

EventSentry v2.60 クイックスタート

平成 17 年 10 月 14 日

翻訳

ジュピターテクノロジー株式会社

目次

1 章	この資料について	3
2 章	概要	4
	マネージメントコンソール	4
	イベントログ & システムヘルスエージェント	4
	ハートビートエージェント	5
	Web レポート	5
3 章	EventSentry インストール	6
	Setup によるインストール	6
	マネージメントアプリケーション	7
	コンフィグレーション	8
	最低構成	8
	実行：最低構成の設定	9
	フィルターとターゲットの動作	10
	EventSentry を設定	10
	Remote Update (リモートアップデート)	11
	グループとリモートアップデート	12
	実行：リモートアップデートにコンピュータをインポートまたは追加	12
	実行：EventSentry を複数コンピュータにインストール	13
	実行：複数コンピュータの EventSentry コンフィグレーションをアップデート	13
	ハートビート監視	13
	イベントログ集中管理	15
4 章	参考情報	17

1 章 この資料について

イベントログ、システムおよびネットワーク管理のために EventSentry を選択していただきましてありがとうございます。この文書の目的はどのように EventSentry が動作するかを簡単に理解していただくことです。EventSentry を使用する前に 10 分間この文書を読んでください。

詳細については EventSentry マニュアルをお読みください。

クイックガイドでは以下の項目について説明します：

- ・ 概要
- ・ インストレーション
- ・ 設定
- ・ ローリングアウト（リモートアップデート）
- ・ ハートビートモニタ
- ・ イベントログ（データベース）集中化

2章 概要

EventSentry は Windows NT4, Windows 2000, Windows XP,または Windows 2003 サーバーのイベントログ、システムヘルス、アップタイムを監視するためのツールです。アプリケーションは 4つの部分で構成されます：

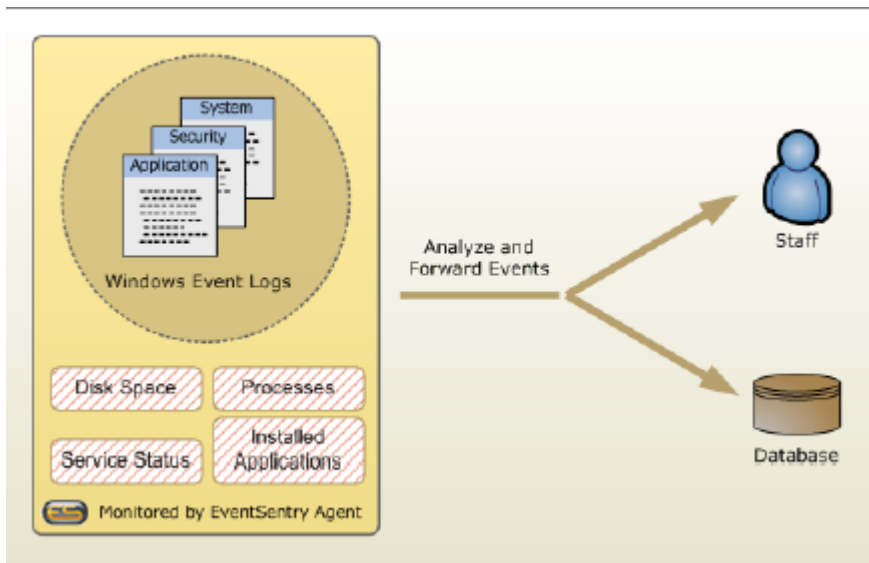
- Management Console (マネージメントコンソール)
- Event Log & System Health Agent (イベントログとシステムヘルスエージェント)
- Heartbeat Agent (ハートビートエージェント)
- Web Reports (Web レポート)

マネージメントコンソール

マネージメントコンソールは監視を行うものではなく、インストール、設定、ローカルまたはリモートコンピュータのエージェント設定にのみ使われます。マネージメントアプリケーションは購入したライセンス数までインストールすることができますが、通常はネットワークあたり 1 または 2 インストールで十分です。

