

GroundWork Monitor Open Source

オペレータガイド

目次

第1部 GroundWork Monitor Open Sourceによるこそ

- 第1章 はじめに
- 第2章 GroundWork Monitor Open Source概要
- 第3章 はじめよう
- 第4章 モニタリングの概念
- 第5章 Nagios 2.0

第2部 ステータスビューアでのモニタリング

- 第1章 概要
- 第2章 OverViewを使ったITインフラストラクチャの監視
- 第3章 NetViewを使ったITインフラストラクチャの監視
- 第4章 TroubleViewで障害のあるホストとサービスを見る
- 第5章 FilterViewを使ってモニタリングデータをフィルタする
- 第6章 ステータスビューア内の処理コマンド処理コマンド
- 第7章 ステータスビューアの使い方ノウハウ

第3部 インサイトレポートの作成

- 第1章 概要
- 第2章 アラームレポート
- 第3章 通知レポート
- 第4章 停止レポート
- 第5章 レポートの詳細

第4部 ブックシェルフ内の文書を参照する

- 第1章 概要
- 第2章 ブックシェルフ内をナビゲートする
- 第3章 ブックシェルフ内を検索する

第1部 GroundWork Monitor Open Sourceによるこそ

本セクションでは、本バージョンのGroundWork Monitor Open Sourceで何が新しいか、GroundWork Monitor Open Source システムの紹介および、どう始めるかについての、このガイドに関する情報を提供します。また、重要なモニタリング(監視)の定義と概念についても説明します。

第1章 はじめに

- このガイドについて

- 関連ドキュメント

- GroundWork Monitor Open Sourceのサポート

- コメントを送る

第2章 GroundWork Monitor Open Source概要

- GroundWork Monitor Open Source

- 現在のGroundWork Monitorの版

- 本バージョンのGroundWork Monitor Open Source新機能

第3章 はじめよう

- GroundWork Monitor Open Sourceにアクセスする

- GroundWork Monitor Open Sourceの操作

第4章 モニタリングの概念

- モニタリングのプロセス

- オープンソース技術の統合と拡張

- 重要な定義と概念

第5章 Nagios 2.0

- Nagios 2.0 リリース

- Nagios ドキュメント

第1章 はじめに

GroundWork Open Source, Inc.が開発したGroundWork Monitor Open Sourceをご使用いただきありがとうございます。

GroundWork Monitor Open Source製品は、御社のITインフラストラクチャ全体にわたる集中化した可視性とコントロールを提供するよう設計されています。それは、システム、アプリケーション、データベースおよびネットワーク装置をモニターします。GroundWork Monitor Open Sourceは、魅力的で、直感的なユーザインタフェース、カスタムコンフィギュレーションとカスタムレポートをサポートする柔軟なアーキテクチャを特徴とします。本システムは、選りすぐったオープンソースと、GroundWorkの専門家によって開発された IT管理のネットワーク 可用性とパフォーマンスを監視して管理するための革新的なソフトウェアを組み合わせた最新のアーキテクチャの上に構築されています。GroundWork Monitor Open Sourceは、リアルタイムのステータスビュー、詳細なコンポーネントのビュー、可用性とパフォーマンス傾向の強力なレポートおよびアラート履歴を提供します。GroundWork Monitor Open Sourceのこれらおよび他の機能は、本文書上で詳しく説明します。

本ガイドについて

このGroundWork Monitor Open Source オペレータ ガイド 1.0にはGroundWork Monitor Open Sourceのための詳しい操作について記述しています。本バージョンへの修正と更新は <http://www.groundworkopensource.com>を通して提供されるでしょう。このガイドは、GroundWork Monitor Open Sourceが初めての人のためにデザインされています。このガイドに記述された情報には、アクセスの仕方、使い方とシステムとのやり取りの仕方、そして、ユーザインタフェースを通しての他のリソースについて説明します。これは、モニタリングステータスや詳細なコンポーネントのビューを見るための方法、可用性 とパフォーマンスレポートやアラート履歴を作成するためのオペレータのインストラクションを提供し、GroundWork Monitor Open Sourceのユーザのためのオペレーションリファレンスとなることを意図しています。読者にはプログラムやソフトウェア開発の知識が必要でないですが、基本的なモニタリング(監視)について慣れているべきです。

関連ドキュメント

初期導入やシステムへのユーザアクセスを管理する一環として、システムのインストールや構成設定(コンフィギュレーション)が必要な管理者のための追加情報やトピックについては、GroundWork Monitor Open Source管理者ガイドを参照してください。GroundWork Monitor Open Source開発者ガイドは、GroundWorkのAPI、コンポーネントの構造とGuavaについて説明しています。

GroundWork Monitor Open Sourceのサポート

- GroundWorkのサブスクリプション(年間契約サービス)契約によって、製品サポートが受けられます。
- 稼動時間帯は、米国太平洋標準時間(PST)の午前6:00 AMから午後6:00です。

GroundWorkサービスデスクにコンタクトする

サービスデスク (Webベース)	ここをクリックして、 GroundWork Support Center にログインします。	これは、当社のWebベースのサービスデスクであり、推奨するコンタクト方法です。チケットの各欄を埋めた後、サービスエンジニアがあなたのチケットをレビューし、できるだけ早くあるいは、 2営業時間以内 にあなたにコンタクトします。ログインIDとパスワードは、GroundWorkの担当者から提供されます。
電話	サービスデスク 866.899.4342 に電話を掛けてください。 (オプション 1)	サービスデスクの担当者は、あなたの問い合わせ番号を記録して、チケットを作成します。チケット作成後、サービスエンジニアが、あなたのチケットをできるだけ早くあるいは、 4営業時間以内 にあなたにコンタクトします。
電子メール	ここをクリックして、 GroundWork Support. にメールを送ります。	メールを使ってチケットの各欄を埋めた後、サービスエンジニアが、あなたのチケットをできるだけ早くあるいは、 4営業時間以内 にあなたにコンタクトします。以下の情報を記述してください： <ul style="list-style-type: none">• あなたの氏名• 会社名• 問題点の説明（詳しく）• 問題の緊急性とそれがどの程度あなたの業務に影響しているかについて
緊急時	サービスデスク 866.899.4342 に電話を掛けてください。 (オプション 1)	時折、あなたが、あなたの業務上、GroundWorkが本当にすぐにその問題に取り掛かる必要があることがあることを我々は知っています。サービスデスクの担当者にあなたのリクエストが緊急であることと、それが新しいか既存の件か、を教えてください。既存の件であれば、問い合わせ番号を教えてください。新チケットや既存チケットへの情報入力の後、サービスエンジニアが緊急案件についてできるだけ早くあるいは、 30分以内(営業時間) にあなたに回答します。

コメントを送る

GroundWorkは、本ユーザガイド(GroundWork Monitor Open Sourceオペレータ ガイド)の品質や有用性に関するコメントや提案を歓迎します。あなたの意見は将来版への重要な情報です。

ぜひ、documentation@groundworkopensource.com。宛てに提案や訂正意見をお寄せください。

第2章 GroundWork Monitor Open Source 概要

GroundWork Monitor Open Source

GroundWork Monitor Open Sourceは会社のITインフラストラクチャをきちんと監視・管理するためのオープンソースのソリューションです。GroundWork Monitorは、可用性とパフォーマンスを計測するために、アプリケーション、ネットワーク装置、サーバ、と他のコンポーネントに問い合わせ、IT情報と分析を整理して、見せるための統合ポイントとしてのブラウザベースのインタフェースを介して、これらのシステム計測基準についてやりとりを行います。そのシステムは、貴社の全ITインフラストラクチャにわたる集中化した可視性とコントロールを提供します。GroundWork Monitor Open Source の主要なコンポーネントについて、下記の表に示します：

表1.2.1 GroundWork Monitor Open Sourceの主要なコンポーネント

アプリケーション	説明
Status	監視インタフェース - 本機能は、Webベースのインタフェースを通じてのNagiosモニタリングシステムへのアクセスを提供します。ここでは、アプリケーション、ネットワークとサーバの可用性とパフォーマンス監視へのアクセラとドリルダウンができます。
Nagios	Nagiosインタフェース - これは、インストール可能なGroundWork Monitor Open Sourceタブで、GroundWork Monitor Open SourceからNagiosインタフェースへの直接アクセスを可能にします。オペレータはここで、Nagiosのタクティカルオーバービューとホストとサービスの詳細、サービスの概要、サマリー、グリッドと問題データにアクセスすることができます。ホストの問題にネットワーク停止、コメントと停止時間情報と一緒に追加します。GroundWork Monitor Open Source機能オプションは、アクセスを容易にするため、ビューに残ります。
Map	Nagiosのマップ - これは、インストール可能なGroundWork Monitor Open Sourceタブで、ユーザに、貴社のネットワーク上で定義されているすべてのホストを表示するNagiosのグラフィックなネットワークマップを直接アクセスできるようにします。
Reports	運用および管理レポート - GroundWork Monitor Open Sourceは、システムの可用性とパフォーマンスについてのリアルタイムと履歴データを提供します。
Nagios Reports	Nagiosレポート - Nagios Reportsは、もうひとつのインストール可能なGroundWork Monitor Open Source機能です。GroundWorkのインサイトレポートに加えて、このオプションをインストールすることで、ユーザは直接、GroundWork Monitor Open SourceのReportsタブから、傾向、可用性、アラートヒストグラム、アラート履歴、アラートサマリ、および通知を含む、Nagiosのレポートにアクセスすることができます。
Bookshelf	製品ドキュメント - GroundWork Monitor Open Sourceのリファレンス - このBookshelf(本棚)機能は、検索機能を持つオンラインのドキュメントシステムを提供します。GroundWorkとオープンソースのリファレンス資料が参照できます。このドキュメントシステムも、あなたの特別のドキュメント手順書を統合するように構成設定(コンフィギュレーション)することができます。
Administration	管理 - GroundWork Monitor Open Sourceのユーザ管理 - この機能は、システム管理、ユーザ、ロール、およびビュー(アプリケーション)管理へのアクセスを提供します。管理に関するさらなる情報は、GroundWork Monitor Open Source管理者ガイドを参照してください。
Configuration EZ	開始するための構成設定ウィザード - Configuration EZは、管理者が、NagiosとGroundWork Monitor Open Source構成設定(コンフィギュレーション)の中心となる手順を実施する、開始するためのウィザードです。高度な構成設定は、Configurationタブを使って行います。
Configuration	高度な構成設定 - NagiosとGroundWork Monitor Open Sourceの構成設定を行う - Monarchは、Webベースのコンフィギュレーションツールです。このツールは、容易で、監視システムの構成設定をスピードアップします。Monarchに関するさらなる情報は、GroundWork Monitor Open Source管理者ガイドを参照してください。

現在のGroundWork Monitorの版

現在、GroundWorkは、GroundWork Monitorの二タイプの版をモニタリングソリューションとして提供しています。各版のコンポーネントの概要を次の表に示します。

表 1.2.2. 製品の版毎のコンポーネントと機能

	GROUNDWORK MONITOR OPEN SOURCE	GROUNDWORK MONITOR PROFESSIONAL
コンポーネント/機能	GroundWork Monitor Open Source版は、貴社のITインフラストラクチャを正しく監視するGroundWorkの基盤のオープンソースソリューションです。	GroundWork Monitor Professional版は、ITインフラストラクチャ 監視と管理のためのGroundWorkの高度なオープンソースソリューションです。
ステータス (Status)	○	○
レポート (Reports)	○	○+
コンソール (Console)	×	○
パフォーマンス (Performance)	×	○
本棚 (Bookshelf)	○	○
Nagios	○	○
Nagiosレポート (Nagios Reports)	○	○
マップ (Map)	○	○+
管理 (Administration)	○	○
簡易構成設定 (Configuration EZ)	○	○
構成設定 (Configuration)	○	○
パフォーマンス構成設定	×	○
プロファイルツール	×	○
監視サーバ	×	○
プロファイルライブラリ	○	○+
ファウンデーション	×	○
PHPフレームワーク	○	○
SNMPトラップ統合	×	○
知識ベースサポート	×	○

○+ : 拡張機能

本バージョンのGroundWork Monitor Open Sourceでの新機能紹介

GroundWork Monitor Open Sourceソフトウェアの各リリースにおいて、機能とソフトウェアの使い勝手の著しい改善が行われました。下記に、バージョン 4.5での重要な変更点を表で示します。

