2017 年 7 月 3 日

WinSyslog イベントログ書き込みアクション設定

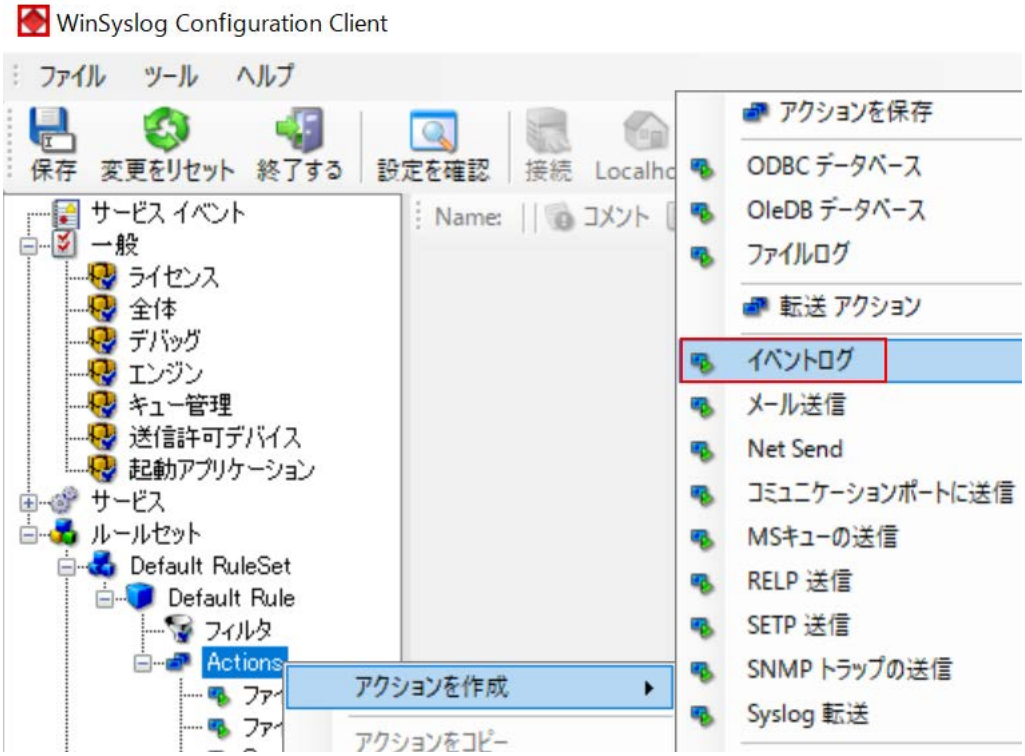
WinSyslog サービスで処理されるメッセージを Windows のイベントログに記録する設定について説明します。

1 WinSyslog Configuration Clientでイベントログアクションを追加

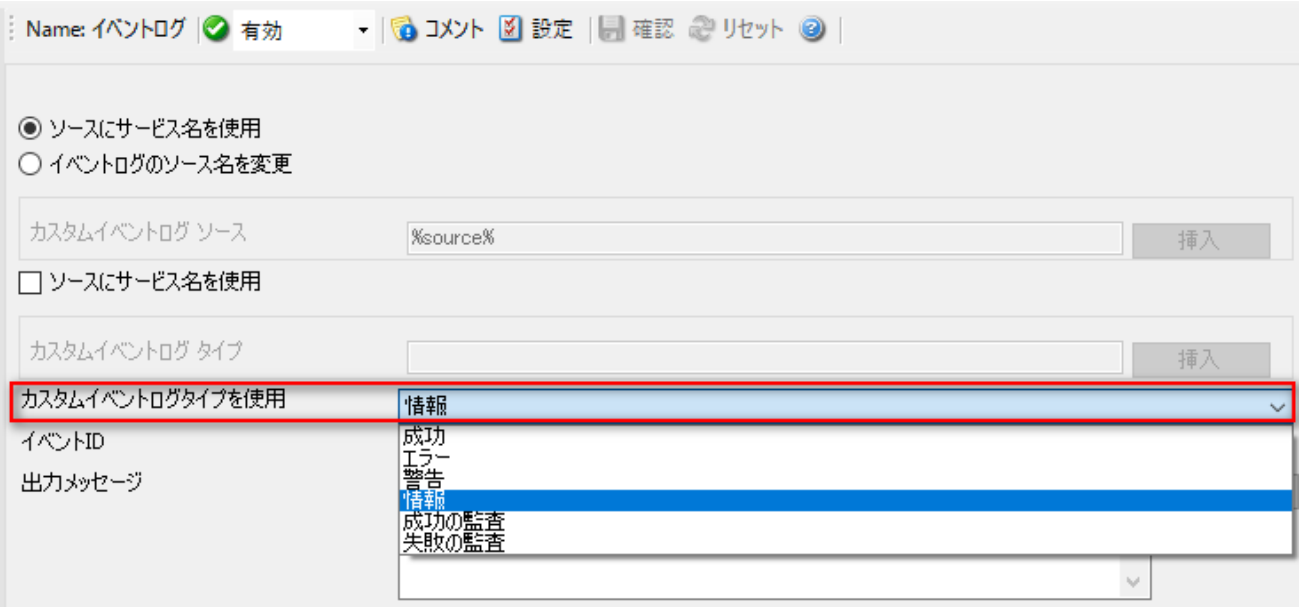
追加したいルールの Action 上で右クリック＞アクションを作成＞イベントログを選択します。