イベントログ & システムヘルスエージェント

EventSentry エージェントは Windows サービスとして実行し、マネージメントコンソールから独立しています。マネージメントコンソールからエージェントを設定するとバックグラウンドでサービスとして実行します。設定にしたがって、イベントログとシステムヘルスの監視を行います。

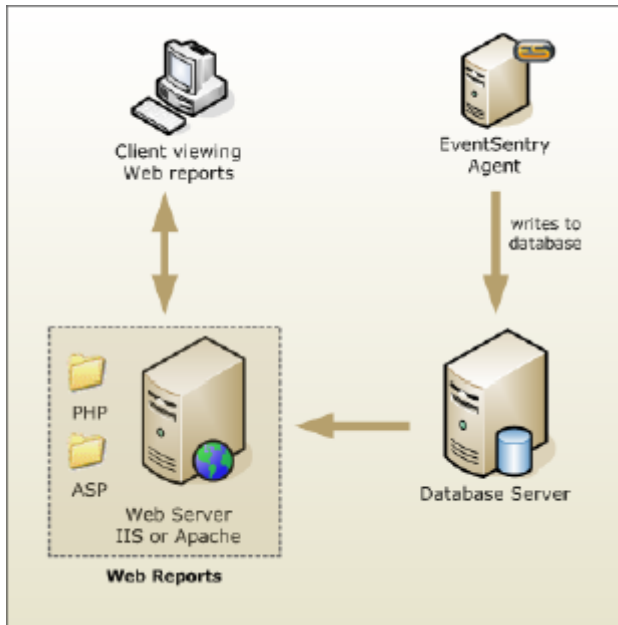


エージェントは全ての監視対象コンピュータにインストールします。

ハートビートエージェント

ハートビートエージェントはリモートホストを、Ping(ICPM)、TCP 接続でアップタイム監視をします。EventSentry イベントログエージェントの監視も行います。

Web レポート

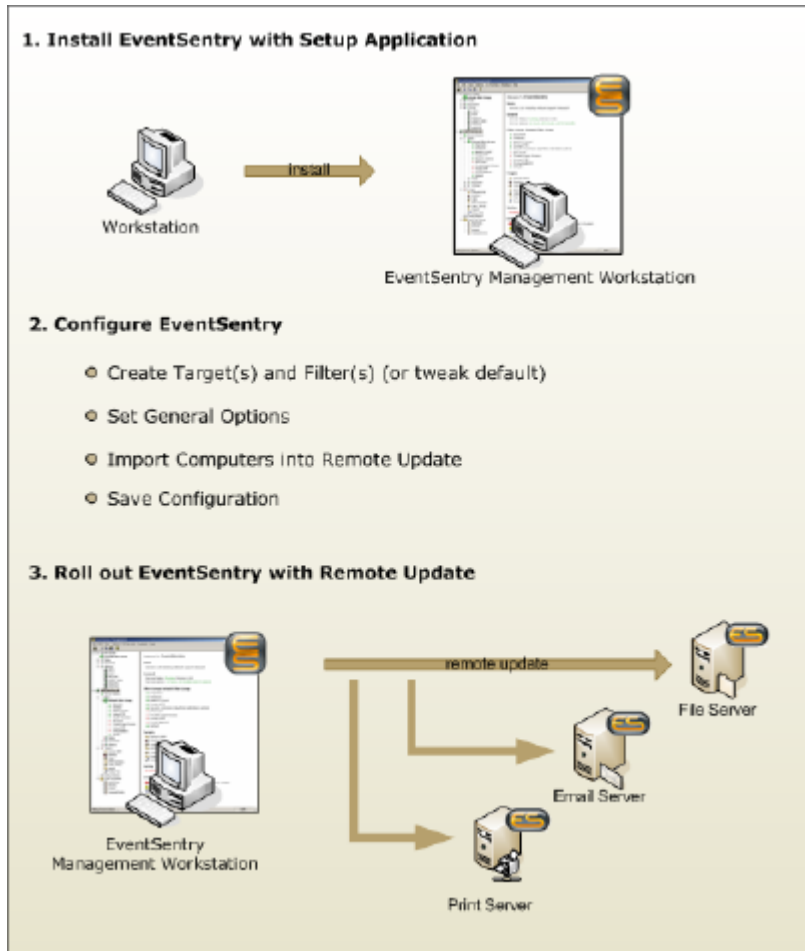


Web レポートは Web サーバー（IIS または Apache）と組み合わせる ASP または PHP ファイルで構成されます。Web レポートが提供する内容は：

