BalaBit

syslog-ng Agent for Windows　6 LTS

管理者ガイド

Rev.1.0

BALABIT

CONTEXTUAL SECURITY INTELLIGENCE

2017.3.23

JTC-i Jupiter Technology corp. ジュピターテクノロジー

目次

1 まえがき 1
1.1 各章の要約 1
1.2 対象読者と前提条件 2
1.3 このガイドに記載されている製品 2
1.4 本ガイドの表記 2
1.5 お問合せ先とカスタマーポータル 4
2 イントロダクション 5
2.1 サポートされているオペレーティングシステム 5
3 syslog-ng エージェントのインストール 6
3.1 スタンドアロンモードで syslog-ng エージェントをインストールする 7
3.2 ドメインコントローラーとドメインのホストに syslog-ng エージェントをインストールする 9
3.2.1 ドメインコントローラーとドメインのホストに syslog-ng エージェントをインストールする 9
3.3 サイレントインストール 12
3.4 syslog-ng エージェントの MSI パッケージをカスタムフォルダにインストールする 14
3.5 syslog-ng Agent for Windows を最新バージョンにアップグレードする 15
3.6 syslog-ng エージェントのアンインストール 16
3.7 サイレントモードでの syslog-ng エージェントのアンインストール 16
4 syslog-ng エージェントの設定方法 17
4.1 スタンドアロンの syslog-ng エージェントの設定 17
4.2 ドメインの syslog-ng エージェントの設定 18
4.2.1 ドメインホストの syslog-ng エージェントの設定 18
4.2.2 ドメインコントローラーの syslog-ng エージェントの設定 19
4.2.3 ドメインとローカルの設定 20
4.3 XML ベースの設定ファイルの使用 21
4.3.1 syslog-ng エージェントの XML 設定ファイルを作成する 22
4.3.2 XML ファイルからの syslog-ng エージェントの設定 22
5 宛先の設定 24
5.1 宛先ログサーバーの設定 25
5.2 メッセージレートを制限する 33
5.3 MARK メッセージの送信 33
5.4 Syslog-ng Agent for Windows のフローコントロール 34
6 メッセージソースの設定 35
6.1 イベントログソース 35

6.1.1 イベントログソースを管理する....37
6.1.2 イベントログソースを追加する....37
6.1.3 Windows Vista 以降でカスタムイベントログコンテナの名前を特定する....39
6.1.4 Windows XP または Server 2003 でカスタムイベントログコンテナの名前を特定する....39
6.2 ファイルソースの管理....40
6.3 内部ソースを管理する....45
6.4 グローバルセッティングの設定....46
6.5 ホスト名のフォーマット設定....47
6.6 ソースとフィルターをグローバルに無効にする....49
7 syslog-ng エージェントでの SSL の使用....50
7.1 暗号化接続を有効にする....50
7.2 syslog-ng エージェントによる相互認証の使用....52
7.2.1 syslog-ng Agent for Windows を使用した相互認証の設定....53
7.3 Microsoft 管理コンソール(MMC)を使用した証明書のインポート....54
8 メッセージのフィルタリング....55
8.1 イベントログメッセージのフィルタリング....56
8.2 ファイルメッセージのフィルタリング....62
9 メッセージフォーマットのカスタマイズ....64
9.1 テンプレートを使用したメッセージのカスタマイズ....64
9.2 syslog-ng エージェントで使用されるタイムスタンプのカスタマイズ....65
9.3 syslog-ng エージェントで使用可能なマクロ....66
9.3.1 プロトコルヘッダーに関連するマクロ....67
9.3.2 時刻関連に関連するマクロ....67
9.3.3 イベントログソースに関連するマクロ....69
9.3.4 ファイルソースに関連するマクロ....71
10 syslog-ng エージェントサービスの制御....72
10.1 コマンドラインオプション....73
11 Windows 用 syslog-ng エージェントのトラブルシューティング....74
11.1 メッセージ送信と CPU 負荷....76
11.2 syslog-ng エージェントのデバッグ....77
11.2.1 コアダンプとメモリダンプの作成....77
11.2.2 syslog-ng エージェントでのデバッグログの有効化....78
11.2.3 ドメイン設定の問題のトラブルシューティング....79
11.3 Windows Vista 以降でイベントログメッセージを読むのが遅い....80
11.3.1 Windows Vista 以降で EVT API を使用する際の制限事項....80
11.3.2 Windows Vista 以降で EVT API を有効にする....81

12 Windows での監査ポリシーの設定 82
12.1 Windows XP でセキュリティログを有効にする 83
12.2 ドメインコントローラーのセキュリティログを有効にする 83
12.3 Windows 2003 Server で監査を有効にする 84

変更履歴

版	発行日	変更内容
Rev. 1.0	2017/3/23	新規作成

1　まえがき

このドキュメントでは、syslog-ng Agent for Windows を設定および管理する方法について説明します。また、製品が使用する技術および概念の背景情報についても説明します。

注意：
syslog-ng Premium Edition アプリケーションの Linux/Unix バージョンの設定と管理の詳細については、「syslog-ng Premium Edition 6 LTS 管理者ガイド」を参照してください。
IBM System i アプリケーション用の syslog-ng エージェントの設定と管理の詳細については、「The syslog-ng Agent for IBM System i Administrator Guide」を参照してください。

1.1　各章の要約

第 1 章：「まえがき」、この章です。

第 2 章：「イントロダクション」では、syslog-ng PE の主な機能と目的について説明します。

第 3 章：「syslog-ng エージェントのインストール」では、さまざまなシナリオで syslog-ng エージェントをインストールする方法と、新しいバージョンにアップグレードする方法について説明します。

第 4 章：「syslog-ng エージェントの設定方法」では、syslog-ng Agent for Windows の設定と管理について詳しく説明しています。

第 5 章：「宛先の設定」では、宛先の設定とメッセージレートの制御について詳しく説明します。

第 6 章：「メッセージソースの設定」では、メッセージソースの設定について説明します。

第 7 章：「syslog-ng エージェントでの SSL の使用」では、syslog-ng エージェントで SSL 暗号化接続を使用する方法について詳しく説明しています。

第 8 章：「メッセージのフィルタリング」では、ブラックリストまたはホワイトリスト形式でログメッセージをフィルタリングする方法について説明します。

第 9 章：「メッセージフォーマットのカスタマイズ」では、テンプレートを使用して、イベントログおよびファイルソースから受信したメッセージの形式をカスタマイズする方法について説明します。

第 10 章: 「syslog-ng エージェントサービス制御」では、syslog-ng エージェントサービスの制御について詳しく説明しています。

第 11 章: 「Windows 用 syslog-ng エージェントのトラブルシューティング」では、一般的なエラーと問題の解決方法について説明します。

第 12 章: 「Windows での監査ポリシーの設定」では、さまざまな Windows プラットフォームで監査を有効にする方法について説明します。

1.2 対象読者と前提条件

このガイドは、ロギングソリューションとログセンターの設計と保守を担当するシステム管理者とコンサルタントを対象としています。また、異機種環境での集中型ロギングを実装するツールを探している IT 意思決定者にとっても便利です。

syslog-ng PE 管理者には、次のスキルと知識が必要です。

- 基本的なシステム管理の知識。
- ネットワーク、TCP / IP プロトコル、一般的なネットワーク用語の理解。
- Microsoft Windows オペレーティングシステムの知識。
- レガシーsyslog(BSD-syslog)プロトコルと新しい syslog(IETF-syslog)プロトコルの理解。

1.3 このガイドに記載されている製品

このガイドでは、次の製品の使用について説明します。

- syslog-ng Agent for Windows(syslog-ng エージェント)6.0.1 以降

1.4 本ガイドの表記

このガイドの使用を開始する前に、ドキュメンテーションで使用される用語および表記規則を理解することが重要です。

次の種類のテキスト書式とアイコンは、ドキュメント内の特別な情報を識別します。

Tips:

Tips はベストプラクティスと推奨事項を提供します。

注意:

注意はトピックに関する追加情報を提供し、重要な事実と考慮事項を強調します。

警告:

警告は、指示に従わない場合、データの消失、または、デバイスの設定を誤った設定にする状況を示します。

コマンド: 実行しなければならないコマンド。または、パラメーター名と属性名。

「参照」: 参照項目、追加項目。

/path/to/file: ファイル名。

[ラベル]: Windwos の GUI 出力メッセージまたはダイアログ・ラベル、Windows のメニューバーのサブメニューまたは、メニュー項目や Windows のダイアログウィンドウのボタンなど。

1.5　お問合せ先とカスタマーポータル

ジュピターテクノロジー株式会社（Jupiter Technology Corp.）

住所：　〒183-0023 東京都府中市宮町 2-15-13 第 15 三ツ木ビル 8F
URL：　http://www.jtc-i.co.jp/
電話番号：　042-358-1250
FAX 番号：　042-360-6221
ご購入のお問い合わせ：
　お問い合わせフォーム　https://www.jtc-i.co.jp/contact/scontact.php
　メール　sales@jtc-i.co.jp
製品サポートのお問い合わせ：
　カスタマーポータル　https://www.jtc-i.co.jp/support/customerportal/

2 イントロダクション

この章では、Microsoft Windows ホストに syslog-ng Agent for Windows（以下、syslog-ng エージェントも同様）をインストールして設定する方法について説明します。

syslog-ng Agent for Windows は、Microsoft Windows プラットフォーム用のログ収集およびログ転送アプリケーションです。 Windows ベースのホストのログメッセージを収集し、通常または TLS で暗号化された TCP 接続を使用して syslog-ng サーバーに転送します。

syslog-ng エージェントの機能と制限事項を以下に要約します。

- イベントログコンテナとログファイルからメッセージを読み込みます。
- TCP を使用してログメッセージを転送します。
- TLS 暗号化をサポートします。
- X.509 証明書を使用してサーバーを認証します。 相互認証もサポートされています。
- イベントログメッセージのフォーマットは、マクロを使用してカスタマイズすることができます。
- パラレルモードとフェールオーバーモードの両方で複数の宛先をサポートします。
- グループポリシーを使用してドメインコントローラから管理できます。
- syslog-ng エージェントがサポートする機能は基本フィルタリングのみです。メッセージの分割、解析、および分類はサポートされていません。
- Windows 上のログメッセージは、すでにハードディスクに保存されているファイル（イベントログコンテナまたはカスタムログファイル）から取得されるため、エージェントは追加のディスクバッファリングを使用しません。

2.1 サポートされているオペレーティングシステム

Microsoft Windows プラットフォームにはセントラル syslog-ng サーバーをインストールできません。syslog-ng エージェントは、ログメッセージをセントラル syslog-ng サーバーに転送できます。syslog-ng エージェントは syslog-ng PE または syslog-ng Store Box(SSB)の一部であり、一緒にライセンスされています。

syslog-ng エージェントアプリケーションは、次のオペレーティングシステムをサポートしています。

特に明記されていない限り、プラットフォームの後続リリース（例えば、Windows Server 2008 の場合は Windows Server 2008 R2、および、そのサービスパック）もサポートされます。

- Microsoft Windows Server 2008 (x86 and x86_64)
- Microsoft Windows Server 2012 (x86_64)
- Microsoft Windows Vista (x86 and x86_64)
- Microsoft Windows 7 (x86 and x86_64)
- Microsoft Windows 8 (x86 and x86_64)
- Microsoft Windows 10 (x86 and x86_64)

注意：

syslog-ng Agent for Windows アプリケーションは、Microsoft Windows Vista 以降のプラットフォームで使用される XML ベースのイベントログ形式をサポートします。 また、64 ビットオペレーティングシステムを完全にサポートしています。

3 syslog-ng エージェントのインストール

syslog-ng Agent for Windows アプリケーションは、独立したホスト上にスタンドアロンモードでインストールできます。また、ホストがドメインのメンバーである場合は、syslog-ng エージェントをドメインコントローラーにインストールし、それらをグローバルに設定できます。

- スタンドアロンモードで syslog-ng Agent for Windows アプリケーションをインストールする方法については、「3.1 スタンドアロンモードで syslog-ng エージェントをインストールする」を参照してください。
- ドメインメンバーに syslog-ng Agent for Windows アプリケーションをインストールする方法のついては、「3.2 ドメインコントローラとドメインのホストに syslog-ng エージェントをインストールする」を参照してください。

注意：

syslog-ng Agent for Windows アプリケーションは、通常、Windows の MMC スナップイン（ドメインコントローラーからグローバルに管理する場合、またはスタンドアロンモードで構成する場合でも）を使用して設定されます。ただし、XML ベースの構成ファイルを使用することもできます。 詳細は、「4.3 XML ベースの設定ファイルの使用」を参照してください。

警告：

XML 設定ファイルを使用している場合、または XML 設定ファイルを使用して syslog-ng エージェントをインストールした場合は、syslog-ng エージェントの設定に MMC スナップインを使用することはできません。

インストーラーの種類：

- **syslog-ng-agent-<version>-setup.exe** は一般的なインストーラです。ローカル設定、XML 設定ファイルで設定できるエージェントがインストールされ、ドメイングループポリシーから設定を受け取ることができます。
- **syslog-ng-agent-nosnapin-<version>-setup.exe** は特別なインストーラです。.NET 環境を必要としません。XML 構成ファイルでのみ構成可能なエージェントがインストールされ、ドメイングループポリシーから設定を受け取ることができます。インストーラには、32 ビットと 64 ビットのバージョンが含まれています。
- **syslog-ng-agent-setup-<version>-<amd64/i386>.msi** は、グループポリシーでインストールしているドメインクライアント用の MSI インストーラです。

3.1 スタンドアロンモードで syslog-ng エージェントをインストールする

syslog-ng Agent for Windows アプリケーションは、独立したホスト上にスタンドアロンモードでインストールできます。ホストがドメインのメンバーである場合は、「3.2 ドメインコントローラーとドメインのホストに syslog-ng エージェントをインストールする」の説明に従って、ドメインコントローラーに syslog-ng エージェントをインストールして下さい。syslog-ng エージェントは約 30 MB のハードディスク容量が必要になります。

スタンドアロンモードで syslog-ng エージェントをインストールするには、次の手順を実行します。

注意:

syslog-ng Agent for Windows の通常の.exe インストーラーには、Microsoft .NET Framework バージョン 3.5 または 4.0 が必要です。このパッケージは、通常、ほとんどのホストにすでにインストールされています。インストールされてない場合は、.NET パッケージをここからダウンロードできます。

インストーラーの種類で nosnapin および.msi バージョンでは、syslog-ng エージェントのグラフィカルな MMC スナップインをインストールしないため、.NET Framework は必要ありません。

手順:

1. インストーラーを起動します。 **syslog-ng-agent-<version>-setup.exe** ファイルを実行します。

   注意:

   syslog-ng エージェントをインストールするには管理者権限が必要です。

2. 使用許諾契約書を読み、[I Agree](同意する)を選択します。
3. syslog-ng Agent for Windows アプリケーションをインストールするインストール先フォルダを選択し、[Next]を選択します。
4. [Standalone mode]を選択し、[Next]をクリックします。

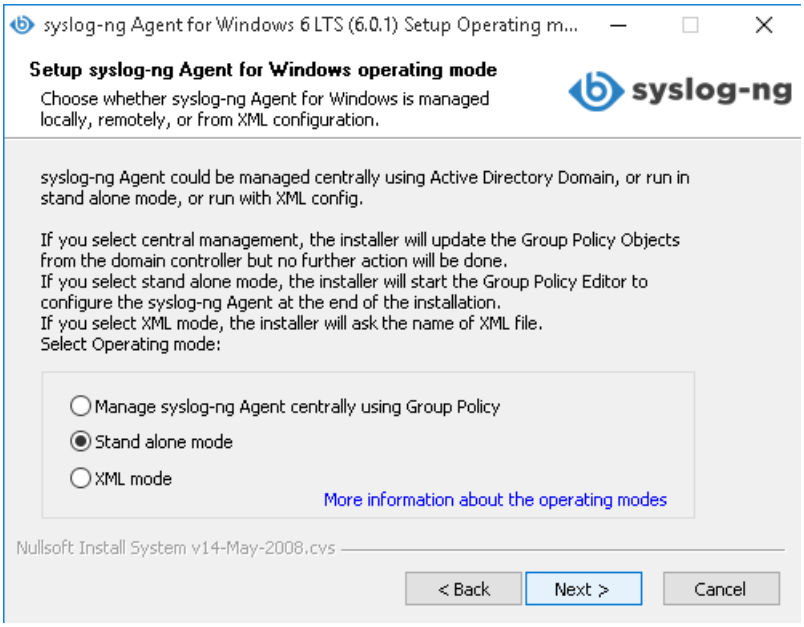

Figure 2.1. Installing in Standalone mode

5. インストーラーによって、syslog-ng エージェントの設定インターフェースが自動的に開きます。少なくとも、宛先サーバーの IP アドレスを設定する必要があります。エージェントは、ログコン

テナからアプリケーション、セキュリティ、およびシステムイベントのイベントログメッセージをセントラルログサーバーに自動的に送信し始めます。

注意：

インストールは、設定インターフェースを閉じた後にのみ完了します。 後で設定を変更する方法については、「4.1 スタンドアロンの syslog-ng エージェントの設定」を参照してください。

3.2 ドメインコントローラーとドメインのホストに syslog-ng エージェントをインストールする

syslog-ng Agent for Windows アプリケーションは、ドメインコントローラーとドメインコントローラーのドメインメンバーにインストールし、グループポリシーを使用してグローバルに設定できます。syslog-ng エージェントには約 30 MB のハードディスク容量が必要になります。

- ドメインに syslog-ng エージェントアプリケーションをインストールする方法ついては、「3.2.1 ドメインコントローラとドメインのホストに syslog-ng エージェントをインストールする」を参照してください。
- ドメインホストの syslog-ng エージェントを設定する方法については、「4.2.1 ドメインホストの syslog-ng エージェントの設定」を参照してください。
- ドメインコントローラの syslog-ng エージェントの設定方法については、「4.2.2 ドメインコントローラーの syslog-ng エージェントの設定」を参照してください。

注意：

.msi バージョンのインストーラーはエージェントの MMC 構成スナップインをインストールしないため、.msi インストーラーは.NET Framework を必要としません。

3.2.1 ドメインコントローラーとドメインのホストに syslog-ng エージェントをインストールする

syslog-ng エージェントアプリケーションをドメインコントローラーとドメインのホストにインストールするには、次の手順を実行します。

この手順では、スタンドアロンモードでドメインコントローラーに syslog-ng エージェントをインスト

ールし、各ドメインコントローラーからドメインホストを設定することを前提としています。

注意:

ドメインコントローラーから syslog-ng エージェントを設定するには、少なくとも 1 つのドメインコントローラーに syslog-ng エージェントをスタンドアロンモードでインストールする必要があります。最初のドメインコントローラーから syslog-ng エージェントの設定をエクスポートし、他のドメインコントローラーにインポートするか、他のドメインコントローラーでエージェントグループポリシーを設定し、syslog-ng エージェントをドメインモードでインストールできます。

注意:

デフォルトでは、syslog-ng Agent for Windows アプリケーションは次のようにメッセージを送信します。

- イベントログのソースから、syslog-ng エージェントアプリケーションは、エージェントのインストール後に作成されたメッセージのみを送信します。
- ファイルソースからは、ファイルの全内容を送信します。

手順:

1. syslog-ng エージェントインストーラの Microsoft Installer(**.msi**)バージョンと実行可能(**.exe**)バージョンの両方をドメインコントローラホストにダウンロードします。この場合、MMC スナップインモジュールを含む実行可能ファイルをダウンロードしてください。.msi インストーラーは、32 ビットおよび 64 ビットオペレーティングシステムで別れています。

   注意:

   syslog-ng エージェントをインストールするには管理者権限が必要ですが、ドメインコントローラーでグループポリシー関連の設定をするには、ドメイン管理者以上(例えば、エンタープライズ管理者)の権限が必要になります。

2. **.exe** インストーラーを使用して、ドメインコントローラーに syslog-ng エージェントアプリケーションをインストールします。

注意：

syslog-ng Agent for Windows の通常の.exe インストーラーには、Microsoft .NET Framework バージョン 3.5 または 4.0 が必要です。このパッケージは、通常、ほとんどのホストにすでにインストールされています。インストールされてない場合は、.NET パッケージをここからダウンロードできます。

インストーラーの種類で nosnapin および.msi バージョンでは、syslog-ng エージェントのグラフィカルな MMC スナップインをインストールしないため、.NET Framework は必要ありません。

3. ・ Windows 2008 の場合： [スタートメニュー]>[コントロールパネル]>[管理ツール]>[グループポリシーの管理]を選択します。
   ・ 他の Windows プラットフォームの場合： [スタートメニュー]>[コントロールパネル]>[管理ツール]>[Active Directory ユーザーとコンピューター]を選択し、syslog-ng エージェントをインストールするホストのドメインの組織単位を右クリックし、[プロパティ]を選択します。
4. ・ Windows 2008 の場合： syslog-ng エージェント設定を追加するグループポリシーオブジェクトを選択して編集します。 または、新しいグループポリシーオブジェクトを作成することもできます。
   ・ 他の Windows プラットフォームの場合： [グループポリシー]を選択し、syslog-ng エージェント設定を追加するグループポリシーオブジェクトを編集します。 または、新しいグループポリシーオブジェクトを作成することもできます。
5. [コンピューターの構成]を選択し、[ソフトウェアの設定]を右クリックし、[新規作成]>[パッケージ]を選択します。
6. syslog-ng Agent for Windows の.msi インストーラーを選んで、[開く]を選択します。
7. [割り当て]を選択して、[OK]をクリックします。
8. [コンピューターの設定]>[syslog-ng Agent Settings]を選択し、syslog-ng エージェントを設定します。 ドメインのメンバーはこの構成を使用します。