注意 ： この GUI が英語表示の場合は、以下の手順で日本語に変更してください。

http://www.jtc-i.co.jp/support/documents/etc/winsyslog_language_setting.pdf



カスタムイベントログタイプを使用フィールドでイベントログに記録されるレベルをプルダウンリストより選択できます。(Ver.14.0 以前は番号を手動で入力します。1: エラー、2: 警告、4: 情報)



2 その他のオプション

2.1 イベントログのソース名を変更

デフォルトで出力されるソース名は、"AdisocnWinSyslog"ですが、送信元 IP(ホスト名)に変更できます。
ただし、IP アドレスをイベントソースとした場合、それは登録されていないので、イベントビューアは、ログの初めにコンポーネントインストールされていないというメッセージをユーザーに警告します。
転送された実際のメッセージは詳細タブでも確認できます。

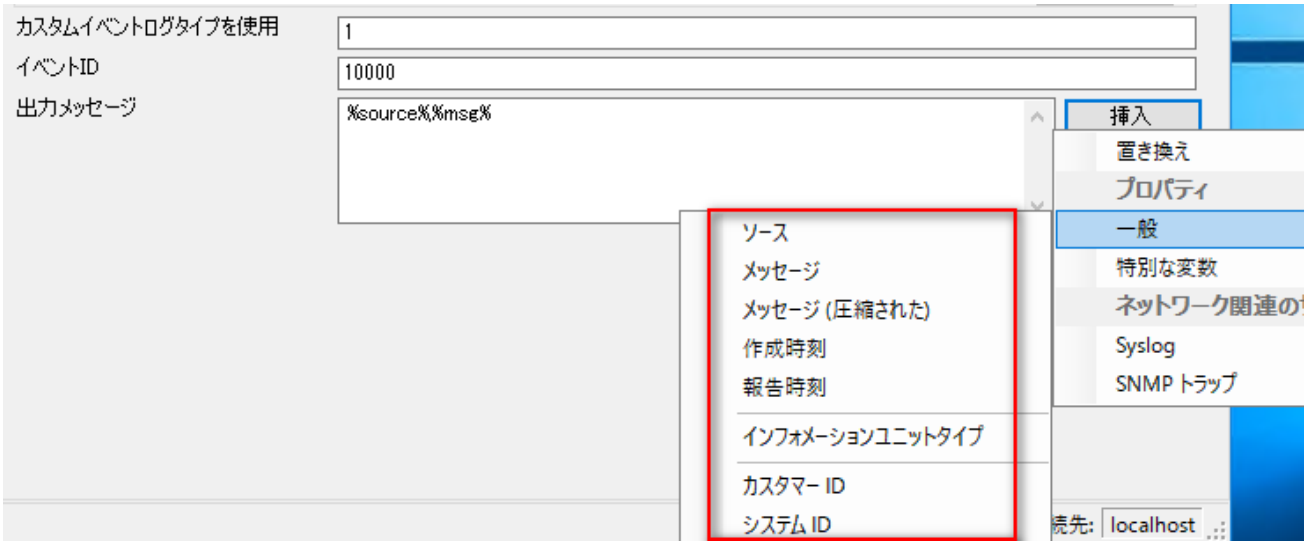
2.2　イベントID

イベントログが書き込まれるイベント ID を変更することができます。デフォルトでは 10000 です。
ただし、オペレーティングシステムで登録されていない ID が書き込まれると、Windows イベントビューアには、実際のメッセージ・テキストより先に未登録を指摘するエラー・メッセージが表示されます。
このエラーを避けるために、OS では 10,000 から 10,100 の ID が設けられています。
ですので、カスタマイズした全てのメッセージにはこれらの ID を使用することをお勧めします。

注意：　10,000 以下の ID は、WinSyslog　によって生成されるイベントと衝突する可能性があるので、おすすめできません。（デフォルトは、10000 です）

2.3　出力メッセージ（ログメッセージ）

Windows　のイベントログに書き込まれるメッセージを設定できます。
「挿入」をクリックし、%msg%（例）などの置換文字を追加することで、イベントビューアに書き込まれるイベントログのメッセージをカスタマイズすることが可能となります。
出力可能なプロパティは、挿入＞一般　より選択できるプロパティです。




Application イベント数: 5,131
レベル
日付と時刻
ソース
イベン...
タスクのカテゴリ
情報
2017/04/19 15:42:35
AdisconWinSyslog
10000
なし
イベント 10000, AdisconWinSyslog
全般
詳細
Notice,これはAuditFailureレベルのテストシスログメッセージです。
ログの名前(M):
Application
ソース(S):
AdisconWinSyslog
ログの日付(D):
2017/04/19 15:42:35
イベント ID(E):
10000
タスクのカテゴリ(Y):
なし
レベル(L):
情報
キーワード(K):
クラシック,失敗の監査