- 全体のネットワークヘルス
- イベントログエントリー検索
- プロセス追跡エントリー検索
- イベント統計表示
- ディスクスペース傾向表示とレポート
- 環境監視グラフ
- ハートビートステータスと履歴表示

3章 EventSentry インストール

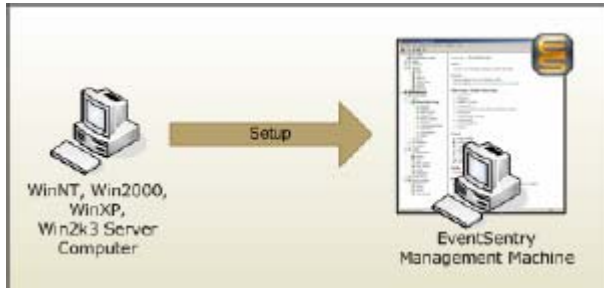
下図はネットワークに EventSentry をインストールする場合の典型的なステップです。



Setup によるインストール

setup プログラムを実行してインストールします。セットアッププログラムは初期設定を行いますのでインストールプロセスをよく注意してください。

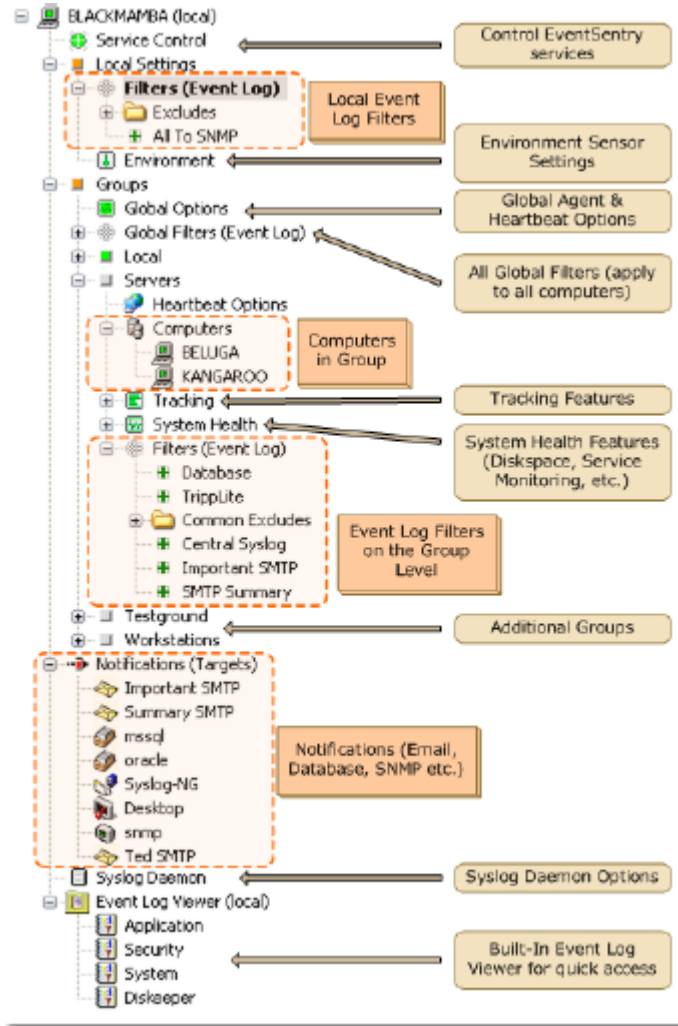
EventSentry をインストールする全てのホストで setup プログラムを実行する必要はありません。複数マシンに EventSentry エージェントをインストールする場合は remote update 機能を使ってください。各グループの Computers を右クリックすると remote update 機能にアクセスできます：