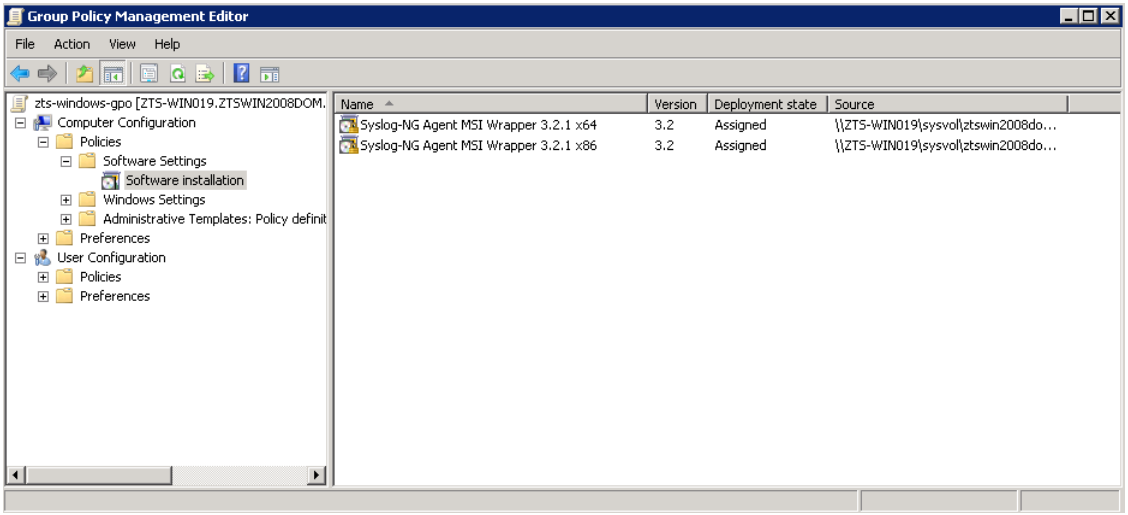

Figure 2.2. syslog-ng Agent Settings

9. syslog-ng Agent for Windows アプリケーションは、次に再起動するときにドメインのメンバーに自動的にインストールされます。

> 注意:
> syslog-ng エージェントをドメインコントローラーから自動的にインストールしたくない場合は、手順 5～7 をスキップして手順 8 を完了し、**syslog-ng-agent-nosnapin-<version>-setup.exe** のファイルを手動でドメインのメンバーにインストールします。この方法は、ドメインのすべてのホストに syslog-ng エージェントをインストールしたくない場合に便利です。

10. ドメインのメンバーを再起動したら、ドメインのメンバーに対して **gpupdate** コマンドを実行します。
    syslog-ng Agent for Windows アプリケーションは、グループポリシーのアップデート中にその設定を受け取り、ログメッセージの処理を開始します。

3.3 サイレントインストール

syslog-ng Agent for Windows アプリケーションは、ユーザーの操作を必要とせずに、サイレントモードでもインストールできます。さまざまなインストーラオプションをコマンドラインオプションとして指定します。サイレントモードでインストールするには **/S** オプションを使用する必要があります。他に、以下のオプションが利用できます。

> 警告:
> すべてのオプションは大文字で記述します。

- /D=<path>

指定したフォルダに syslog-ng エージェントをインストールします。 空白文字が含まれていても、フォルダ名の前後に引用符(' ')や二重引用符(" ")を使用しないでください。

警告:

/D オプションを使用する場合は、これがコマンドラインの最後のオプションであることを確認してください。 例えば、syslog-ng-agent-nosnapin-<version>-setup.exe /S /XMLCONFIG =c:¥test.xml /LOCALUPGRADE /D=c:¥Program Files¥agent¥

- /LOCAL

スタンドアロンモードで syslog-ng エージェントをインストールします。 これは、syslog-ng エージェントのデフォルトのインストールモードです。 このオプションを使用するときは、次の 2 つのオプションを設定することもできます。

- /GPOUPGRADE: インストール中に syslog-ng エージェント設定を持つすべての GPO (グループポリシーオブジェクト)設定をアップグレードします。

警告:

ドメインコントローラー上でのみ使用してください。

- /LOCALUPGRADE: ローカル設定をアップグレードします。

注意:

syslog-ng エージェントがローカル設定のみを使用し、このオプションを指定しない場合、syslog-ng エージェント MMC スナップインでローカル設定を開いてローカル設定をアップグレードしている間は syslog-ng エージェントが起動しない可能性があります。

- /NOMENU

[スタートメニュー]に syslog-ng エージェントに関するエントリを追加しません。

- /NOUPGRADE

インストーラーは、インストール中にアップグレードを実行しません(デフォルト)。設定が GPO

（グループポリシーオブジェクト）から、または、XML 設定を使用しており、アップグレードする必要がない場合に使用します。（この場合、エージェントは起動後に一時的にアップグレードします）。

- /REMOTE

ドメインモードで syslog-ng エージェントをインストールします。

- /S

サイレントモードでインストーラーを起動します。このオプションは、サイレントインストールするのに必須オプションです。

- /XMLCONFIG=

syslog-ng エージェントの設定に指定された XML 設定ファイルを使用します。このオプションを使用する場合は、次のオプションも設定できます。

  - /XMLUPGRADE: XML 設定ファイルが使用されている場合は、インストール時に XML 設定をアップグレードします。

アップグレード操作は、指定された設定に対して実際にアップグレードが必要な場合にのみ実行されます。例えば、syslog-ng エージェントの現在のバージョンと以前のバージョンを切り替える設定がない場合（例えば、バージョン 3.0.7 からバージョン 3.0.8 へのアップグレードの場合）、**/LOCALUPGRADE** オプションを指定しても、ローカル設定はアップグレードされません。

/LOCAL, **/XMLCONFIG**、および、**/REMOTE** オプションは互いに競合します。複数指定した場合は、**/REMOTE** が他の 2 つのオプションより優先され、**/XMLCONFIG** が/**LOCAL** オプションよりも優先されます。

3.4 syslog-ng エージェントの MSI パッケージをカスタムフォルダにインストールする

syslog-ng エージェントの.msi インストーラパッケージを変更して、syslog-ng エージェントアプリケーションをカスタムフォルダにインストールすることができます。

手順:

コマンドラインから syslog-ng エージェントアプリケーションをインストールする場合は、カスタムインストールフォルダを指定して、次のコマンドを実行します。

msiexec /i syslog-ng-agent-setup-<version>-<amd64/i386>.msi INSTDIR=C:¥<path-to-custom-folder>¥

さもなければ、次の手順を実行して.msi パッケージを変更します。

Orca MSI エディタをダウンロードします。

1. Orca を起動し、変更する **syslog-ng-agent-setup-<version>-<amd64/i386>.msi** ファイルをロードします。
2. [Transform]>[New Transform]を選択します。
3. Property テーブルに **INSTDIR** プロパティを追加し、その値を syslog-ng エージェントアプリケーションをインストールするフォルダのフルパスに設定します。
4. [Transform]>[Generate Transform]を選択し、**.mst** ファイルの変更を保存します。
5. Orca MSI エディタを閉じます。
6. [スタートメニュー] >[コントロールパネル]>[管理ツール]>[Active Directory ユーザーとコンピューター]を選択し、syslog-ng エージェント設定を含むグループポリシーオブジェクトを編集します。
7. 保存された**.mst** パッケージを syslog-ng エージェント**.msi** パッケージの変更として追加します。

3.5 syslog-ng Agent for Windows を最新バージョンにアップグレードする

syslog-ng Agent for Windows アプリケーションの正確なアップグレード手順は、インストール方法とエージェントの管理方法によって異なります。

警告:

- ドメインモードで実行されているエージェントをアップグレードする場合は、ドメインホストで実行されているエージェントをアップグレードしてから、ドメインコントローラで実行されているエージェントをアップグレードしてください。
- ドメインのホスト(ドメインコントローラを含む)は、同じバージョンの syslog-ng エージェントを実行する必要があります。ホスト上で異なるバージョンを実行することはサポートも推奨もされていません。
- MMC の[サービス]ウィンドウが開いている場合は、エージェントサービスの登録が正常に行われないため、アップグレードする前に閉じてください。

- ホストが syslog-ng エージェントをスタンドアロンモードで実行している場合、ホスト上で **syslog-ng-agent-<version>-setup.exe** インストーラをダウンロードして実行し、表示された情報が正しいことを確認します。エージェントは、設定ウィンドウを閉じると自動的に再起動されます。
- ドメインホストが**.msi** インストーラパッケージからドメインコントローラによってインストールされ

た syslog-ng エージェントを実行している場合、「3.2 ドメインコントローラとドメインのホストに syslog-ng エージェントをインストールする」の手順を実行します。システムは、新しいパッケージが syslog-ng Agent for Windows アプリケーションを更新されたことを自動的に認識します。

- ドメインホストが **syslog-ng-agent-nosnapin-<version>-setup.exe** ファイルから手動でインストールされた syslog-ng エージェントを実行している場合、新しい **syslog-ng-agent-nosnapin-<version>-setup.exe** ファイルをホスト上で実行します。インストールが完了したら、[スタートメニュー] >[ファイル名を指定して実行]を選択し、**gpupdate** コマンドを実行してエージェントのドメイン設定を更新します。

- **syslog-ng-agent-<version>-setup.exe** または **syslog-ng-agent-nosnapin-<version>-setup.exe** を使用して syslog-ng エージェントが XML 設定ファイルでインストールされている場合は、同じインストーラをダウンロードして実行してください。以前の XML 設定ファイルが表示され、必要に応じてアップグレードされます。

3.6 syslog-ng エージェントのアンインストール

syslog-ng エージェントアプリケーションをアンインストールするには、次の手順を実行してください。なお、コマンドラインから syslog-ng エージェントをアンインストールするには、「3.7 サイレントモードでの syslog-ng エージェントのアンインストール」を参照してください。

手順:

1. syslog-ng エージェントのインストールディレクトリに移動します。
2. **uninstall.exe** ファイルを起動します。
3. 画面の指示に従ってアンインストールします。

3.7 サイレントモードでの syslog-ng エージェントのアンインストール

コマンドラインから syslog-ng エージェントアプリケーションをアンインストールするには、次の手順を実行します。グラフィカルインタフェースを使用して syslog-ng エージェントをアンインストールするには、「3.6 syslog-ng エージェントのアンインストール」を参照してください。

手順:

1. コマンドプロンプトを起動し、syslog-ng Agent のインストールディレクトリに移動します。
2. ・ syslog-ng エージェントをアンインストールし、レジストリからその設定も削除するには、**uninstall.exe /S /DELCONF** コマンドを実行します。
   ・ 設定を削除せずに syslog-ng エージェントのみアンインストールするには、**uninstall.exe /S** コマンドを実行します。

4 syslog-ng エージェントの設定方法

この章では、syslog-ng エージェントアプリケーションを設定する方法について説明します。適切な方法は、インストール方法および使用する設定方法（通常または XML ベース）によって異なります。syslog-ng Agent for Windows アプリケーションは、通常、ウィンドウズの MMC スナップイン（ドメインコントローラーからグローバルに管理する場合、またはスタンドアロンモードで構成する場合）を使用して設定されます。ただし、XML ベースの設定ファイルを使用することもできます。

- スタンドアロンモードでインストールされた syslog-ng エージェントの設定方法については、「4.1 スタンドアロンの syslog-ng エージェントの設定」を参照してください。
- ドメインホストの syslog-ng エージェントを設定する方法については、「4.2.1 ドメインホストの syslog-ng エージェントの設定」を参照してください。
- ドメインコントローラーの syslog-ng エージェントの設定方法については、「4.2.2 ドメインコントローラーの syslog-ng エージェントの設定」を参照してください。
- syslog-ng エージェントをファイルから設定する方法については、「4.3 XML ベースの設定ファイルの使用」を参照してください。

4.1 スタンドアロンの syslog-ng エージェントの設定

既にインストールされているスタンドアロンの syslog-ng エージェントを設定するには、次の手順を実行します。

手順:

1. 次のいずれかの方法を使用して、syslog-ng Agent コンフィギュレーションインターフェイスを開始します。
   - [スタートメニュー]>[プログラム]>[syslog-ng Agent for Windows]>[Configure syslog-ng Agent for Windows]を選択します。
   - MMC を起動します（例：[スタートメニュー]>[Windows Powershell]で **mmc** と入力します）。ファイルメニューから[スナップインの追加と削除]>[利用できるスナップイン]>[syslog-ng Agent]を選択します。.NET 3.5 がインストールされていない場合は、Windows 7、Windows Vista、および Windows 2008 Server プラットフォームで、この方法を使用しないでください。
2. [syslog-ng Agent Settings]>[Local Settings]を選択し、環境に合わせて必要に応じて

syslog-ng エージェントを設定します。

3. 設定変更後、変更を有効にする為に syslog-ng エージェントサービスを再起動する必要があります。 syslog-ng エージェントサービスを再起動するには、[スタートメニュー]>[ファイル名を指定して実行]を選択し、**services.msc** と入力してサービスマネージャーから[syslog-ng Agent]サービスを再起動します。

4.2 ドメインの syslog-ng エージェントの設定

このセクションでは、ドメインモードで syslog-ng Agent for Windows アプリケーションを設定する方法について説明します。

- ドメインホストの syslog-ng エージェントを設定する方法については、「4.2.1 ドメインホストの syslog-ng エージェントの設定」を参照してください。
- ドメインコントローラーの syslog-ng エージェントの設定方法ついては、「4.2.2 ドメインコントローラーの syslog-ng エージェントの設定」を参照してください。
- 異なるグループポリシーレベルの関係については、「4.2.3 ドメインとローカルの設定」を参照してください。

4.2.1 ドメインホストの syslog-ng エージェントの設定

既にインストールされている syslog-ng エージェントをドメインコントローラーから設定するには、次の手順を実行します。

手順:

1. 次のいずれかの方法を使用して、syslog-ng Agent コンフィギュレーションインターフェイスを開始します
   - [スタートメニュー]>[プログラム]>[syslog-ng Agent for Windows]>[Configure syslog-ng Agent for Windows]を選択します。
   - MMC を起動します(例:[スタートメニュー]>[Windows Powershell]で **mmc** と入力します)。ファイルメニューから[スナップインの追加と削除]>[利用できるスナップイン]>[syslog-ng Agent]を選択します。.NET 3.5 がインストールされていない場合は、Windows 7、Windows Vista、および Windows 2008 Server プラットフォームで、この方法を使用しないでください。
2. [Client Group Policy]に移動し、変更するグループポリシー(例えば、[Default Domain

Policy]）を選択します。

3. ドメインのホストに必要に応じて syslog-ng エージェントを設定します。この変更は、ドメインホストがドメインコントローラーから設定を更新するときに反映されます。デフォルトでは、これはドメインの設定に応じて 90 分ごとに更新されます。以前の設定をダウンロードするには、ドメインのメンバーに対して **gpupdate** コマンドを実行します。

注意：

ドメインホストが設定を更新すると、古い設定と新しい設定の間に違いがない場合を除き、新しい設定をロードするために syslog-ng エージェントが自動的に再起動されます。

4.2.2 ドメインコントローラーの syslog-ng エージェントの設定

ドメインコントローラーで実行されている syslog-ng エージェントを設定するには、次の手順を実行します。

手順：

1. 次のいずれかの方法を使用して、syslog-ng PE コンフィギュレーションインターフェイスを開始します

   - [スタートメニュー]>[プログラム]>[syslog-ng Agent for Windows]>[Configure syslog-ng Agent for Windows]を選択します。

   - MMC を起動します（例：[スタートメニュー]>[Windows Powershell]で **mmc** と入力します）。ファイルメニューから[スナップインの追加と削除]>[利用できるスナップイン]>[syslog-ng Agent]を選択します。.NET 3.5 がインストールされていない場合は、Windows 7、Windows Vista、および Windows 2008 Server プラットフォームで、この方法を使用しないでください。

2. ・ シングルドメインコントローラでのみ syslog-ng Agent を設定するには、[Local Settings]を選択します。ドメインコントローラーに影響を与えるグループポリシーでも syslog-ng Agent を設定した場合は、グループポリシーの設定がこれらのローカル設定を上書きすることに注意してください。

   ・ すべてのドメインコントローラーで syslog-ng Agent を構成するには、[Client Group Policy]を選択し、ドメインコントローラーの適切なグループポリシー（例：[Default Domain Controllers Policy]）を選択します。

3. ドメインコントローラーに必要に応じて、syslog-ng エージェントを設定します。複数のドメインコ

ントローラーを使用している場合は、他のドメインコントローラーは、このドメインコントローラーから設定が更新されると、変更が反映されます。

注意

ドメインコントローラーが新しい設定を受信すると、古い設定と新しい設定の間に違いがない場合を除き、新しい設定をロードするために syslog-ng エージェントが自動的に再起動されます。

4.2.3 ドメインとローカルの設定

syslog-ng エージェントは、Windows の標準的なポリシー継承方法に従います。

親コンテナからの GPO(グループポリシーオブジェクト)は、デフォルトで継承されます。複数の GPO がこれらのコンピューターに適用される場合、GPO の設定が集約されます。特定のポリシー設定の最終値は、その設定を含むより高い優先順位の GPO によってのみ設定されます。(ただし、いくつかの設定の最終値は、実際には GPO 間の値の組み合わせになります)。この処理順序では、サイトが最初に適用されますが、優先順位は最も低くなります。OU(組織単位)は最後に処理されますが、優先順位が最も高くなります。

複数のグループポリシーオブジェクトが割り当てられている場合、グループポリシーは次の順序で適用されます。

1. ローカルグループポリシーオブジェクトが適用されます。
2. サイトにリンクされたグループポリシーオブジェクトが適用されます。サイトに複数の GPO が存在する場合は、管理者が指定した順序で適用されます。
3. ドメインにリンクされた GPO は、指定された順序で適用されます。
4. OU にリンクされた GPO が適用されます。OU グループのポリシーオブジェクトは、上位の組織単位から下位の組織単位に設定されます。つまり、最初に親 OU、次に子 OU を設定します。デフォルトでは、後で適用されるポリシーは、以前に適用されたポリシーを上書きします。したがって、子 OU の設定は、親 OU の設定を上書きできます。
5. グループポリシーが設定されていない場合、syslog-ng エージェントはローカルポリシー設定をチェックし、使用可能な場合はローカル設定を使用します。

グループポリシー設定の継承に関する規則は次のとおりです。

- 親 OU のポリシー設定([有効]または[無効])が構成されていて、子 OU に対して同じポリシ

一設定が構成されていない場合は、子 OU は親のポリシーを継承します。

- 親 OU のポリシー設定（[有効]または[無効]）が構成され、その子 OU に対して同じポリシー設定が構成されている場合、子 OU 設定は、親 OU から継承した設定を上書きします。この設定のタイプがリストの場合、次の特定のケースがあります。
  - syslog-ng エージェントはこれらのリストの内容を集約し、同じ要素を 1 回だけ使用します。
  - いずれかのポリシーが構成されていない（[未設定]）場合、継承は行われません。

注意：
この場合、以前に設定した値を引き続き使用できるため、ローカル設定で未設定を使用しないでください。設定を有効または無効にしてください。

4.3 XML ベースの設定ファイルの使用

syslog-ng Agent for Windows バージョン 3.2 以降では、syslog-ng エージェントの設定を XML ファイルにエクスポートすることができます。この設定ファイルは、syslog-ng エージェントを別のホストにインストールするときのデフォルト設定として使用することも、コマンドラインユーティリティを使用して既存の syslog-ng エージェントにインポートすることもできます。

警告：
エクスポートされた XML ファイルを手動で編集または変更しないでください。
XML ファイルを確認する場合は、syslog-ng Agent for Windows のインストールディレクトリにある **syslog-ng-agent-conf.xsd** ファイルを使用します。

警告：
XML 設定ファイルを使用している場合、または XML 設定ファイルを使用して syslog-ng エージェントをインストールした場合は、syslog-ng エージェントの設定に MMC スナップインを使用することはできません。

4.3.1 syslog-ng エージェントの XML 設定ファイルを作成する

他の syslog-ng エージェント設定で使用できる XML 設定ファイルを作成するには、次の手順を実行します。

手順:

1. ホストに syslog-ng Agent for Windows アプリケーションをインストールします。
2. グラフィカルインタフェースを使用して他のホストで使用する設定を作成します。syslog-ng Agent for Windows アプリケーションは、この設定をレジストリに保存します。
3. [syslog-ng Agent Settings]を右クリックし、[Export]を選択して syslog-ng エージェントの設定をレジストリから XML ファイルにエクスポートします。XML ファイルを保存する場所を選択します。