表 1.2.3. バージョン 4.5の重要項目

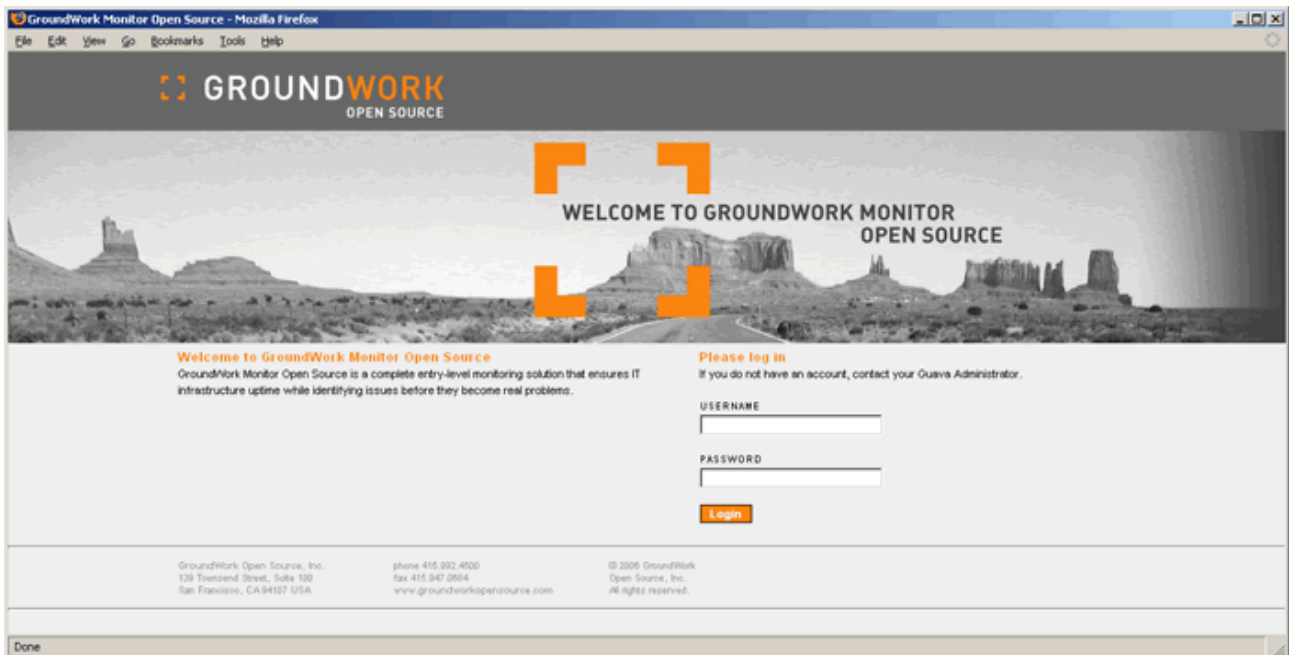
重要点	説明
Nagios 2.0 サポート	GroundWork Monitor Open Sourceは、新しいNagios 2.0機能を活用し、より高速なパフォーマンス、新しいNagiosディレクティブの提供、および、Nagios 1.2からの容易なマイグレーションプロセスを提供します。
ステータスビューアの改善	GroundWorkのステータスビューア (Status Viewer) は、管理者がNagiosステータスの鳥瞰的なビューを見るようにできます。ステータスビューアの改善には、全体的なネットワークの健康状態のグラフィカルなビューと共に、モニタリング状況を表示するタクティカルオーバービューを含みます。Netviewインタフェースは、サイドナビゲーション・ツリー、色によるステータスコード分けと、より容易なナビゲーションと明快なビュー可能にする合理化されたデザインでのインタフェースを提供します。ステータスビューアは、AJAXベースであり、全体ページのリロードを行うことなく、データ更新が行われます。
構成設定 (Configuration) の改善	GroundWorkのモニターアーキテクト (Monarch)は、Nagiosネットワーク監視システムの構成設定と管理のためのWebベースのエンジンです。Monarchは、今や、使い勝手を改善するため機能強化しナビゲーションを持ち、複数のホストプロファイルをマルチアサインする能力を持ち、そして、ホストプロファイルへ複数のサービスをアサインする能力を持ちます。サービスの依存性、エスカレーション、とサービステンプレートのエリアでにおいて、Monarchの機能拡張を行いました。さらに、プロファイルのインポートが追加されました。
簡易構成設定 (Configuration EZ)	Monarchに、管理者が主な構成設定 (コンフィギュレーション) をザッと実施することができる、開始のためのウィザードが付属しました。高度な構成設定は、Configurationタブを通して実施できます。
ホストとサービスプロファイル	GroundWork Monitor Open Sourceは、Nagiosプラグイン、Monarch構成設定定義、ドキュメント、パフォーマンスグラフ定義とCGIプログラム、(必要な場合) サポートパッケージ、(必要な場合) 検出スクリプトおよび、インポートツールを含む、管理エレメントを監視するのに要求されるすべてのコンポーネントを含むパッケージを、あなたが作ることができるようにします。あなたは、Monarchの中のホストにプロファイルをアサインすることで容易にモニターを作ることができます。 GroundWork Monitor Open Sourceのサービスプロファイル: ServicePing、SNMP Network および SSH Unixは GroundWork Monitor Open Source版に添付されています。追加のプロファイルは GroundWorkのWebサイトから入手できます。
ドキュメントの改善	GroundWork Monitor Open Sourceのドキュメントは、今回、オペレータ、管理者および開発者向けのユーザガイドの形式で提供されます。GroundWork Monitor Open Source オペレータガイドはシステム アプリケーションの操作に関わる情報を持ち、管理者ガイドは、システムのインストレーションと構成設定を記述し、開発者ガイドは、システムのカスタマイズの情報を含んでいます。 GroundWork Monitor Open Source製品のオープンソースコンポーネントについても、製品と共に配布されるNagiosプラグインを含み、文書化されています。
PHPフレームワーク	GroundWork Monitor Open Sourceのユーザインタフェースは、Guavaと呼ぶ、強力なPHP5ベースのアプリケーション フレームワークと環境を土台にします。このPHP フレームワークは、ステータスビューア、構成設定 (Configuration) と本棚 (Bookshelf) を含む GroundWork Monitor Open Source機能のための開発プラットフォームを提供し、他の開発者がダイナミックなAJAX駆動型のWebアプリケーションを構築するのに使用できるツールキットでもあります。ユーザは、システムのユーザ、ロール (役割)、とパッケージを定義することができます。

第3章 はじめよう

GroundWork Monitor Open Sourceをアクセスする

GroundWork Monitor Open Sourceにアクセスするため、システム管理者からURLを教えてください、Webブラウザのアドレスバーに入力します。画面表示が下記ようになるでしょう。これが、GroundWork Monitor Open Sourceのログイン画面です。この画面が表示されなかったら、URLを正しく入力したか、あなたのシステム管理者に正しいURLかどうかを確認するためコンタクトしてください。作業を続けるため、正しいユーザ名とパスワードを入力して、ログインしなければなりません。

図 1.3.1. GroundWork Monitor Open Sourceのウェルカム画面



システムにログインする

1. GroundWork Monitor Open Sourceのログイン画面で**ユーザ名**を USERNAME ボックスに入力する
2. PASSWORDボックスに**パスワード**を入力する
3. **Login**ボタンをクリックする。

ログインできない場合、下記をチェックしてください：

1. ユーザ名とパスワードを正しく入力したかを確認してください。大文字かどうか。すべては小文字である必要があります。
2. システム管理者に連絡し、あなたが正しいユーザ名とパスワードの組み合わせを持っているかを確認します。
3. あなたのアカウントがディスエイブルになっているかもしれません。システム管理者に連絡してください。

セキュリティ・タイムアウト

セキュリティの見地から、あなたが一定時間何も作業を行わなかった場合、システムは自動的にあなたをログアウトします。デフォルトでは、何も行わないで30分間経過するまでは、あなたをログアウトはしません。

デフォルトのロール定義の中にある機能

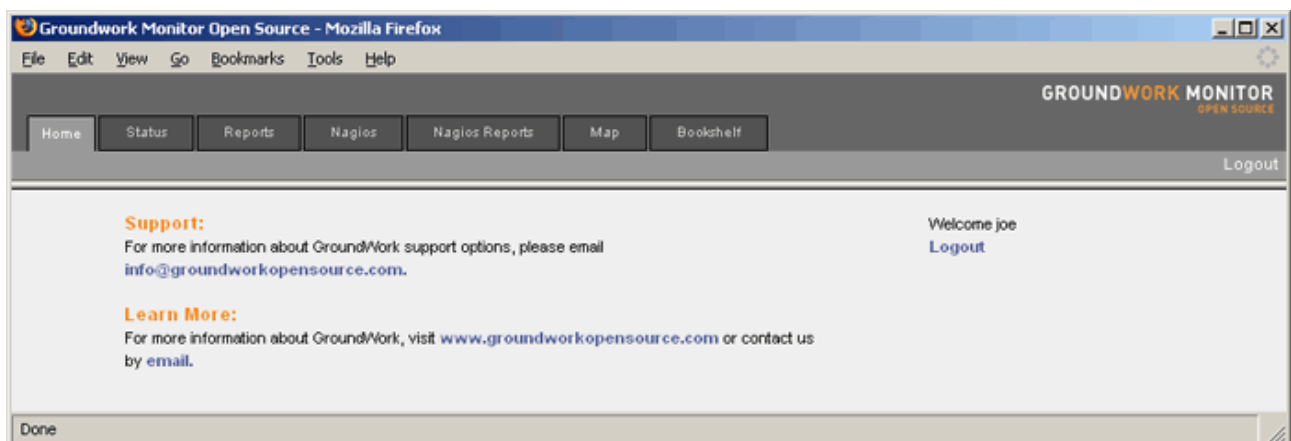
GroundWork Monitor Open Sourceに入ると、トップ画面の中に表示された機能タブが見えるでしょう。あなたが入力したユーザのログインのタイプで、どのタブが表示、アクセスできるかが決まります。下記の表は、デフォルトのロール(役割)からアクセスできるGroundWork Monitor Open Sourceの機能を示します。予め定義され、編集可能なオペレータ(Operator)と管理者(Administrator)ロールが、特定機能のユーザアクセスを定義します。下にある図は、使用可能なタブオプションを表示している、オペレータと管理者の画面を示します：

表1.3.1. デフォルトのロール定義で表示される機能

機能	ロール(役割)	
	オペレータ	管理者(アドミニストレータ)
Status	○	×
Nagios	○	×
Map	○	×
Reports	○	×
Nagios Reports	○	×
Bookshelf	○	○
Administration	×	○
Configuration EZ	×	○
Configuration	×	○

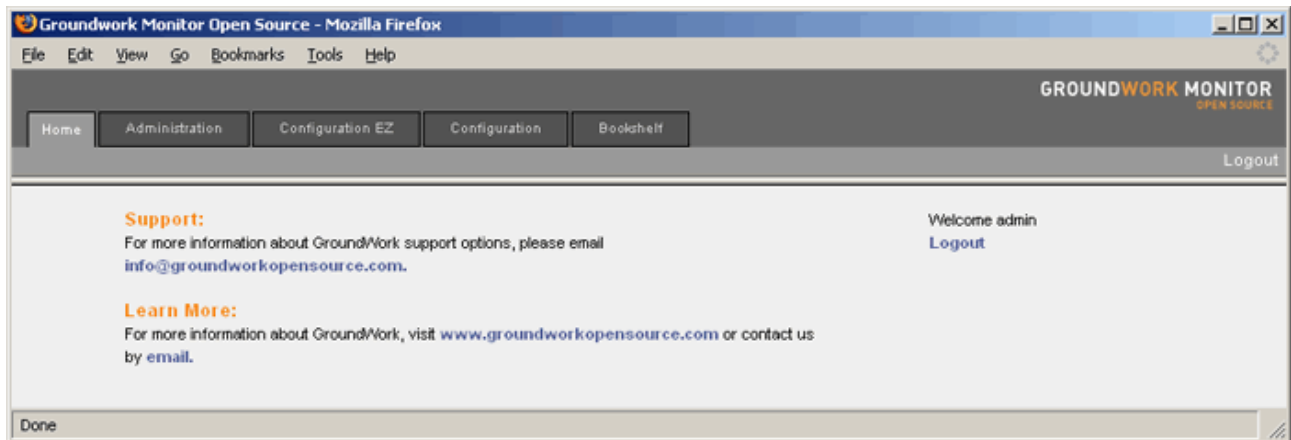
標準のモニター機能をアクセスするには、オペレータとしてログインします。下記の画面で、オペレータでログインした時にアクセス可能なタブが見えます。

図1.3.2. オペレータログイン画面



管理者機能をアクセスするには、管理者としてログインします。下記の画面で、管理者でログインした時にアクセス可能なタブが見えます。

図1.3.3. 管理者ログイン画面



パスワードの管理

GroundWork Monitor Open Sourceサーバは、基本認証を使用します。サーバのセキュリティ確保の主な理由は、高度なセキュリティシステムを導入するより、ユーザIDをベースとして部門や個人にロール(役割)を委託することで。システムは、あなたが使用するIDによって、何ができて、何をできるようにするかを随意にフィルタできます。パスワードの変更と他の管理業務は、GroundWork Monitor Open Source管理者ガイドに詳しく記述されています。パスワードは、管理者ログインでセットアップされ、管理されます。もし、パスワードを忘れた場合、必ず、パスワードの再設定を行うシステム管理者に連絡してください。セキュリティの目的から、システムに一度ログインしたら、あなた自身が選ぶ他の値にパスワードを変更するように促されるでしょう。

システムからログアウトする

システムでの作業が終わったら、Homeタブを選んでLogoutのリンクを選ぶことで、ログアウトできます。他の方法として、各アプリケーション画面の右上端にLogoutのオプションがあります。それで、ブラウザウィンドウを閉じることができます。システムからログアウトしないで、ブラウザのウィンドウを閉じると、システムにログインしたままです。