マネージメントアプリケーション

全ての機能はマネージメントアプリケーションから設定できます。デスクトップまたはプログラムフォルダーの EventSentry Management アイコン、または `eventsentry_gui.exe` のダブルクリックでマネージメントアプリケーションをスタートします。

左のコンテナをクリックするとほとんどの機能をアクセスできます。しかし多くの機能（フィルターやターゲットなど）では右クリックが必要です。たとえば新たなフィルターを追加するには Filters コンテナを右クリックします。



コンフィグレーション

最低構成

最も基本的なコンフィグレーションは以下の内容です：

- ・ターゲット x 1
- ・インクルードフィルター x 1
- ・エージェント x 1
- ・マネージメントマシン x 1

実行：最低構成の設定

セットアップ中に SMTP 設定を指定する場合、EventSentry インストーラーは自動的に以下のコンフィグレーションを生成します：

- ・グループ x 1 (例 Group)
- ・サンプルフィルター
- ・ターゲット x 1 (デフォルト SMTP)

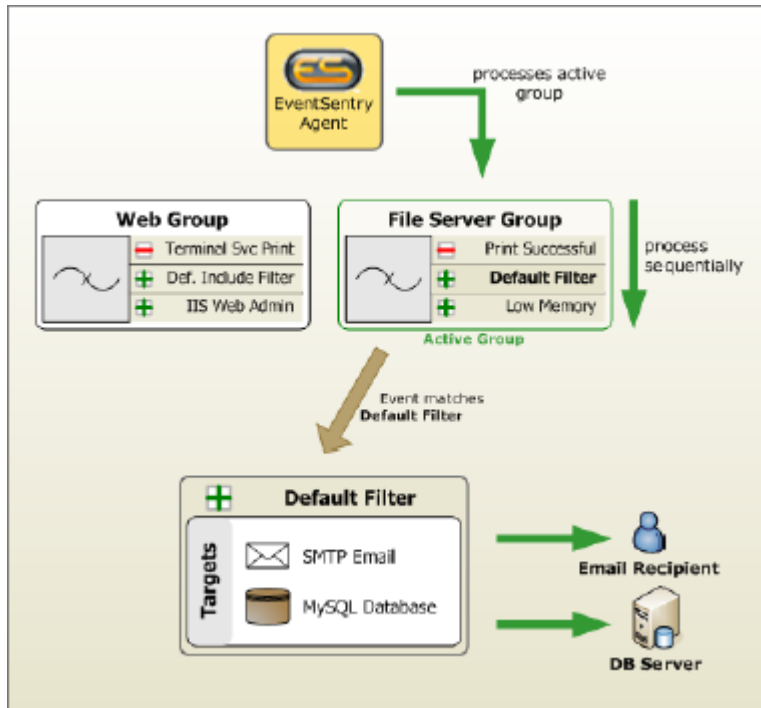
自分で最低構成を行う場合は以下の手順になります：

1. 左ペーンの Groups ノードの下に最低 1 つのグループがあることを確認します。無ければ Groups ノードを右クリックし Add Group を選択します。
2. 最低 1 つのグループがアクティブであることを確認します。アクティブグループは緑色です。レギュラーグループは違います。
3. Targets ノードの下に最低 1 つのターゲットが存在することを確認します。無ければ Targets ノードを右クリックし Add Target を選択します。
4. アクティブグループに最低 1 つのフィルターがあることを確認します。無ければ Active Group を右クリックし Add Filter を選択します。このフィルターは監視するイベントを指定し、1 つ以上の既存ターゲットを実行します。
5. オプション：Groups コンテナを右クリックし General Options でブートスキャンやワールドカードサポートの有効/無効を指定することができます。

EventSentry コンフィグレーションの完了後、ツールバーの save ボタンをクリック、または File メニューで Save を選択して保存します。コンフィグレーション変更は保存するまでは有効にならないことを記憶してください。

