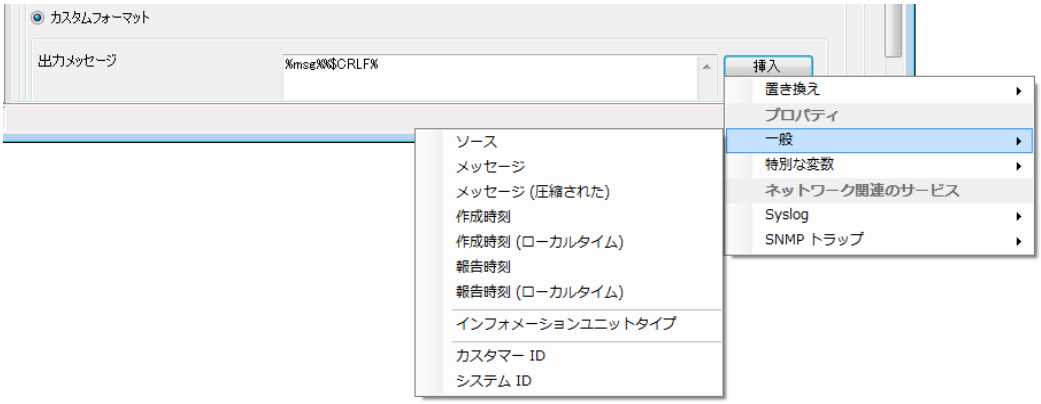
2017/11/21

WinSyslogプロパティリスト（挿入可能な変数）

WinSyslog ver.14.3

■WinSyslogのアクションでは、様々なプロパティを変数として出力することができます。（例：「ファイルログ」アクション）



※出力エンコードを**UTF-8**として日本語メッセージの文字化けが発生する場合など、メッセージに日本語が含まれる場合は、
カスタムフォーマットを使用してください。

置き換え：デフォルトで準備されている出力フォーマットを選択できます。	
フォーマット名	**設定内容**
Adiscon Eventlog Format	%timegenerated:1:10%,%timegenerated:12:19%,%source%,%syslogfacility%,%syslogpriority%,EvntSlog: %id%,%user%,%sourceproc%,%NTEventLogType%,%severity%,%category%,%msg%%$CRLF%
Monilog Format	%timegenerated:1:10%,%timegenerated:12:19%,%source%,%syslogfacility%,%syslogpriority%,EvntSlog: %severity% %timereported:::uxTimeStamp%: %source%/%sourceproc% (%id%) - "%msg%"%$CRLF%
EventReporter レガシーフォーマット	%severity% %timegenerated:::uxTimeStamp%: %user%/%nteventlogtype%/%source%/%sourceproc% (%id%) - "%msg:::spacecc,compressspace%"%$CRLF%

※上記はいずれもUTC時刻表示となりますので、ローカルタイムで記録したい場合は、下記のように入力します。
%timegenerated:1:10:localtime%, %timegenerated:12:19:localtime%, %timegenerated:::uxLocalTimeStamp%

プロパティ		
プロパティ名	**値**	**内容**
一般		
ソース	%source%	メッセージ送信元（IPまたはhostname）
メッセージ	%msg%	メッセージ
メッセージ (圧縮された)	%msg:::spacecc,compressspace%	メッセージ内の制御文字をスペースに置き換え、更に2つ以上連続したスペースを1文字に圧縮します。
作成時刻	%timegenerated% ***1**	メッセージ生成時刻（受信時刻） （**UTCタイム**で記録されます）
作成時刻 (ローカルタイム)	%timegenerated:::localtime%	ローカルタイムでのメッセージ生成時刻
報告時刻	%timereported% ***1** ***2**	メッセージが報告された際、発信元が報告する時間 Syslogの場合はメッセージのタイムスタンプとなります。 デバイス時刻によるので、正確でない場合があります。 Windowsイベントログの場合、イベントログレコードからのタイムスタンプが含まれます。（**UTCタイム**で記録されます）
報告時刻 (ローカルタイム)	%timereported:::localtime%	ローカルタイムでのメッセージ報告時刻
インフォメーション ユニット タイプ	%iut%	メッセージのタイプ 1-syslogメッセージ 2-ハートビート 3-Windowsイベントログ 4-SNMPトラップ・メッセージ
カスタマー ID	%CustomerID%	全体（General）オプションで設定可能
システム ID	%SystemID%	全体（General）オプションで設定可能

***1「作成時刻」「報告時刻」はUTCを基準とした時刻となります。ローカルタイムで記録する場合、直ぐ下の（ローカルタイム）を使用します。**
***2 メッセージ中に含まれる報告時刻を出力するには他にも設定する項目があります。詳しくはJTCブログ**
「WinSyslog 使い方ガイド#2～受信時刻とデバイスタイムスタンプ両方を出力～ 」を参照してください。↓

https://jtc-logmanagementmaster.blogspot.jp/2017/06/winsyslog-2.html

特別な変数		
TAB	%$TAB%	US-ASCIIの水平タブ（HT、0x09）
改行コード(CRLF)	%$CRLF%	CRとLFから構成されているWindows改行文字シーケンス
改行(CR)	%$CR%	US-ASCIIのCR
ラインフィード(LF)	%$LF%	US-ASCIIのLF
新規 UUID(Universally Unique Identifiers)	$NEWUUID	新しいUUID（Universally Unique Identifiers)を含みます。これは、32桁の16進数として表される128bit数です。