   あるいは、**configmanager.exe -export <source> "destination xml file"** コマンドを使用して、コマンドラインから syslog-ng エージェントの設定をエクスポートすることもできます。**<source>**パラメーターは、どのコンフィグレーションをエクスポートするかを決定します。

   - {GPO ID}: 指定したグループポリシーオブジェクト ID に関連する構成をエクスポートします(例:{99AF1185-AB80-40B2-B4B8-41A1E907F329})。
   - localsettings: ホストのローカル設定をエクスポートします。
   - domainsettings: ホストがドメインコントローラーから受け取った設定をエクスポートします。

   注意:

   XML 構成ファイルを上書きするには、/F オプションを使用します。これにより、ファイルが既に存在する場合でも強制的にエクスポートされます。

4. 他のホスト上の構成ファイルを使用する、さまざまなオプションの詳細については、「4.3.2 XML ファイルからの syslog-ng エージェントの設定」を参照してください。

4.3.2 XML ファイルからの syslog-ng エージェントの設定

XML 設定ファイルを使用するように syslog-ng エージェントアプリケーションを設定する方法は、使用環境によって異なります。 以下のリストは利用可能な方法を示しています。

警告:

- エクスポートされた XML ファイルを手動で編集または変更しないでください。
- XML 構成ファイルを削除しないでください。syslog-ng Agent for Windows は、起動または再起動するたびにファイルを検索します。ファイルの場所を変更する必要がある場合は、HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥syslog-ng Agent¥ImagePath レジストリキーを編集してください。

- syslog-ng エージェントアプリケーションのインストール中に XML ファイルを使用するには、[Setup syslog-ng Agent for Windows operating mode]に移動し、[XML mode]を選択します。次のウィンドウで、XML 設定を参照します。XML スキーマファイルは、syslog-ng エージェントディレクトリにインストールされることに注意してください。

- XML ファイルで.msi インストーラーを使用する場合は、**syslog-ng-agent-setup-<version>-<amd64/i386>.msi SLNGOPTS="/xmlconfig=fullpath¥myconfigfile.xml"**コマンドを使用するか、Orca MSI エディタを使用してインストーラーを編集し、[Customization]タブのインストールパラメータに **SLNGOPTS="/xmlconfig=fullpath¥myconfigfile.xml"**を追加します。

- syslog-ng Agent for Windows の設定ファイルとして XML ファイルを使用する: 既ににインストールされているスタンドアロンの syslog-ng エージェントを、XML 設定ファイルを使用して起動するには、コマンドラインで次の手順を実行します。この場合、syslog-ng Agent の設定は XML ファイルに保存され、レジストリにインポートされません(XML ファイルからレジストリに設定をインポートする方法の詳細については、「XML 設定をレジストリにインポートする」を参照してください)。

  1. **cd <syslog-ng agent installation directory>¥bin**
  2. **net stop "syslog-ng agent"**
  3. **syslog-ng-agent.exe /r**
  4. **syslog-ng-agent.exe /I <PATH>¥configuration.xml**
  5. **net start "syslog-ng agnent"**

- XML 設定をレジストリにインポートする: XML 構成ファイルをホストのレジストリにインポートするには、**configmanager.exe -import <destination> "source xml file"**コマンドを使用してから、syslog-ng エージェントサービスを再起動します。**<destination>**パラメータは、XML 構成をどの構成に変換するかを決定します。

- {GPO ID}: 指定したグループポリシーオブジェクト ID に設定をインポートします。(例: {99AF1185-AB80-40B2-B4B8-41A1E907F329})。
- localsettings: 設定をホストのローカル設定としてインポートします。
- domainsettings: 構成をホストのドメイン設定としてインポートします。

警告:

syslog-ng エージェントが XML 設定ファイルを使用するように設定されている場合、XML ファイルからホストのレジストリに設定ファイルをインポートしても効果はありません。

5 宛先の設定

syslog-ng Agent for Windows アプリケーションは、Windows ホストのログメッセージをセントラルログサーバーまたはリレーサーバーに送信できます。各サーバーが同じメッセージを受信すると、複数のサーバーに同じメッセージを送信することができます。また、エージェントがプライマリサーバー、または、プライマリが使用できなくなった場合にフェールオーバーサーバーにメッセージを送信するときに、フェールオーバーサーバーを設定することもできます。エージェントが宛先サーバーへの接続を失って再接続に失敗すると、イベントログメッセージが生成されます。再接続が成功した時も記録されます。(サーバーを長時間使用できない場合、エージェントは失敗した接続に関するログメッセージを 10 秒に 1 回生成します)。

フェールオーバーサーバーも使用できなくなると、アプリケーションは次のフェールオーバーサーバーに切り替えることなどします。最後のフェールオーバーサーバーが使用できない場合は、プライマリサーバーに戻ります。アプリケーションが再び使用可能になった場合、アプリケーションは自動的にプライマリサーバーに切り替わりません。ただし、syslog-ng Agent for Windows が再起動された場合のみ切り替わります。

注意:

フェールオーバーサーバーは、プライマリサーバーが使用するのと同じオプションを使用します。 フェールオーバーサーバーには、名前とアドレスのみを構成できます。

Linux バージョンと同様に、クライアントホストは稼動しているが送信するログメッセージがないことを示すために、エージェントは MARK メッセージをサーバーに送信します。MARK メッセージは 10 分毎に送信されます。

警告:

syslog-ng Agent for Windows アプリケーションは、信頼性の低い UDP プロトコルをサポートしていません。セントラルログサーバーが TCP または TLS 接続を使用してログを受け入れるように設定してください。また、必要に応じて、ログサーバーへのトラフィックを許可するようにファイアウォールの設定を調整する必要があります。

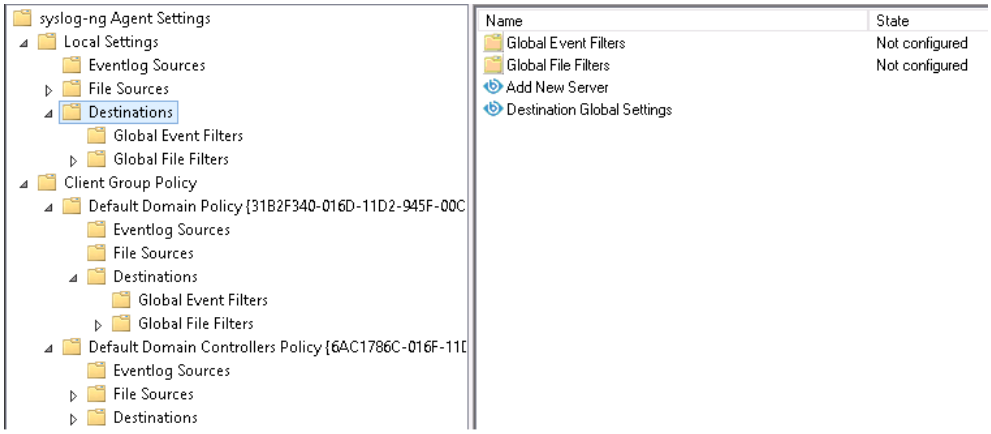

Figure 4.1. Adding new destinations

5.1 宛先ログサーバーの設定

新しい宛先を設定するには、次の手順を実行します。

手順:

1. syslog-ng Agent for Windows アプリケーションの設定インターフェースを開きます。
2. [syslog-ng Agent Settings]>[Local Settings または Client Group Policy 以下]>[Destinations]を選択し、[Add new server]をダブルクリックします。
3. [Server Name or Address (IPv4)]フィールドにログサーバーのホスト名または IP アドレスを入力します。ログサーバーが非スタンダード(ウェルノウン)ポートでメッセージを受け入れるように設定されている場合は、[Server Port]フィールドにポート番号を入力してください。デフォルトのポート(RLTP™が有効な場合は 35514、RLTP™が無効の場合は 514)を使用するには、[Reset to Default Port]をクリックしてください。

   フロー制御を有効にするには、[Enable flow-control]にチェックします。詳細については、「5.4 Syslog-ng Agent for Windows のフローコントロール」を参照してください。

   SSL 暗号化を使用するには、[Use SSL encryption]をチェックし有効にします。詳細については、「7 syslog-ng エージェントでの SSL の使用」を参照してください。

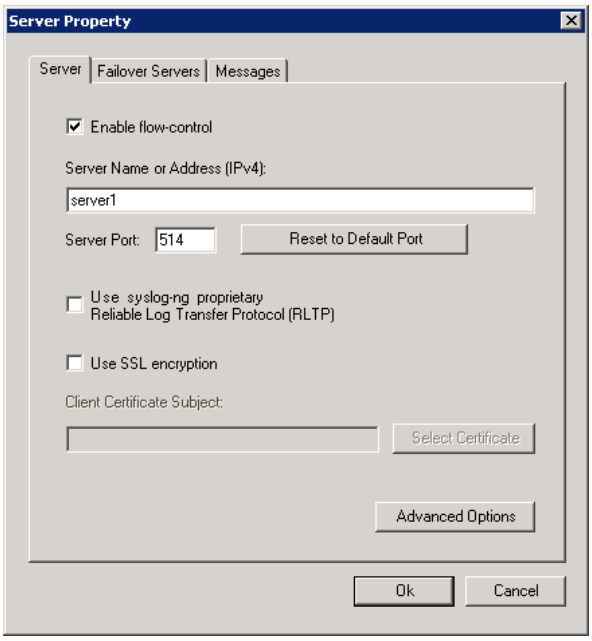

Figure 4.2. Adding new server

4. オプションのステップ： Reliable Log Transfer Protocol™（RLTP™）を使用するには、[Use syslog-ng proprietary Reliable Log Transfer Protocol (RLTP)]をチェックし有効にします。RLTP™の概念の詳細については、「syslog-ng Premium Edition 6 LTS 管理者ガイド」の「第 12 章 Reliable Log Transfer Protocol™」を参照してください。

注意：
Reliable Log Transfer Protocol™（RLTP™）を使用する場合、フロー制御を無効にすることはできません。

a. [Advanced Options]をクリックします。

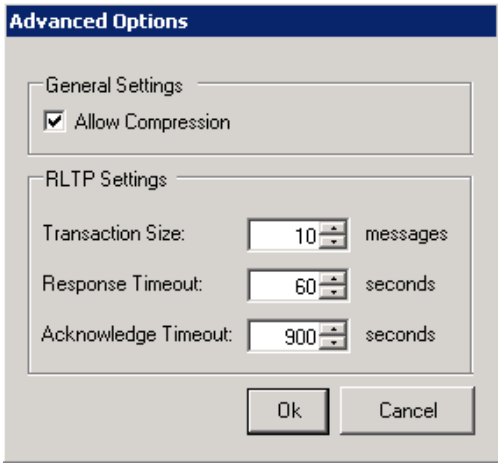

Figure 4.3. Adding new server

メッセージを圧縮して転送中の帯域幅を節約するには、[Allow Compression]オプションをチェックします。syslog-ng エージェントが実際に圧縮を使用するには、以下の点に注意する必要があります。

- [Server]>[Advanced Options]>[Allow Compression]オプションが有効になっている必要があります。
- ログサーバーにメッセージを送信するには、SSL および/または RLTP を使用する必要があります(つまり、[Use syslog-ng proprietary Reliable Log Transfer Protocol (RLTP)]または[Use SSL encryption]オプションを有効にする必要があります)。
- ログサーバー側では、(圧縮されたメッセージを受信できるように)圧縮を有効にするように設定する必要があります。ログサーバーが syslog-ng PE の場合、適切に**allow-compress()**オプションがソースで有効なっている必要があります。(詳細については、「syslog-ng Premium Edition 6 LTS 管理者ガイド」の「12.2. RLTP™オプション」およびを「10.4. TLS オプション」参照してください。)また、ログサーバーが syslog-ng Store Box(SSB)の場合、[Log]>[Sources]>[Allow compression]オプションを有効にします。圧縮されたメッセージを syslog-ng Store Box に送信するには、RLTP™プロトコルを使用する必要があります。(詳細については、「syslog-ng Store Box 管理者ガイド」の「第 7 章 メッセージソースの設定」を参照してください)。

b. 必要に応じて次のオプションを変更します。

注意:

次のオプションの情報を正確に把握してない限り、次の設定を調整または変更はしないでください。

- Transaction Size: サーバーからの確認応答を待つ前に送信されたメッセージの数。
- Response Timeout: 指定された時間内にメッセージを受信しないと、syslog-ng エージェントはサーバーとの接続を終了します。
- Acknowledge Timeout: 指定された時間内にメッセージへの応答を受信しないと、syslog-ng エージェントはサーバーとの接続を終了します。

c. [Enter]をクリックします。

5. [Messages]タブで、ログメッセージを転送するプロトコルを選択し、選択したテンプレートを適用するのに[Reset Protocol Template]をクリックします。以下のプロトコルテンプレートが利用

できます。(デフォルトテンプレートおよびメッセージフォーマットのカスタマイズについては、「9 メッセージフォーマットのカスタマイズ」を参照してください)。

- Legacy BSD Syslog Protocol: RFC3164 で規定されているレガシーBSD-syslog プロトコルを使用します。このオプションでは、次のメッセージテンプレートを使用します。<${PRI}>${BSDDATE} ${HOST} ${MSGHDR}${MESSAGE} syslog-ng エージェントは、メッセージ部分を、CRLF を 2 スペースで、TAB 文字を 1 スペースで置き換えます。

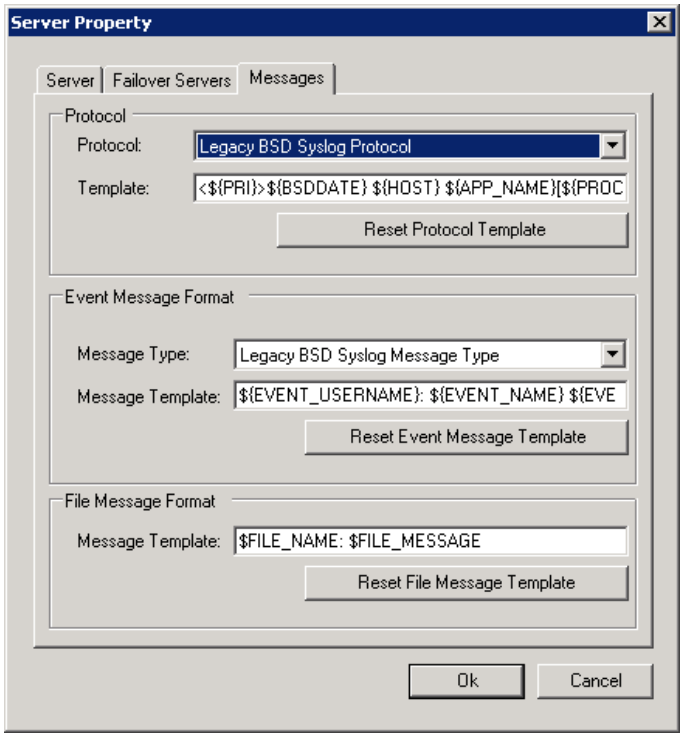

Figure 4.4. Legacy BSD Syslog Protocol

Example 4.1. Legacy BSD Syslog Protocol log

<134>Oct 04 14:45:33 zts-win019.ztswin2008dom.balabit Microsoft-Windows-Eventlog[2880]: ZTSWIN2008DOM¥balabit: System Microsoft-Windows-Eventlog: [Information] The Application log file was cleared. (EventID 104)

- Syslog Protocol: RFC 5424-5426 で規定されている新しい IETF-syslog プロトコルを使用します。これがデフォルト設定です。

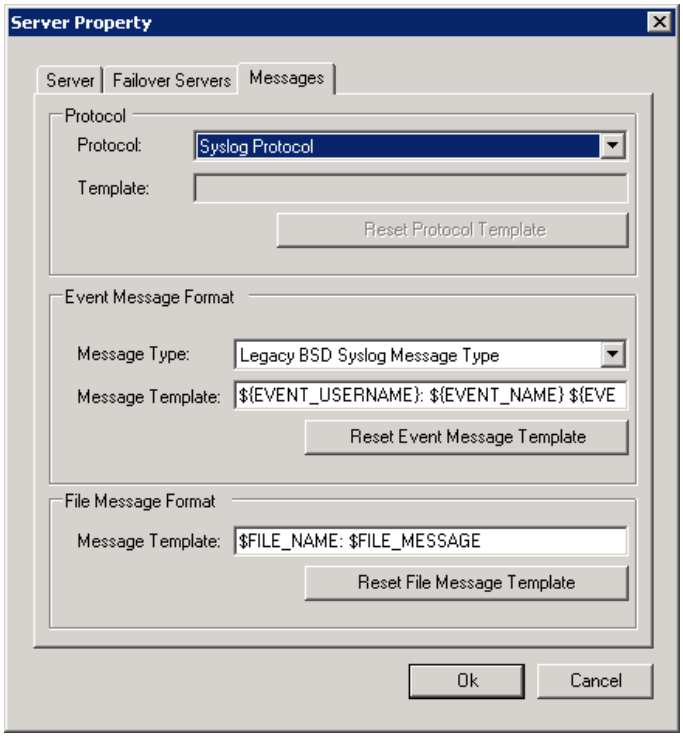

Figure 4.5. Syslog Protocol

IETF-syslog プロトコルを使用して Eventlog メッセージを転送する場合、syslog-ng エージェントアプリケーションは、デフォルトでログメッセージの SDATA 部分にマクロ（名前と値のペア）を含めます。これには、使用可能なすべてのイベントマクロ（EVENT_MSG (EVENT_MESSAGE), EVENT_MSG_XML (EVENT_MESSAGE_XML)を除く）が含まれます。値を持たないマクロはメッセージには含まれません。

```
499 <132>1 2010-09-28T12:02:30+02:00 zts-win004.ztswin2003dom.balabit testapp 1220 - [win@18372.4 EVENT_ID="1000" EVENT_NAME="Application" EVENT_REC_NUM="1673" EVENT_SID="S-1-5-21-3460971693-970282485-2299281428-1001" EVENT_SID_TYPE="User" EVENT_SOURCE="testapp" EVENT_TYPE="Warning" EVENT_USERNAME="ZTS-WIN004¥¥balabit"][meta sequenceId="1" sysUpTime="1"] ZTS-WIN004¥balabit: Application testapp: [Warning] test message (EventID 1000)
```

注意：

SDATA フィールドの名前は、次の形式でなければなりません。

name@<private enterprise number>

例えば、mySDATA-field@18372.4（18372.4 は、syslog-ng Agent for Windows の開発元 BalaBit IT セキュリティの民間企業番号です。）

- イベントログソースから受信したメッセージには、win@18372.4 SD-ID が含まれます。例えば、syslog-ng PE サーバーでは、次のようなメッセージフィールドを参照することができます： ${.SDATA.win@18372.4.EVENT_SOURCE}
- ファイルソースから受信したメッセージには file@18372.4 SD-ID が含まれます。例えば、syslog-ng PE サーバーでは、次のようなメッセージフィールドを参照することができます： ${.SDATA.file@18372.4.name}

RFC5424 で規定されているデータのみを含めるには、[Include Eventlog message metadata as SDATA]を無効にします。これを行うには、[Destinations]>[Destination Global Settings]に移動し、[Enable]を選択し、[Include Eventlog message metadata as SDATA]の選択を解除します。例えば、次のデータのみがメッセージに含まれます。

```
[meta sequenceId="value" sysUpTime="value"]
```

- Snare Protocol： Snare ログ監視ツールと互換性のある形式でログメッセージを送信します。

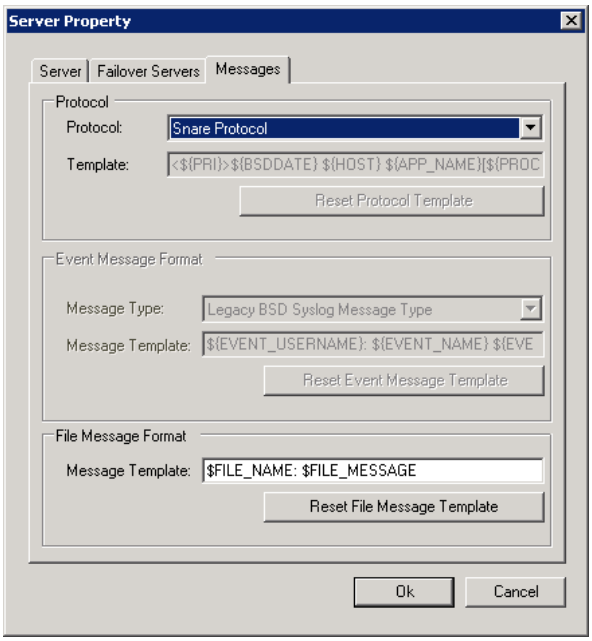

Figure 4.6. Snare Protocol

注意:

Snare は、タブで区切られたメッセージ形式です。メッセージ部分では、エージェントは CRLF を 2 スペース、TAB 文字を 1 スペースで置き換えます。

このプロトコルを選択した場合、ログ形式を変更することはできません。

Example 4.2. Snare log

```
<134>Oct 06 13:49:41 zts-win019.ztswin2008dom.balabit MSWinEventLog 1 Application 1 Wed Oct 06 13:49:41 2010 1 syslog-ng Agent S-1-5-21-551780264-1021859348-3425375765-1003 User Information zts-win019.ztswin2008dom.balabit None Application started 1
```