フィルターとターゲットの動作

フィルターは EventSentry のコアであり、どのイベントを処理するかを決定します。EventSentry が新たなイベントを受け取ると、設定したフィルターとターゲットにしたがって処理します。

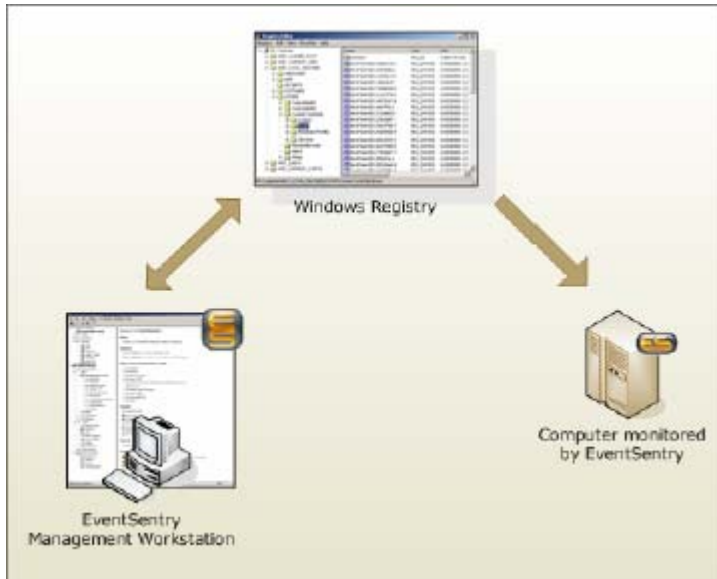


上のシナリオではエージェントはエージェントのアクティブグループの File Server Group にある3つのフィルターで処理されます。Default Filter ルールだけが現在のイベントに一致しますので Default Filter で指定されたターゲット (SMTP Email、MySQL DB) を実行します。

EventSentry を設定

save ボタンのクリック、または File メニューから Save オプションを選択するまでコンフィグレーションは保存されませんので、エージェントのコンフィグレーションを自由にコントロールできます。また EventSentry はリモートエージェントのコンフィグレーションを自動的に更新しません。そのかわり Remote Update 機能でコンフィグレーションやその変更をネットワークのエージェントに送信できます。

EventSentry コンフィギュレーションはレジストリーキー `HKEY_LOCAL_MACHINE\netikus.net\EventSentry`の下に保存されます。マネージメントアプリケーションはレジストリーからコンフィギュレーションを読み書きします。エージェントは主にレジストリーからコンフィギュレーションを読みます。



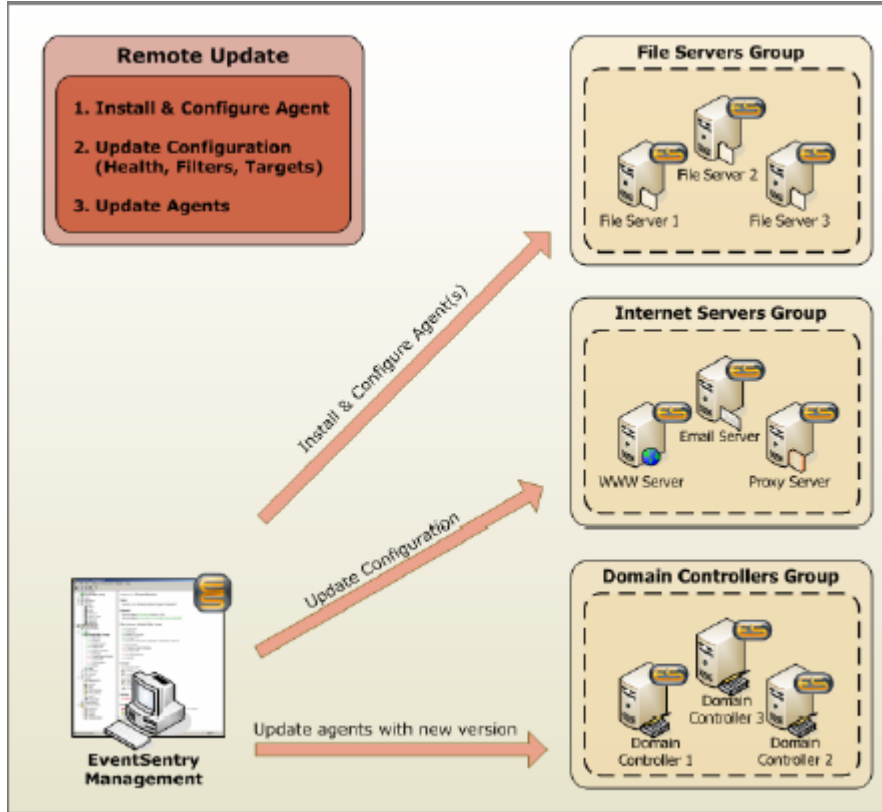
Remote Update (リモートアップデート)