GroundWork Monitor Open Source内のナビゲーション

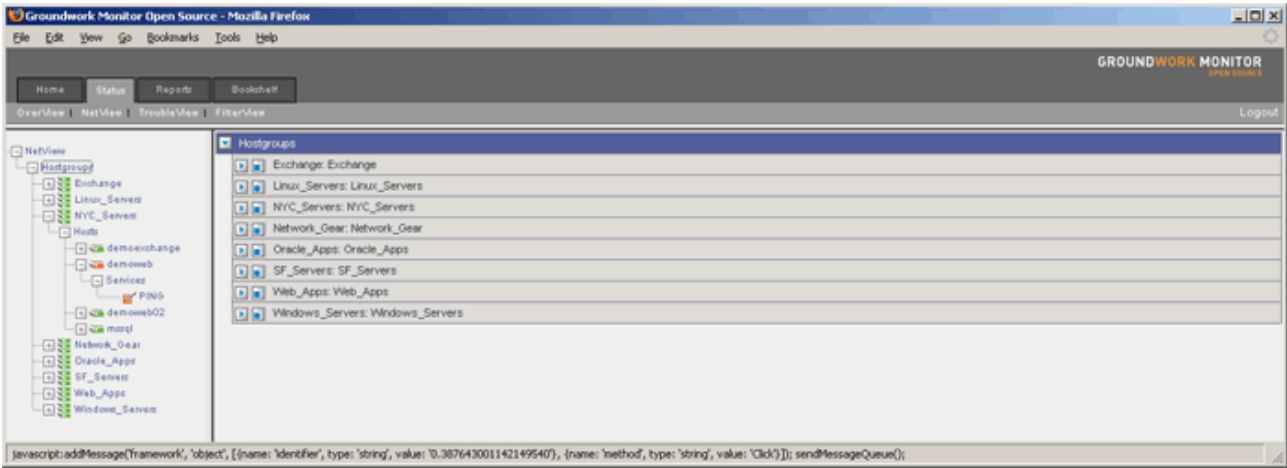
アプリケーション

画面の上部のメインタブは、GroundWork Monitor Open Source内のアプリケーションにリンクされています。これらのタブは、サイトのナビゲーションのために、サイトとサーバ全体にわたって、常に見ることができます。

ナビゲーション・ツリー

GroundWork Monitor Open Source内のタブになったアプリケーションの多くは、階層的なナビゲーションツリーを持っています。左側のウィンドウは、その機能のコンポーネントの親子関係を示しています。階層的なメニューは動的に変化し、機能の内容へのリンクを含んでいます。このメニューは、サイト内を移動するに従って変わっていきます。GroundWork Monitor Open Sourceで使用される付加的なナビゲーション要素には、リンク、アイコンとタブがあります。ステータスビューアのナビゲーション・ツリーを例として下記に示します。

図1.3.4. ステータスビューアのナビゲーション・ツリー



第4章 モニタリングの概念

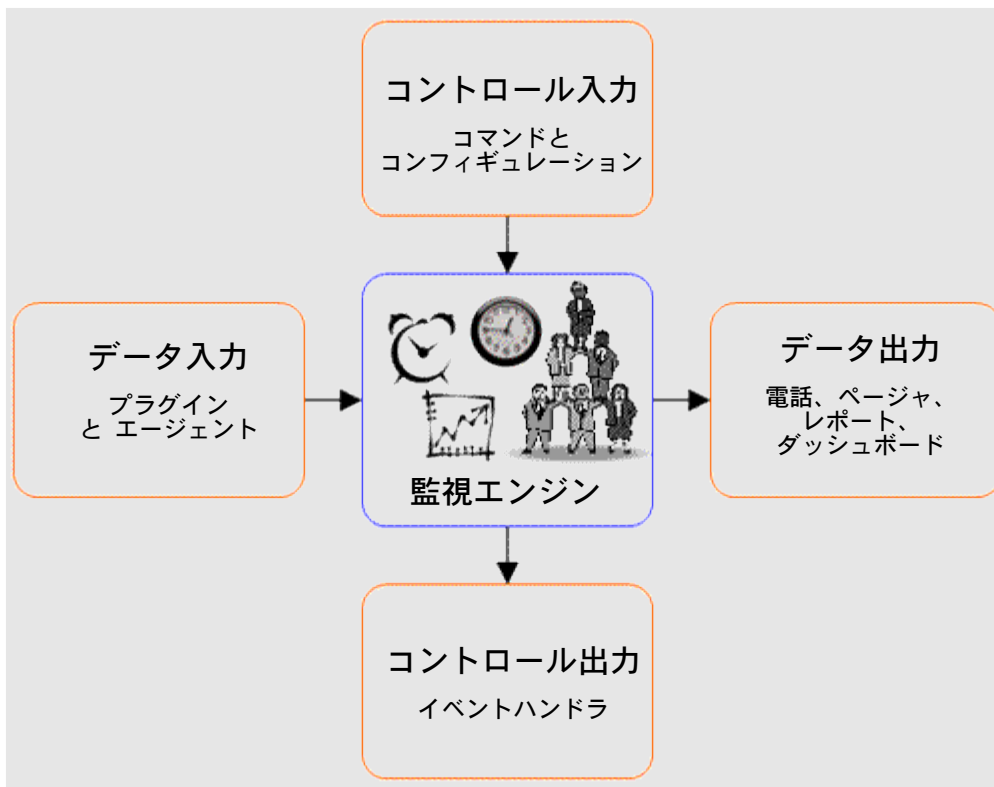
モニタリングプロセス

下図は、基本的なモニタリングのプロセスを示します。ホストやサービスステータスをチェックするコマンドラインから起動されるプラグインとエージェントから監視エンジンにデータ入力されます。監視エンジンの下記を含む四つの機能を持ちます：

1. モニタをスケジュールして起動するスケジューラ
2. 障害時のアラームを生成するアラームエンジン
3. 通知とエスカレーションが管理されるロケーション
4. レポートが作成されるエリア

監視エンジンのコントロール入力は、コンフィギュレーションファイル（Nagiosがどのように働くかに影響するディレクトティブ）とコマンドライン（外部アプリケーション）入力から来ます。コントロール出力は、プロアクティブな障害解決のための他のシステムアクションのトリガーとなるために、ホストやサービスイベントの際に起動されるイベントハンドラを使用します。そして、サービスチェックとホストチェックのロジックを基本として、電子メール、ページャやユーザが定義した方法を通して問題解決が行われるように、通知（Notification）がデータ出力として送りだされます。通知に加えて、出力はレポートとダッシュボードの形態をとります。

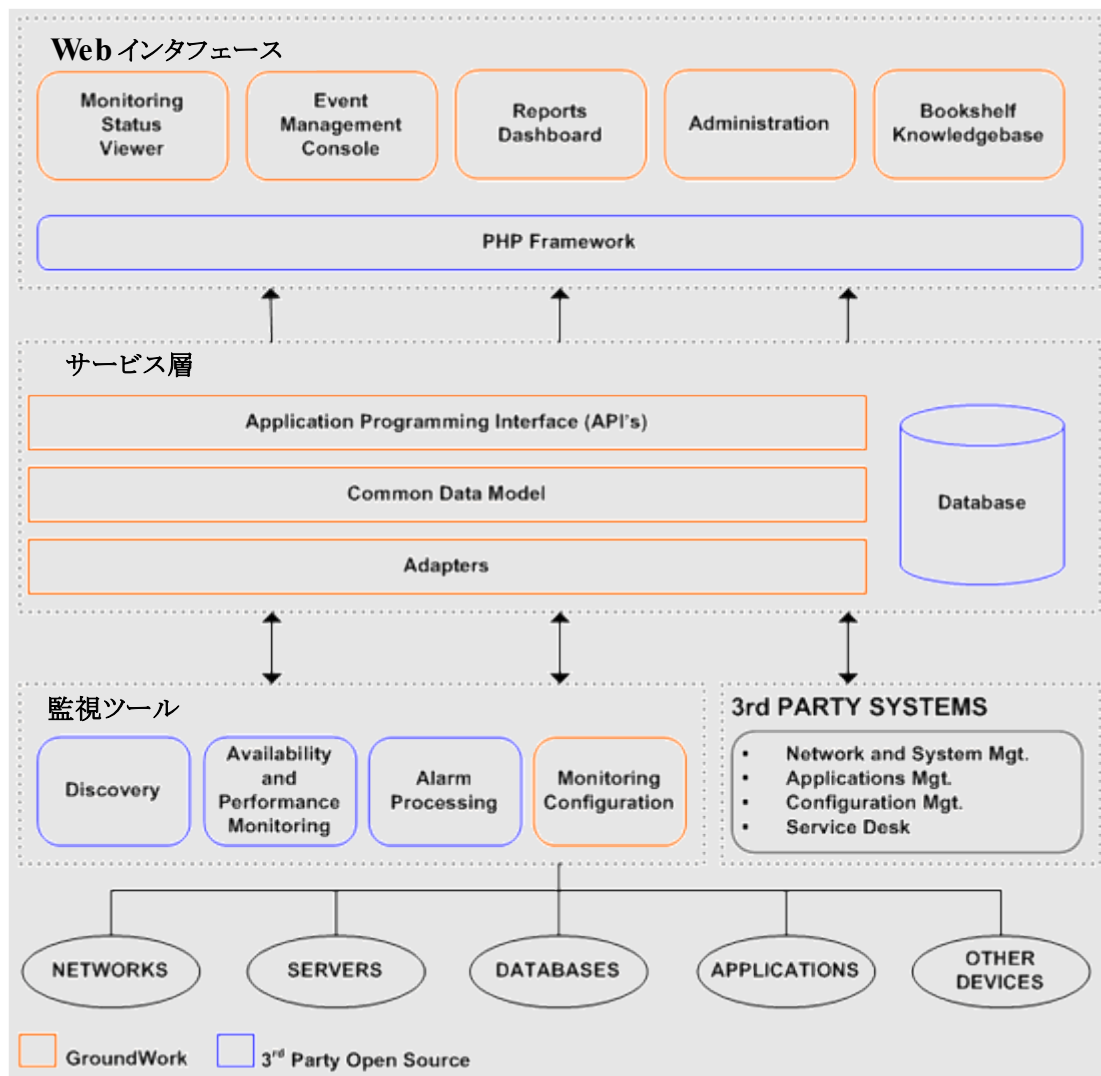
図1.4.1. 基本的なモニタリングプロセスの概念



オープンソース技術の統合と拡張

GroundWorkの統合オープンソースアーキテクチャは、下記のように3層の機能—監視ツール層、サービス層、およびWebインタフェースあるいはプレゼンテーション層から構成されます。このアーキテクチャは、完全にオープンで開発者が追加のデータソースを組み込んだり、プレゼンテーション層のアプリケーションを開発するなどの拡張ができます。監視ツール層は、Nagios、Syslog-NG、SNMPTTやサードパーティの商用監視システムなどのIT監視や管理システムからのデータを抽出します。サービス層は、IT監視や管理データを標準化し、データベースに格納します。この層は、プレゼンテーション層のアプリケーションとビューアを書くためのアプリケーションプログラミングインタフェース(API)を含みます。そして、Webインタフェース層はオペレータや管理者がITインフラストラクチャを監視したり管理するために必要なデータを表示するGroundWorkのWebインタフェースを構成します。データはステータス画面、パフォーマンスグラフ、イベントコンソール、レポートとダッシュボードを介して表示されます。

