順で行います。
Technician Interface プロンプトで、変更するメッセージマッピングを入力します:

a. ルータFAULT メッセージをマッピングします:

```
$: set wfSyslogEntFltrEntry.wfSyslogEntFltrFaultMap.  
<host_IP_address>.<entity_code>.<filter_index> <1 - 8>
```

wfSyslogEntFltrFaultMap のデフォルトは3であり、ルータのFAULT レベルメッセージを UNIX システムレベルCRIT メッセージにマッピングします。

b. ルータのWARNING メッセージをマッピングします:

```
$: set wfSyslogEntFltrEntry.wfSyslogEntFltrWarningMap.  
<host_IP_address>.<entity_code>.<filter_index> <1 - 8>
```

wfSyslogEntFltrWarningMap のデフォルトは5であり、ルータのWARNING レベルメッセージをUNIX システムレベルWARNING メッセージにマッピングします。

例:

```
$: set wfSyslogEntFltrEntry.wfSyslogEntFltrWarningMap 5
```

例のコマンドは各Warning レベルルータイベントメッセージをWarning レベルUNIX システムエラーメッセージにマッピングします。

c. ルータのINFO メッセージマッピングを変更します:

```
$: set wfSyslogEntFltrEntry.wfSyslogEntFltrInfoMap.  
<host_IP_address>.<entity_code>.<filter_index> <1 - 8>
```

wfSyslogEntFltrInfoMap のデフォルトは7であり、ルータのINFO レベルメッセージをUNIX システムレベルINFO メッセージにマッピングします。

d. ルータのTRACE メッセージマッピングを変更します:

```
$: set wfSyslogEntFltrEntry.wfSyslogEntFltrTraceMap.  
<host_IP_address>.<entity_code>.<filter_index> <1 - 8>
```

The default value of *wfSyslogEntFltrTraceMap* のデフォルトは3であり、ルータのTRACE レベルメッセージをUNIX システムレベルCRIT メッセージにマッピングします。

e. ルータのDEBUG メッセージマッピングを変更します:

```
$: set wfSyslogEntFltrEntry.wfSyslogEntFltrDebugMap.  
<host_IP_address>.<entity_code>.<filter_index> <1 - 8>
```

wfSyslogEntFltrDebugMap のデフォルトは8であり、ルータのDEBUG レベルメッセージをUNIX システムレベルDEBUG メッセージにマッピングします。

Task 7: ホストやエンティティフィルターをさらに追加

syslog 設定にホストやエンティティフィルターをさらに追加するには、次のようにします:

1. このリモートホストへのエンティティフィルターの追加を完了し、タノリモートホストを追加するのであればタスク8へ、それ以外はステップ2へ行きます。
2. 同一リモートホストへタノエンティティフィルターを追加するには、タスク6へ、それ以外はステップ3へ行きます。
3. ルータからsyslogメッセージを受信する他のホストを追加するにはタスク5へ戻ります。

Task 8: Syslog 設定をルータに保存

NVFS volumeのファイルに保存し、syslog 設定を追加するため次の入力を行います:

```
save config <vol>:<filename>
```

Task 9. Technician Interface からログアウト

Technician Interface コマンドラインインターフェイスから次の入力を行います:

```
$: logout
```

Nortel Networks ルータ

この情報に関しFlavio Ramos に感謝します。

Bay Command Console (BCC)から、次のコマンドを入力する:

```
stack# syslog  
syslog  
  log-poll-timer 10  
  log-host address <IP Address of PC running Kiwi Syslog Daemon>  
  filter name WILDCARD entity all  
    severity-mask {fault warning}  
  slot-lower-bound 1  
  slot-upper-bound 14  
  back  
back  
back
```

ZyXEL ZyWALL 10

この情報に関しKillian McCourtに感謝します。

www.netgear.org

WebインターフェイスはSyslog設定をサポートしません。Telnetもしくはコンソールポートからのコマンドラインでのみ可能です。

Menu 24.3.2 - System Maintenance - UNIX Syslog

Syslog:
Active= Yes
Syslog IP Address= xxx.xxx.xxx.xxx (IP address of the syslog)
Log Facility= Local 1 (Send messages with a facility of Local1)

Types:
CDR= No
Packet triggered= No
Filter log= No
PPP log= No
Firewall log= Yes
VPN log= No

設定はNetgear/Zyxel RT311/RT314 とほとんど変わりません。

Netgear / ZyXEL RT311/RT314

この情報は非正規の Netgear サポートページからのものです

www.netgear.org

WebインターフェイスはSyslog構成をサポートしておりません。Telnetコマンドから実行してください。

Menu 24.3.2 - System Maintenance - UNIX Syslog

Syslog:
Active= Yes
Syslog IP Address= xxx.xxx.xxx.xxx <---- ip address of the syslog
Log Facility= Local 1 <----- Make sure you set it as the same group in your syslog
Types:
CDR= Yes
Packet triggered= Yes
Filter log= Yes
PPP log= Yes

Netgear RP114 ルータ

この情報は Netgear RP114 ドキュメントファイルからのものです。

さらに多くの情報は : www.netgear.com

WebインターフェイスではSyslog設定をサポートしておりません。Telnetコマンドから実行してください。

Syslog はMenu24.3.2で設定できます – システムメンテナンス - UNIX Syslog. Menu 24.3.2 はルータがUnixシステムログを他のマシンに送信するよう設定します。Syslogをアクティベートする様、パラメータを設定します。