ネットワーク上の EventSentry インストールを Remote Update で管理できます。この機能はリモートコンピュータにおける以下のタスクを実行します：

- EventSentry エージェントのインストール、アップデート、アンインストール
- EventSentry ステータスの問い合わせ
- リモートコンピュータへのコンフィギュレーションのプッシュ設定
- EventSentry サービスのコントロール (スタートとストップ)

リモートアップデートで最も普通に使われる EventSentry オプションを以下で説明します：

- 1 Install & Configuration : リモートコンピュータにエージェントをインストール、ローカルコンピュータのコンフィギュレーションをリモートコンピュータにコピーしスタート
- 2 Update Configuration : コンピュータにすでにエージェントがインストールされていたら、このオプションでリモートホストのコンフィギュレーションを最新に保ちます。Update Configuration でリモートコンピュータにゼネラルオプション、システムヘルス、フィルターおよびターゲットをプッシュできます。
- 3 Manage Agent(s) -> Update : マネージメントアプリケーションマシンに EventSentry 新バージョンをインストールしたら、EventSentry エージェントを実行するネットワークのコンピュータに新しいバージョンを配布できます。エージェントのロールアウトする前に、新しいオプションのコンフィギュレーションを行うことを確認してください。



グループとリモートアップデート

サーバーをグループ化し、各グループに異なるフィルタールールをアサインすることができます。グループフィルターはローカル×1、グローバル×2の3回処理されます。

実行：リモートアップデートにコンピュータをインポートまたは追加

リモートアップデートを使用する前にすべきことは：

- 1 1つ以上のグループがあることを確認
- 2 Remote Update グループにコンピュータをインポートまたはマニュアルで追加

Create Groups: Groups ノードを右クリックし Add Group を選択すると最大 254 グループまで追加できます。追加しているグループは Groups ノードにすぐ表示されます。

Manually Add Computers : Group ノードの下の Computers ノードを右クリックし、メニューで Add を選択します。コンピュータ名を入力し Enter を押します。追加する全てのコンピュータを繰り返します。

Import Computers : 1つずつコンピュータを追加する代わりに、ネットワークコンピュータ、アクティブディレクトリーまたは ASCII テキストファイルからインポートできます。Groups を右クリックし、import computers を選択してインポートウィザードをスタートします。ASCII ファイルでは 1 行に 1 台のコンピュータを記述します。

実行 : EventSentry を複数コンピュータにインストール

ターゲットとフィルターを設定し、リモートアップデートリストにコンピュータを追加した後は、リモートコンピュータに EventSentry エージェントをインストールできます。

- 1 Computers ノードを右クリックし、Install & Configure Agent を選択します。コンピュータの横にチェックボックスがあれば、どこかを右クリックしメニューから Go を選択します。
- 2 複数コンピュータにエージェントのみをインストールするのであれば、Computers コンテナを右クリックし Use Checkboxes を選択します。

ヒント : 特定のグループのコンピュータをアップデートするだけでなく、全てのグループのコンピュータをアップデートできます。ルート Group アイコンを右クリックし同じオプションを選択すると、グループ単位でできます (Remote Update サブメニュー)。