図1.4.2. GroundWork Monitor Open Sourceのアーキテクチャ



重要な定義と概念

ここで、監視環境の中で使われるいくつかの重要な定義と概念について、説明します。

表1.4.1. 定義と概念

重要な定義	説明
ホスト	可用性(稼動)状態をトラッキングしたり、マップにしたりする要素(アイテム:物理的なサーバ、ワークステーション、ネットワーク デバイスなど)
サービス	ホストに関連付けられた特定のパラメータや状態(ステータス)をのモニター。これは、ホスト上で稼動する実際のサービス(POP, SMTP, HTTP,など)や、ホストに関連付けられた他のタイプの計測基準(pingへの応答、ログインユーザ数、など)になり得ます。
ホストグループ	名前を付けられた任意のホストの集合体。The usage of ホストグループを使うことにより、アクセスのコントロールや階層の表示、ステータス表示、通知、定期メンテナンス、複数サーバコマンドとレポートを簡素化します。定義された各ホストは、少なくともひとつのホストグループのメンバーである必要があります。
プラグイン	監視対象のホストやサービスのチェックが必要な場所で実行される、外部 (Nagios に対しての) プログラム。
フラッピング	フラッピングは、ホストやサービスのステータスが非常に頻度高くに変化する時に発生し、障害と回復の通知の嵐を引き起こします。フラッピングは、コンフィギュレーションの問題(例、しきい値が低すぎる)や実際のネットワーク問題を 暗示します。
通知 (Notifications)	監視対象要素のステータスに関するコンタクトやコンタクトグループへのコミュニケーション。通知は、例えばホストやサービスが継続的に不正 (non-OK)ステータスにある場合に承認を得るためなど、ハードステータス変化を含む状況についても構成設定(コンフィギュレーション)することができます。
イベントハンドラ	イベントハンドラは、ホストやサービスのステータス変化が発生した時に常に実行されるオプションなコマンドです。イベントハンドラ(特に、サービスについて)の明白な利用方法は、Nagiosが誰かに通知する前に、プロアクティブに障害を回復できるようにすることです。他の潜在的なイベントハンドラの利用方法は、サービスやホストのイベントを外部データベースにログすることでしょう。
タイムピリオド(時間帯)	タイムピリオド定義は、通知やサービスチェックのための時間が正しいかを判断するために、さまざまな日にちの間の時間のリストを識別します。
コマンド	ホストとサービスチェック、ホストとサービス通知と、ホストとサービスイベントハンドラを含む、Nagiosによって定義、実行されるコマンド。コマンド定義には、一般的なコマンドの使用を容易にするため、マクロを含むこともできます。
コンタクト(連絡先)	コンタクトは、あなたのネットワーク上の障害イベントの際に連絡するべき誰かを識別するための定義し使用されます。コンタクトグループは、アラート/回復通知を送る目的のために、ひとつ以上のコンタクトをお互いにグループ化したものです。コンタクトグループ内の全コンタクトは、ホストやサービスに障害や回復の際に、通知を受けます。
プロファイル	プロファイルは、複数のサービスやホストの集合です。Monarchは、予め定義されたのと、ユーザ定義可能な監視パラメータ設定の両方を含む、デバイス固有のプロファイルを使用します。プロファイルを使って、管理者は、同種のデバイスを監視するためにすばやくGroundWork Monitor Open Sourceを構成設定することができます。GroundWorkの監視設計についての深い専門知識が推奨案のメリットを得ることができます。

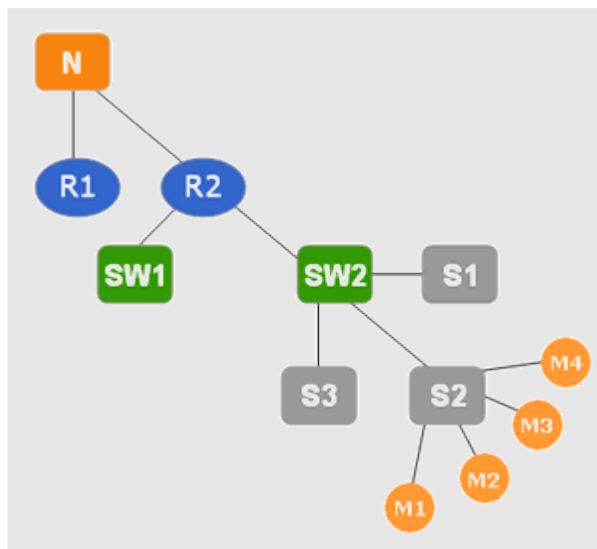
依存 (Dependencies)

監視対象要素が監視サーバと同一サブネット上に無い時、その監視は両者の間にあるスイッチやルータに依存します。

GroundWorkの標準の依存関係

- ・上流のスイッチとルータ監視
- ・ホスト上のサービスステータス
- ・ポートベースの監視エージェントの可用性

図1.4.3. 依存関係



ステータス (State) とステータス変化 (State Changes)

誤認警報 (false alarms) を予防するため、Nagiosは、ホストやサービスに本当に障害が発生したと認識する前に、何度サービスやホストチェックを繰り返す (リトライ) かを定義することができます。ホストやサービスチェックで障害と判断するまでのリトライの最大値は、ホストとサービス定義内の <max_check_attempts> オプションでそれぞれ制御されます。現時点でホストやサービスチェックが何を確認しているかは、それが今どのようなステータスにあるかによって決まります。

ステータスのタイプは、いつイベントハンドラが実行され、いつ通知が送られるか決めるときに使われます。現在のサービスとホストステータスは、二つのから構成されます：

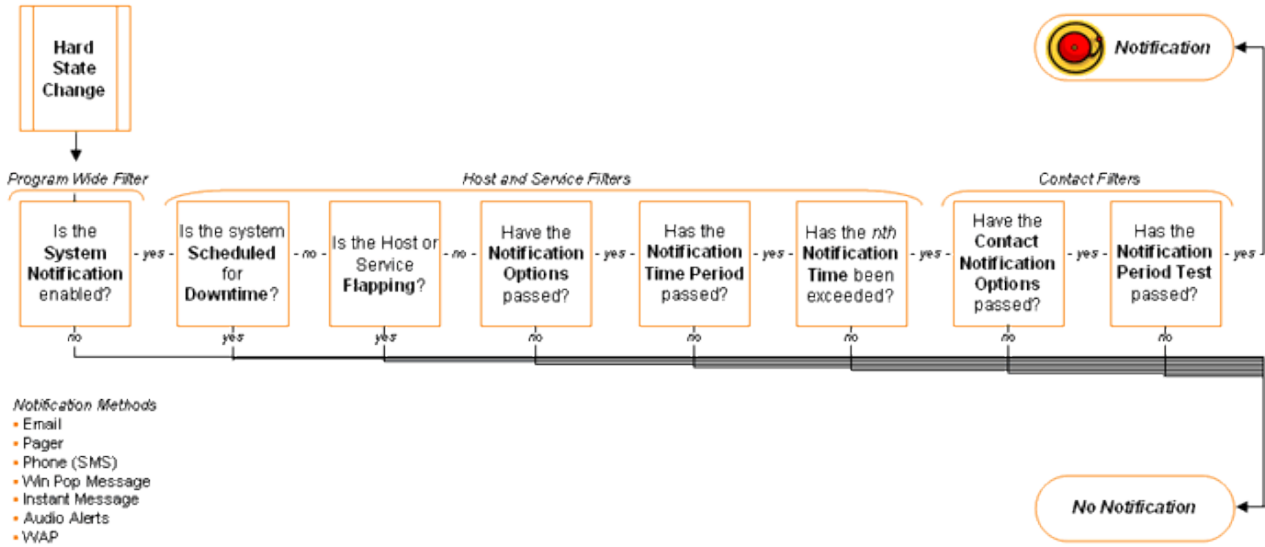
1. ホストやサービスのステータス。ホストステータスは、稼動 (UP)、停止 (DOWN)、到達不可 (UNREACHABLE) や保留 (PENDING) となります。サービスステータスは、正常 (OK)、ワーニング (WARNING)、クリティカル (CRITICAL)、未知 (UNKNOWN) や保留 (PENDING) となります。
- 2.. それがあるステータスのタイプ。

Nagiosにおけるステータスのタイプには、以下の二つがあります：

1. ソフトステータス (Soft states)
2. ハードステータス (Hard states)

通知とエスカレーション

図1.4.4. 通知ロジック



いつ通知が発生するか？

- ➔ ハードステータスの変化が発生し、すべてのフィルタをパスしたとき
- ➔ ホストやサービスが、正常でない(non-OK) ハードステータスに継続してあり、ホストやサービス定義の <notification_interval> オプションで指定された時間が(そのホストやサービスに対する)その前の通知をしてから経過したとき

誰が通知を受け取るか？

- ➔ ホスト - 各ホストは、ひとつ以上のホストグループに所即しています。各ホストグループは <contact_groups> オプションを持ち、それがそのホストグループに所属するホストについて、どのコンタクトグループが通知を受けるかを指定します。
- ➔ サービス - 各サービス定義は、<contact_groups>オプションを持ち、それがそのサービスのためにどのコンタクトグループが通知を受けるかを指定します。

通知を送出する前にどのフィルタをパスする必要があるか？

- ➔ プログラム全体(Program Wide)フィルタ
 - システム通知 - プログラム全体にわたって、通知をできるようにします。メインの設定ファイルの <enable_notifications> ディレクティブで指定しますが、実行中にWebインタフェースから変更することも可能です。
- ➔ ホストとサービスフィルタ
 - 計画停止 (Scheduled Downtime) - ホストやサービスが計画停止の時間帯か？
 - フラッピング - ホストやサービスがフラッピング状態か(フラッピング検出を可能にしている場合)？
 - 特定のホストやサービスの通知オプション - 各ホストとサービス定義で、通知を送るかどうかを定義するオプションが含まれています。
 - 通知時間帯 (Notification Time Period) - 各ホストとサービス定義の <notification_period> オプションで、どの時間帯がホストやサービスのための通知時間として正しいかを定義します。
 - 通知時間 (Notification Time) - 過去のある時点ですでにホストやサービス通知が行われており、最後の通知が送られた後もホストやサービスの不正(non-OK)ステータスが継続している場合、Nagiosは、前の通知から時間が経過して、ホストとサービス定義の中の <notification_interval> オプションに指定されている時間が経過したあるいは過ぎたかをチェックして確認します。

→ コンタクトフィルタ

この時点で、通知のプログラムのモードフィルタとすべてのホストやサービスフィルタがパスし、Nagiosは、通知されるべきすべての人に通知を開始します。このことは、すべてのコンタクト(連絡先)が通知を受け取れることを意味するのでしょうか？ 必ずしもそうではありません、各コンタクトは、彼らが通知を受け取る前にパスする必要のあるそれぞれの一組の通知フィルタを持っています。

- コンタクト通知オプション(Contact Notification Options) - 各コンタクト定義は、ホストやサービス通知を送出するかどうかのオプションを持っています。
- 通知時間帯テスト(Notification Period Test) - 各コンタクト定義は、どの時間帯がそのコンタクトに対する正しい通知時間かを指定する、<notification_period> オプションを持っています。

監視GUI

さまざまなCGIがNagiosと一緒に配布されています。デフォルトでは、CGIは、あなたがWebサーバの認証を受けて情報を参照する権限を付与されていることを要求します。

あなたは、Webインタフェースをセットアップし、CGIに承認を得る必要があります。GroundWork Monitor Open Sourceは、NagiosのWebインタフェースを置き換えるステータスビューアと呼ぶ、PHPベースの代替インタフェースを持っています。ステータスビューアは、監視されている全てのホストとサービスの完全なステータスを提供します。ステータスビューアは、トラブルシューティングや障害解決のためにNagiosデータを参照するユーザフレンドリーな方法です。

基本認証

ユーザ名とパスワードが、GroundWork Monitor Open Sourceをアクセスするために要求されます。これらは、オペレーティングシステムのログインアカウントと独立しており、監視システムでユニークです。このシステムは、ロールベースでログインIDは、ユーザが何を見るかをロールで定義します。認証を受けたユーザは、GroundWorkのWebベースのフレームワークから、ローカル認証かLDAP基本認証を使って認証を受けた人です。Webベースのフレームワークは、システムとその下にあるNagiosのGUIの両方をアクセスするために、シングル・サイン・オンをサポートしています。ユーザIDは、管理者によって構成設定されます。ログインの仕方についての説明は、第1部 第3章の「はじめよう」を参照してください。

通知アラームメッセージのフォーマット

下記に示すテキストは、通知アラームのためのフォーマットです。ホストとサービスは、IPアドレスと一緒に表示されます。ステータスが明確に表示されます:ここでは、クリティカルです。アラームの日付と時刻、追加の情報と、オペレータがアラームを承認することのできる場所へのリンクも含まれます。

通知コマンドは、通常、`/usr/local/groundwork/nagios/etc/misccommands.cfg` の中にあります。このファイルは、通知の内容を変更するために編集することができます。

図1.4.5. 通知 - アラームメッセージのフォーマット

```
Service: myapp_url_port Host: myapp Address: 10.0.0.10 State: CRITICAL
Date/Time: Tue Aug 6 3:54:07 PDT 2003
Additional Info: Socket timeout after 10 seconds
Acknowledge alarms at: http://nagios.mydomain.com/nagios/cgi-bin/cmd.cgi?
cmd_typ=34&Host=myapp&Service=myapp_url_port
```

停止時間やメンテナンス

Nagiosは、監視しているホストとサービスの計画停止時間の時間帯をスケジュールすることができます。これは、実際にアップグレードなどのためにサーバを停止することを知った場合などに便利です。ホストとサービスが計画停止時間にある場合、そのホストやサービスの通知は抑制されます。

なぜ計画停止時間を使うか？

- アラーム疲れを回避する

- より正確なレポートを提供する
- 変更コントロールに規律を徹底する

レポートینگ

Nagiosレポート(Nagios reports)

Nagiosレポートは、監視傾向(トレンド)、可用性、通知とイベントログデータについて、さまざまなレポート形式、さまざまな時間帯、ステータス、イベントと他のユーザの指定したパラメータで提供します。Nagiosレポートには、Trends (傾向)、Availability (可用性/稼働率)、Alert Histogram (アラートヒストグラム)、Alert History (アラート履歴)、Alert Summary (アラートサマリ)と通知(Notifications)が含まれています。Nagiosレポートがインストールされていれば、Nagiosレポートは GroundWork Monitor Open Sourceの Nagios Reportsのタブからアクセスできます。

パフォーマンスグラフ

パフォーマンス図表は、ネットワークバンド幅、CPU使用率、マシンルームの温度、トランザクションの応答時間とサーバのロードアベレージの時系列のデータを表示します。パフォーマンス図表は、GroundWork Monitor Professional版で提供されます。