注意:

[Syslog Protocol]オプションを選択することは、syslog-ng の Linux/Unix バージョンで syslog ドライバを使用することと同じです。同様に、[Legacy BSD Syslog Protocol]の選択は syslog-ng の tcp ドライバ設定と同等です。

[Legacy BSD Protocol]に変更しても元のテンプレートは自動的に復元されません。これを行うには、プロトコルを変更した後に[Reset Protocol Template]をクリックします。

6. 必要に応じて、メッセージのテンプレートを変更します。 メッセージの形式は、イベントログとフ

ァイルソースによって異なる場合があります。

警告:

テンプレートの最大長は 1023 文字です。

7. プライマリログサーバーが使用できなくなった場合にログメッセージを受け入れることができるバックアップサーバーがある場合は、[Failover Servers]タブを選択して[Add]をクリックし、[Server Name]フィールドにバックアップログサーバーのホスト名または IP アドレスを入力します。複数のバックアップサーバーがある場合は、この手順を繰り返します。

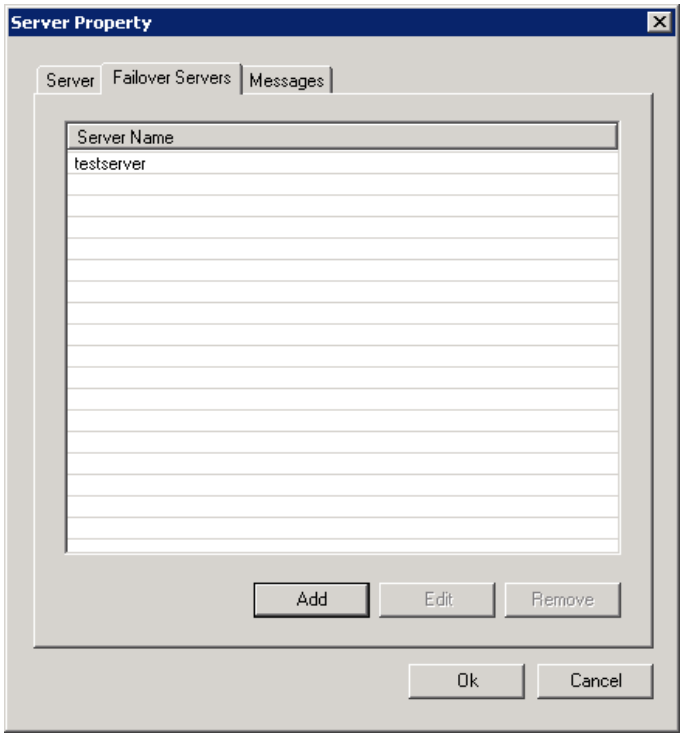

Figure 4.7. Failover Servers

8. すべてのサーバーがすべてのメッセージを受け取るように、ログメッセージを複数のサーバーに並行して送信する場合は、手順 3～4 を繰り返して、他の宛先サーバーを追加します。これらのサーバーにもフェールオーバーサーバーがあります。
9. [OK]をクリックします。変更を有効にするのに、syslog-ng Agent サービスを再起動します。
10. オプションの手順: syslog-ng エージェントを実行しているホストがドメインにログインしている時も、そうでない時もあります。そのホスト名は実際のドメインメンバーシップによって変わることがあります。これにより、syslog メッセージに表示されるホスト名は、ホストのドメインメンバーシップによって異なります。このような状況を回避するには、[syslog-ng Agent Settings]>[Local Settings または Client Group Policy 以下]>[Global Settings]>[Hostname]>[Use

FQDN]を選択します。こうすることで、syslog-ng エージェントはホストの名前を DNS サーバーから解決し、解決された FQDN(Fully Qualified Domain Name)を syslog メッセージに使用します。

5.2 メッセージレートを制限する

syslog-ng エージェントは、セントラルサーバーに送信されるメッセージレート(1 秒あたりのメッセージ数)を制御できます。そうすれば、突然のメッセージバーストを避けることができ、サーバーの負荷が軽減されます。

送信先に送信されるメッセージの数を制限するには、次の手順を実行します。

手順:

1. syslog-ng Agent for Windows アプリケーションの設定インターフェースを開きます。
2. [syslog-ng Agent Settings]>[Local Settings または Client Group Policy 以下]>[Destinations]を選択します。
3. 右クリックして[Destination Global Settings]を選択します。syslog-ng エージェントがサーバーに送信する 1 秒あたりのメッセージの数を制限するには、[Enable]を選択して、[Throttle]フィールドに望む制限値を入力します。デフォルト(0)では、syslog-ng エージェントは送信されるメッセージの数を制限しません。

   このパラメーターは、送信されたメッセージの合計数に適用され、すべてのソースの個々に適用されません。同じ値がすべての宛先に適用されます。
4. [OK]をクリックします。 変更を有効にするには、syslog-ng Agent サービスを再起動します。

5.3 MARK メッセージの送信

宛先サーバーに送信する必要がある新しいメッセージがない場合は、syslog-ng Agent for Windows アプリケーションは、接続がまだアクティブであることをサーバーに通知するために 10 分おきに自動で MARK メッセージを送信します。MARK メッセージの正確な形式は、プロトコルによって異なります。

Legacy BSD protocol (RFC3164):

```
<46>Apr 18 11:34:21 <hostname> -- MARK --
```

Snare protocol:

```
<46>Apr 18 11:34:21 <hostname> -- MARK --
```

Syslog protocol (RFC5424):

```
82 <46>1 2013-04-23T10:51:29+02:00 <hostname> - - - [meta sequenceId="3"] -- MARK --
```

syslog-ng エージェントがこれらのメッセージを送信する頻度を変更するには、次の手順を実行

します。

手順:

1. syslog-ng Agent for Windows アプリケーションの設定インターフェースを開きます。
2. [syslog-ng Agent Settings]>[Local Settings または Client Group Policy 以下]を選択し、[Global Settings]をダブルクリックします。
3. [Settings]>[Enable]を選択し、[Mark Mode Options]を選択します。
4. syslog-ng Agent for Windows アプリケーションが送信する MARK メッセージの頻度を設定します。

   - Never: MARK メッセージを送信しません。
   - When destination idle: 指定された期間内に宛先に送信されたメッセージが他にない場合にのみ、MARK メッセージを送信します。
   - Periodically: 指定された期間毎に MARK メッセージを送信します。

5. [The number of seconds between two MARK messages]で 2 つの MARK メッセージ間隔を秒数で設定します。デフォルトでは 600 秒(10 分)です。
6. [適用]をクリックし、次に[OK]をクリックします。 変更を有効にするには、syslog-ng Agent サービスを再起動してください。

5.4 Syslog-ng Agent for Windows のフローコントロール

バージョン 5 LTS から、syslog-ng Premium Edition のフロー制御機能が宛先に対して自動的に有効になりました。フロー制御を使用すると、宛先が(例えば、ネットワークエラーのために)メッセージを受信できない場合、syslog-ng エージェントはソースからのメッセージの読み取りを停止します。フロー制御の概念の詳細については、「syslog-ng Premium Edition 6 LTS 管理者ガイド」の「8.2 フロー制御による着信メッセージと発信メッセージの管理」を参照してください。

宛先のフロー制御を有効または無効にするには、[syslog-ng Agent Settings]>[Local Settings または Client Group Policy 以下]>[Destinations]を選択し、宛先サーバーを選択し[Properties]をダブルクリックして、[Server]>[Enable flow-control]にチェックします。

注意:

Reliable Log Transfer Protocol™(RLTP™)を使用する場合、フロー制御を無効にすることはできません。

注意:

syslog-ng Agent 5 LTS のフロー制御は、以前のバージョンの Primary Server オプションに代わるものです。

フローコントロールと複数の宛先

ソースのメッセージを複数の宛先に送信する場合、ソースのフロー制御を使用することは重要な副作用を伴います。フロー制御が使用されていて、宛先の 1 つがメッセージを受け入れることができない場合、syslog-ng がソースの読み込みを停止するため、他の宛先にもメッセージは受信されません。例えば、送信元からのメッセージが 2 つのリモートサーバーに送信され、いずれかのサーバーへのネットワーク接続が利用できなくなった場合、いずれのサーバーもいずれのメッセージも受信しません。

注意:

同じフロー制御ソースを使用する宛先のログパスを別々に作成しても、この問題を回避されません。

6 メッセージソースの設定

syslog-ng Agent for Windows アプリケーションは、イベントログコンテナおよびテキストファイルからメッセージを読み取ることができます。 以下のセクションでは、これらのメッセージソースの設定方法について説明します。

- イベントログコンテナからメッセージを転送する方法については、「6.1 イベントログソース」を参照してください。
- (プレーン)テキストログファイルからメッセージを転送する方法については、「6.2 ファイルソースの管理」を参照してください。
- グローバル設定の中には、両方のタイプのソースに適用できるものもあります。詳細については、「6.4 グローバルセッティングの設定」を参照してください。

6.1 イベントログソース

syslog-ng Agent for Windows アプリケーションは、標準の Windows イベントログコンテナおよび

カスタムコンテナからメッセージを収集できます。エージェントは、3 つの標準イベントログコンテナ（**アプリケーション**、**セキュリティ**、**システム**）からのメッセージを自動的に転送します。これらのソースを有効または無効にする、またはカスタムイベントログコンテナを追加するには、次の手順を実行します。

注意：

syslog-ng Agent for Windows は、独自のログメッセージをアプリケーションイベントログコンテナに送信します。

エージェントは、宛先サーバーに送信された最後のメッセージの ID を保存します。エージェントが一定時間動作していない（例えば、再起動時）場合、最後に保存されたメッセージ ID からのメッセージの読み取りが開始され、新しいメッセージがすべて送信されます。

警告：

イベントログコンテナが破損すると、エージェントはイベントソースの処理を停止します。ログメッセージは、エラー（Eventlog file is corrupt：ファイルが壊れていること）について通知するためにログサーバーに直接送信されます。

警告：データ損失の危険！

イベントコンテナにアーカイブを設定することは推奨されません。アーカイブの開始時にイベントコンテナに処理されていないイベントがあると、ログを失う可能性があります。Windows は、イベントコンテナを閉じて名前を変更し、読み取りアプリケーションに関係なく新しいものを開始します。これを防ぐには、以下の条件で Windows イベントビューアに[必要に応じてイベントを上書きする]モードを有効にして、以下の条件を満たしてください。

- メッセージはエージェントの処理速度より速く生成されてはいけません。
- 予定されたエージェント停止のために最初のイベントと最後のイベントの間に十分なウィンドウが必要です。新しいイベントが、エージェント停止中にエージェントによって最後に読み取られたイベントを上書きしないようにします。

6.1.1 イベントログソースを管理する

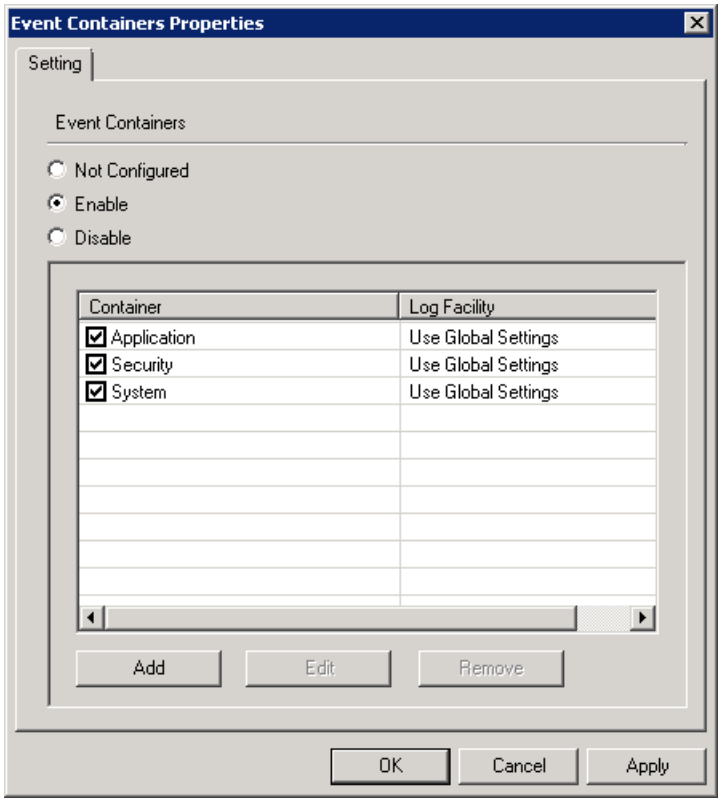

Figure 5.1. Managing eventlog sources

手順:

1. syslog-ng Agent for Windows アプリケーションの設定インターフェースを開きます。
2. [syslog-ng Agent Settings]>[Local Settings または Client Group Policy 以下]>[Eventlog Sources]を選択し、[Event Containers]をダブルクリックします。[Enable]を有効にします。
3. ・イベントログコンテナからのメッセージの送信を無効にするには、コンテナの名前の前にあるチェックボックスのチェックを解除します。
   ・コンテナのメッセージに関連付けられたログファシリティーを変更するには、コンテナを選択して[Edit]をクリックし、[Log Facility]フィールドで使用するログファシリティーを選択します。
4. [適用]をクリックし、次に[OK]をクリックします。変更を有効にするには、syslog-ng Agent サービスを再起動します。

6.1.2 イベントログソースを追加する

イベントログコンテナからセントラルログサーバーにメッセージを転送するには、次の手順を実行します。

前提条件:

イベントログコンテナの名前を知る必要があります。コンテナの名前がわからない場合は、「6.1.3 Windows Vista 以降でカスタムイベントログコンテナの名前を特定する」または、「6.1.4 Windows XP または Server 2003 でカスタムイベントログコンテナの名前を特定する」を参照してください。

手順:

1. syslog-ng Agent for Windows アプリケーションの設定インターフェースを開きます。
2. [syslog-ng Agent Settings]>[Local Settings または Client Group Policy 以下]>[Eventlog Sources]を選択し、[Event Containers]をダブルクリックします。
3. [Add]をクリックし、[Event Container Name]フィールドにコンテナの名前を入力します。コンテナ名に*と？のワイルドカード文字を使用できます。そうすれば、単一のソースで複数のイベントログコンテナを処理できます。

   イベントログコンテナの名前にワイルドカードを使用する場合は、次の点に注意してください。

   - 既存のイベントログコンテナのいずれもパターンに一致しない場合は、syslog-ng エージェントはデバッグログに警告メッセージを送信します。デバッグログを有効にする方法については、「11.2 syslog-ng エージェントのデバッグ」を参照してください。
   - syslog-ng エージェントアプリケーションは、新しいイベントログコンテナが開始または再起動されたときにのみ確認します。新しいイベントログコンテナがイベントログソースのパターンと一致する名前で作成された場合は、syslog-ng エージェントサービスを再起動します。

   警告：データ損失の危険！

   複数のイベントログソース名にワイルドカードを使用する場合は、各コンテナ名に一致するパターンが 1 つだけであることを確認してください。2 つのイベントログソースが同じコンテナに一致すると、syslog-ng のエージェントは、イベントログコンテナのメッセージを無視することがあります。

4. [適用]をクリックし、次に[OK]をクリックします。 変更を有効にするには、syslog-ng Agent サービスを再起動します。

期待される結果:

syslog-ng エージェントアプリケーションは、新しく追加されたイベントログコンテナから新しいメッセージの送信を開始します。syslog-ng エージェントは、[Read Old Records]オプションを選択した場合にのみ、イベントログコンテナから既存のメッセージを送信します。

6.1.3 Windows Vista 以降でカスタムイベントログコンテナの名前を特定する

Windows Vista、Server 2008、および Windows 7 でカスタムイベントログコンテナの名前を確認するには、次の手順を実行します。

手順:

1. イベントビューアアプリケーションを開きます。
2. 探している(メッセージを抽出したい)カスタムコンテナ(例:DNS Server)を選択します。
3. コンテナを右クリックし、[プロパティ]を選択します。
4. コンテナの名前は、ログ名フィールドに表示されるファイル名(拡張子なし)です。 (例えば、**C:¥WINDOWS¥system32¥winevt¥Logs¥Security.evtx** の場合は **Security** になります。)
5. 「6.1.1 イベントログソースを管理する」で説明している手順で、この名前をカスタムイベントログコンテナの名前として使用します。

注意:

Windows Vista および Server 2008 では、一部のコンテナは実際のコンテナではなく、複数のコンテナから収集され選ばれたメッセージを表示しています。このようなメッセージを syslog-ng サーバーに転送するには、コンテナに表示されている実際のコンテナを見つけて、それらを syslog-ng エージェントの設定に追加する必要があります。

それらのコンテナには、名前に%4 文字が含まれています。これらを syslog-ng エージェントに追加する場合は、%4 を/(スラッシュ)文字に置き換えます。例えば、microsoft-windows-bits-client%4analytic は microsoft-windows-bits-client/analytic にします。

古いメッセージをサーバーに送信している場合にも、syslog-ng エージェントはコンテナに格納されている最初のメッセージを送信しません。これは Windows API のバグです。

6.1.4 Windows XP または Server 2003 でカスタムイベントログコンテナの名前を特定する

Windows XP または Server 2003 でカスタムイベントログコンテナの名前を確認するには、次の手順を実行します。

手順:

1. クライアントホストで、[スタートメニュー]>[ファイル名を指定して実行]で **regedit** と入力します。(レジストリエディターを起動します。)
2. **HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Eventlog¥**まで移動します。カスタムコンテナがここにリストされています。例えば、有効なコンテナ名は次のとおりです。

DFS Replication, File Replication Service, DNS Server.

3. 「6.1.1 イベントログソースを管理する」で説明している手順で、この名前をカスタムイベントログコンテナの名前として使用します。

6.2 ファイルソースの管理

syslog-ng Agent for Windows アプリケーションは、テキストファイルからログメッセージを収集できます。複数の行にまたがるメッセージを処理でき、ファイル名にワイルドカード(*, ?)を使用することをサポートしているので、自動的にローテーションされるログファイルに対応することができます。改行文字で終わるファイル内のすべての行は、別々のメッセージとみなされることに注意してください。ただし、改行文字で終わらないシングル行だけが含まれるファイルは、syslog-ng エージェントは、その行を処理しません。

ファイルソースを設定するには、以下のステップを実行します。

警告:

ファイルソースとして使用されるファイルは、syslog-ng エージェントアプリケーションが実行されているホスト上にローカルに存在する必要があります。syslog-ng Agent for Windows アプリケーションはローカルサービスとして実行されており、ネットワーク共有にアクセスする権限を持たないため、ネットワーク共有にあるファイルはサポートされていません。

警告:

アプリケーションがログファイルを削除する場合、アプリケーションはメッセージを失わないように、syslog-ng エージェントがファイルからセントラルサーバーにメッセージを転送するのに十分な時間を確保する必要があります。

Example 5.1. Collecting the logs of multiple applications from a single folder

2 つのアプリケーションが同じフォルダ(例:C:¥logs)にログを取るとき、2 つのファイルソースを作成する必要があります。例えば、ログファイルの名前が、それぞれ application1-*.log および application2-*.log の場合、[Base Directory]は C:¥logs で 2 つのファイルソースを作成します、[File Name Filter]にそれぞれ、異なる application1-*.log および application2-*.log を設定します。

