

BOM 6.0 Kiwi Syslog Server 連携キット

セイ・テクノロジーズ株式会社

目次

1. 概要	1
1.1. 環境条件	1
2. 連携キットの適用手順	2
2.1. 事前準備	2
2.2. Kiwi Syslog Server 用設定ファイルのインポート	2
2.3. BOM 監視設定のインポート	3
2.4. 監視項目の選定	4
2.5. Syslog 監視でのログファイルパスの修正	4
2.6. Syslog 監視での検索文字列の追加	5
2.7. それぞれのサービスの起動	6

1. 概要

BOM 6.0 Kiwi Syslog Server 連携キットは、Windows OS 上で動作する Kiwi Syslog Server にて受信し書き出したログを、BOM for Windows Ver.6.0 (以降 BOM 6.0 と記)にて検知するために必要な、双方の設定ファイルやその手順書から構成されています。

特に SNMP Trap や syslog プロトコルが、サーバーや OS の各種アラートの主な伝達手段になっている構成下では、既存のサーバー監視要件と合わせて効率的なサーバー監視ソリューションを構築可能です。

1.1. 環境条件

BOM 6.0 Kiwi Syslog Server 連携キットは、以下の条件を満たしている場合にご利用頂けます。

BOM for Windows Ver.6.0 の動作要件を満たし、正常にインストールされ監視インスタンスが正常に動作していること。

※BOM の監視形態はローカル監視インスタンスでも代理監視インスタンスでも本キットは使用可能ですが、本書ではローカル監視インスタンスを前提として記載いたします。

Kiwi Syslog Server Version 9.3.4 の動作要件を満たし、正常にインストールされ動作していること。

※Kiwi Syslog Server はサービス版としてインストールする事を推奨いたします。本書では以降サービス版がインストールされている事を前提として記載いたします。

動作要件の詳細はそれぞれのドキュメント(‘BOM for Windows Version 6.0 Readme’ 並びに ‘Kiwi Syslog Server ver.9.3 ユーザーズマニュアル’)を参照下さい。

2. 連携キットの適用手順

2.1. 事前準備

BOM 6.0 と Kiwi Syslog Server を各製品に同梱されているインストール手順に従いインストールしてください。

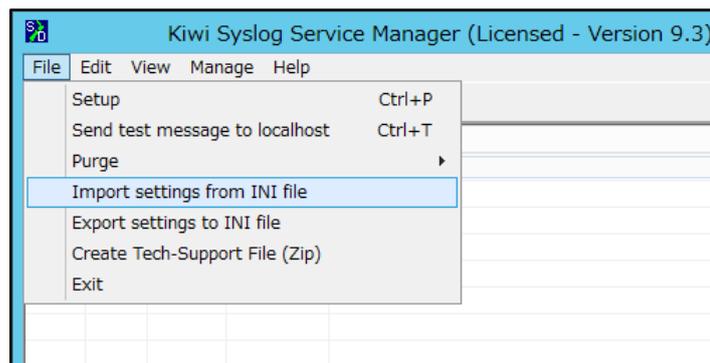
BOM 6.0 での監視インスタンスを作成した上で監視サービスを停止状態にしてください。

Kiwi Syslog Service Manager にて Syslogd サービスを停止状態にしてください。

2.2. Kiwi Syslog Server 用設定ファイルのインポート

Kiwi Syslog Server での設定ファイルのインポート方法については‘Kiwi Syslog Server ver.9.3 ユーザーズマニュアル’を参照してください。