インサイトレポート

インサイトレポートは、全アラートと通知の週間傾向、通知される回数、ホストとサービスおよびホストグループの上位の計測データを参照できる、経営・管理者レベルのレポートを目的としたものです。インサイトレポートには、アラーム(Alarms)、通知(Notifications)と停止(Outages)を含み、GroundWork Monitor Open SourceのReportsタブからアクセスできます。

第5章 Nagios 2.0

Nagios 2.0リリース

前述のとおり、GroundWork Monitor Open Sourceは新しいNagios 2.0機能を活用してより高速なパフォーマンスを提供し、その上、GroundWorkのコンフィギュレーションツール、Monarchが新しいNagiosディレクティブをサポートします。また、GroundWork Monitor Open Sourceは、Nagios 1.2からの容易なマイグレーションプロセスを提供します。Nagios 2.0機能について詳しくは、Nagios 2.0 (http://nagios.sourceforge.net/docs/2_0/whatsnew.html)を参照してください。

Nagiosドキュメント

Nagiosモニタリングシステムのドキュメントは、広大で、学び応えのあるものです。読むのに最も重要なセクションは、Nagiosドキュメントの「Theory of Operation」にリストされており、オンラインで Nagios 2.0 Documentationのサイト (http://nagios.sourceforge.net/docs/2_0/)を参照できます。

第2部 ステータスビューアでのモニタリング

ここでは、ステータスビューアを紹介し、このアプリケーション内でのナビゲーションと特定の監視情報にどのようにしてドリルダウンするかについて説明します。この部の各章は、ステータスビューア内の異なるビュー: OverView、NetView、TroubleViewとFilterViewの使い方を含んでいます。特定のホストとサービスステータス情報を表示するためにどのようにドリルダウンするかと、コマンドを参照したり開始する方法を説明します。

第1章 概要

- ステータスビューアについて
- ライセンスと入手
- ステータスビューア内のナビゲーション

第2章 OverViewを使ったITインフラストラクチャの監視

- OverViewについて
- 監視環境とステータス
- 監視システム機能ステータス

第3章 NetViewを使ったITインフラストラクチャの監視

- NetViewについて
- ドリルダウン

第4章 TroubleViewで障害のあるホストとサービスを見る

- TroubleViewについて
- ホストとサービスステータス

第5章 FilterViewを使って監視データをフィルタする

- FilterViewについて

第6章 ステータスビューア内の処理コマンド

- コマンド画面のレイアウト
- コマンドをコミットする
- ホストグループ、ホストおよびサービスのコマンド説明

第7章 ステータスビューアの使い方ノウハウ

第1章 概要

ステータスビューアについて

Nagiosのためのオープンソースのユーザインタフェース

GroundWorkステータスビューアは、Nagiosからの監視データの可視化と管理性を向上するためにデザインされた高速でスケーラブルなオープンソースのインタフェースツールです。ステータスビューアは、監視しているホストの、拡張したり縮小したりするツリー形式のメニューを提供し、詳しいホスト状態をすばやく見ることができます。FilterViewとTroubleViewで、特に興味を持ったことがらに焦点を当てることができます。ステータスビューアのインタフェースによって、Nagiosユーザは、全てのサーバ、アプリケーション、ネットワークおよびサービスが、しきい値の近くか、あるいはしきい値を超えたかの高いレベルのステータスを含む、企業のITインフラストラクチャについて、いくつかの重要なビューをアクセスできるようになります。

GroundWorkのステータスビューアは、GroundWorkが開発した技術で、監視データを抽出、正規化および独立してMySQLデータベースへ格納することと、アプリケーションプログラミングインタフェース (API)を介してデータを利用することを具現化します。そのインタフェース自体は広く使われているオープンソースのスクリプト言語であるPHPを使って書かれ、コモンゲートウェイインタフェース(CGI)を使って開発されたNagiosの現在のインタフェースよりはるかに高いパフォーマンスとなっています。

Overviewは、ITインフラストラクチャ状態の鳥瞰ビューを提供し、より詳しい情報をドリルダウンできるようにしたカラーコード化された見やすいビューです。**NetView** は全ネットワークインフラストラクチャの階層的なビューです。それは、監視されているすべてのホストとサービスの現在のステータスを見ることができるようになります。**TroubleView**は、すぐに対処が必要なホストとサービスすべてについて、一目で見るビューとドリルダウンビューを提供します。そして、**FilterView**は、ユーザに監視対象のデバイスやサービスのグループについて特別のステータスビューを定義する能力を提供します。これらの機能は、Nagiosユーザに彼らのITインフラストラクチャにわたる、より良い可視性と、コントロールと、ネットワーク内問題に関する情報へのより迅速なアクセスを提供します。ObjectViewのウィンドウは、ステータスビューア内の異なるレベルの情報へのドリルダウンとして、アクセスすることができます。それらはユーザがサーバやネットワークデバイスに関する詳細なステータス情報のウィンドウを開き、断続的に参照できるようにそれをデスクトップに固定します。

ライセンスと入手

GroundWorkのステータスビューアは、GroundWork Monitor Open Sourceと独立してインストールすることができ、現在、GNU General Public License (GPL)のオープンソースソフトウェアライセンスに基づいて下記のサイトからダウンロードできます:






- [GroundWork](http://www.groundworkopensource.com/products/os-license_faq.html) (http://www.groundworkopensource.com/products/os-license_faq.html)
- [SourceForge](http://sourceforge.net/projects/gwsv) (http://sourceforge.net/projects/gwsv)

ステータスビューア内のナビゲーション

オペレータはGroundWork Monitor Open Sourceにオペレータ・ログインし、Statusのアプリケーションタブを選ぶことで、ステータスビューアのアプリケーションをアクセスすることができます。Overview、NetView、TroubleViewおよびFilterViewメニューの選択肢は、Statusタブの下でアクセスできます。ステータスビューアは、アプリケーションの異なる部分へのアクセスのために、リンクとツリー・ナビゲーションおよびドリルダウンオプションを組み込んでいます。下表に、各ナビゲーションツールの簡単な説明をします。

表 2.1.1. ナビゲーションツール

ナビゲーションツール	説明
	NetViewの左側のナビゲーション枠で使用。NetView全体にわたるナビゲーションに使用。このアイコンは、NetView左のナビゲーション枠全体に渡ってナビゲートするために使用でき、選んだホストグループやホスト、サービスに 広げ ることができる
	NetViewの左側のナビゲーション枠で使用。NetView全体にわたるナビゲーションに使用。このアイコンは、NetView左のナビゲーション枠全体に渡ってナビゲートするために使用でき、選んだホストグループやホスト、サービスに対して広げられたナビゲーションを 縮小 する。
	NetViewの左側のナビゲーション枠で使用。この青色のアイコンは、 保留 (Pending) 状態にあるサーバを表す。
	NetViewの左側のナビゲーション枠で使用。この緑色のアイコンは、 正常 (OK) 状態にあるサーバを表す。
	NetViewの左側のナビゲーション枠で使用。この黄色のアイコンは、 ワーニング (Warning) 状態にあるサーバを表す。
	NetViewの左側のナビゲーション枠で使用。この赤色のアイコンは、 クリティカル (Critical) 状態にあるサーバを表す。ホストが 停止 (Down) や到達不能 (Unreachable) 状態の場合、サーバは赤となる。
	NetViewの左側のナビゲーション枠で使用。この緑色のアイコンは、 正常 (OK) 状態にあるサーバグループを表す。
	NetViewの左側のナビゲーション枠で使用。この黄色のアイコンは、 ワーニング (Warning) 状態にあるサーバグループを表す。
	NetViewの左側のナビゲーション枠で使用。この赤色のアイコンは、 クリティカル (Critical) 状態にあるサーバグループを表す。グループ内のどれかのホストが赤色状態の場合、サーバグループは赤となる。
	NetViewの左側のナビゲーション枠で使用。この青色のアイコンは、 保留 (Pending) 状態にあるサービスを表す。
	NetViewの左側のナビゲーション枠で使用。この緑色のアイコンは、 正常 (OK) 状態にあるサービスを表す。
	NetViewの左側のナビゲーション枠で使用。この黄色のアイコンは、 ワーニング (Warning) 状態にあるサービスを表す。
	NetViewの左側のナビゲーション枠で使用。この赤色のアイコンは、 クリティカル (Critical) 状態にあるサービスを表す。
	NetView、ObjectViewとTroubleViewで使用。ホスト、ホストグループ、サービスのリストを 広げる 。
	NetView、ObjectViewとTroubleViewで使用。ホスト、ホストグループ、サービスのリストを 縮小 する。
	NetViewとTroubleViewで使用。選んだホスト、ホストグループ、サービスのための ObjectView を生成する。これは、NetViewや他のビューを見続けながら、あなたが選んだモニタを継続して見張ることができるようにします。
	NetViewとTroubleViewで使用。 アクティブチェック がONかOFFになっていることを示す。

ナビゲーションツール	説 明
	NetViewとTroubleViewで使用。 エスカレーション がONかOFFになっていることを示す。
	NetView、ObjectViewとTroubleViewで使用。 ホストとサービスのステータス を示す。 緑 = 稼動 (Up)、黄 = 保留 (Pending)、赤 = 停止 (Down)、灰 = 未知 (Unknown)
	NetView、ObjectViewとTroubleViewで使用。マウスを乗せた時に選んだ要素に ステータス情報 を表示する。
	TroubleViewで使用。 ホストとサービスが承認状態 を示す。 チェック付の黄 = 承認済みワーニング状態、X付の黄 = 未承認のワーニング状態、 チェック付の赤 = 承認済みクリティカル状態、X付の赤 = 未承認のクリティカル状態、 チェック付の灰 = 承認済み未知状態、X付の灰 = 未承認の未知状態
	ダウンタイム状態 を示めすため、ステータス画面で使用。

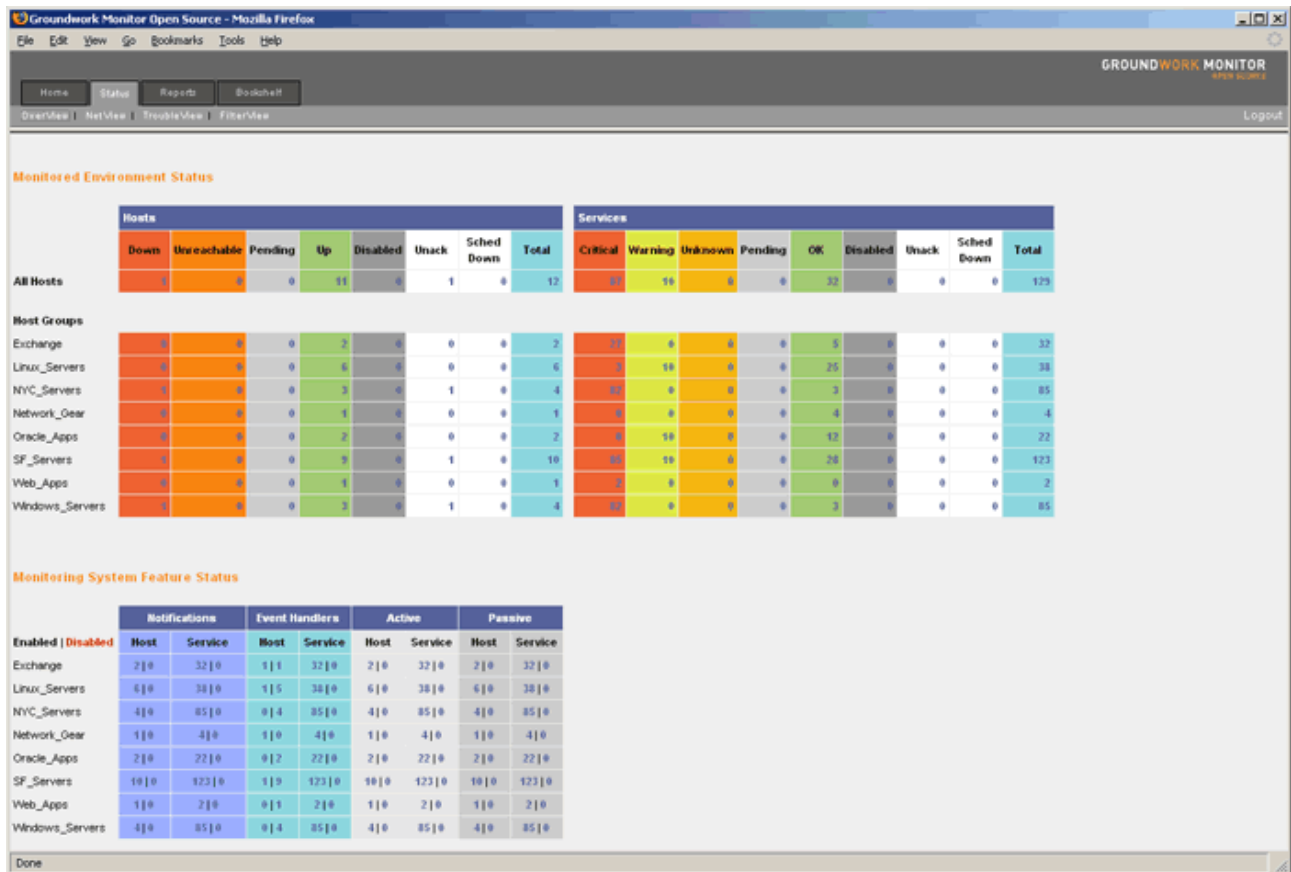
第2章 Overviewを使ったITインフラストラクチャの監視

Overviewについて

Overview画面

ステータスビューに入ったときに最初に表示されるビューがOverviewです。Overviewは、あなたのネットワークインフラストラクチャのひと目で分かる状態表示を提供します。それで、ホストグループ毎のすべてのホストとサービスの現在のステータスもみることができます。この戦略的なオーバービューは、違反、ワーニング、OKサマリを含む、収集された監視情報の即座のサマリを提供します。これは、ホストグループにわたるものと、未承認の問題の両方のサマリを提供するので、どれが重要な問題かを見ることができます。上位レベルのビューから、ドリルダウンすることができます。下図は、Overviewの全体を示します。このビューの異なるセクションが、**監視対象環境ステータス (Monitored Environment Status)**と、**監視システム機能ステータス (Monitoring System Feature Status)**を盛り込みます。