フィールド: Active
コマンド: スペースバーでyes / noを反転
説明: syslog オプションがオン、オフになる

フィールド: Syslog IP Address
コマンド: IPアドレスを入力
説明: syslog 送信先のIPアドレス

フィールド: Log Facility
コマンド: Facility値を入力
説明: 7個のLocalオプションから選択。メッセージをサーバーの異なるファイルに記録できる。

フィールド: Types: CDR, Packet triggered, Filter log, PPP log
コマンド: 各タイプ共、スペースバーでyes / noを反転
説明: 次のロギングをイネーブル : Call detail record (CDR), Packet trigger, Filter event (match or not match), PPP event.

ローカルホストのsyslogでルータのロギングをするための設定 :

1. Menu 24.3.2 - System Maintenance - UNIX Syslogへ移動
2. Active をYesにする
3. Syslog IP Address フィールドでSyslogホストPCのIPアドレスを入力
4. Log Facility 番号を選ぶ
5. 記録するactivity タイプを選ぶ

ルータから次のsyslogメッセージを送信できます：

- Call detail record (CDR)
- Packet trigger
- Filter event log
- PPP event log

6. メニューをセーブ

FVS318 VPN ファイアーウォール

この情報に関してPaul Bohn、 Mount Sterling Ohio に感謝します。

さらに多くの情報は：http://www.netgear.com/product_view.asp?xrp=4&yyp=12&zrp=129

必要なファームウェアレベル: NETGEAR FVS318 FIRMWARE 1.01j beta
2002年8月7日以降

syslog メッセージ送信のための設定:

- Netgearルータにサインオン
- 左のSECURITYのSecurity logsを選ぶ。
- Security logs画面のSYSLOGボックスをチェック
- Send syslog to this addressフィールドでSyslog Daemonを実行するシステムのIPアドレスを入力

HP JetDirect プリンタ

HP JetDirect のsyslog設定はHP JetAdmin プログラムまたはビルトインWebインターフェイスで行います。

Webインターフェイスで接続するには、ブラウザでhttp://print_server_address:8000/と入力します。

- メインメニューのHP・ロゴをクリック
- デバイスリストからプリンタを選択
- Configuration リンクをクリック
- 左側メニューからNetwork リンクをクリック
- System Log Server にカーソルを移動
- Kiwi Syslog Daemonを実行するマシンアドレスを入力する
- Apply ボタンを押す

W-Linx MB ブロードバンドルータ

この情報はPhilipp Beckersから提供されました。

これ以上の情報は：http://www.w-linx.com.tw/products/multifunction/soho_mate.htm

1. webブラウザを使って W-Linx boxに接続し、 (<http://192.168.1.254>) adminでログインします
2. "Advanced Setting"をクリックしSystem Logに移動
3. "IP Adress for Syslog" フィールドにKiwi Syslog Daemonを実行するPCのIPアドレスを入力
4. "enable" がチェックされていることを確認しsaveをクリック
5. ルータをリブートするとsyslogが使えます

NetScreen ファイアウォール

この情報を頂いた George McCashinに感謝します。

Web ベースの設定:

- 1). "admin" でwebインターフェイスにログオンする
- 2). Configuration->Report Settings->Syslog に移動
- 3). 'Enable Syslog'をクリック
- 4). すべてのトラフィックをログ出力するには'Include Traffic Log' をクリック
- 5). ログホストアドレスとポートを入力 (Kiwi Syslog Daemon アドレスとUDPポート514)

Kevin Branchによる追加情報:

Netscreen ポリシーの(permit/deny/tunnel)すべてのタイプのすべてのトラフィックを、デフォルト(不許可指定されない場合、Netscreen は許可セッションです)で許可されたログトラフィックと同様に、Netscreen ポリシーの(permit/deny/tunnel)すべてのタイプのすべてのトラフィックをログ出力します、.

"Log Packets Terminated to Self"オプションはNetscreen全体のセッションとは関係ありませんが、, Netscreen自身にセッションをログ出力します (Netscreen管理トラフィックですが、インターネットからのプローブを示します)。

代わりに、CLIからNetScreenを設定することができます。

コマンドラインインターフェイス設定:

この特定のコマンドは下記のようにSyslog サーバーを設定するために必要です:

```
set syslog config ip_address security_facility
local_facility
set syslog enable
set syslog traffic
set log module system level level destination syslog
```

注意: set syslog config コマンドではsecurity facility とlocal facilityを定義する必要があります。syslog コマンドのsecurity_facility とlocal_facilityの完全なオプションリストはNetScreen CLI Reference Guideを参照してください。

注意: 各メッセージレベルでset log コマンドを入力します。レベルのオプションは下記のとおりです:

```
emergency
alert
critical
error
warning
notification
information
```

Bintech アクセスルータ

この情報を頂いたTorsten Richter に感謝します。

これ以上の情報はここから: <http://www.bintec.net/en/index.php>

Command Line Interface configuration:

- Telnet to the router
- goal - (input / action)
- switch off the time-out for this session - (type "t 0")
- open setup - (type "setup")
- choose - (select "SYSTEM")
- choose - (select "External System Logging")
- choose - (select "ADD")
- field: Log Host - (enter the Kiwi Syslog machine [IP or Hostname])
- field: Level - (select with space tab)
- field: facility - (select with space tab)
- field: Type - (select with space tab)
- field: Timestamp - (select with space tab)
- save - (save)

- exit to setup tool/system - (exit)
- exit to setup tool - (save)
- save and exit - (select "Save as boot configuration and exit")

Syslogd エラーとe-mail ログ

エラーログ

Syslogdがログファイルにメッセージを記録できない時や、ログファイルのアーカイビングに問題がある時、エラーログテキストファイルにエラーが記録されます。

ファイル名はInstallPath¥Errorlog.txt です。

エラーログファイルを見る

メインSyslog Daemon 画面から...