実行 : 複数コンピュータの EventSentry コンフィグレーションをアップデート

ネットワーク上の監視対象コンピュータにエージェントがインストールされていれば、1ステップでコンフィグレーションをアップデートできます。目的グループの Computers コンテナを右クリックし Update Configuration を選択します。次にアップデートしたいコンフィグレーションオプションを選択します。OK をクリック後アップデートされたコンフィグレーションがリモートコンピュータに送信されます。サービスのリスタートは不要です。

ハートビート監視

ハートビート監視はエージェントログとシステムヘルスのエージェントベース監視には理想的です。ハートビート監視機能で一箇所からリモートホストを監視できます。

ハートビート監視は下記内容を含みます :

1.Ping

ICMP パケットでリモートホストを監視します。送信パケット数やサイズ、何%の応答を期待するかをカスタマイズできます。

2.TCP

TCP ポートを使うアプリケーション (たとえば Web サーバー、Email サーバー) ではそのポートをチェックします。

3.EventSentry エージェント

EventSentry イベントログステータスを監視しシステム監視エージェントが正しく実行しているか確認します。

ハートビート監視はレポートとアラートを提供します：

1.Web レポート

ハートビートエージェントはホストのステータスを記録し、その変化をデータベースに保存します。Web レポートでリアルタイムに閲覧できます。

2.ローカル HTML ステータスページ

Web サーバーがない場合やデータベースが使用できない場合、ハートビートエージェントは HTML ページを生成しますのでマネージメントコンソールや Web ブラウザで閲覧できます。

3.アラート送信

リアルタイムレポートに加え、クリティカルなステータス変化を EventSentry エージェントがサポートする方法 (Email, Syslog, SNMP など) で通知できます。たとえばホストがオフラインになったとき、オンラインに戻ったときなど Email を受信できます。そのためにはハートビートエージェントに加え EventSentry エージェントもインストールします。

1. View Heartbeat Status through Web Reports

Host Name	IP Address	Host	IP	Port	State	Last Update	Heartbeat Interval	Event Log
Server1	192.168.1.10	OK	OK	22	OK	1/10/2008 10:10:10 AM	30	OK
Server2	192.168.1.11	OK	OK	22	OK	1/10/2008 10:10:10 AM	30	OK
Server3	192.168.1.12	OK	OK	22	OK	1/10/2008 10:10:10 AM	30	OK
Server4	192.168.1.13	OK	OK	22	OK	1/10/2008 10:10:10 AM	30	OK
Server5	192.168.1.14	OK	OK	22	OK	1/10/2008 10:10:10 AM	30	OK
Server6	192.168.1.15	OK	OK	22	OK	1/10/2008 10:10:10 AM	30	OK
Server7	192.168.1.16	OK	OK	22	OK	1/10/2008 10:10:10 AM	30	OK
Server8	192.168.1.17	OK	OK	22	OK	1/10/2008 10:10:10 AM	30	OK
Server9	192.168.1.18	OK	OK	22	OK	1/10/2008 10:10:10 AM	30	OK
Server10	192.168.1.19	OK	OK	22	OK	1/10/2008 10:10:10 AM	30	OK

2. Immediate Notification through EventSentry

EVENT # 4709
EVENT LOG Application
EVENT TYPE Error
SOURCE System
CATEGORY Application Monitoring
EVENT ID 1000
COMPLETION SUCCESS
TIME 1/10/2008 10:10:10 AM
TEXT Host WWW.ASCSOFT.COM (Internal Host) changed its Ping status from OK to ERROR. The reason for the status change was: "Socket connection error".