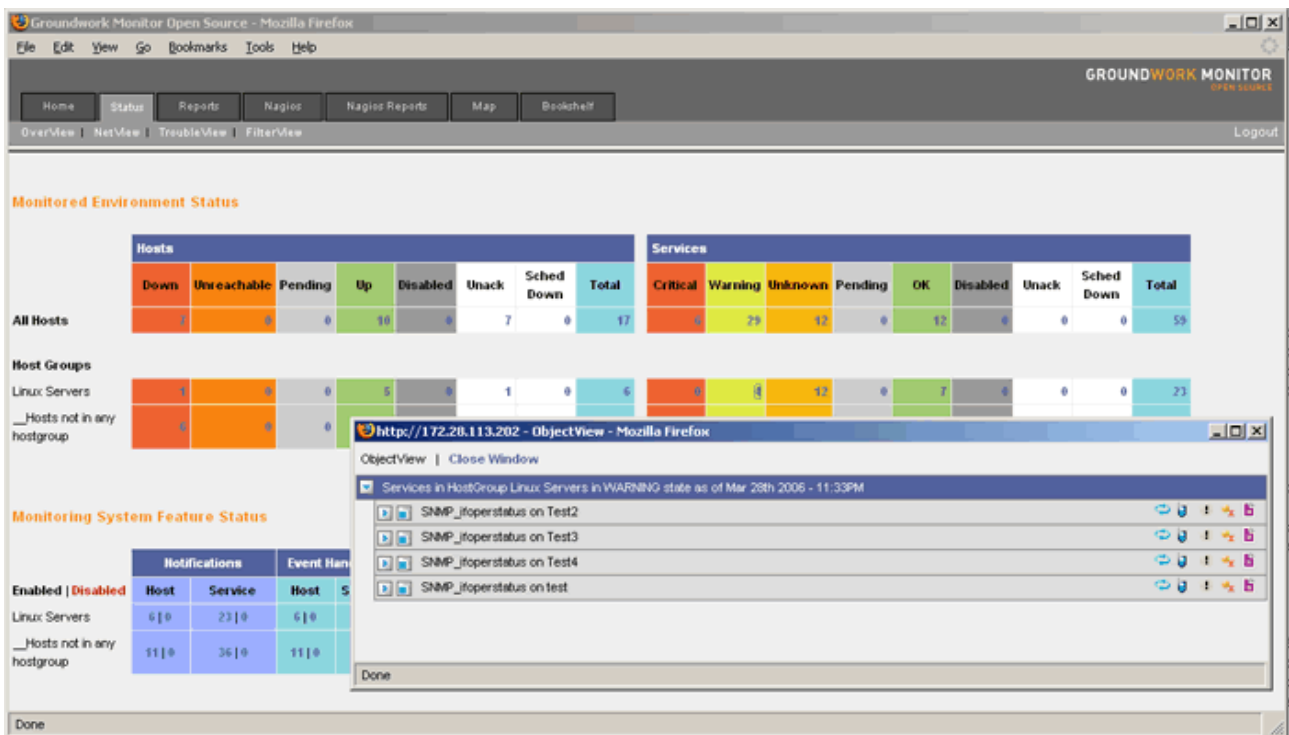
図2.2.1. ステータスビューア - Overview



ObjectView

Overview内のステータスの数字は、特定の情報にリンクされています。数字を選ぶと、特定のホストやサービスおよびシステム機能に関するより詳細な情報にドリルダウンすることができます。たとえば、特定のホストグループ(例。Linux_Servers)で現在ワーニング状態にあるサービス(例。SNMP_ifoperstatus)を見るために、ワーニング-サービスの箱の中の数字を選ぶことができます。選ぶと、ObjectViewウィンドウが開き、サービスのステータスと他の詳しい情報が表示されます。Overview内で、NetViewとTroubleViewのように、ドリルダウンして、各ホストやホストグループのためにコマンドやコメントを入力することができます。これから、本セクションで各ビューの操作を説明します。

図2.2.2. ObjectView



監視対象環境ステータス(Monitored Environment Status)

監視対象環境ステータス(Monitored Environment Status)セクションは、ホストグループ毎に一行で表示されます。表示される値は、停止(Down)、到達不可(Unreachable)、保留(Pending)、稼動(Up)、ディスエイブル(Disabled)、未承認(Unacknowledged)および計画停止(Scheduled Down)の各状態にあるホストの数を示しています。合計(total)の行は、各状態にある全ホスト数を示します。注意点として、ホストは複数のホストグループに所属するので、カラムの数値を加算して全ホスト数を求める必要はありません。画面右側に表示されている数値は、クリティカル(Critical)、ワーニング(Warning)、未知(Unknown)、保留(Pending)、正常(OK)、ディスエイブル(Disabled)、未承認(Unacknowledged)および計画停止(Scheduled Down)状態にあるホストのサービスの数を表します。下表でホストとサービスの各状態を説明します。

図 2.2.3. Overview - 監視対象環境ステータス

	Hosts							Total	Services							Total	
	Down	Unreachable	Pending	Up	Disabled	Unack	Sched Down		Critical	Warning	Unknown	Pending	OK	Disabled	Unack		Sched Down
All Hosts	1	0	0	11	0	1	0	12	27	10	0	0	32	0	0	0	129
Host Groups																	
Exchange	0	0	0	2	0	0	0	2	27	0	0	0	5	0	0	0	32
Linux_Servers	0	0	0	6	0	0	0	6	3	10	0	0	25	0	0	0	38
NYC_Servers	1	0	0	3	0	1	0	4	27	0	0	0	3	0	0	0	85
Network_Gear	0	0	0	1	0	0	0	1	0	0	0	0	4	0	0	0	4
Oracle_Apps	0	0	0	2	0	0	0	2	0	10	0	0	12	0	0	0	22
SF_Servers	1	0	0	5	0	1	0	10	27	10	0	0	28	0	0	0	123
Web_Apps	0	0	0	1	0	0	0	1	2	0	0	0	0	0	0	0	2
Windows_Servers	1	0	0	3	0	1	0	4	27	0	0	0	3	0	0	0	85

表 2.2.1. ホストの状態

ホスト	
停止 (Down)	停止状態は、ホストは正常でない(non-OK)の状態にあり、ホスト定義の中の max_check_attempts オプションで指定された回数分再チェックされたものです。
到達不能(Unreachable)	到達不能状態は、ホストに到達できないか、正常でない(non-OK)の状態です。このディレクティブは、ホスト定義の中の notification_options 引数で指定されません。
保留 (Pending)	保留状態は、通常、一時的なもので、その状態がまだはっきりしないことを意味します。
稼動 (Up)	稼動状態は、ホストが正常 (OK) 状態で完全に動作しているいます。
ディスエイブル (Disabled)	ディスエイブル状態はホストがDisableにセットされ、実施できない状態です。
未承認 (Unacknowledged)	未承認は、いくつかのホストやホストグループのアラームが、まだ承認 (acknowledge)されていないことを示します。
計画停止 (Scheduled Downtime)	Nagiosでは、監視対象のホストとサービスの予定した時間帯の計画停止ができます。このことは、たとえば、アップグレードのためにサーバを停止する時に便利です。ホストとサービスが計画停止時間帯にあるとき、そのホストやサービスのための通知は抑制されます。Overviewの数は、何台のホストが計画停止になっているかを警告します。
合計 (Total)	合計のカラムは、監視されているホストやホストグループの総数を表します。

表 2.2.2. サービスの状態

サービス	
クリティカル (Critical)	クリティカルは、使用できないか停止ですぐに対処が必要な、ホストや ホストグループのサービスの数です。例: <code>ssh_sendmail-services CRITICAL - Cannot make SSL connection 15011: error:142342424FC:SSL:...</code> 。
ワーニング (Warning)	ワーニングは、ゆくゆくは対処が必要な何かを持つホストやホストグループのサービスの数です。例: <code>ssh_ldap-services WARNING NAGIOS host key verification failed..</code>
未知 (Unknown)	未知は、他の状態で認識されていないか認識できない、ホストやホストグループのサービスの数です。例: <code>ssh_sendmail-services UNKNOWN NAGIOS check_smtp: Warning time must be a positive integer</code>
保留 (Pending)	保留は、まだ判断されていないホストやホストグループのサービスの数です。通常、保留状態は長期間そのままにはなりません。
正常 (OK)	正常、モニタがOK、あるいは正しく機能しているホストやホストグループのサービスの数です。
ディスエイブル (Disabled)	ディスエイブルは、disabledにセットされ、実施できないホストやホストグループのサービスの数です。これら、ディスエイブルされたサービスに対しては、アラームは発生されません。
未承認 (Unacknowledged)	未承認は、まだ承認されていないホストやホストグループのサービスの数です。
計画停止 (Scheduled Downtime)	Nagiosでは、監視対象のホストとサービスの予定した時間帯の計画停止ができます。このことは、たとえば、アップグレードのためにサーバを停止する時に便利です。ホストとサービスが計画停止時間帯にあるとき、そのホストやサービスのための通知は抑制されます。この数値は、全てのホストとホストグループ内のいくつかのサービスが、停止時間としてスケジュールされているかを示します。
合計 (Total)	合計のカラムは、全てのホストやホストグループのための監視されているサービスの総数を表します。

監視システム機能ステータス(Monitoring システム Feature Status)

監視システム機能ステータスは、ホストグループ毎のモニタ機能が監視実施(enabled)と監視停止(disabled)になっているホストとサービスの数を示します。この機能設定には、下表に示すように、**通知(Notifications)**、**イベントハンドラ(Event Handlers)**、**アクティブ(Active)**および**パッシブ(Passive)**があります。

図 2.2.4. 監視システム機能ステータス

Monitoring System Feature Status								
Enabled Disabled	Notifications		Event Handlers		Active		Passive	
	Host	Service	Host	Service	Host	Service	Host	Service
Linux Servers	6 0	23 0	6 0	23 0	6 0	23 0	6 0	23 0
__Hosts not in any hostgroup	11 0	36 0	11 0	36 0	11 0	36 0	11 0	36 0

表 2.2.3. 機能設定

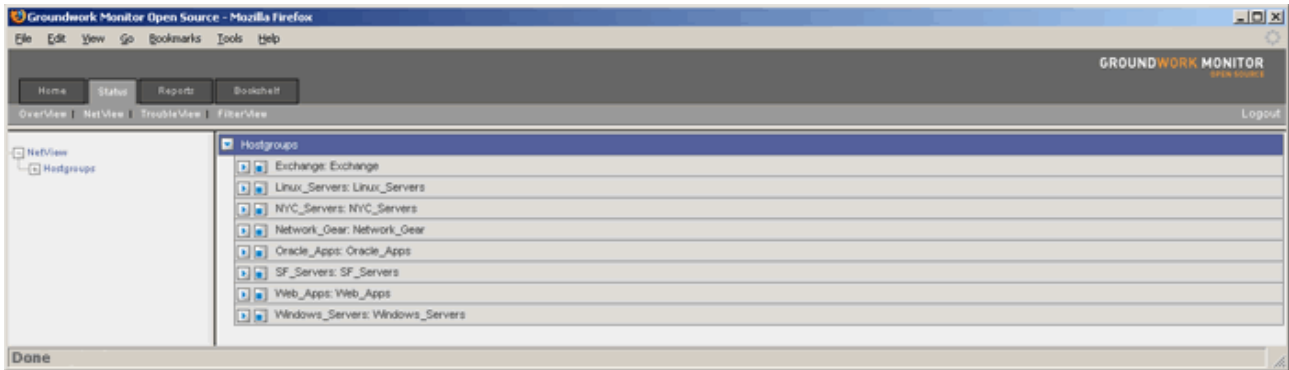
機能	説明
通知(Notifications)	各ホストとサービス定義は、通知を送るかどうかを決めるオプションを含んでいます。ここで選択されたホストグループ内の通知(Notifications)のステータスが通知実施(enabled) 停止(disabled)であるホストとサービスの数を示します。
イベントハンドラ(Event Handlers)	イベントハンドラ(ホストとサービス)は、誰かに通知する前にプロアクティブに問題を解決するために使用するオプションなコマンドです。それらは、ホストやサービスの状態変化が発生したときにはいつでも実行されます。このイベントハンドラ状態は、選択されたホストグループのイベントハンドラのステータスが実施(enabled) 停止(disabled)であるホストとサービスの数を示します。
アクティブ(Active)	アクティブチェックは、Nagiosによって開始されるホストとサービスチェックです。このアクティブチェック状態は、選択されたホストグループのアクティブチェック状態が実施(enabled) 停止(disabled)であるホストとサービスの数を示します。
パッシブ(Passive)	パッシブチェックは、外部アプリケーションによって行われるホストとサービスチェックです。このパッシブチェック状態は、選択されたホストグループのパッシブチェック状態が実施(enabled) 停止(disabled)であるホストとサービスの数を示します。