View | **View Error log file** を選ぶか **Ctrl+R** を押す

エラーログがあればノートパッドでエラーログテキストファイルを開きます。

SMTP メールのログ

警告メールや、デイリー統計がe-mailで送られると詳細がメールログファイルに記録されます。

ファイル名はInstallPath¥SendMailLog.txt です。

e-mail ログファイルを見る

メインSyslog Daemon 画面から...

View | **View e-mail log file** を選ぶか **Ctrl+M** を押す。

メールアクティビティログがあればノートパッドでSendMailLog textファイルを開きます。

Syslog プロトコル

Syslog ファシリティ

各Syslogメッセージはテキストの先頭にプライオリティを含みます。プライオリティは0~191までありファシリティとレベルで構成されます。プライオリティは<>が区切り記号です。

BSD Unix Syslog メッセージの形式です：

<PRI>HEADER MESSAGE

プライオリティは0~191でありスペースや先頭の0パディングはありません。

SyslogメッセージのフォーマットはRFCをお読みください。

ファシリティはマシンのどのプロセスが生成したメッセージかを示します。Syslogプロトコルは最初BSD Unix用に書かれたものであるためファシリティはUnixのプロセスやデーモンを反映しています。

プライオリティは次の式で計算されます：

Priority = Facility * 8 + Level

可能なファシリティリスト:

0	kernel messages
1	user-level messages
2	mail system

3	system daemons
4	security/authorization messages (note 1)
5	messages generated internally by syslogd
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon (note 2)
10	security/authorization messages (note 1)
11	FTP daemon
12	NTP subsystem
13	log audit (note 1)
14	log alert (note 1)
15	clock daemon (note 2)
16	local use 0 (local0)
17	local use 1 (local1)
18	local use 2 (local2)
19	local use 3 (local3)
20	local use 4 (local4)
21	local use 5 (local5)
22	local use 6 (local6)
23	local use 7 (local7)

Unixシステムから受信したメッセージは最初にUserファシリティに注目します。Local0～Local7はUnixでは使用されておらず、伝統的にネットワーク装置が使っています。例えばCiscoルータはLocal6とLocal7を使っています。

Syslog レベル

各Syslogメッセージはテキストの先頭にプライオリティを含みます。プライオリティは0～191でありファシリティとレベルで構成されます。プライオリティは<>が区切り記号です。

BSD Unix Syslog メッセージの形式です：

<PRI>HEADER MESSAGE

プライオリティは0～191でありスペースや先頭の0パディングはありません。

SyslogメッセージのフォーマットはRFCをお読みください。

プライオリティは次の式で計算されます：

Priority = Facility * 8 + Level

セバリティレベルリスト：

0	Emergency: システム不能
1	Alert: 対応至急必要
2	Critical: 危険な状態
3	Error: エラー発生
4	Warning: 警報発生
5	Notice: 正常だが重大な事態
6	Informational: 情報
7	Debug: デバッグレベルメッセージ

通常のメッセージはNoticeまたはInformationalレベルをお奨めします。

セバリティレベルの詳細説明：

DEBUG:

開発者のアプリケーション開発に有効だが、運転には不向き

INFORMATIONAL:

正常運転メッセージ - レポートや性能測定には適している。対応は不要

NOTICE:

普通ではないがエラーでもない - 緊急な対応は不要だが問題の可能性を開発者や管理者にe-mailで連絡する必要

WARNING:

ワーニングメッセージ - エラーではないが対応されなければエラーが発生する可能性を示す。例：ファイルシステム85%フル - 一定時間内での対応が必要

ERROR:

緊急ではない問題 - 開発者が管理者に連絡が必要；各項目は一定時間内に解決が必要

ALERT:

至急対応が必要 - 問題解決できるメンバーに連絡 - 予備ISP接続断など

CRITICAL:

至急対応が必要。主要システムに問題有り – ALERTより先にCRITICALを解決 – 一次ISPとの接続断など

EMERGENCY:

パニック状態 – 技術スタッフ全員に通達? (地震? 竜巻?) – 複数apps/servers/sites...に影響

Syslog プライオリティ

各Syslogメッセージはテキストの先頭にプライオリティを含みます。プライオリティは0から191までありファシリティとレベルで構成されます。Priorityは<>が区切り記号です。

BSD Unix Syslog メッセージの形式です:

<PRI>HEADER MESSAGE

プライオリティは0~191でありスペースや先頭の0パディングはありません。

SyslogメッセージのフォーマットはRFCをお読みください。

プライオリティは次の式で計算されます:

Priority = Facility * 8 + Level

手で特定のプライオリティをセットするにはPriorityフィールドに数字を入力しUse this valueボックスをチェックします。この値はSyslogメッセージの<PRI>フィールドに送られます。191~255まで使用できます。191以上は不正な値であり不測の結果を引き起こす可能性があります。

転送

Kiwi Syslog Daemon はUDPメッセージもTCPメッセージも受信します。通常SyslogメッセージはUDPで受信されます。Cisco PIXの様にパケットが確実に受信され、Syslog Daemonからの返信を受け取るようにTCPで送信できるものもあります。

UDP送信ポートは通常514です。

TCP送信ポートは通常1468です。

Syslog RFC 3164 ヘッダーフォーマット

HEADERには時刻とデバイスのホスト名またはIPアドレスが入ります。

HEADERにはTIMESTAMPとHOSTNAMEフィールドがあります。

TIMESTAMPはPRIから > に続きTIMESTAMPとHOSTNAMEには一つのスペースが入ります。

HOSTNAMEにはホスト名が入ります。ホスト名が無ければIPアドレスが入ります。

TIMESTAMPには現地時刻が入りそのフォーマットはMmm dd hh:mm:ssです。

MSG部分にはTAGとCONTENTフィールドがあります。TAGフィールドにはメッセージを生成したプログラムかプロセス名が入ります。CONTENTには詳細なメッセージが入ります。伝統的に自由形式でイベントの情報を書きます。TAGはABNF英数字で32文字以内です。英数字以外でTAGフィールドが終わりCONTENTフィールドとみなされます。普通CONTENTフィールドは[、:またはスペースで始まります。

Kiwi SyslogGen は次のメッセージフォーマットです:

<PRI>Jul 10 12:00:00 192.168.1.1 SyslogGen MESSAGE TEXT

BSD Syslog プロトコルはRFC 3164で議論されています

<http://community.roxen.com/developers/idoocs/rfc/rfc3164.html>

syslog プロトコル全般は次を見てください:

<http://www.sans.org/infosecFAQ/unix/syslog.htm>

問題解決

問題解決

メッセージが表示されないあるいはロギングされない場合：

送信デバイスからSyslog DaemonマシンにPingでネットワーク接続を確認して下さい。
Kiwi Syslog Daemon が一つだけ実行中かを確認して下さい(タスクリストはCtrl-Alt-Del で得られます)
ZoneAlarm やBlackIce のようなパーソナルファイアウォールをストップしてください。
コマンドプロンプトでホスト名をPingし、DNS解決が正常か確認して下さい。
受信したいメッセージのfacilityとlevelのアクションがDisplayか確認して下さい。
Ctrl+Tでテストメッセージを送信してください。
無料のSyslog Daemon Message Generator (SyslogGen)をダウンロードしてください。
SyslogGenをインストールし127.0.0.1 (local host)に1秒ごとにメッセージを送ってください。
メッセージが表示されれば問題はSyslogメッセージ送信側デバイスです。
他のマシンからSyslogGenでSyslog Daemonにメッセージを送信してください。
送信デバイスがメッセージにPriority値を含まない恐れがある場合は、properties **ウィンドウのModifiers**オプションでデフォルトPriority値を設定してください。
Ciscoルータのメッセージを受信しない場合、Logging source-interfaceコマンドで送信元インターフェイスを指定してください。Cisco IOSのバグにより、このコマンドで指定しないとUDPチェックサム不正になります。

まだSyslog Daemon がメッセージ表示できない場合：

コンピュータをリスタートしてください(出来れば電源を切ってください)。
IPアドレス解決しないようDNS設定をディセーブルにしてください。
Alarm とStatistics 通知オプションのチェックをはずしe-mail送信をディセーブルにしてください。
Defaults/Import/Exportで**Load default Rules and Settings**ボタンを押してください。次にOKを押してください。

まだSyslog Daemon がメッセージ表示できない場合：

support@kiwisyslog.com またはsupport@jtc-i.co.jpに連絡してください。技術的な詳細情報を忘れないで下さい。

上級者用の情報

Kiwi Syslog Daemonのレジストリー設定

次のレジストリーがKiwi Syslog daemon に影響します。

レジストリー変更にあたってはKiwi Syslog Daemonがストップしていることを確認して下さい。サービス版であればService Manager のManageメニューからストップしてください。
値の変更にはRegEdit を使ってください。

変更後Kiwi Syslog Daemon をリスタートすると新しい設定を読み込みます。

送信e-mail メッセージの制限

セクション: HKEY_LOCAL_MACHINE¥SOFTWARE¥Kiwi Enterprises¥Syslogd¥Properties

キー: MailMaxMessageSend

最小値: 1

最大値: 1000

デフォルト: 50

タイプ: メッセージ数

E-mail メッセージはしばらく内部キューに入り、それから一緒に送信されます。これはSMTP サーバー接続は1回でよいことを意味します。各メッセージは別々に送られ、サーバーへの接続がクローズされます。

MailMaxMessageSend は1分間に送信されるメッセージ数の最大数です。送信されないメッセージは再びキューに入り、1分後送信されます。

このオプションはメッセージ送信に制限があるSMSゲートウェイ経由で大量のe-mailを送信する場合有効です。メールサーバーの負荷を減少させメッセージ負荷を何回もの間隔にわたって分散させます。