Servers monitored through PING and TCP connections

Network Devices monitored through PING

Workstations with monitored EventSentry agents

EventSentry Management Workstation with Heartbeat Monitor

イベントログ集中管理

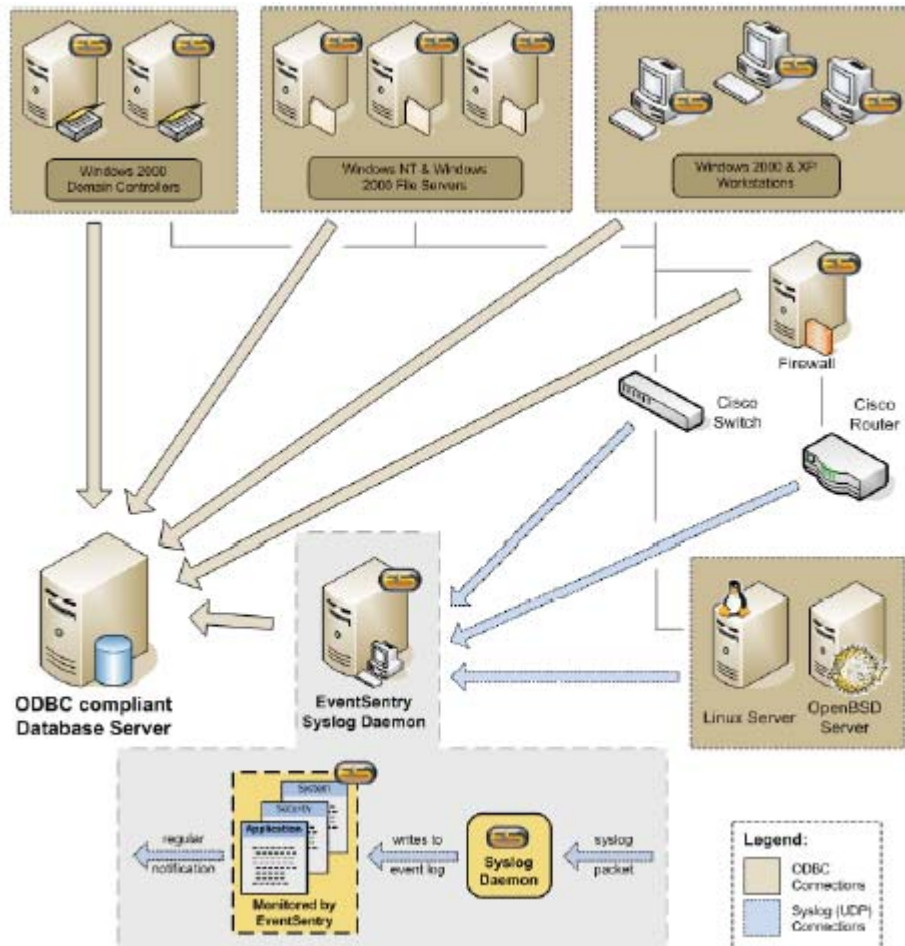
複数サーバー/ワークステーションのイベントをセントラル ODBC データベースに集中できます

- ・バックアップの作成
- ・ネットワーク間の複数イベントを検索しレポート
- ・政府規制、たとえば Sarbanes-Oxley, HIPPA などに適合

イベントログを集中するには：

- 1 EventSentry データベースを設定（テーブル、権限、インデックス）
- 2 Web サーバーに Web レポートを設定（IIS または Apache）
- 3 EventSentry で ODBC ターゲットを作成
- 4 ODBC ターゲットを実行するフィルターを作成

下図は集中化のイメージです：



システムメッセージのフロー

EventSentry の Syslog 機能を使えば、Windows 以外のデバイスのイベントをデータベースに保存できます。Unix ベースマシンや Cisco ネットワークデバイスは EventSentry の Syslog デーモン機能を実行しているマシンに UDP プロトコルでシスログメッセージを送信します。このホストは全てのシスログメッセージを集中 ODBC データベースに記録します。

- 1 シスログプロトコルをサポートするデバイスからシスログメッセージを送信
- 2 EventSentry Syslog デーモンが受信
- 3 シスログメッセージはマシンの Application イベントログに書かれる
- 4 EventSentry は Application イベントログを監視し、イベントレコードをフォワードする

シスログメッセージはまず Application イベントファイルに書かれ、次に EventSentry が取り出しフィルターとターゲットの設定にしたがってそれを処理します。

4 章 参考情報

EventSentry の詳細については日本語マニュアルを御参照ください。