第3章 NetViewを使ったITインフラストラクチャの監視

NetViewについて

NetViewは、ネットワークインフラストラクチャ全体の階層的なビューです。それは、監視している全てのホストとサービスの現在状態を見せてくれます。目的の場所に着いたら、チェックを停止、停止をスケジュールしたり、ホストやサービスのコメントの参照や追加など、適切なホストやサービスコマンドを実行することができます。

図 2.3.1. ステータスビューア - NetView



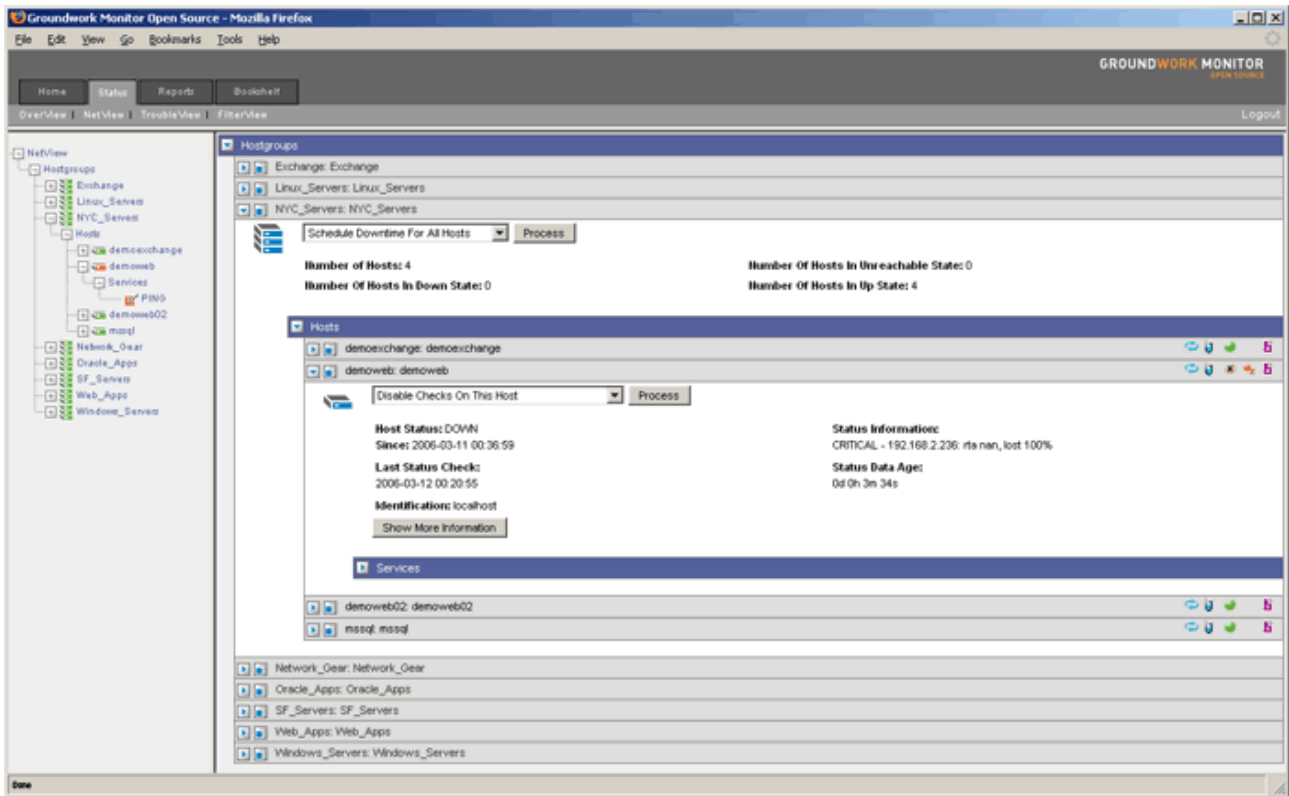
ドリルダウン

NetViewのウィンドウは、二つのフレームから構成されます。左のフレームで、オペレータはナビゲーションツリーのホストグループのレベルから、特定のホストやサービスまでナビゲートすることができます。個々のホストグループ、ホストやサービスのステータスは、アイコンの色で表されます。☑は、クリティカルを表します。ナビゲーションアイコンの完全なリストは、表2.1.1.ナビゲーションツールを参照してください。左のナビゲーションフレームでオブジェクトを選べると、右フレームの表示が変わります。

右フレームは選ばれたオブジェクトの詳細を示します。右フレームでは、オブジェクトのドリルダウンアイコンを選択することでナビゲートし、▶で情報画面を拡大したり、◀で縮小、つまり広げたオブジェクト全てをグループ化した表題の中に折り込んだり、そして、📄で複製を作る、つまり別の独立したObjectViewウィンドウに入ってオブジェクトの詳細を参照したりコマンドを実行したりすることができます。

注意: ホストグループをナビゲーションツリーの中やObject Viewで開くと、現時点のホストのリストが表示されます。このホストのリストは、コンフィギュレーション変更が行われても、ダイナミックにリフレッシュされません。リストをリフレッシュするには、ホストグループオブジェクトを一度閉じて、開いてください。また、ナビゲーションツリーの中やObject Viewでホストを開くと現時点のサービスのリストが表示されます。このサービスのリストは、コンフィギュレーション変更が行われても、ダイナミックにリフレッシュされません。リストをリフレッシュするには、ホストオブジェクトを一度閉じて、開いてください。

図 2.3.2. ステータスビューア - ドリルダウン

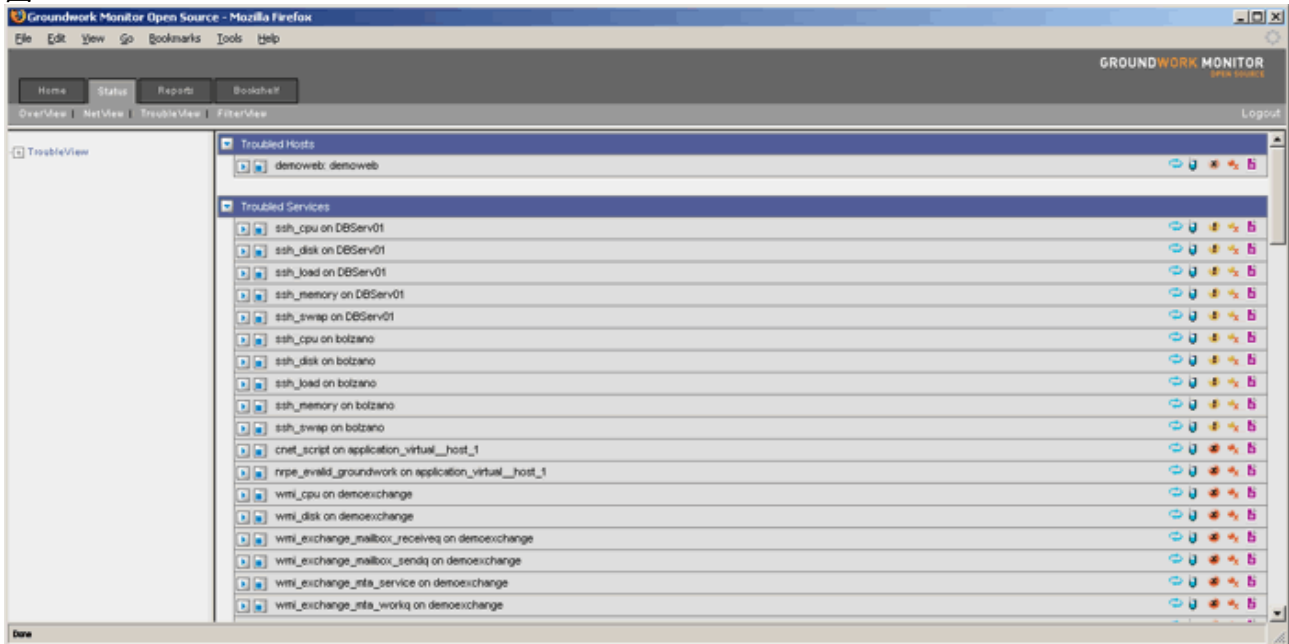


第4章 TroubleViewで障害のあるホストとサービスを見る

TroubleViewについて

TroubleViewは、異常(たとえば、クリティカルや停止)状態にあって、調子が良くない、全てのホストとサービスを監視するビューです。このビューで、対処が必要な赤と黄色のホストやサービスのみをすばやく見ることができます。Overview とNetViewのように、一度目的の場所に至ったら、ホストやサービスのコメントの参照や追加など、適切なホストやサービスコマンドを実行することができます。

図 2.4.1. TroubleView



ホストとサービスのステータス



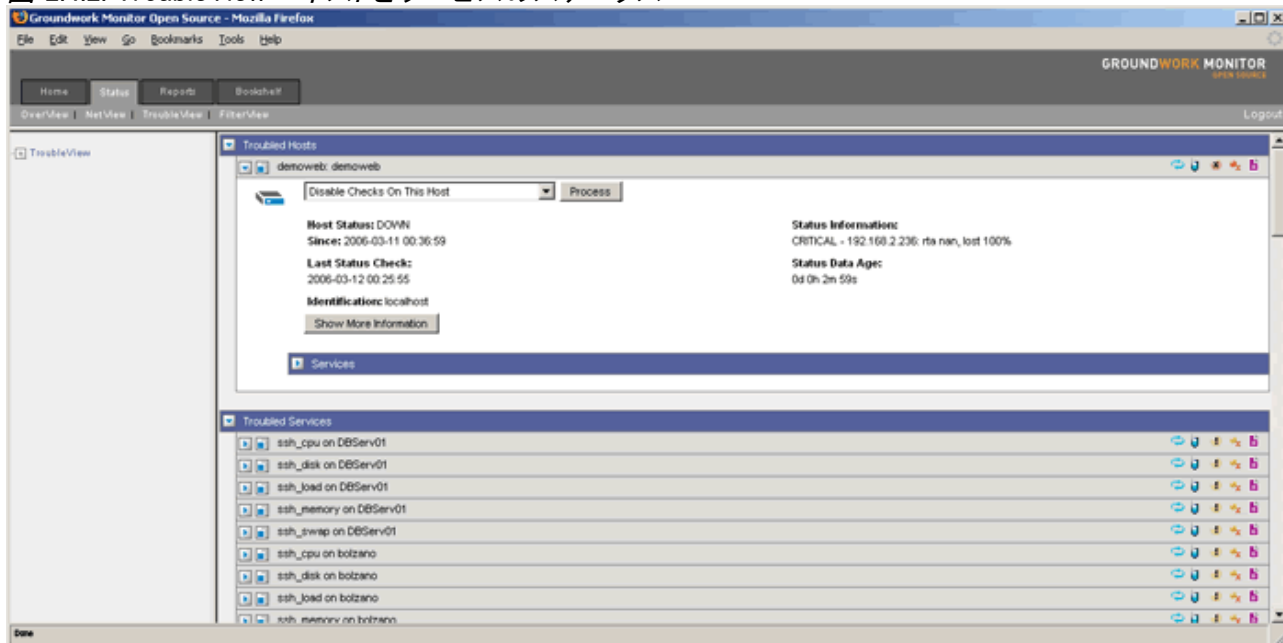
このビューからホストやサービスを  で開いて、選んだホストやサービスのステータス情報を参照できます。また、 (clone) ボタンを選び、ホストやサービスを独立したウィンドウに分けることができます。NetViewで説明したように、異常状態のホストとサービスの詳細な情報にドリルダウンし適切なコマンドを実行することができます。

図 2.4.2. TroubleView - ホストとサービスのステータス



第5章 FilterViewを使って監視データをフィルタする

FilterViewについて

FilterViewは、検索条件、つまりユーザが作成したフィルタで制限して表示するツールです。ひとつの便利な例は、オペレータがアクセスする必要がある特定の問題についてのホストやサービスの名前のフィルタでしょう。他の例は、多分、全てのメールに関連するホストとサービスを分離して参照することでしょう。さらにもうひとつの例としては、サンフランシスコにある全プリンターのフィルタです。たとえば、ホストの名前を *location.*type* の形式にしている場合、ホストの判断基準として、ホストのエイリアスが、*sf.*printer* に一致するなどです。