他のアプリケーションが C:¥logs フォルダにログを取る場合、アプリケーションごとに別の式を追加します。

デフォルトでは、syslog-ng エージェントは監視対象のログファイルのいずれかに届いたロ

グをメッセージとして、すべてのメッセージをサーバーに送信します。

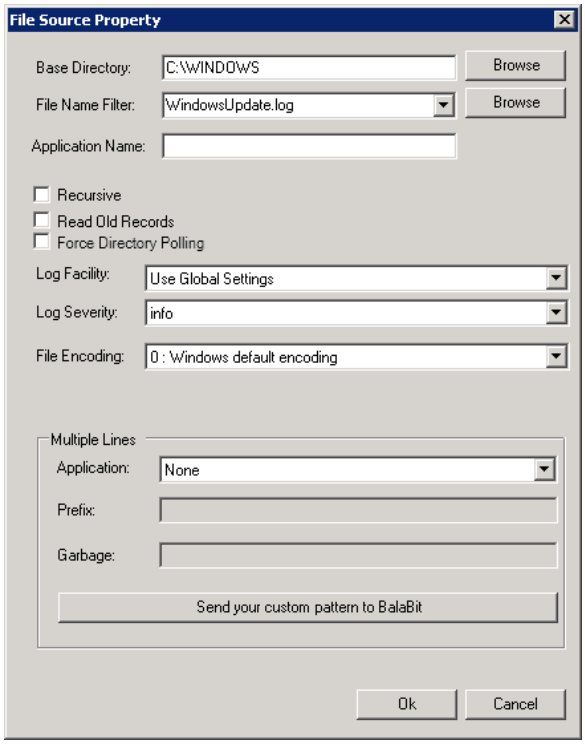

Figure 5.2. Managing file sources

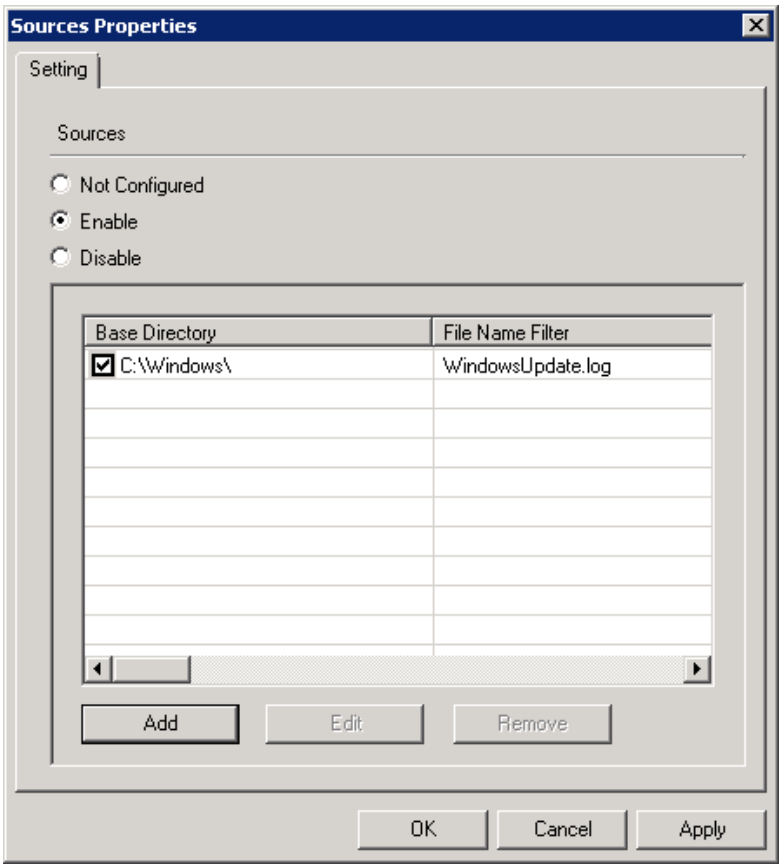

Figure 5.3. Sources properties

手順:

1. syslog-ng Agent for Windows アプリケーションの設定インターフェースを開きます。
2. [syslog-ng Agent Settings]>[Local Settings または Client Group Policy 以下]>[File Sources]を選択し、[Sources]をダブルクリックして[Enable]オプションをチェックします。
3. [Add]>[Browse]を選択し、[Base Directory]フィールドにログファイルが存在するフォルダを選択します。[File Name Filter]フィールドにログファイルの名前と拡張子を選択または入力します。ワイルドカードが使用できます。syslog-ng エージェントは、このフォルダに存在するフィルター式に一致する名前を持つ、すべてのファイルからログメッセージを転送します。

警告:

複数のファイルソースでワイルドカードを使用する場合は、ワイルドカードに一致するファイルとフォルダが重複しないようにしてください。 つまり、すべてのファイルとフォルダは 1 つのファイルソースにのみ属する必要があります。 複数のワイルドカードソースからファイルを監視すると、データが失われる可能性があります。

警告:

ファイルソースとして使用されるファイルは、syslog-ng エージェントアプリケーションが実行されているホスト上にローカルに存在する必要があります。 syslog-ng Agent for Windows アプリケーションはローカルサービスとして実行されており、ネットワーク共有にアクセスする権限を持たないため、ネットワーク共有にあるファイルはサポートされていません。

Tips:

[Base Directory]を指定する場合に、Windows の環境変数(例:%WINDIR%, %SYSTEMROOT%, %PROGRAMFILES%など)が使用できます。

警告:

ドメインのメンバーを管理する場合は、選択したパスをドメインメンバーで使用できる必要があります。例えば、C:¥logs はドメインコントローラーではなくクライアントホストで使用できる必要があります。

4. ・ ベースディレクトリとして設定されたフォルダのサブフォルダにあるファイルからメッセージを送信するには、[Recursive]オプションを選択します。

・ ファイルソースに関連したログファシリティーまたはログセベリティーを変更するには、[Log Facility]フィールドまたは[Log Severity]フィールドで、それぞれ、目的のファシリティーまたはプライオリティーを選択します。

注意:

ファイルソースの設定を大幅に変更すると、syslog-ng エージェントは一致するファイルの内容全体を再送信する可能性があります。これは、既に syslog-ng サーバーに送信済みのログメッセージが再送信され、サーバログに複製される可能性があることを意味します。 このような動作を引き起こす可能性のある構成の変更は次のとおりです。

- ベースディレクトリ[Base Directory]の変更
- フィルタオプション[File Name Filter]の変更
- 再帰オプション[Recursive]を変更

5. オプションの手順: デフォルトでは、syslog-ng エージェントアプリケーションはファイルの先頭からメッセージの送信を開始します。新しくファイルに追加されたメッセージのみを送信する場合は、[Read Old Records]オプションを無効にします。

注意:

[Read Old Records]が無効になっているときには注意してください。syslog-ng エージェントが停止している間に新しいファイルが作成された場合、このファイルの内容は転送されず、新しいレコードだけが転送されます。メッセージの損失を避けるために、設定で[Read Old Records]を無効にしないでください。

6. オプションの手順: デフォルトでは、アプリケーションがログファイルを変更すると、オペレーティングシステムは syslog-ng エージェントアプリケーションに通知します。ただし、Windows のファイル監視 API は、Windows DHCP サービスのログファイルを監視する場合など、ファイルが変更されたことを通知しない場合があります。

このような場合は、[Force Directory Polling]オプションを選択します。ただし、このオプションを有効にすると、たくさんのログファイルを監視する場合、syslog-ng エージェントのパフォーマンスが低下することに注意してください。

7. デフォルトでは、syslog-ngエージェントアプリケーションは、ソースファイルがホストのロケール [1]で特定されたデフォルトのウィンドウズのANSIコードページを使用してエンコードされてい

[1] ロケール(locale)とは、ソフトウェアに内蔵される、言語や国・地域ごとに異なる単位、記号、日付、通貨などの表記規則の集合。または単に、利用する言語や国・地域の指定。

ることを前提としています。ファイルのエンコーディングが異なる場合は、[File Encoding]フィールドからエンコーディングを選択します。ログメッセージは、UTF-8 エンコーディングを使用して宛先に送信されることに注意してください。

8. ログファイル内のログメッセージが複数の行で構成されている場合（つまり、ログメッセージに改行文字が含まれている場合）、syslog-ng エージェントは設定により、関連する行を単一のメッセージとして処理します。

   syslog-ng エージェントアプリケーションは、Apache, Tomcat, Catalina および Oracle SQL のログメッセージを自動的に処理できます。このような（複数行から成る）メッセージを処理するには、[Multiple Lines]>[Application]フィールドからアプリケーション名を選択します。Tomcat のログメッセージのタイムスタンプは、ホストのロケールによって異なることに注意してください。syslog-ng Agent for Windows アプリケーションは、複数行のメッセージから最後の CRLF 制御文字を自動的に削除します。

   別のアプリケーションの複数行のログメッセージを処理するには、以下の手順を実行します。

   a. [Multiple Lines]>[Application]>[Custom]を選択し、[Prefix]フィールドと[Garbage]フィールドにオプションを設定します。

   b. [Multiple Lines]>[Prefix]フィールドにログメッセージの先頭に一致する文字列または正規表現を指定してください。[Prefix]オプションが設定されている場合、syslog-ng エージェントは、行が正規表現と再び一致するまで、ソースからの改行文字を無視し、一致するまでの行の間の行を単一のメッセージとして扱います。

   注意：

   複雑な正規表現は、複数行のメッセージの処理速度を著しく低下させる可能性があるため、できるだけ単純な正規表現として使用します。

   c. メッセージ間に不必要な部分が含まれている複数行のメッセージを処理する場合は、[Multiple Lines]>[Garbage]オプションを使用してください。不要なメッセージ部分の先頭に一致する文字列または正規表現を指定します。[Garbage]オプションが設定されている場合、syslog-ng エージェントは、[Garbage]で一致する行と[Prefix]に一致する次の行との間の行を無視します。

   [Garbage]オプションが設定されているのに、[Prefix]と一致する 2 行の間に一致する行がない場合、ソースから複数行のメッセージを受信すると、syslog-ng エージェントアプリケーションは、[Garbage]と一致する行が受信されるまで、読み込む行を単一のメッセージとして処理し続けます。

警告:

[Garbage]オプションが設定されている場合、syslog-ng エージェントアプリケーションは、[Garbage]と一致する行と[Prefix]で一致する行の間の行を破棄します。

d. オプションのステップ: カスタムパターンを作成してテストした後、そのパターンを Balabit に送ることを検討してください。そうすれば、syslog-ng Agent の将来のバージョンに含めることができます。Balabit や他の syslog-ng Agent ユーザーとパターンを共有するには、[Multiple Lines]>[Send custom pattern to BalaBit]をクリックします。電子メールアプリケーションが開き、アプリケーション名とパターンを含む電子メールが表示されます。

9. [File Source Property]ダイアログを[OK]で戻り、[適用]をクリックし、次に[OK]をクリックします。 変更を有効にするには、syslog-ng Agent サービスを再起動します。

6.3 内部ソースを管理する

syslog-ng Agent for Windows アプリケーションによって内部的に生成されたすべてのメッセージは、内部ソースを使用します。syslog-ng Agent for Windows アプリケーションは、内部ソースから発生したメッセージを特定の宛先に転送できます。内部ソースを設定するには、次の手順を実行します。

手順:

1. syslog-ng Agent for Windows アプリケーションの設定インターフェースを開きます。
2. [syslog-ng Agent Settings]>[Local Settings または Client Group Policy 以下]を選択し、[Global Settings]をダブルクリックします。
3. [Enable]を有効にします。
4. [Internal Messages]に移動します。
5. [Application event container]または、[Remote destinations]に転送する内部メッセージタイプを選択します。(通常の TCP の宛先として設定されているすべてのサーバーを意味します)。メッセージタイプは、それぞれのメッセージシビリティーに対応します。デフォルトの設定では、内部のエラーメッセージと警告メッセージが[Application event container]に転送され、情報メッセージが[Remote destinations]に転送されます。

選択したメッセージタイプのみが転送されます。

警告:

[Application event container]と[Remote destinations]の両方で同じメッセージタイプを選択し、アプリケーションイベントコンテナのソースも同じであれば、メッセージを複製することができます。

注意:

これらのオプションは、GPO(グループポリシーオブジェクト)から継承されます。詳細は、「4.2.3 ドメインとローカルの設定」を参照してください。また、XML 設定からエクスポート/インポートすることもできます。

6. [適用]をクリックし、次に[OK]をクリックします。 変更を有効にするには、syslog-ng Agent サービスを再起動します。

6.4 グローバルセッティングの設定

syslog-ng Agent for Windows アプリケーションには、イベントログとファイルソースの両方に適用できるグローバル設定があります。グローバル設定を構成するには、次の手順を実行します。

手順:

1. syslog-ng Agent for Windows アプリケーションの設定インターフェースを開きます。
2. [syslog-ng Agent Settings]>[Local Settings または Client Group Policy 以下]を選択し、[Global Settings]をダブルクリックします。
3. [Enable]を有効にして、メッセージに関連付けられたデフォルトのログファシリティーを設定します。
4. デフォルトでは、メッセージフィルタで使用されるフィルターと正規表現は大文字と小文字が区別されます。(「8 メッセージのフィルタリング」を参照)。大文字と小文字を区別しないようにするには、[Regular Expressions Ignore Case]または、[Filters Ignore Case]オプション、または、その両方を選択します。

注意：

[Regular Expressions Ignore Case]オプションは、ファイルとイベントログの両方のソースでメッセージ内容のフィルタが大文字と小文字を区別しなくなります。[Filters Ignore Case]オプションは、[Computers]，[Sources]，[Categories]および[Users]フィルターで大文字と小文字を区別しなくなります。

5. [適用]をクリックし、次に[OK]をクリックします。 変更を有効にするには、syslog-ng Agent サービスを再起動します。

6.5 ホスト名のフォーマット設定

syslog-ng Agent for Windows アプリケーションは、ホストのドメインメンバーシップとメッセージのソース（イベントログまたはファイル）に応じて、異なる形式の形式（FQDN または短いホスト名）でホスト名マクロを送信できます。ホスト名の設定は、ファイルソース、イベントログソース、MARK メッセージ、および syslog-ng エージェントの内部メッセージ（例：start/stop メッセージなど）から発生するすべてのログに影響します。

信頼できるソースから 2 つのホストライセンスを使用しないようにするには、すべての送信メッセージに同じホスト名タイプを使用します。

ホスト名を決定するために、syslog-ng エージェントは起動時にマシンの短いホスト名を参照し、FQDN を取得するために DNS サーバーから解決しようとします。DNS 解決が不可能な場合、ホスト名は短いホスト名になります。

注意：

syslog-ng エージェントは決してホスト名を書き換えません。

ホスト名のフォーマットをグローバルに設定するには、次の手順を実行します。

手順：

1. syslog-ng Agent for Windows アプリケーションの設定インターフェースを開きます。
2. [syslog-ng Agent Settings]>[Local Settings または Client Group Policy 以下]を選択し、[Global Settings]をダブルクリックします。
3. [Enable]を有効にし、[Hostname]に移動します。
4. グローバルに使用するホスト名の種類を選択します。

   - 送信メッセージの**$HOST** マクロで短いホスト名のみを使用するには、[Use only hostname]を選択します。これはデフォルト設定です。

- ファイルソース、MARK メッセージ、および syslog-ng Agent の内部メッセージの場合、発信ホスト名はマシンの短いホスト名になります。
- イベントログソースの場合、ホスト名はイベントメッセージの短いホスト名（例：mypc）になります。または、syslog-ng エージェントは FQDN からドメイン名切り捨て、短いホスト名部分を使用します。（例：mypc.mycompany.local は mypc になります）。

- 送信メッセージの**$HOST** マクロで FQDN（ホスト名.ドメイン名）を使用するには、[Use FQDN]を選択します。
  - ファイルソース、MARK メッセージ、および syslog-ng Agent の内部メッセージの場合、ホスト名はマシンの FQDN になります。

注意：
DNS サーバーがない場合、または DNS サーバーがホスト名を解決できない場合は、マシンの単純なホスト名だけが使用されます。

  - イベントログソースの場合、イベントメッセージのホスト名がすでに FQDN である場合、syslog-ng エージェントはそれをホスト名として、そのまま使用します（例えば、mypc.mycompany.local のように使用されます）。もし、これが FQDN でない場合、syslog-ng エージェントはこのホスト名の名前解決を試み、受信した FQDN をホスト名として使用します（例えば mypc は mypc.mycompany.local になります）。

注意：
DNS サーバーがない場合、または DNS サーバーがホスト名を解決できない場合は、イベントメッセージの短いホスト名のみが使用されます。

- FQDN を受信するために短いホスト名の後ろにドメイン名を追加するには、カスタムドメイン名を使用します。[Use hostname with custom domain name]を選択し、下のフィールドに短いホスト名の後に追加するドメイン名を入力します。このオプションは、すべての発信メッセージ（イベントログソース、ファイルソース、MARK メッセージ、および syslog-ng エージェントの内部メッセージ）に影響します。
  - ホスト名が短いホスト名である場合、カスタムドメイン名はホスト名の後ろに追加されます（例えば、mypc は mypc.customcompany.local になります）。

- ホスト名が FQDN の場合は、ドメイン名の部分がカスタムドメイン名に置き換えられます。(例えば、転送されたメッセージの FQDN が mypc.mycompany.local で、カスタムドメイン名が customcompany.local の場合、送信メッセージのホスト名は mypc.customcompany.local になります)。

注意:
イベントログメッセージにイベントのホスト名がマシンのホスト名と異なる場合、ホスト名は送信メッセージでも異なる場合があります。

- 転送イベントログの場合は元のマシンのホスト名がホスト名になります。
- マシンのホスト名が、DNS サーバーが提供するものと異なる場合(DNS サーバーが存在し、ホスト名を解決できる場合)。

5. すべてのホスト名で小文字を使用するには、[Convert to lower-case]を有効にします。これはデフォルトで有効になっています。無効にすると、ホスト名に大文字(存在する場合)と小文字が混在します。このオプションは、すべての発信メッセージ(イベントログソース、ファイルソース、MARK メッセージ、および syslog-ng エージェントの内部メッセージ)に影響します。
6. [適用]をクリックし、次に[OK]をクリックします。 変更を有効にするには、syslog-ng Agent サービスを再起動します。

6.6 ソースとフィルターをグローバルに無効にする

フィルターとソースはグローバルにも無効にすることができます。フィルターまたはソースを無効にすると、syslog-ng エージェントは無効な設定を無視します。つまり、ファイルソースが無効になっている場合、エージェントはファイルからサーバーにメッセージを送信しません。 詳細は、次の手順を参照してください。

手順:

1. syslog-ng Agent for Windows アプリケーションの設定インターフェースを開きます。
2. ・イベントログのソースを無効にするには、[syslog-ng Agent Settings]>[Local Settings または Client Group Policy 以下]を選択し、[Eventlog Sources]を右クリックして、[プロパティ]>[Disable]を選択します。
   ・ファイルソースを無効にするには、[syslog-ng Agent Settings]>[Local Settings または Client Group Policy 以下]を選択し、[File Sources]を右クリックして、[プロパティ]>[Disable]を選択します。

・イベントログフィルタを無効にするには、[syslog-ng Agent Settings]>[Local Settings または Client Group Policy 以下]>[Destinations]を選択し、[Global Event Filters]を右クリックし、[プロパティ]>[Disable]を選択します。

・ファイルフィルタを無効にするには、[syslog-ng Agent Settings]>[Local Settings または Client Group Policy 以下]>[Destinations]を選択し、[Global File Filters]を右クリックして、[プロパティ]>[Disable]を選択します。

3. [適用]をクリックし、次に[OK]をクリックします。 変更を有効にするには、syslog-ng Agent サービスを再起動します。

7 syslog-ng エージェントでの SSL の使用

暗号化された接続を使用して syslog-ng サーバーに接続するときは、syslog-ng Agent for Windows は、サーバーの証明書を確認します。syslog-ng Agent for Windows が syslog サーバーの証明書を確認できる場合にのみ接続は確立できます。そのためには、Windows ベースのホストの証明書ストア([MMC]>[証明書]>[コンピュータアカウント]>[ローカルコンピュータ]>[信頼されたルート証明書])に次の証明書のいずれかをインポートします。

- サーバーの証明書を発行した認証局(CA)の証明書。
- サーバーが自己署名証明書を使用している場合は、自己署名証明書をインポートします。

証明書のインポートの詳細については、「7.3 Microsoft 管理コンソール(MMC)を使用した証明書のインポート」を参照してください。

注意

この証明書(サーバーの CACert とも呼ばれます)は、サーバーの証明書ではなく、サーバーの証明書に署名した CA の証明書です。

7.1 暗号化接続を有効にする

SSL 暗号化されたサーバーへの接続を有効にするには、次の手順を実行します。

手順:

1. syslog-ng Agent for Windows アプリケーションの設定インターフェースを開きます。
2. [syslog-ng Agent Settings]>[Local Settings または Client Group Policy 以下]>[Destinations]を選択します。

3. SSL 暗号化接続する宛先サーバーを右クリックし、[Properties]を選択します。
4. [Use SSL encryption]オプションを選択します。

警告:

SSL 暗号化接続は syslog-ng Agent for Windows が syslog サーバーの証明書を確認できる場合にのみ接続は確立できます。そのためには、Windows ベースのホストの証明書ストア([MMC]>[証明書]>[コンピュータアカウント]>[ローカルコンピュータ]>[信頼されたルート証明書])に次の証明書のいずれかをインポートします。

- サーバーの証明書を発行した認証局(CA)の証明書。
- サーバーが自己署名証明書を使用している場合は、自己署名証明書をインポートします。

証明書のインポートの詳細については、「7.3 Microsoft 管理コンソール(MMC)を使用した証明書のインポート」を参照してください。

注意:

サーバー証明書の **subject_alt_name** パラメーター(または、**subject_alt_name** パラメーターが空の場合は **Common Name** パラメーター)には、サーバーのホスト名または IP アドレス(syslog-ng クライアントおよびリレーから解決されたもの)が含まれていなければなりません(例:syslog-ng.example.com)。

あるいは、**Common Name** または **subject_alt_name** パラメーターには、汎用ホスト名(例:*.example.com)を含めることができます。

証明書の共通名に汎用ホスト名が含まれている場合は、**subject_alt_name** パラメーターに特定のホスト名または IP アドレスを指定しないでください。

5. [Advanced Options]オプションをクリックします。

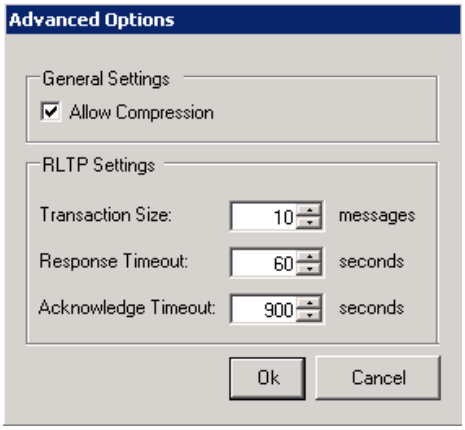

Figure 6.1. Adding new server

転送中にメッセージを圧縮して帯域幅を節約するには、[Allow Compression]オプションを選択します。syslog-ng エージェントが実際に圧縮を使用するには以下の点に注意する必要があります。