統計メール配信時刻

セクション: HKEY_LOCAL_MACHINE¥SOFTWARE¥Kiwi Enterprises¥Syslogd¥Properties

キー: MailStatsDeliveryTime

最小値: 00:00

最大値: 23:59

デフォルト値: 00:00

タイプ: HH:MM

この値はデイリー統計の送信時刻を指定します。デフォルトでは真夜中(00:00)になります。統計メールを午後6時に送信するには18:00と設定します。

サービス – スタート/ストップ タイムアウト

セクション: HKEY_LOCAL_MACHINE¥SOFTWARE¥Kiwi Enterprises¥Syslogd¥Properties

キー: ServiceStartTimeout

最小値: 1

最大値: 120

デフォルト値: 30

タイプ: 秒

どのくらいの時間Service Manager がService StartあるいはService Stopを待つかを指定します。10アクション以上を設定した場合あるいは300Mhz以下のCPUではその値を大きくしてください。

サービス – プロパティ更新タイムアウト

セクション: HKEY_LOCAL_MACHINE¥SOFTWARE¥Kiwi Enterprises¥Syslogd¥Properties

キー: ServiceUpdateTimeout

最小値: 1

最大値: 120

デフォルト値: 5

タイプ: 秒

どのくらいの時間Service Manager がProperties Update 完了を待つかを指定します。10アクション以上を設定した場合あるいは300Mhz以下のCPUではその値を大きくしてください

DNS – ビジー時にwaitをディセーブルにする

セクション: HKEY_LOCAL_MACHINE¥SOFTWARE¥Kiwi Enterprises¥Syslogd¥Properties

キー: DNSAbortWhenBusy

最小値: 0

最大値: 100

デフォルト値: 10

タイプ: パーセンテージ

ビジー時にWaitをディセーブルにする

通常、IPアドレスがDNSキャッシュに見つからない場合、プログラムはIPアドレスが解決されるまで一定時間待ちます。負荷が高い場合この遅れがメッセージ入力バッファをフルにし、あふれて新しいメッセージが失われます。

このオプションはDNS解決待ちをディセーブルにする前に入力メッセージバッファをフルにする指定ができます。デフォルトでは、入力バッファが10%に達するとSyslog Daemon はIPアドレスが解決されるまで待ちます。

プリオエンティブルックアップをイネーブルにしていると、IPアドレスはバックグラウンドで解決が続けられ結果がキャッシュに入ります。このオプションはバッファに負荷がある間"DNS timeout" 待ち時間をディセーブルにします。解決が行われるのを待たずにバッファに入ったメッセージを処理することができるようプログラムをフリーにします。

入力バッファレベルが設定値を下回ると、通常の解決待ちタイムアウトは再びイネーブルになります。

DNS – 最大キャッシュサイズ

セクション: HKEY_LOCAL_MACHINE¥SOFTWARE¥Kiwi Enterprises¥Syslogd¥Properties

キー: DNSCacheMaxSize

フリーウェア版:

最小値: 50

最大値: 100

デフォルト値: 100

タイプ: キャッシュエントリーの最大値

正規登録版:

最小値: 50

最大値: 20000

デフォルト値: 5000

タイプ: キャッシュエントリーの最大値

キャッシュエントリーの最大数:

キャッシュバッファメモリーサイズを制限します。フリーウェア版は100エントリーまで、正規登録版では20,000エントリーまで可能です。キャッシュに保存したいIPアドレスの数を設定します。

メッセージバッファサイズ

セクション: HKEY_LOCAL_MACHINE¥SOFTWARE¥Kiwi Enterprises¥Syslogd¥Properties

キー: MsgBufferSize

フリーウェアモード:

最小値: 100

最大値: 500

デフォルト: 500

タイプ: メッセージバッファエントリーの最大値

登録正規版:

最小値: 100

最大値: 10,000,000 (1000万)

デフォルト: 20,000

タイプ: メッセージバッファエントリーの最大値

Maximum number of message buffer entries:

受信されたメッセージ(UDP, TCP, SNMP, Keep Alive)は内部キューに入ります。次にメッセージはキューから取り出され到着順(FIFO)に処理されます。プロセスエンジンがビジー状態のとき大量のメッセージが到着すると、メッセージはキューに入ります。付加の重い場合でもメッセージは失われません。

キューに入ったメッセージは少量のメモリーを使います。多くの場合、20,000 メッセージのバッファで十分です。メッセージがバースト状態で受信すると、バッファを大きくできます。バッファ処理はメッセージの流れをスムーズにし、処理エンジンが全部処理できるようにします。

メッセージはUnicodeで保存され、1文字2バイト使います。つまり、各メッセージが100文字であれば200バイトのメモリーが使われます。メッセージは内容によりサイズが異なりますが、100文字の20,000メッセージは4,000,000 bytes (4MB) のメモリーを使います。各メッセージが200文字ならば8MB のメモリーになります。メモリーはメッセージがキューに入る場合だけ使われます。通常のトラフィック負荷では、プロセスエンジンはメッセージフローに追従できメッセージはキューに入りません。

E-mail 追加件名テキスト

セクション: HKEY_LOCAL_MACHINE¥SOFTWARE¥Kiwi Enterprises¥Syslogd¥Properties

キー: MailAdditionalSubjectText

デフォルト: ブランク

タイプ: テキスト

e-mail 件名の前にテキストメッセージが追加されます:

デイリー統計とアラームe-mails件名の先頭にテキスト文字を追加します。デイリー統計とアラームe-mailsを多数のsyslog daemonから受信する場合、どのsyslog daemonから送信されたか特定するための有効な方法を含みます。

syslog daemonの名前やロケーションを最適に説明するテキストを追加します。テキストはe-mail件名の先頭に追加されます。

例:

通常の最大メッセージアラームe-mail 件名です:

Syslog Alarm: 16000 messages received this hour.