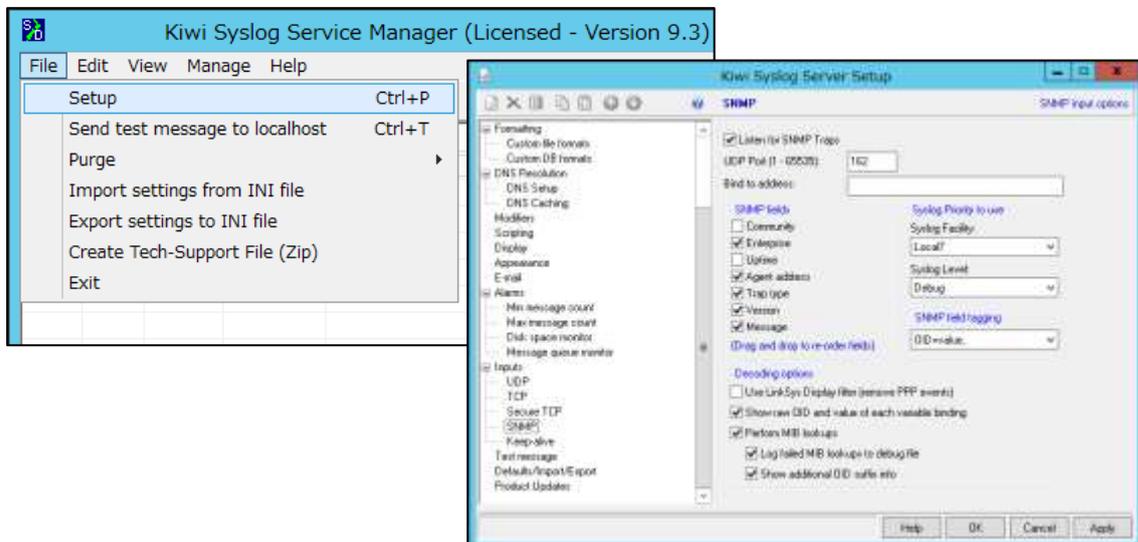
1. 連携キットよりファイル“Syslog Server Settings.ini”を任意のフォルダーに展開します。
2. Kiwi Syslog Service Manager を起動し、メニューの[File]-[Import settings from INI file]より、“Syslog Server Settings.ini”ファイルをインポートします。



3. Input (入力) の SNMP の部分が連携用の設定になりますので、ご確認ください。

その後、必要に応じてそれ以外の追加設定も行ってください。

設定の確認・修正は Kiwi Syslog Service Manager メニューの[File]-[Setup]から行う事が可能です。

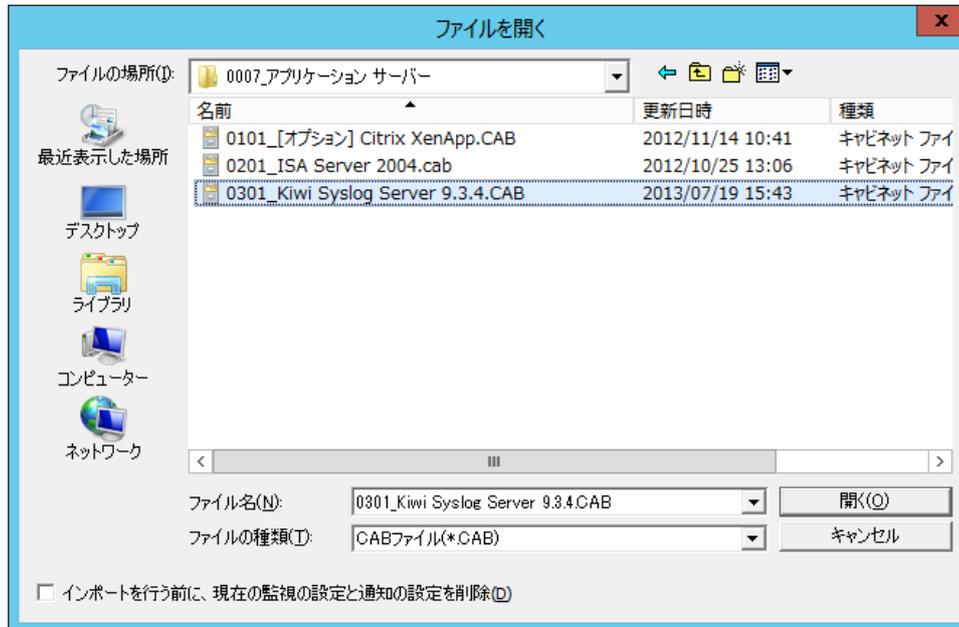


2.3. BOM 監視設定のインポート

BOM 6.0 での監視設定ファイルのインポート方法については‘BOM for Windows Ver.6.0 ユーザーズ マニュアル’の“3.7.2 監視設定のエクスポートとインポート”を参照してください。