- [Server]>[Advanced Options]>[Allow Compression]オプションが有効になっている必要があります。
- ログサーバーにメッセージを送信するには、SSL および/または RLTP を使用する必要があります(つまり、少なくとも[Use syslog-ng proprietary Reliable Log Transfer Protocol (RLTP)]または、[Use SSL encryption]オプションを有効にする必要があります)。
- ログサーバーは、圧縮を有効にするように構成する必要があります。ログサーバーが syslog-ng PE の場合、適切な **allow-compress()**オプションをソースで有効にする必要があります(詳細については、「syslog-ng Premium Edition 6 LTS 管理者ガイド」の「12.2 RLTP™オプション」と「10.4 TLS オプション」を参照してください)。ログサーバーが syslog-ng Store Box(SSB)の場合、[Log]>[Sources]>[Allow compression option]オプションを有効にします。圧縮メッセージを syslog-ng Store Box(SSB)に送信するには、RLTP™プロトコルを使用する必要があることに注意してください(詳細については、「syslog-ng ストアボックス管理者ガイド」の「第 7 章 メッセージソースの設定」を参照してください)。

注意:

RLTP は、syslog-ng store box のフィーチャーリリース版でサポートされています。

6. [OK]をクリックします。 変更を有効にするには、syslog-ng Agent サービスを再起動します。

7.2 syslog-ng エージェントによる相互認証の使用

syslog-ng サーバーが相互認証を使用するように設定されている場合、syslog-ng クライアントか

ら証明書を要求します。syslog-ng エージェントアプリケーションは、ローカルコンピュータの個人証明書ストア（[MMC]>[証明書]>[コンピュータアカウント]>[ローカルコンピュータ]>[信頼されたルート証明書]）で利用可能である場合、接続が確立されたときに要求された証明書をサーバーに自動的に表示できます。証明書のインポートウィザードを使用して、この証明書をインポートします。詳細については、「7.3 Microsoft 管理コンソール(MMC)を使用した証明書のインポート」を参照してください。

注意：

証明書失効リスト（CRL）がローカルコンピュータ/個人証明書ストアで使用可能な場合、syslog-ng エージェントは syslog-ng サーバーの証明書がこのリストにないことを確認します。

7.2.1 syslog-ng Agent for Windows を使用した相互認証の設定

syslog-ng サーバーが syslog-ng エージェントからの認証を要求する場合は、次の手順を実行します。

手順：

1. クライアントの証明書を作成します。デフォルトでは、syslog-ng エージェントは、セントラル syslog-ng サーバーのホスト名または IP アドレスを[Common Name]に含む証明書を検索します。別の[Common Name]を使用する場合は、手順 3 で証明書の[Common Name]を設定して完了することを忘れないでください。

   証明書には秘密鍵が含まれている必要があり、PKCS12 形式である必要があります。

   Tips：

   証明書と鍵を PEM 形式から PKCS12 に変換するには、次のコマンドを使用します。

   ```
   openssl pkcs12 -export -in agentcertificate.pem -inkey agentprivatekey.pem -out agentcertificatewithkey.pfx
   ```

2. 証明書のインポートウィザードを使用して、この証明書をローカルコンピュータの個人証明書ストアにインポートします。 詳細については、「7.3 Microsoft 管理コンソール(MMC)を使用した証明書のインポート」を参照してください。
3. デフォルトでは、syslog-ng エージェントはセントラル syslog-ng サーバーのホスト名または IP アドレスが Common Name に含まれている証明書を検索します（エージェントは、宛先の

[Server Name]フィールドに設定されているサーバー名またはアドレスを検索します)。クライアントの証明書に異なる Common Name がある場合は、次の手順を実行します。

a. syslog-ng Agent for Windows アプリケーションの設定インターフェースを開きます。

b. [syslog-ng Agent Settings]>[Local Settings または Client Group Policy 以下]>[Destinations]を選択します。

c. 相互認証が必要な宛先サーバーを右クリックし、[Properties]を選択します。

d. [Use SSL encryption]オプションを選択し、[Select Certificate]をクリックして、使用する証明書を選択します。[Client Certificate Subject]フィールドに証明書の共通名を入力することもできます。

同じ Common Name を持つ複数の証明書がある場合は、証明書の識別名(DN)を[Client Certificate Subject]フィールドに入力することもできます。識別名を使用する場合は、名前の要素のみをコンマで区切って入力します。例えば、"US, Maryland, Pasadena, Example Inc, Sample Department, mycommonname"。

注意

一般的な方法は、syslog-ng エージェントを実行しているホストのホスト名または IP アドレスを証明書の共通名(例:syslog-ng-agent1.example.com)として使用することです。

4. [OK]をクリックします。変更を有効にするには、syslog-ng Agent サービスを再起動します。

7.3 Microsoft 管理コンソール(MMC)を使用した証明書のインポート

証明書をインポートするには、次の手順を実行します。

手順:

1. **mmc.exe** を実行して Microsoft 管理コンソールを起動します([スタート]から「ファイル名を指定して実行」)。

注意:

mmc.exe を実行するには、管理者権限が必要です。

2. [ファイル]メニューの[スナップインの追加と削除]を選択します。
3. [利用できるスナップイン]フィールドから[証明書]を選択して[追加]をクリックします。
4. 表示されたウィンドウで[コンピュータアカウント]を選択し、[次へ]をクリックします。
5. [ローカルコンピュータ]を選択し、[完了]をクリックします。[OK]をクリックして管理コンソール

画面に戻ります。

6. syslog-ng サーバーの証明書の CA 証明書をインポートするには、[コンソールルート]>[証明書]>[信頼されたルート証明機関]>[証明書]に移動します。
   相互認証を実行するために syslog-ng エージェントの証明書をインポートするには、[コンソールルート]>[証明書]>[個人]>[証明書]に移動します。
7. [証明書]フォルダを右クリックし、コンテキストメニューから[すべてのタスク]>[インポート]を選択します。証明書のインポートウィザードが表示されます。[次へ]をクリックします。
   オプションの手順: 相互認証で syslog-ng エージェントを認証するために使用される証明書には、秘密鍵が含まれます。要求されたときに秘密鍵のパスワードを入力します。
8. Windows ではデフォルトで適切な証明書ストアが用意されているため、[次へ]をクリックします。
9. 要約ウィンドウで[完了]をクリックし、証明書のインポートが成功したことを示すウィンドウで[はい]をクリックします。

8 メッセージのフィルタリング

syslog-ng Agent for Windows アプリケーションは、ブラックリストとホワイトリストの両方でログメッセージをフィルタリングできます。ブラックリストを使用すると、フィルターを定義することができ、フィルターに一致するすべてのメッセージはエージェントによって無視されます。つまり、フィルターに一致しないメッセージのみがセントラルサーバーに送信されます。ホワイトリストを使用すると、フィルターを定義することができ、フィルターに一致するメッセージはセントラルサーバーに転送されます。他のメッセージは無視されます。デフォルトでは、ブラックリストフィルタリングが使用されます。

複数のフィルターを定義する場合、メッセージはすべてのフィルターと一致する必要があります。言い換えれば、フィルターは、論理積演算によって互いに連結されます。

イベントログとファイルソースには、異なるフィルターを使用できます。syslog-ng エージェントはメッセージを処理するときに、関連するフィルターを 1 つずつチェックします。例えば、メッセージに一致するブラックリストフィルタが見つかった場合、エージェントはメッセージをサーバーに送信せずに処理を停止します。

注意:
デフォルトでは、すべてのフィルタで大文字と小文字が区別されます。この動作を変更する方法の詳細については、「6.4 グローバルセッティングの設定」を参照してください。

- イベントログソースから受信したメッセージをフィルタリングする方法については、「8.1 イベント

ログメッセージのフィルタリング」を参照してください。

- ファイルソースから受信したメッセージをフィルタリングする方法ついては、「8.2 ファイルメッセージのフィルタリング」を参照してください。
- グローバルにフィルタリングを無効にする方法については、「6.6 ソースとフィルターをグローバルに無効にする」を参照してください。

8.1 イベントログメッセージのフィルタリング

イベントログソースには、次のタイプのフィルターを使用できます。 特に断りのない限り、フィルターは、メッセージの関連フィールドに同じ文字列が含まれている場合にのみ一致します。

注意:
メッセージソースでフィルタリングする場合、[Source]フィールドの値が誤っていることがあります。問題を回避するには、メッセージの **EVENT_SOURCE** フィールドを確認してください。

- Sources: メッセージを作成したソース(アプリケーション)でフィルタリングします。**EVENT_SOURCE** マクロに対応します。
- Sources and Event ID: メッセージを作成したソース(アプリケーション)でフィルタリングし、必要に応じてイベントの識別(ID)番号でフィルタリングします。**EVENT_SOURCE** マクロと **EVENT_ID** マクロに対応します。
- Message Contents: メッセージのテキスト、つまり、**EVENT_MESSAGE** マクロの内容をフィルタリングします。このフィルタでは、正規表現を使用できます。
- Sources and Categories: メッセージを作成したソース(アプリケーション)でフィルタリングし、必要に応じてイベントのカテゴリをフィルタリングします。**EVENT_SOURCE** マクロと **EVENT_CATEGORY** マクロに対応します。

Example 7.1. Filtering on Sources and Categories
例えば、次のメッセージをフィルター処理するとします。

```
Source: Microsoft Windows security auditing
Category: Process Creation
New Process Name: C:¥Windows¥System32¥SearchProtocolHost.exe
```

[Source]を Microsoft Windows security auditing(Microsoft Windows セキュリティ監査)に設定し、[Category]を Process Creation(プロセス作成)に設定します。

- Users： イベントに関連付けられているユーザー名をフィルタリングします。**EVENT_USERNAME** マクロに対応します。
- Computers： イベントを作成したコンピュータ（ホスト）の名前をフィルタリングします。**HOST** マクロに対応します。
- Event Types： イベントの種類をフィルタリングします。**EVENT_TYPE** マクロに対応します。

イベントログメッセージに使用されるフィルターを変更するには、次の手順を実行します。

手順：

1. メッセージのソースをフィルタリングする場合は、次の手順を実行します。
   a. イベントビューアを起動し、フィルタリングするソースからメッセージを探します。
   b. [全般]タブを選択し、[ソース]フィールドの値を右クリックします。

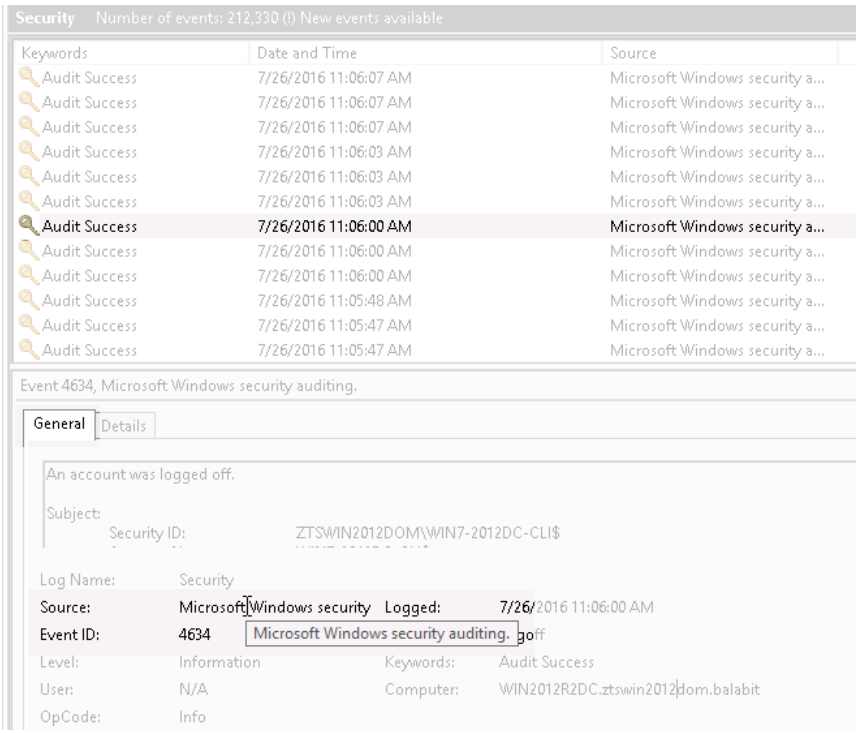

Figure 7.1. Finding the name of the Event Source

   c. コンテキストメニューで[コピー]を選択します。保存された値はどこかに保存してください。後で syslog-ng エージェントでフィルターを設定する必要があります。

注意：

Source フィールドの実際の値は、Event Viewer が表示する値よりも長くなる可能性があるため、このメソッドを使用することが重要です。（例えば、セキュリティメッセージの場合、表示されるソースは、多くの場合「Microsoft Windows security」ですが、ソースの完全な名前は「Microsoft Windows security auditing.」です。 最後にドット文字が含まれています）。

「ソース」フィールドの値にマウスを移動しても、ソースの完全な名前がポップアップされます。

2. syslog-ng Agent for Windows アプリケーションの設定インターフェースを開きます。
3. ・ フィルターを、すべてのイベントログメッセージにグローバルに適用するには、[syslog-ng Agent Settings]>[Local Settings または Client Group Policy 以下]>[Destinations]>[Global Event Filters]を選択し、[Global Event Filters]を右クリックします。

   ・フィルターを、特定の宛先にのみ適用するには、[syslog-ng Agent Settings]>[Local Settings または Client Group Policy 以下]>[Destinations]を選択し、送信先サーバーを選択して[Event Filters]を選択します。そして、[Event Filters]を右クリックします。

注意：

グローバルとローカル（サーバー側）の両方にフィルタリングを使用する場合、最初にグローバルフィルタがイベントログメッセージに適用され、次にローカルフィルタが適用されます。

4. [Properties]>[Enable]を選択します。

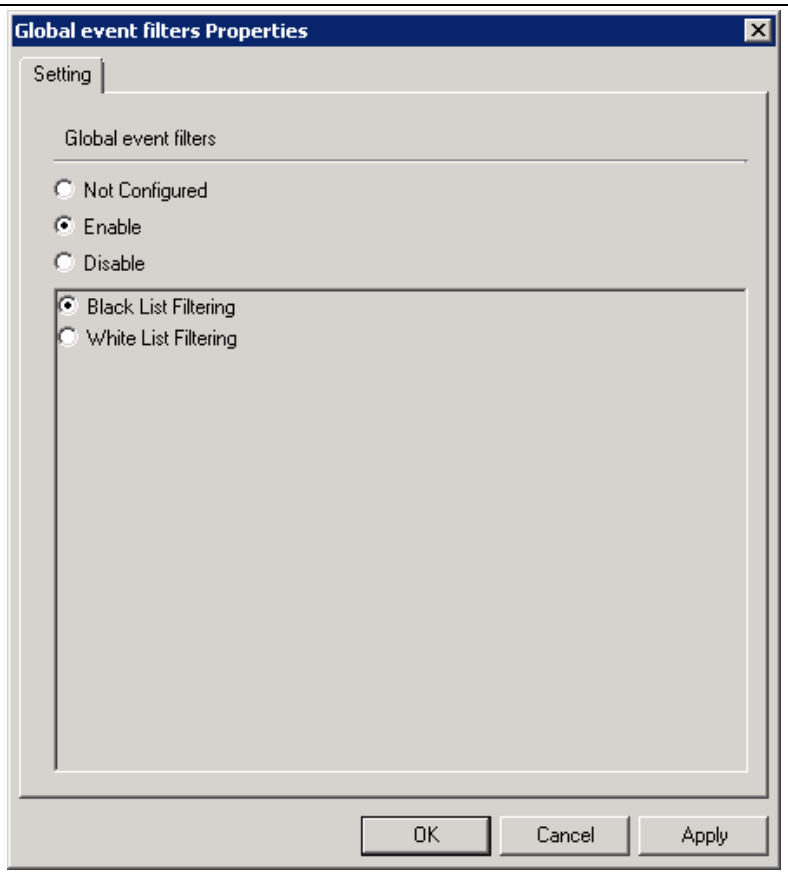

Figure 7.2. Global event filters

5. ホワイトリストフィルタリングを使用するには、[White List Filtering]を選択します。デフォルトでは、syslog-ng エージェントはブラックリストフィルタリングを使用します。[OK]をクリックします。
6. [Global Event Filters]または[Event Filters]を選択します。右側のペイン [2]で、作成するフィルターのタイプをダブルクリックします。
7. ・ 特定のアプリケーションによって送信されたメッセージ、または特定のイベント ID を持つアプリケーションのメッセージを無視するには、[Sources and Event Ids]をダブルクリックし、[Enable]を選択して[Add]をクリックします。メッセージを無視するソース(アプリケーション)の名前を[Source Name]フィールドに入力します。アプリケーションの特定のメッセージのみを無視するには、[Event ID]フィールドにイベントの ID を入力し、[Add]をクリックします。

[2] ウィンドウを複数の表示領域に分割して使用する表示方式における、分割された個々の表示領域のこと。

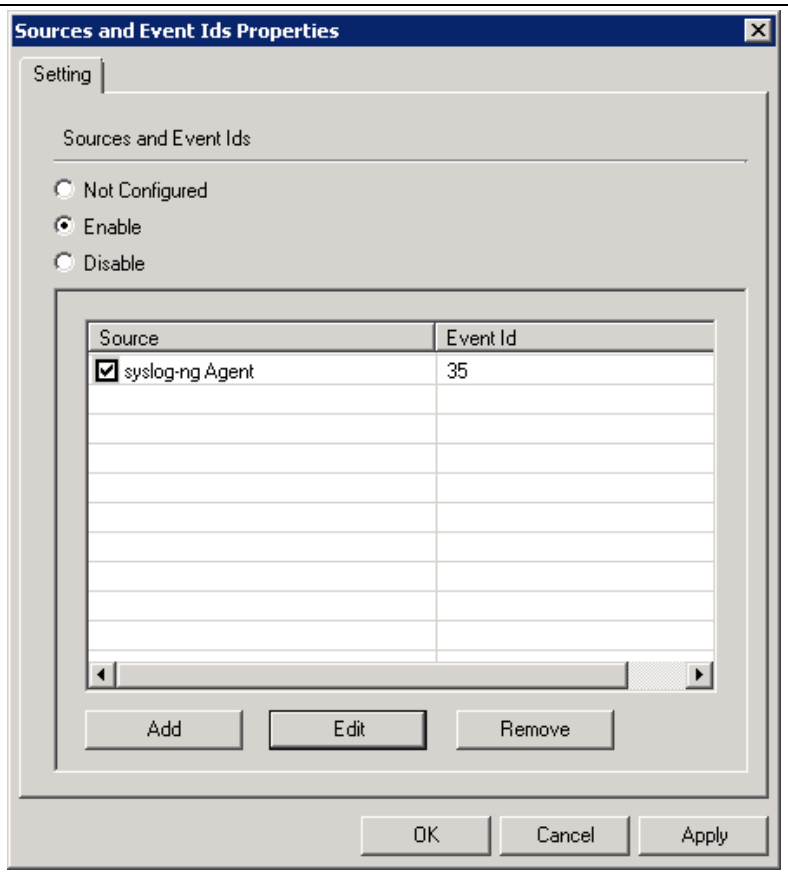

Figure 7.3. Sources and Event ID

- 特定のアプリケーションによって送信されたメッセージ、を無視するには、[Sources]をダブルクリックし、[Enable]を選択して[Add]をクリックします。メッセージを無視するソース（アプリケーション）の名前を[Source Name]フィールドに入力し、[Add]をクリックします。
- 特定の文字列またはテキストを含むメッセージを無視するには、[Message Contents]をダブルクリックし、[Enable]を選択して、フィルターにかける用語または POSIX 正規表現を[Regular Expression]フィールドに入力して、[Add]をクリックします。