MailAdditionalSubjectText を"[London]"に設定すると、アラーム件名e-mailは次のようになります:

[London] Syslog Alarm: 16000 messages received this hour.

既存の件名と分離するため自動的にスペースが追加されます。

E-mail additional body textも参照してください。

E-mail 追加本文テキスト

セクション: HKEY_LOCAL_MACHINE¥SOFTWARE¥Kiwi Enterprises¥Syslogd¥Properties

キー: MailAdditionalBodyText

デフォルト: ブランク

タイプ: テキスト

e-mail 本体への追加テキストメッセージ:

この設定はデイリー統計とアラームe-mailsを含む追加テキストを指定します。デイリー統計とアラームe-mailsを多数のsyslog daemonから受信する場合、どのsyslog daemonから送信されたか特定するための有効な方法を含みます。

syslog daemonの名前やロケーションを最適に説明するテキストを追加します。テキストはe-mail本体の先頭に追加されます。

例:

通常の統計e-mail です:

```
///      Kiwi Syslog Daemon Statistics      ///
```

```
24 hour period ending on: Fri, 06 Feb 2004 13:04:55 +1300
Syslog Daemon started on: Fri, 06 Feb 2004 13:03:54
Syslog Daemon uptime:    24 hours, 0 minutes
-----
```

```
+ Messages received - Total:          20000
+ Messages received - Last 24 hours:  20000
```

MailAdditionalBodyText を"London - Firewall Monitoring Syslog Daemon"に設定すると、デイリー統計e-mail は次のようになります:

```
London - Firewall Monitoring Syslog Daemon
```

```
///      Kiwi Syslog Daemon Statistics      ///
```

```
24 hour period ending on: Fri, 06 Feb 2004 13:04:55 +1300
Syslog Daemon started on: Fri, 06 Feb 2004 13:03:54
Syslog Daemon uptime:    24 hours, 0 minutes
-----
```

```
+ Messages received - Total:          20000
+ Messages received - Last 24 hours:  20000
```

CRLF をテキストの前後に追加してわかりやすくします。

E-mail additional subject textも参照してください。

サービス - Inter-App 通信ポート

セクション: HKEY_LOCAL_MACHINE¥SOFTWARE¥Kiwi Enterprises¥Syslogd¥Properties

キー: NTServiceSocket

最小値: 1

最大値: 65535

デフォルト値: 3300

タイプ: TCP port number

Kiwi Syslog Daemon のManager はサービスとTCP3300で通信します。2つのアプリケーションが通信できます。サービスは表示、警告、統計情報をManagerに送り表示できるようにします。他のプロセスがこのポートを使っている時に変更します。

ファイル書き込みキャッシュ

大量のメッセージ受信時、"Log to file" アクション性能はファイル書き込みキャッシュにより大幅に向上します。

イネーブルにしたとき、"Log to File"アクションはファイル書き込み前にX秒、またはXメッセージをキャッシュに入れます。データはログファイルが更新されるまでメモリーにキャッシュされます。これはメッセージ受信の都度ファイルに書くのに比べ効果的です。

各出力ファイルごとにそれぞれのメモリーキャッシュがあります。多くの場合出力ファイルは一つですが、AutoSplit やフィルターを使うとメッセージは複数ファイルに分類されます。

出力ファイルキャッシュがX秒使用されないと、リソースの節約のためキャッシュは破壊されます。

プログラムが終了すると、すべてのキャッシュがファイルに書かれるため、データの喪失はありません。

ファイル書き込みキャッシュをイネーブルにする

セクション: HKEY_LOCAL_MACHINE¥SOFTWARE¥Kiwi Enterprises¥Syslogd¥Properties

キー: FileWriteCacheEnabled

最小値: 0

最大値: 1

デフォルト: 1

タイプ: 有効 = 1, 無効 = 0

イネーブルにしたとき、"Log to File"アクションはファイル書き込み前にX秒、またはXメッセージをキャッシュに入れます。データはログファイルが更新されるまでメモリーにキャッシュされます。これはメッセージ受信の都度ファイルに書くのに比べ効果的です。

キャッシュ タイムアウト

セクション: HKEY_LOCAL_MACHINE¥SOFTWARE¥Kiwi Enterprises¥Syslogd¥Properties

キー: FileWriteCacheTimeout

最小値: 1

最大値: 120

デフォルト: 5

タイプ: 秒

タイムアウト後キャッシュの内容はディスクにかかれます。タイマーは最初のメッセージがキャッシュ到着時スタートします。キャッシュがフルにならず、タイムアウト前に書き込まれない場合、その内容が自動的に書かれます。この値はメッセージがディスクに書き込まれる前の最長キャッシュ時間です。ディスク書き込み回数が少ないほど、ファイル書き込みは効率的です。