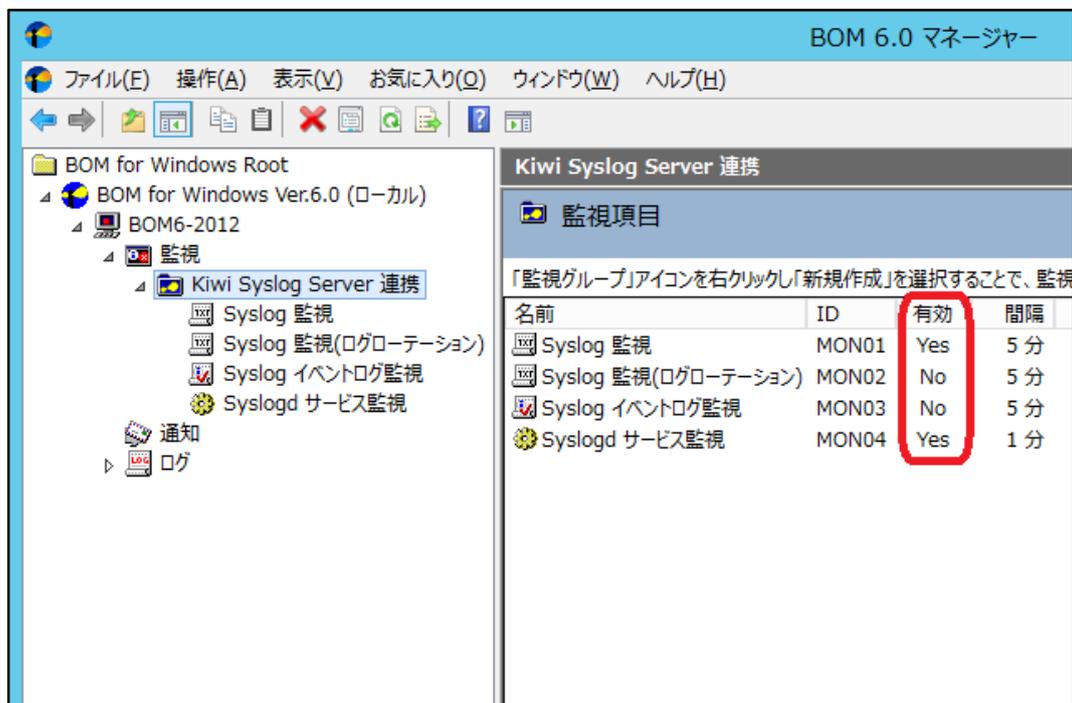
また本キットは BOM 6.0 のテンプレート形式に準拠していますので、あらかじめテンプレートフォルダーに必要なファイルを展開の上、テンプレートのインポート機能を使用してください。テンプレートのファイルの展開方法とテンプレートのインポートについては‘Kiwi Syslog Server 9.3.4 連携テンプレート ReadMe’と‘BOM for Windows Ver.6.0 ユーザーズ マニュアル’の“3.7.1 テンプレートのインポート”を参照してください。

1. 連携キットよりファイル“0301_Kiwi Syslog Server 9.3.4.CAB”を任意のフォルダーに展開します。
2. BOM 6.0 マネージャを起動し、当該サーバーに接続した上で、監視インスタンスを右クリックしコンテキストメニューより“監視設定のインポート”をクリックし、ファイル“0301_Kiwi Syslog Server 9.3.4.CAB”をインポートします。



2.4. 監視項目の選定

監視設定ファイルをインポートした直後は“Syslog 監視”と“Syslog サービス監視”の2つが有効となっています。



この“Syslog 監視”は単一のテキストログファイルを想定した設定になっていますので、Kiwi Syslog Server の設定がログローテーションになっている場合には、“Syslog 監視(ログローテーション)”を有効にし、“Syslog 監視”は無効にします。

また、Kiwi Syslog Server の設定がイベントログへの出力になっている場合には、上記の代わりに“Syslog イベントログ監視”を有効にします。

※Kiwi Syslog Server は出力対象のログに日本語文字を含む場合に、イベントログへの出力には対応しておりません。テキストログへの出力での運用をお願いいたします。

Kiwi Syslog Server をアプリケーションモードで運用する場合には“Syslog サービス監視”を無効にします。

2.5. Syslog 監視でのログファイルパスの修正

“Syslog 監視” および、“Syslog 監視(ログローテーション)”の監視項目内に設定してある既定の有効なログファイルのパス下記のいずれかになっています

“C:\Program Files (x86)\Syslogd\Logs\SyslogCatchAll.txt”