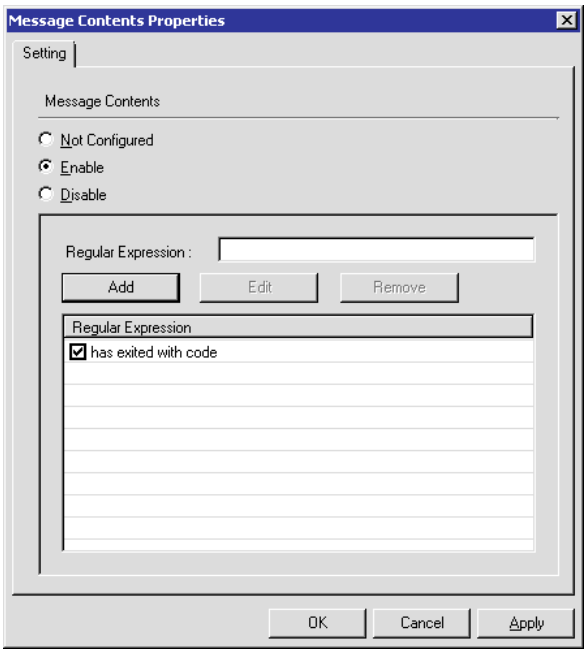

Figure 7.4. Message Contents

- 特定のアプリケーションによって送信されたメッセージ、または特定のカテゴリーに分類されるアプリケーションのメッセージを無視するには、[Sources and Categories]をダブルクリックし、[Enable]を選択し、[Add]をクリックして、メッセージを無視するアプリケーションの名前を[Application Name]フィールドに入力します。特定のカテゴリーに該当するアプリケーションのメッセージのみを無視するには、[Category]フィールドにカテゴリーの名前を入力します。[Add]をクリックします。
- 特定のユーザーが送信したメッセージを無視するには、[Users]をダブルクリックし、[Enable]を選択し、[User]フィールドにユーザーの名前を入力して、[Add]をクリックします。
- 特定のコンピューター(ホスト)から送信されたメッセージを無視するには、[Computers]をダブルクリックし、[Enable]を選択し、[Computer]フィールドにホストの名前を入力して、[Add]をクリックします。
- 特定のイベントタイプのメッセージを無視するには、[Event Types]をダブルクリックし、[Enable]を選択し、[Event Types]フィールドから選択します。

注意:

Windows Vista および Server 2008 では、Windows は特定のメッセージをレベル 3 とラベル付けし、イベントビューアはそのようなメッセージを警告として分類します。しかし、これは正式な仕様に反しています。レベル 3 は使用しないでください。レベル 2 のメッセージだけが警告です。これらのイベントをフィルタリングするには、レジストリに新しいイベントタイプを手動で追加し、その値を 3 に設定する必要があります。

例:**HKEY_LOCAL_MACHINE¥SOFTWARE¥BalaBit¥syslog-ng Agent¥Local Settings¥EventSources¥Filter¥Type¥Rule0¥Type=3**

8. 最後に[適用]をクリックし、次に[OK]をクリックします。変更を有効にするには、syslog-ng Agent サービスを再起動します。

8.2 ファイルメッセージのフィルタリング

ファイルソースには、次のタイプのフィルターを使用できます。

- Message Contents: メッセージのテキスト、つまり **FILE_MESSAGE** マクロの内容をフィルタリングします。 このフィルタでは、正規表現を使用できます。
- File Name: ファイル名でフィルタリングします。**FILE_NAME** マクロに対応します。このフィルタでは、ワイルドカード(*,?) が使用できます。宛先ファイルフィルタでのみ使用できます。

ファイルメッセージに使用されるフィルターを変更するには、次の手順を実行します。

手順:

1. syslog-ng Agent for Windows アプリケーションの設定インターフェースを開きます。
2. ・ フィルターを、すべてのファイルメッセージにグローバルに適用するには、[syslog-ng Agent Settings]>[Local Settings または Client Group Policy 以下]>[Destinations]>[Global File Filters]を選択し、[Global File Filters]を右クリックします。
   ・ 特定の宛先にのみフィルターを適用するには、[syslog-ng Agent Settings]>[Local Settings または Client Group Policy 以下]>[Destinations]を選択し、送信先サーバーを選択して[File Filters]を選択します。[File Filters]を右クリックします。

注意：

グローバルとローカル（サーバー側）の両方のフィルタリングを使用する場合、最初にグローバルフィルタがファイルメッセージに適用され、次にローカルフィルタに適用されます。

3. [プロパティ]>[Enable]を選択します。

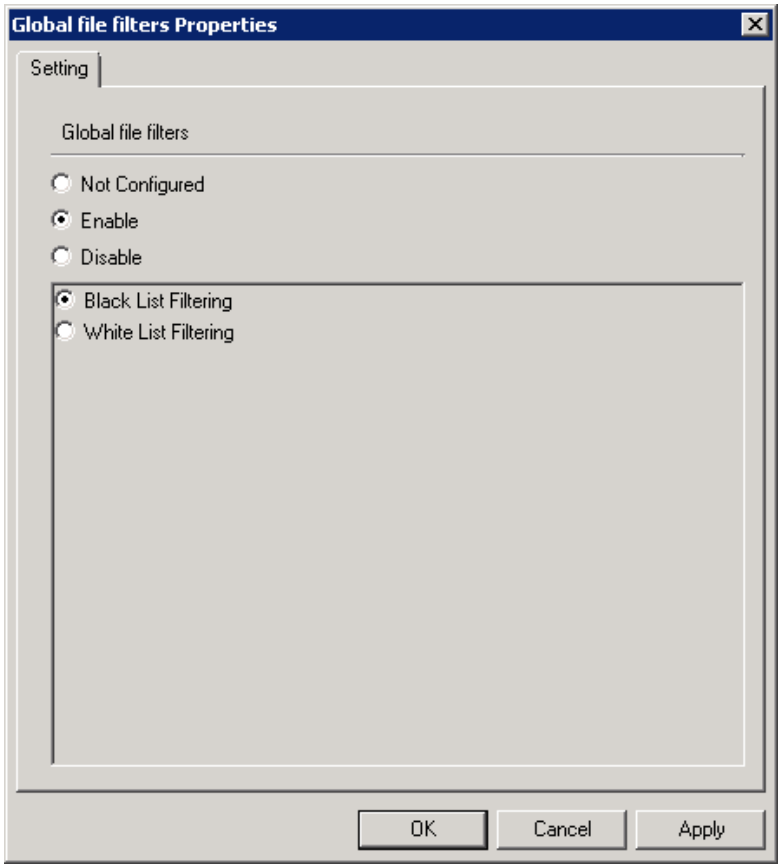

Figure 7.5. Global file filters

4. ホワイトリストフィルタリングを使用するには、[White List Filtering]を選択します。 デフォルトでは、syslog-ng エージェントはブラックリストフィルタリングを使用します。[OK]をクリックします。
5. [Global File Filters]または[File Filters]を選択し、右側のペイン[3]で、作成するフィルターのタイプをダブルクリックします。
6. 特定の文字列またはテキストを含むメッセージを無視するには、[Message Contents]をダブルクリックし、[Enable]を選択し、検索用語または正規表現を[Regular Expression]フィールド

[3] ウィンドウを複数の表示領域に分割して使用する表示方式における、分割された個々の表示領域のこと。

に入力して、[Add]をクリックします。

7. 最後に[適用]をクリックし、次に[OK]をクリックします。変更を有効にするには、syslog-ng Agent サービスを再起動します。

9 メッセージフォーマットのカスタマイズ

イベントログおよびファイルソースから受信したメッセージのフォーマットは、テンプレートを使用してカスタマイズできます。イベントログとファイルソースに別々のメッセージフォーマットを定義することができます。複数の送信先サーバーが設定されている場合は、サーバーごとに個別のテンプレートを定義できます。メッセージのフォーマットをカスタマイズするためのテンプレートを作成するときは、マクロ、すべての英数字、および次の特殊文字<>,():;-+/_を使用できます。

デフォルトでは、syslog-ng エージェントは次のテンプレートを使用してメッセージを転送します。

- BSD プロトコルの場合： **<${PRI}>${BSDDATE} ${HOST} ${MSGHDR}${MESSAGE}**
- イベントログから読み取ったメッセージの場合、**$MESSAGE** 部分はすべてのプロトコルについて**${EVENT_USERNAME}: ${EVENT_NAME} ${EVENT_SOURCE}: [${EVENT_TYPE}] ${EVENT_MSG} (EventID ${EVENT_ID})**です。
- ファイルから読み取ったメッセージの場合、**$MESSAGE** 部分はすべてのプロトコルについて **$FILE_NAME: $FILE_CURRENT_POSITION/$FILE_SIZE: $FILE_MESSAGE** です。

9.1 テンプレートを使用したメッセージのカスタマイズ

テンプレートを作成するには、次の手順を実行します。

警告：

これらのマクロは、syslog-ng Agent for Windows でのみ使用できます。syslog-ng サーバー上で、ログメッセージの Windows 固有の要素（例えば、イベントログ関連のマクロ）を認識するには、syslog-ng サーバーでパーサーを使用する必要があります。パーサーは、syslog-ng エージェントで設定されたメッセージフォーマットと一致するように設定する必要があります。syslog-ng Premium Edition サーバーでのパーサーの設定の詳細については、「syslog-ng Premium Edition 6 LTS 管理者ガイド」の「第 14 章 構造化メッセージの解析とセグメント化」を参照してください。

手順：

1. syslog-ng Agent for Windows アプリケーションの設定インターフェースを開きます。
2. [syslog-ng Agent Settings]>[Local Settings または Client Group Policy 以下]>[Destinations]を選択します。転送先のログサーバーを選択し、[Properties]をダブルクリックします。
3. [Messages]タブを選択します。イベントログソースから受信したメッセージのフォーマットを変更するには、使用するメッセージのフォーマットを[Event Message Format]>[Message Template]フィールドに入力します。

   ファイルソースから受信したメッセージのフォーマットを変更するには、使用するメッセージのフォーマットを[File Message Format]>[Message Template]フィールドに入力します。

   マクロの前に"$"文字を追加することを忘れないでください。使用可能なマクロのリストについては、「9.3 syslog-ng エージェントで使用可能なマクロ」を参照してください。

   例えば、**DATE HOSTNAME MESSAGE** フォーマットでメッセージを送信するには、**Date:$DATE Hostname:$HOST Logmessage:$MESSAGE** と入力します。

   $MESSAGE マクロには、ログメッセージのテキストだけでなく、イベントログ固有のテンプレートやファイル固有のテンプレートに設定されているイベントログコンテナの名前やファイル名など、メッセージソースから受信した追加の情報も含まれていることに注意してください。

   注意:

   テンプレートは個々の宛先サーバーに割り当てられるため、異なるサーバーに異なるテンプレートを使用することができます。ただし、サーバーとそのフェールオーバーサーバーで構成している場合は、常に同じメッセージを受信します。
4. [OK]をクリックします。
5. 変更を有効にするには、syslog-ng Agent サービスを再起動します。

9.2 syslog-ng エージェントで使用されるタイムスタンプのカスタマイズ

syslog-ng エージェントは、ISO または BSD タイムスタンプフォーマットのいずれかを使用して syslog メッセージを送信できます。BSD フォーマットよりもはるかに多くの情報を含んでいるので、ISO 形式を使用することをお勧めします。

syslog-ng エージェントでは、接頭辞(R_)のないマクロ(DATE など)は、メッセージがイベントコンテナに到着した時にメッセージの受信日(R_DATE など)を常に参照しています。接頭辞のないマクロは互換性の理由でのみ存在します。

警告:

syslog-ng Agent for Windows を実行しているローカルホストのイベントログにリモートホストがログインしている場合、イベントログメッセージに送信者ホストのタイムゾーン情報が含まれないため、両方のホストが同じタイムゾーンになければなりません。 そうしないと、リモートホストから受信したメッセージの日付が正しくなりません。

9.3 syslog-ng エージェントで使用可能なマクロ

以下のセクションでは、使用可能なマクロの一覧を示します。

警告:

これらのマクロは、syslog-ng Agent for Windows でのみ使用できます。syslog-ng サーバー上で、ログメッセージの Windows 固有の要素(例えば、イベントログ関連のマクロ)を認識するには、syslog-ng サーバーでパーサーを使用する必要があります。パーサーは、syslog-ng エージェントで設定されたメッセージフォーマットと一致するように設定する必要があります。syslog-ng Premium Edition サーバーでのパーサーの設定の詳細については、「syslog-ng Premium Edition 6 LTS 管理者ガイド」の「第 14 章 構造化メッセージの解析とセグメント化」を参照してください。

- 9.3.1 プロトコルヘッダーに関連するマクロ
- 9.3.2 時刻関連に関連するマクロ
- 9.3.3 イベントログソースに関連するマクロ
- 9.3.4 ファイルソースに関連するマクロ

注意:

Syslog プロトコルテンプレート(IETF-Syslog プロトコルを使用してメッセージが送信されることを意味する)を使用する場合、ログメッセージのメッセージ部分のみをカスタマイズでき、ヘッダーの構造およびその他の情報はプロトコルによって固定されます。

9.3.1 プロトコルヘッダーに関連するマクロ

- APP_NAME

説明: APPLICATION_NAME マクロのエイリアスです。

- APPLICATION_NAME

説明:
・ イベントコンテナの場合: メッセージの元になったアプリケーションの名前。
・ ファイルの作成者の名前(デフォルト値:syslog-ng-agent)。

- HOST

説明: メッセージを送信しているホストの名前。 ホスト名は自動的に小文字に変換されます。

- MESSAGE

説明: メッセージのテキスト、およびソースに設定されているファイルまたはイベント固有のマクロを含む、メッセージの内容。

- MSG

説明: MESSAGE マクロのエイリアスです。

- MSGHDR

説明: **PROGRAM [PID]**:フォーマットでログメッセージを送信したプログラムの名前とPID。末尾の空白を含みます。メッセージの PROGRAM フィールドと PID フィールドの両方が空の場合、マクロは空の値を返すことに注意してください。

- PRI

説明: メッセージの優先度ヘッダー。機能とメッセージのレベルを格納します。

- PROCESS_ID

説明: メッセージが送信されたアプリケーションの PID。

9.3.2 時刻関連に関連するマクロ

- BSDDATE, R_BSDDATE, S_BSDDATE

説明: BSD タイムスタンプフォーマットのメッセージの日付(月/日/時/分/秒、それぞれ 2 桁で表されます)。 これは、年情報のないオリジナルの syslog タイムスタンプです(例:Jun 13 15:58:00)。 可能であれば、タイムスタンプに ISODATE を使用することをお勧めします。

- DATE, R_DATE, S_DATE

説明: BSD-syslog フォーマットのタイムスタンプフォーマット(月/日/時/分/秒、それぞれ 2 桁で表示)を使用するメッセージの日付。 これは、年情報のないオリジナルの syslog タイムスタンプです(例:Jun 13 15:58:00)。

- DAY, R_DAY, S_DAY

説明: メッセージが送信された日。

- FULLDATE, R_FULLDATE, S_FULLDATE

説明: **${DATE}**と同じ書式を使用しますが、年を含むメッセージの日付の非標準形式です(例:2006 Jun 13 15:58:00)。

- HOUR, R_HOUR, S_HOUR

説明: メッセージが送信された時間。

- ISODATE, R_ISODATE, S_ISODATE

説明: ISO 8601 互換の標準タイムスタンプ形式(yyyy-mm-ddThh:mm:ss +-ZONE)のメッセージの日付(例:2006-06-13T15:58:00.123 +01:00)。 可能であれば、タイムスタンプに ISODATE を使用することをお勧めします。 syslog-ng エージェントは、タイムスタンプ内に秒数分(例えば、ミリ秒)を生成できないことに注意してください。

- MIN, R_MIN, S_MIN

説明: メッセージが送信された分。

- MONTH、R_MONTH、S_MONTH

説明: メッセージが送信された 10 進数の月。10 より小さい場合は 0 の接頭辞を付加します。

- MONTHNAME, R_MONTHNAME, S_MONTHNAME

説明: メッセージが送信された月の英語名。省略名は 3 文字(例:Jan, Feb など)です。

- SEC, R_SEC, S_SEC

説明: 送信されたメッセージの秒。

- TZ, R_TZ, S_TZ

説明: **${TZOFFSET}**マクロのエイリアス。

- TZOFFSET, R_TZOFFSET, S_TZOFFSET

説明: GMT からの時間オフセットとしてのタイムゾーン(例:-07:00)。syslog-ng 1.6.x ではこれは-0700 でしたが、**${ISODATE}**はコロンを必要とするため**${TZOFFSET}**に追加されました。

- UNIXTIME, R_UNIXTIME, S_UNIXTIME

説明: 標準の UNIX タイムスタンプ。1970-01-01T00:00:00 以降の秒数で表されます。

- YEAR, R_YEAR, S_YEAR

説明: メッセージが送信された年。

- WEEK、R_WEEK、S_WEEK

説明: 年の最初の 9 週間はゼロの接頭辞が付けられた年の週番号。(今年の最初の月曜日が最初の週です)。

- WEEKDAY, R_WEEKDAY, S_WEEKDAY

説明: メッセージが送信された曜日の 3 文字の名前です(例:Thu)。

9.3.3 イベントログソースに関連するマクロ

- EVENT_CATEGORY

説明: イベントのカテゴリー。

- EVENT_DATA

説明: 空のマクロで、データが含まれていません。

- EVENT_CONTAINER_COUNTER

説明: syslog-ng Agent for Windows が開始されてからコンテナごとに受信されたメッセージの数。

- EVENT_FACILITY

説明: メッセージを送信したファシリティー。

- EVENT_GLOBAL_COUNTER

説明: 受信ホストで受信時に生成されたメッセージの一意の ID。 同じホストまたは異なるホスト上の異なるファイルに配布される可能性があるメッセージ間の関係の定義を容易にします。

- EVENT_HOST

説明: ログメッセージを送信したホストの名前。

- EVENT_ID

説明: イベントの識別番号。

- EVENT_LEVEL

説明: 数値として表されるメッセージの重要度:6 - 成功、5 - 情報、4 - 警告、または 3 - エラー)。

- EVENT_MESSAGE

説明: メッセージの内容。

- EVENT_MESSAGE_XML

説明: メッセージ全体を XML 形式で格納します。 Windows Vista、Server 2008、およびそれ以降のプラットフォームでのみ使用できます。

- EVENT_MSG

説明: メッセージの内容。 これは EVENT_MESSAGE のエイリアスです。

- EVENT_MSG_XML

説明:メ ッセージ全体を XML 形式で格納します。 これは EVENT_MESSAGE_XML のエイリアスです。 Windows Vista、Server 2008、およびそれ以降のプラットフォームでのみ使用できます。

- EVENT_NAME

説明: Windows イベントログコンテナの名前(例えば、アプリケーションまたはセキュリティ)。

- EVENT_PROVIDER

説明: ログメッセージを生成したサービスの名前。

- EVENT_REC_NUM

説明: イベントログ内のイベントのレコード番号。

- EVENT_SID

説明: イベントのセキュリティ識別番号。

- EVENT_SID_TYPE

説明: セキュリティ ID 番号が名前に解決されました。次のいずれか:**User, Group, Domain, Alias WellKnownGroup, DeletedAccount, Invalid, Unknown, Computer**。

- EVENT_SOURCE

説明: メッセージを作成したアプリケーション。

- EVENT_TASK

説明: イベントのタスクカテゴリ。 Windows Vista、Server 2008、およびそれ以降のプラットフォームでのみ使用できます。

- EVENT_TYPE

説明: テキスト形式のメッセージの重要度。

- EVENT_USERNAME

説明: メッセージを作成したアプリケーションを実行しているユーザー。

9.3.4 ファイルソースに関連するマクロ

- FILE_CURRENT_POSITION

説明: ファイルの先頭からのメッセージの位置(バイト単位)。

- FILE_FACILITY

説明: メッセージを送信したファシリティー。

- FILE_LEVEL

説明: 数値として表されるメッセージの重要度:6 - 成功、5 - 情報、4 - 警告、または 3 - エラー)。

- FILE_MESSAGE

説明: メッセージの内容。

- FILE_MSG

説明: メッセージの内容。 これは **FILE_MESSAGE** マクロのエイリアスです。

- FILE_NAME

説明: syslog-ng PE がメッセージを受信したログファイルの名前(パスを含む)。

- FILE_SIZE

説明: ファイルの現在のサイズ(バイト単位)。

10 syslog-ng エージェントサービスの制御

syslog-ng エージェントは、インストール時に、ホストの起動時に自動的に起動される syslog-ng エージェントサービスを登録します。syslog-ng エージェントの自動起動を無効にするには、[スタートメニュー]>[コントロールパネル]>[管理ツール]>[サービス]を使用します。このサービスは、**NT AUTHORITY¥SYSTEM** ユーザーの権限で実行されています。

手動でサービスを開始または停止するには、[スタートメニュー]>[コントロールパネル]>[管理ツール]>[サービス]を立ち上げるか、または、[スタートメニュー]>[プログラム]>[syslog-ng Agent for Windows]に移動します。後者の場合、ユーザーアクセス制御(UAC)が有効になっている場合、syslog-ng エージェントを起動または停止するには、"管理者として実行"が必要です。

syslog-ng エージェントサービスが開始または停止すると、syslog メッセージがセントラルログサーバーに送信され、イベントログメッセージがホストのアプリケーションイベントログコンテナに送信されます。

警告:

syslog-ng エージェントの実行中にホストのタイムゾーン設定を変更した場合は、syslog-ng エージェントを再起動する必要があります。そうしないと、更新されたタイムゾーン情報が受信されず、イベントの日付が間違ってきます。

注意：

“サービスとしてログオン”権限を持つ管理者アカウントでサービスを実行することは可能です（ユーザー権限を設定するには、[スタート]>[コントロールパネル]>[管理ツール]>[ローカルセキュリティポリシー]>[ローカルポリシー]>[ユーザー権限の割り当て]に移動します）。これらの設定はサポートされていません。使用するには自己責任で行ってください。また、次のアップグレード手順では、これらの設定は出荷時のデフォルト設定で上書きされます。