ネットワーク関連のサービス		
プロパティ名	値	内容
Syslog		
ファシリティ	%syslogfacility%	syslogメッセージのファシリティ値 KERN(0)～LOCAL7(23)
プライオリティ	%syslogpriority%	syslogメッセージのシビラティ(Severity)値（プライオリティ値） 0(Emergency)～7(Debug)
ファシリティ テキスト	%syslogfacility_text%	ファシリティ値に対応して変換されます。 "Kernel", "User", "Mail","Daemons", "Auth", "Syslog", "Lpr", "News", "UUCP","Cron", "System0", "System1", "System2", "System3","System4", "System5", "Local0", "Local1", "Local2","Local3", "Local4", "Local5", "Local6", "Local7"
プライオリティ テキスト	%syslogpriority_text%	Severity値に対応して変換されます。 "Emergency", "Alert", "Critical", "Error", "Warning", "Notice", "Informational", "Debug"
Syslog タグ	%syslogtag%	syslogタグ値（短い文字列）。 フィルタで使用されます。
Syslog バージョン	%syslogver%	RFC5424メッセージが受信された場合に1以上のシスログバージョン番号を含みます。それ以外は0になります。
Syslog Appname	%syslogappname%	RFC5424形式のメッセージの場合のみ、使用可能なアプリケーション名ヘッダが含まれます。または、このフィールドはSyslogTagによってエミュレートされます。
Syslog ProcID	%syslogprocid%	RFC5424形式のメッセージの場合のみ、procidフィールドが含まれます。
Syslog MSGID	%syslgomsgid%	RFC5424形式のメッセージの場合のみ、msgidフィールドが含まれます。
Syslog Structdata	%syslogstructdata%	RFC5424形式のメッセージの場合のみ、構成ヘッダフィールド（RAW形式）が含まれます。
RAW Syslog Message	%rowsyslogmsg%	RAWメッセージ（未解析）を含みます。
SNMP トラップ		
バージョン	%snmp_version%	SNMPトラップのバージョン
Uptime	%snmp_uptime%	システムの稼働時間
Version 1 parameters		[SNMP version1の変数]
コミュニティ	%snmp_community%	SNMPのコミュニティ名
エンタープライズ	%snmp_enterprise%	SNMPのエンタープライズOID
Generic Name	%snmp_generic_name%	SNMPのGeneric name
Specific Type	%snmp_specifictype%	SNMPのSpecific Type
Agent IP	%snmp_agentip%	SNMPのエージェントIPアドレス
Version 2 parameters		[SNMP version2の変数]
Snmp variable 1	%snmp_var_1%	SNMPトラップで設定されている場合、その値が割り当てられます。
Snmp variable 2	%snmp_var_2%	SNMPトラップで設定されている場合、その値が割り当てられます。
Snmp variable 3	%snmp_var_3%	SNMPトラップで設定されている場合、その値が割り当てられます。

イベントログに関するプロパティ：EventReporterよりSETP送信されたイベントログで使用できます（Enterprise版のみ有効な機能）

参考： プロパティ変換について

WinSyslogには以下のようにプロパティ値を切り出して再構築する機能があります。
詳細はマニュアル↓ 項番9.2.1 Acessing Properties（P.134)をご参照ください。

http://www.jtc-i.co.jp/support/documents/guide-e/winsyslog-131.pdf

%property:fromPos:toPos:options%

fromPos プロパティ値全部の文字列を使用したくない場合は、開始位置を指定できます。最初の文字は1からスタートします。
toPos プロパティ値全部の文字列を使用したくない場合は、終わりの位置を指定できます。最初の文字は2からスタートします。
options オプションを追加するとプロパティの内容を変更することができます。オプションはカンマで区切って複数セットできます。

例1）%timereported:::localtime% ：メッセージのタイムスタンプをローカルタイムで表示（fromPosとtoPosの指定はなし）
例2）%msg:::spacecc,compressspace% ：制御文字をスペースに置き換え、更に2つ以上連続したスペースを1文字に圧縮
例3) %source:::toipv4address% :名前解決が可能な場合、ホスト名を有効なIPアドレス文字列に変換

参考： Retrospectiveで閲覧する場合のサンプルフォーマット

Syslog ファシリティやレベルで検索しやすいように、プロパティは「**ファシリティ テキスト**」および「**プライオリティ テキスト**」を出力します。
%timereported:::localtime%,**%syslogfacility_text%**.**%syslogpriority_text%**,%source%,%msg%%$CRLF%