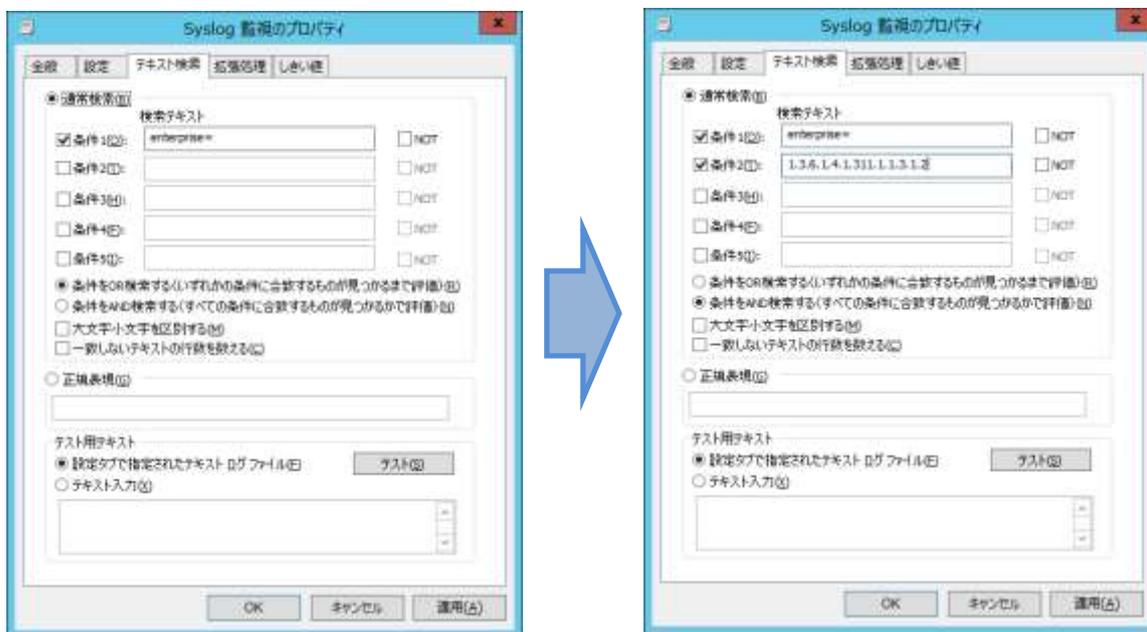
“C:\Program Files (x86)\Syslogd\Logs\SyslogCatchAll.txt.*”

Kiwi Syslog Server のインストールパスや出力ログファイルパス、または OS の種類(32 ビット or 64 ビット)によっては変更する必要がありますので、ご利用の環境を確認の上適切なアドレスへ変更してください。

※32 ビット OS の場合には“Program Files (x86)”の部分が“Program Files”となります。

2.6. Syslog 監視での検索文字列の追加

監視設定ファイルをインポートした直後の検索テキストは“enterprise=”だけが設定されています。必要に応じて検索テキストを追加する事により検知したいログを絞り込む事が可能になります。

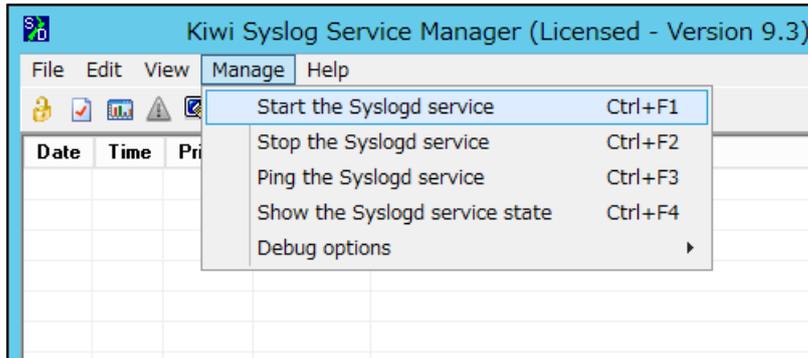


OID を指定する事によってさらにログを絞り込む設定

2.7. それぞれのサービスの起動

変更した設定内容を適用するため、それぞれのサービスを開始します。

Kiwi Syslog Service Manager などから Syslogd サービスを開始状態にします。



BOM 6.0 マネージャや OS のサービスなどから監視サービスを開始状態にします。