10.1 コマンドラインオプション

syslog-ng Agent for Windows アプリケーションには、以下のコマンドラインオプションがあります。

注意：

コマンドラインオプションは大文字と小文字を区別しません。オプションは、″ - ″または ″/″のいずれかで指定されたシングル文字で構成されます。

注意：

Windows Vista 以上では、コマンドラインオプションは管理者権限でのみ動作します。

- /c

  指定された XML 設定ファイルを使用して syslog-ng エージェントを起動します。

- /d

  syslog-ng エージェントをデバッグモードで起動します。

- /h

  コマンドラインオプションに関するヘルプメッセージを表示します。

- /i

  サービスリストに syslog-ng エージェントサービスをインストールします。

- /r

サービスリストから syslog-ng Agent サービスを削除します。

- /v

バージョン情報を表示します。

- /x

XML 構成ファイルをインポートせずに検証します。

これらのオプションを使用するには、コマンドプロンプト（[スタートメニュー]>[ファイル名を指定して実行]で **cmd** を入力）で、syslog-ng エージェントがインストールされているディレクトリ（例：**cd C:¥Windows¥Program Files¥BalaBit¥syslog-ng Agent¥**）に移動して **syslog-ng-agent.exe** ファイルに必要なオプションを指定して実行します。

Example 9.1. Using command line options

syslog-ng エージェントをデバッグモードで起動するには：

```
syslog-ng-agent.exe /d
```

syslog-ng エージェントを XML 設定ファイルで起動するには：

```
syslog-ng-agent.exe /c C:¥ConfigFiles¥syslog-ng-agent-conf.xml
```

XML 設定ファイルを使用して syslog-ng エージェントをサービスとして登録するには：

```
syslog-ng-agent.exe /i C:¥ConfigFiles¥syslog-ng-agent-conf.xml
```

11 Windows 用 syslog-ng エージェントのトラブルシューティング

syslog-ng Agent for Windows アプリケーションで問題が発生した場合は、次の点が役立ちます。

注意

以下は、syslog-ng エージェントに固有の問題のみに解説しています。サーバーとクライアント間の通信は正常に動作しているものとします（つまり、サーバーはメッセージを受信するように適切に構成されており、ネットワーク上で受信可能で、名前解決はクライアント上で正しく構成されています）。

- 設定の変更が反映されません。

設定の変更は、syslog-ng サービスを再起動した後、または、システムをリブートした後にのみ有効になります。また、ホストのタイムゾーン設定を変更した後、または、エージェントとサーバー間の通信を認証するために使用する証明書をインポートした後も、システムの再起動が必要です。前回の再起動以降にエージェントの構成が変更された場合、syslog-ng エージェントは、新しい設定の hmac-sha-1 ハッシュを含む変更メッセージを送信します。

また、クライアントがドメインコントローラーから管理されている場合は、構成の変更はすぐにはクライアントホストにダウンロードされません、次回のグループポリシーの更新時にのみ有効になります。もっと早くクライアントホストの設定を更新するには、クライアントホストでコマンドプロンプトを開き、**gpupdate /force** コマンドを実行します。ドメインコントローラーから設定をダウンロードした後、設定が変更されていた場合、syslog-ng エージェントサービスが自動的に再起動されます。

注意:

syslog-ng エージェントに影響を与える特定のドメイン設定は、マシンが再起動されたときにのみダウンロードされます。例えば、あるグループポリシーから別のグループポリシーにコンピューターを移動するには、再起動する必要があります。

- syslog-ng エージェントが、サーバーにメッセージを送信しません。

アプリケーションイベントログに、syslog-ng エージェントのメッセージが出力されているか確認します。接続エラーや証明書の問題が発生した場合は、syslog-ng エージェントはイベントログにエラーメッセージを出力します。サーバーの宛先アドレスが正しく設定されていることを確認してください。また、SSL 暗号化を使用している場合は、サーバーの認証局の証明書とクライアントの証明書が適切にインポートされていることを確認します。エラーメッセージがない場合は、ログサーバーのログを確認してください。syslog-ng エージェントは、送信する他のメッセージがない場合でも、10 分ごとに MARK メッセージ(MARK メッセージを無効にしていない限り)を送信します。

- syslog-ng エージェントが MARK メッセージしかサーバーに送信していません。

イベントログとファイルソースが設定されていて、グローバルに無効にされていないことを確認します。これらの設定は正しいが、サーバーにまだメッセージを送信しない場合は、すべてのフィルターを一時的に無効にして、すべてのメッセージを無視するように設定されていないことを確認してください。フィルターを使用する時は、大文字と小文字の区別の設定も確認することをお勧めします。

- メッセージに使用されているホスト名が変更されます。

ホストがドメインに参加している時も、そうでない場合もあります。ホスト名にはこれが反映されていることがあります。このような状況を回避するには、[syslog-ng Agent Settings]>[Local Settings または Client Group Policy 以下]を選択し、[Global Settings]ダブルクリックします。[Enable]選択し、[Hostname]に移動して[Use FQDN]を選択します。これにより、syslog-ng エージェントは DNS から自身のホスト名を解決し、syslog メッセージに解決された FQDN を使用します。詳細については、「6.5 ホスト名のフォーマット設定」を参照してください。

- コマンドラインパラメーターが Windows Vista および 2008 Server で無視されます。

コマンドパラメーターはユーザーアカウント制御（UAC）が有効な場合、管理者のみが使用できます。コマンドラインパラメーターを使用して syslog-ng エージェントを実行するには、[スタートメニュー]>[プログラム]>[アクセサリ]を選択し、[コマンドプロンプト]を右クリックしてコンテキストメニューで[管理者として実行]を選択します。

syslog-ng Agent for Windows の問題についてカスタマーポータルに問い合わせる場合は、コマンドラインから **syslog-ng-agent -V** コマンドを実行し、サポートリクエスト時に、表示されるすべてのバージョンとプラットフォーム情報を含めてください。

- CPU 負荷が高いです。

「11.1 メッセージ送信と CPU 負荷」を参照してください。

- イベントログコンテナからのメッセージが損失します。

イベントログコンテナは特別なファイルです。エージェントはこのファイルを読み取り、メッセージをフォーマットしてリモートログサーバーに送信します。イベントログコンテナは、特定のサイズにのみ設定できます。コンテナがそのサイズに達すると、Windows はファイルの先頭に次のメッセージを書き込みます。結果として、エージェントが長時間動作しない（または宛先サーバーが使用できない）場合、イベントログコンテナがいっぱいになり、メッセージを喪失する可能性があります。

11.1 メッセージ送信と CPU 負荷

syslog-ng エージェントアプリケーションは、Windows スケジューラからリソースが提供されると、サーバーにメッセージを送信することができます。ログソースに未送信のログメッセージが多く、ホスト上にその他の重要なアクティビティがない場合、syslog-ng はサーバーにメッセージを送信し始め、CPU 負荷を 100%に増加させる可能性があります。すべてのメッセージが送信された後、または別のアプリケーションがリソースを必要とする場合、CPU 負荷は通常の状態に戻ります。

Tips:

CPU の初期負荷が大きくなるのを避けるため、メッセージの送信速度を一時的に制限してください。古いメッセージが送信された後で、制限を削除できます。 詳細については、「5.2 メッセージレートを制限する」を参照してください。

複数のソースからメッセージを中継する場合、syslog-ng エージェントは、各ソースから一度に 1 つのメッセージを送信します。これにより、大きなログトラフィックを持つシングルソースがある場合でも他のログソースの送信をブロックすることはなくなります。

11.2 syslog-ng エージェントのデバッグ

デバッグオプションを有効にするには、syslog-ng エージェントのインストールディレクトリに **debug.ini** ファイルを作成します。

Example 10.1. Content of the debug.ini file

debug.ini は、次の内容で構成されます。

```
[AgentDbgLog]
enabled=on/off
path=<debug_file_folder_path>

[GpoDbgLog]
enabled=on/off
path=<debug_file_folder_path>

[WriteMiniDump]
enabled=on/off
```

注意:

debug.ini ファイルは配布できません。 ローカルマシン上でのみ使用できます。

11.2.1 コアダンプとメモリダンプの作成

サポートが、特定の問題を調査するために syslog-ng エージェントのコアダンプを送るよう求めることがあります。有効にすると、予期しないシャットダウンが発生した場合、syslog-ng Agent for Windows アプリケーションによってコアダンプが自動的に作成されます。

手順:

1. コアダンプを有効にするには、**debug.ini** ファイルに次の行を入力します。

```
[WriteMiniDump]
enabled=on
```

コアダンプは syslog-ng Agent のインストールフォルダ以下にファイル名 **syslog-ng-agent.PID.dmp** に書き込まれます。コアファイルのサイズは、通常約 40～50MB です。

注意：

デフォルトでは、このオプションは有効です。ディスクスペースの制限のため、ハードディスクが一杯になることを防ぐ為に無効にすることができます。

2. 変更を適用するには、**debug.ini** ファイルの[WriteMiniDump]部分を変更した後で syslog-ng エージェントを再起動します。

11.2.2 syslog-ng エージェントでのデバッグログの有効化

syslog-ng エージェントで問題が発生した場合、サポートは、アプリケーションのデバッグログから問題のトラブルシューティングを支援することがあります。デバッグログを取るには、次の手順を実行します。

注意：

デバッグログは、syslog-ng サービスが開始できなかった理由を検出するのに適していません。エージェントサービスが起動できなかったことをチェックする唯一の方法は、手動でデバッグモードを実行することです（**syslog-ng-agent.exe /D** コマンドを使用してください）。**debug.ini** ファイルの[AgentDbgLog]部分が存在する場合、**enabled=off** に設定されていることを確認してください。

手順：

1. デバッグログを記録するには、**debug.ini** ファイルに次の行を入力します。

```
[AgentDbgLog]
enabled=on
```

デバッグメッセージは、他にパスが指定されていない場合、syslog-ng エージェントのインストールフォルダ以下にデフォルトでファイル名 **syslog_ng_agent_dbg.log** に書き込まれます。デバッグログファイルの保存先フォルダを変更するには、path=<debug_file_folder_path>行にパスを入力します。

警告:

オプションのパスを使用する場合は、syslog-ng エージェントに書き込み権限があることを確認してください。また、パスが存在することを確認してください。 そうしないと、syslog-ng エージェントはファイルに書き込みできません。

2. 変更を適用するには、**debug.ini** ファイルの[AgentDbgLog]部分を変更した後で syslog-ng エージェントを再起動します。

   再起動後、タイムスタンプとログファイルのパスを使用して、デバッグログモードの開始に関するログメッセージが自動的に生成されます。

   Example 10.2. Debug logging enabled log message

   ```
   Apr 16 13:14:02 zts-win015 syslog-ng[252]: syslog-ng Agent debug mode is enabled; output file='.¥syslog_ng_agent_dbg.log'
   ```

3. エラーを再現します。 これはデバッグログに含まれます。
4. 問題を解決したら、デバッグログを無効にしてください。そうしないと、ログファイルが大きくなり、使用可能なハードディスク領域が消費される可能性があります。 ログファイルには、syslog-ng エージェントによって受信され処理されたログメッセージも含まれます。

11.2.3 ドメイン設定の問題のトラブルシューティング

ドメイン設定がドメインホストにダウンロードされていない場合、syslog-ng エージェント(バージョン 3.0.6 以降)は、ドメイン設定がクライアント上で更新されない理由をデバッグするためのログファイルを作成できます。次の手順を実行します。

手順:

1. ドメイン更新エラーのログを有効にするには、**debug.ini** ファイルに次の行を入力します。

   ```
   [GpoDbgLog]
   enabled=on
   ```

   デバッグメッセージは、他にパスが指定されていない場合、syslog-ng エージェントのインストールフォルダ以下にデフォルトでファイル名 **syslog_ng_agent_gpo_dbg.log** に書き込まれます。デバッグログファイルの保存先フォルダを変更するには、path=<debug_file_folder_path>行にパスを入力します。

警告:

オプションのパスを使用する場合は、syslog-ng エージェントに書き込み権限があることを確認してください。また、パスが存在することを確認してください。 そうしないと、syslog-ng エージェントはファイルに書き込みできません。

2. [スタートメニュー]>[ファイル名を指定して実行]で **gpupdate** を入力して、エラーを再現します。
3. 問題を解決した後はドメインの更新エラーを記録しないようにしてください。そうしないと、クライアントのドメイン設定が更新されるたびにログファイルが増加します。

11.3 Windows Vista 以降でイベントログメッセージを読むのが遅い

イベントログコンテナからメッセージを読み取るには、syslog-ng Agent for Windows アプリケーションはネイティブ Windows API ツールを使用します。Windows Vista 以降のプラットフォームでは、XML ベースのイベントログフォーマットが使用されています。イベントログコンテナから XML メッセージを読み取って syslog-ng エージェントに渡す API(EVTX)は、本質的に遅く、syslog-ng エージェントのパフォーマンスを著しく制限します。

syslog-ng エージェントが Microsoft Windows XP および 2003 Server プラットフォームで使用する API ツールは、新しいプラットフォームでも使用でき、イベントログコンテナからの読み込み速度を最大 500%まで向上させることができます。ただし、この古い API(EVT)を使用すると、XML ベースのイベントログコンテナで使用するときに制限があります。

11.3.1 Windows Vista 以降で EVT API を使用する際の制限事項

EVT API を使用して XML ベースのイベントログコンテナからメッセージを読み取るときは、次の制限に注意してください。

- EVT API は、レジストリ内の **HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Eventlog¥**キーにリストされているコンテナのみをサポートします。3 つのデフォルトコンテナ(セキュリティ、アプリケーション、システム)がデフォルトでここにリストされています。
- 派生コンテナはサポートされていません(例:**microsoft-windows-bits-client/analytic**)。
- 次のマクロは機能しません。つまり、値は空になります。**${EVENT_CATEGORY}**, **${EVENT_MESSAGE_XML}**, **${EVENT_MSG_XML}** および **${EVENT_TASK}**。

- マイクロソフトが提供する EVT API が XML ベースの値をどのように読み取るかは、完全ではありません。 したがって、これらのマクロを使用するフィルタが正しく動作しない可能性があります。 次のリストに、既知の制限とエラーを示します。

  - ${EVENT_LEVEL}: このマクロの値が正しくない可能性があります。これは常に期待どおりの数値ですが、必ずしも正しい値ではありません。

  - ${EVENT_SOURCE}: このマクロの値の形式が異なる可能性があります。 例えば、**Microsoft Windows security auditing** ではなく **Microsoft-Windows-Security-Auditing** などです。

  - ${EVENT_TYPE}: 次のシナリオでは、このマクロの値が正しくないことが判明しています。

    - セキュリティ監査ログの場合、**${EVENT_LEVEL}**が 4 の時、**${EVENT_TYPE}**マクロの値は“情報”ではなく“監査成功”になります。これは、“監査ログのクリア”イベントが生成されたときに発生することが知られています。

    - 非セキュリティ監査ログの場合、**${EVENT_LEVEL}**が 0 の時、**${EVENT_TYPE}**マクロの値は“情報”ではなく“未定義”になります。

  - ${EVENT_USERNAME}: EVT API は、常にこのマクロに UserName フィールドの値を追加します。イベントの UserName フィールドが空の場合、EVTX API は代わりに TargetUserName または SubjectUserName を使用しましたが、これは EVT API では不可能です。例えば、セキュリティコンテナからのイベントのユーザー名フィールドは、しばしば N/A になります。

  - ${PRI}: このマクロの値は**${EVENT_LEVEL}**に基づいているため、間違っている可能性があります。

11.3.2 Windows Vista 以降で EVT API を有効にする

Windows Vista 以降で EVA API を処理するには、次の手順を実行します。

警告:

- データ損失の危険！ API を変更すると、最後に読み取られたメッセージの位置が失われ、syslog-ng エージェントアプリケーションがメッセージを複製または失う可能性があります。

- EVT API は EVTX API と完全に互換性がありません。設定を変更する前に、「11.3.1 Windows Vista 以降で EVT API を使用する際の制限事項」を必ずお読みください。

- API を変更すると、ホスト上のすべてのイベントログコンテナに影響します。 選択したコンテナに対してのみ EVT API を使用することはできません。

手順:

1. Windows Vista および Server 2008 では、修正プログラム(KB 961099)をインストールします。この修正プログラムは Windows Vista および Server 2008 の Service Pack 2 に含まれています.Windows 7 はこの修正プログラムの影響を受けません。
2. syslog-ng Agent for Windows アプリケーションの設定インターフェースを開きます。
3. [syslog-ng Agent Settings]>[Local Settings または Client Group Policy 以下]>[Eventlog Sources]を選択し、[Eventlog Sources]をダブルクリックします。
4. [Enable]を選択します。
5. [Event API]>[Event Logging (EVT)]を選択します。

注意:

デフォルトでは、syslog-ng Agent for Windows アプリケーションは、すべてのプラットフォームでネイティブ API を使用します。Windows XP および Server 2003 では EVT、Windows Vista 以降では EVTX。

6. [適用]をクリックし、次に[OK]をクリックします。変更を有効にするには、syslog-ng Agent サービスを再起動します。

期待される結果:

syslog-ng Agent for Windows アプリケーションは、EVT API を使用してイベントログコンテナからメッセージを読み取り、パフォーマンスを向上させます。

12 Windows での監査ポリシーの設定

このセクションでは、さまざまなバージョンの Microsoft Windows でログと監査のポリシーを設定する方法について説明します。syslog-ng エージェントは、実際にログに記録されたイベントについてのみログメッセージを転送できるため、重要なイベントはログに記録するように監査ポリシーを設定する必要があります。

Microsoft Windows オペレーティングシステムは、ログオンしているユーザーなどのシステム全体のイベントから、特定のユーザーが特定のファイルの読み込みを試みようとしているところまで、さまざまな種類のイベントを記録できます。それらのアクションの成功と失敗の両方の試みを記録することができます。監査ポリシーは、監査するイベントのタイプを指定します。このようなイベントが発生すると、コンピューターのログファイルにエントリが追加されます。

以下では、さまざまなバージョンの Microsoft Windows で監査ポリシーを設定する方法の概要を

説明します。詳細については、オペレーティングシステムのマニュアルを参照するか、Microsoft TechNet を参照してください。IIS サーバーや ISA Server などのさまざまなアプリケーションの監査とログの構成の詳細については、製品のマニュアルを参照してください。

12.1 Windows XP でセキュリティログを有効にする

次の手順では、Windows XP Professional ホストでセキュリティログを有効にする方法について説明します。

手順:

1. 管理者としてログインします。
2. [スタートメニュー]>[ファイル名を指定して実行]をクリックして、**mmc /a** と入力します。
3. [ファイル]メニューの[スナップインの追加と削除]を選択し、[追加]をクリックします。
4. [スナップイン]の下の[グループポリシー]をクリックし、[追加]をクリックします。
5. [グループポリシーオブジェクトの選択]で、[ローカルコンピュータ]を選択し、[完了]をクリック、[閉じる]をクリックし、[OK]をクリックします。
6. [コンソールルート]で、[ローカルコンピュータポリシー]を選択し、[監査ポリシー]をクリックします。
7. 詳細ペインで、監査する属性またはイベントを右クリックします。
8. [プロパティ]で必要なオプションを設定します。
9. 監査したいイベントごとに手順 7～8 を繰り返します。

注意:

ワークステーション、メンバサーバー、およびドメインコントローラーのセキュリティログをリモートで有効にする方法の詳細については、「12.2 ドメインコントローラーのセキュリティログを有効にする」を参照してください。

12.2 ドメインコントローラーのセキュリティログを有効にする

次の手順では、Windows XP Professional ドメインコントローラーでセキュリティログを有効にする方法について説明します。

手順:

1. 管理者としてログインします。
2. [スタートメニュー]>[コントロールパネル]>[管理ツール]>[Active Directory ユーザーとコンピューター]をクリックします。

3. コンソールツリーから[ドメインコントローラー]をクリックします。
4. [アクション]をクリックし、次に[プロパティ]をクリックします。
5. [グループポリシー]タブで、変更するポリシーを選択し、[編集]をクリックします。
6. [グループポリシー]ウィンドウのコンソールツリーで、[監査ポリシー]をクリックします。
7. 詳細ペインで、監査する属性またはイベントを右クリックします。
8. [プロパティ]で必要なオプションを設定します。
9. 監査したいイベントごとに手順 7～8 を繰り返します。

12.3 Windows 2003 Server で監査を有効にする

次の手順では、Windows 2003 Server ホストで監査を設定する方法について説明します。

手順:

1. 管理者としてログインします。
2. [スタートメニュー]>[コントロールパネル]>[管理ツール]>[ドメインセキュリティポリシー]をクリックします。
3. コンソールツリーから[ローカルポリシー]>[監査ポリシー]をクリックします。
4. イベントをダブルクリックし、[これらのポリシー設定を定義する]オプションを選択します。
5. ログに記録するイベントのタイプを[成功]または[失敗]から選択します。
6. 監査するイベントごとに手順 4～5 を繰り返します。

日本語マニュアル発行日　2017 年 3 月 23 日

本書は 『The syslog-ng Agent for Windows 6 LTS Administrator Guide February 02, 2017』 をベースに編集しています。

ジュピターテクノロジー株式会社 技術グループ