最大キャッシュエントリー数

セクション: HKEY_LOCAL_MACHINE¥SOFTWARE¥Kiwi Enterprises¥Syslogd¥Properties

キー: FileWriteCacheEntries

最小値: 10
最大値: 100,000
デフォルト: 1000
タイプ: キャッシュエントリーの最大数(メッセージ)

ファイル書き込み前、各出力にキャッシュされるメッセージの最大数。

最大数に達するまであるいはタイムアウトまでメッセージはキャッシュに追加されます。メッセージはUNICODEでメモリーに保存されますので、メッセージ1文字当たり2バイト必要です。たとえば、100文字のメッセージは200バイトのメモリーを使います。

キャッシュクリーンアップタイム

セクション: HKEY_LOCAL_MACHINE¥SOFTWARE¥Kiwi Enterprises¥Syslogd¥Properties

キー: FileWriteCacheCleanup

最小値: 10
最大値: 1440
デフォルト: 10
タイプ: 分

キャッシュがインアクティブでメッセージを受信しない場合、クリーンアッププロセスは資源を開放するためキャッシュを破壊します。クリーンアッププロセスはすでにファイルに書かれたインアクティブキャッシュのみを破壊しますので、データの喪失はありません。

ログファイルのロック

セクション: HKEY_LOCAL_MACHINE¥SOFTWARE¥Kiwi Enterprises¥Syslogd¥Properties

キー: FileWriteCacheFileLock

最小値: 0
最大値: 1
デフォルト: 0
タイプ: 有効 = 1, 無効 = 0

効率とセキュリティのため、ログファイルは"append shared"モードでオープンできます。書き込みごとにファイルのオープン、クローズを行うよりも効率を改善します。ファイルのオープンの間、他のアプリケーションが内容を変更したり、削除することができません。新しいエントリーのみを追加できます。見るためにファイルをオープンできますが、変更のためにはオープンできません。

大量のsyslog メッセージを受信する場合、このオプションをイネーブルにして性能を上げます。唯一の欠点は、ファイルが新しいログエントリーをすぐには反映しないことです。OSは内部バッファがフルになるまでデータをキャッシュし、それからファイルに書きます。メッセージが多いときは、すぐにこの状態になりますが、少ないときはバッファがフルになりデータが書かれるまで時間がかかります。キャッシュがFileWriteCacheCleanup分間インアクティブの間、ログファイルが自動的に更新されクローズされます。

オープンログファイルの最大数

セクション: HKEY_LOCAL_MACHINE¥SOFTWARE¥Kiwi Enterprises¥Syslogd¥Properties

キー: FileWriteCacheOpenFiles

最小値: 1
最大値: 250
デフォルト: 100
タイプ: 最大数

FileWriteCacheFileLock が1のとき(有効)、各ログファイルは"append shared" モードでオープンされています。プログラムは同時に最大255ファイルまでオープンできます。この値は同時オープンファイルの最大数を設定します。この制限に達すると、現在のキャッシュの**FileWriteCacheFileLock** 値がディセーブルになり、キャッシュ書き込みの都度オープン、クローズされます。Log to File アクションがAutoSplit 文でログホストごとに独立したファイルを作成すると、同時に255ファイル以上がオープンされる可能性があります(255のアクティブ送信ホストがあれば)。システム資源の利用を適切にするには100ファイルをお勧めします

アーカイブ置き換え文字

セクション: HKEY_LOCAL_MACHINE¥SOFTWARE¥Kiwi Enterprises¥Syslogd¥Properties

キー: ArchiveFileReplacementChr

デフォルト: "-" (dash)

タイプ: 文字、文字列

アーカイブプロセスは現在のシステム日時を使ってアーカイブのためのファイルやフォルダーを作成します。

日付フォーマットはユーザーが選択できますので、ファイル名として正しくない文字を含むことがあります。アーカイブプロセスは不正な値 ("&*+=:;./¥|?<>") を正しい文字 ("-") に置き換えて正しいファイルやフォルダー名を作成します。

Fたとえば、システム日時が"2004/12/25 12:45:00"であれば、アーカイブプロセスは名前を"2004-12-25 12-45-00"と変更します。この文字列がアーカイブプロセスのファイルやフォルダー名となります。 "-"の代わりに、他の文字を選択できます。不正な文字を使用すると、アーカイブプロセスは不正なファイルやフォルダー名を作成しますので注意してください。

アーカイブ分離文字

セクション: HKEY_LOCAL_MACHINE¥SOFTWARE¥Kiwi Enterprises¥Syslogd¥Properties

キー: ArchiveFileSeparator

デフォルト: "-" (dash)

タイプ: 文字、文字列

アーカイブスケジュールを"Use dated file names"に設定すると、既存のファイル名と現在のシステム日時の間にセパレータが入ります。通常この文字はダッシュ("-")です。レジストリー設定を変更して代替文字を使用することができます。

コマンドライン引数

コマンドライン引数

Syslogd.exeのスタート時、次のコマンドライン引数が使われます。パラメータは大文字、小文字を区別しません。複数パラメータを指定する時はスペースで区切ってください。

デバッグ開始

コマンドラインの値: DEBUGSTART

適用: Syslogd.exe, Syslogd_Service.exe & Syslogd_Manager.exe

効果:

この値で実行すると、インストールディレクトリーにデバッグファイルが作成されます。ファイル名はexeで異なります(下記)。デバッグファイルにはプログラムスタートアップとソケット初期化ルーティンの結果が含まれます。

作成されるファイル:

SyslogNormal = Syslogd_Startup.txt

SyslogService = Syslogd_Service_Startup.txt

SyslogManager = Syslogd_Manager_Startup.txt

使用する時:

プログラムがInput設定オプションで指定したポートのメッセージを受信していないように見える時。ソケットの初期化が正常化をstart-upデバッグファイルでチェックします。

プログラムがスタートアップでストップする時、問題のありかを探す手助けになります。

サービスインストール

コマンドラインの値: -INSTALL

適用: Syslogd_Service.exe

効果:

NTあるいは2000マシンでSyslog Daemon をサービスとしてインストールする。メッセージボックスに成功又は失敗が示されます。

使用する時:

Syslog Daemon Service ManagerのManageメニューでインストールエラーになった時。あるいはバッチファイルで自動サービスインストールが要求された時。

サービスアンインストール

コマンドラインの値: -UNINSTALL

適用: Syslogd_Service.exe

効果:

NTあるいは2000マシンのSyslog Daemon サービスをアンインストールする。メッセージボックスに成功又は失敗が示されます。

When to use:

Syslog Daemon Service ManagerのManageメニューでアンインストールエラーになった時。あるいはバッチファイルで自動サービスインストール/アンインストールが要求された時。

アンインストールの前にサービスがストップしていることを確認して下さい。

設定にINI ファイルを使用

通常プログラムのスタート時設定がレジストリーから読み込まれます。遠隔地から設定を変更したい時特別なINIファイルをインストールフォルダーに置き、そこから設定を読みます。このINIファイルは遠隔地のマシンからフォルダーにコピーできます。次にサービス又はスタンダード版がスタートする時、INIファイルから設定を読みそれ以降のためレジストリーに書かれます。設定が読まれたことを示すため特別なINIファイルは削除されます。INIファイルが削除されないようにするにはそのファイルの属性をReadのみにします。

プログラムのスタートアップ時プログラムはインストールフォルダーのLoadNewSettings.ini を探します(通常は C:¥Program files¥Syslogd)。見つかったら、INIファイルから設定が読まれ、レジストリーキー: HKEY_LOCAL_MACHINE¥SOFTWARE¥Kiwi Enterprises¥Syslogd のレジストリーに置かれます。

その後ファイルが削除され、再度読み込まれるのを防ぎます。プログラムはレジストリーから設定を読みいつもの様にスタートします。INIファイルの設定は既存のレジストリー設定に上書きされます。

INIファイルはどのような正規のKiwi Syslog Daemon INI でもかまいません。File | Export メニューまたは Defaults/Import/Export で設定のエクスポートができます

INIファイルは手で変更するものではありません。多くのエンコードされたルール、アクション、フィルターを含んでいます。しかし、もし手で変更するのであればドライブ名を変更してください(例 CをDにする)。ノートパッドの検索と置き換えでできます。エンコードされた文字は変更しないで下さい。INIファイルの読み込みで予期しないエラーになります。不明な時はsupport@kiwisyslog.com または support@jtc-i.co.jp まで連絡してください。

Syslog 関連ソフトウェア

Kiwi SyslogGen

Windows 95/98/ME/NT4/2K/XP用Syslogメッセージジェネレーターです。

Kiwi SyslogGen はGUIからUnixタイプのSyslogメッセージを生成しSyslog Daemonに送信します。

Kiwi SyslogGen でSyslog Daemon 設定と通信の問題をテストできます。

メッセージ生成オプション

- ランダムにFacility とLevelでプライオリティを選択できます
- 既成またはユーザー入力によるメッセージ
- 送信繰り返し(一度、毎秒、毎分、連続的)
- Kiwi Syslog Daemon にプロキシー送信
- Syslog Daemon サーバーの受信テストでランダムな不正パケットを発生
- (メッセージプロキシーはSyslog Daemon から他のサーバーに本来の送信元IPとホスト名のままメッセージを送ることです)

Kiwi SyslogGen の最新バージョンはwww.kiwisyslog.comからダウンロード可能です。

Kiwi Logfile Viewer

Kiwi Logfile viewer はWindows 95/98/ME/NT4/2K/XP 用の無料アプリケーションです。

Kiwi Syslog Daemon のタブ区切りログファイルを読み易く表示します。

機能:

- 列でソート
- ドラッグ&ドロップで列の並び替え
- タブ区切りファイルフォーマットで出力
- カンマ区切りファイルフォーマットで出力
- ブラウザ用にHTMLテーブルで出力
- タブ区切りファイルの読み込み
- カンマ区切りファイルの読み込み
- コマンドラインオプションとスイッチ
- ヘッダーに標準Syslog フィールドタイトルを使用
- デフォルトを設定

訳者 あとがき

可能な限り原文に即して翻訳しましたが、意図的に変更した部分もあります。気づかない誤訳もあり得ますので、お気づきの点がありましたらコンピュータテクノロジー(株)までご連絡ください。

Your index page goes here...

In MS-Word, select INDEX AND CONTENTS from the INSERT menu.
Select INDEX and click OK.