下記に、フィルタを作成する際に表示されるフォームを示します。判断基準(Criteria)は、多分、ホストグループ、ホストおよびサービスをベースとし、下表のようにそれぞれに複数の判断基準と一緒に使用されるでしょう。作成されたフィルタは、各ユーザIDのプロファイルの一部で、ログインで固有です。他のユーザは、作成されたフィルタを参照したり、使ったり、削除したりはできません。

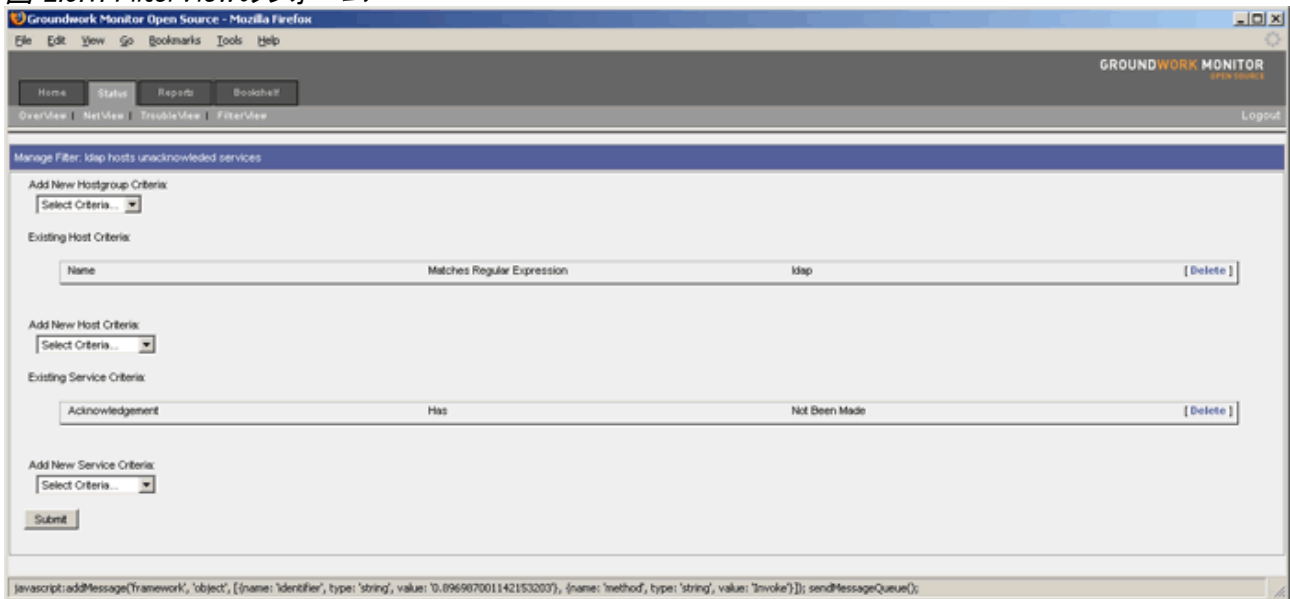
フィルタのセットアップ

1. StatusオプションからFilterViewを選択します。
2. Filter Nameボックスに新しいフィルタの名称を入力します。
3. **Create**を選択。Create Filter画面が表示されます。
4. **ホストグループ、ホストやサービスのためのクライテリア(判断基準)**を設定します(各カテゴリで使用できる個別の判断基準は、表 2.5.1を参照してください)。
5. **Submit**を選びます。

表 2.5.1. Filterviewの判断基準

	ホストグループ	ホスト	サービス
Name(名称)	<input type="radio"/>	<input type="radio"/>	
Alias(エイリアス)	<input type="radio"/>	<input type="radio"/>	
Status(ステータス)		<input type="radio"/>	<input type="radio"/>
Acknowledgment(承認)		<input type="radio"/>	<input type="radio"/>
Description(説明)			<input type="radio"/>
Host(ホスト)			<input type="radio"/>

図 2.5.1. FilterViewのフォーム

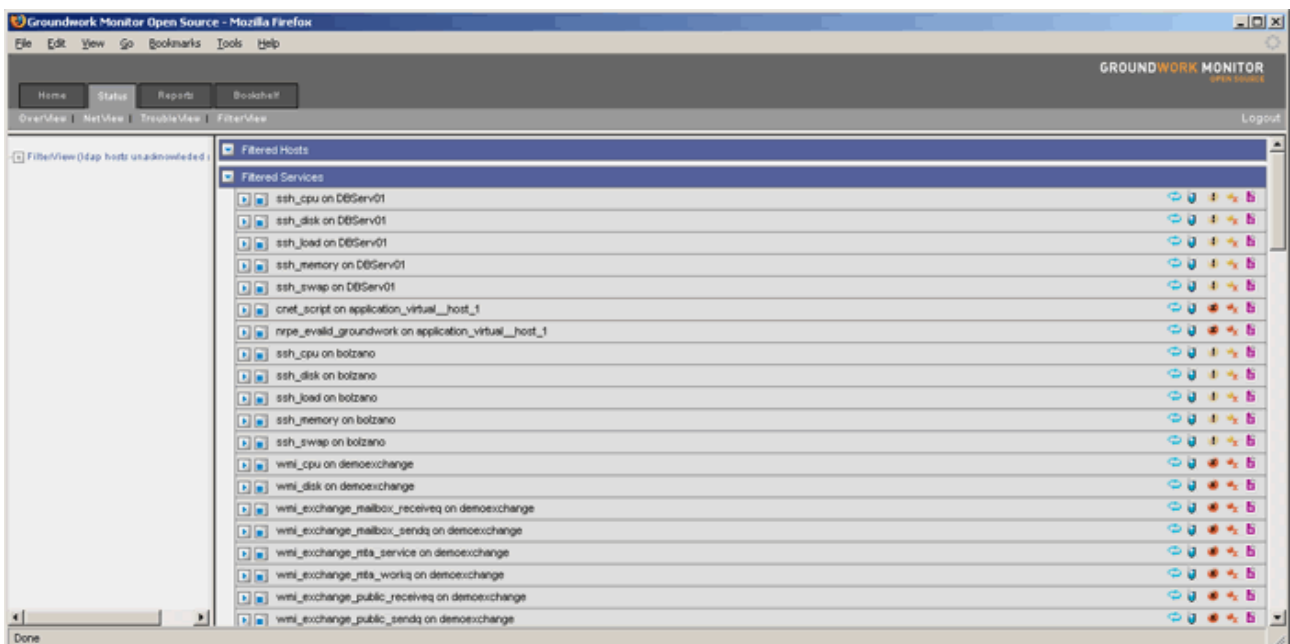


フィルタを実行する

1. Statusオプションから**FilterView** を選択します。
2. **Manage Filters** の下にある既に定義されたフィルターのリストからフィルタを選ぶ。FilterViewはそのフィルタ定義に合致する全ホストとサービスを表示します。使用された現在のフィルタは、左側の枠表示されます。
3. ここで、NetViewとTroubleView内のように、よりはっきりと限定された情報にドリルダウンすることができます。
4. フィルタされていないホストとサービスをリストするために Overview、NetViewやTroubleViewを選びます。

下のイメージは、未承認のサービスを持つ全てのLDAPホストを返すフィルタを実行したアウトプットの例を示します。

図 2.5.2. FilterView - 実行されたフィルタ



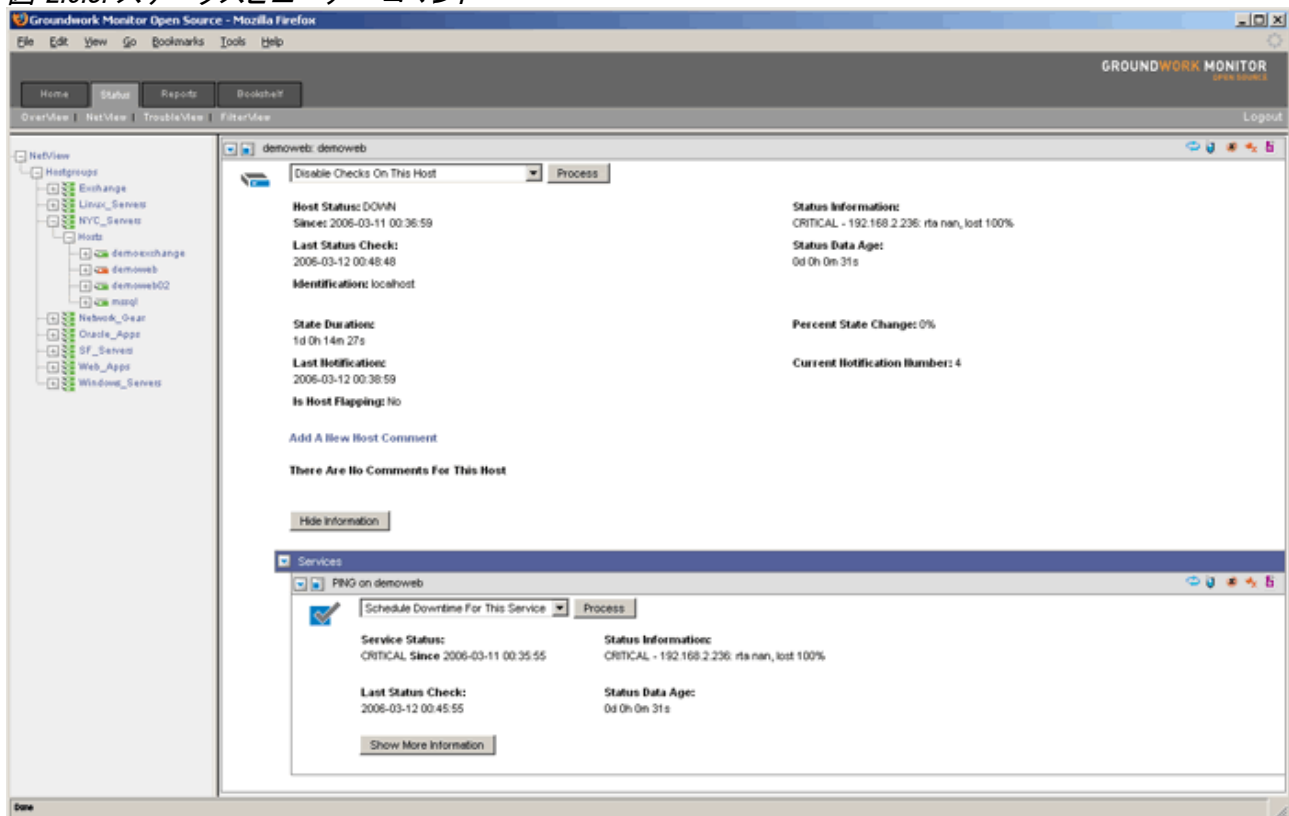
第6章 ステータスビューア内の処理コマンド

コマンド画面のレイアウト

NetView内でホストとサービスコマンドの開始と実行ができ、またホストやサービスのコメントを参照したり追加できます。ホストとサービスのためのコマンド画面は、現在ステータスと前のステータスチェックの日付けと時刻、ステータス情報とステータスデータの古さを含む、ステータス情報を表示します。

加えて、監視対象要素のステータスを示すために使う三つのカラーコード化されたアイコンを見ることができます。完全なリストは、表2.1.1. ナビゲーションツール を参照してください。ドロップダウン・ボックスで、今のイベントに適切なホストとサービスコマンドを開始したり、実行(submit)することができます。

図 2.6.3. ステータスビューア - コマンド



コマンドをコミットする

下記のステップで、コマンドを開始して、コミットするまでを行えます。下記の図はホストの問題を承認するために要求されたコマンドオプションを示します。

1. ドロップダウン・ボックスから適切なコマンドを選びます。表 2.6.1 からの3つの表はホストグループ、ホストとサービスのコマンドのオプションのリストを示します。
2. **Process** を選択します。
3. 別のobjectViewウィンドウが開き、指定されたコマンドの説明を表示します。要求されるコマンドの情報を入力し、**Submit** を選んで、コマンドを実施します。
4. 前のオペレータエントリを見るためにコメントが使用できますし、他の人のためにあなたが追加することもできます。青いリンクを選び、コメントの参照や追加を行います。

図 2.6.4. ステータスビューア - コマンド

The screenshot displays the Groundwork Monitor Open Source interface in a Mozilla Firefox browser. The main content area shows the status for the host 'demoweb: demoweb'. The host status is 'DOWN', with a 'Since' time of 2006-03-11 00:36:59. The last status check was on 2006-03-12 00:48:48. The status information is 'CRITICAL - 192.168.2.236: rta nan, lost 100%'. The status data age is '0d 0h 0m 31s'. The percent state change is 0%, and the current notification number is 4. The host is not flapping. Below the host status, there is a 'Services' section for 'PING on demoweb'. The service status is 'CRITICAL Since 2006-03-11 00:35:55'. The last status check was on 2006-03-12 00:45:55. The status information is 'CRITICAL - 192.168.2.236: rta nan, lost 100%'. The status data age is '0d 0h 0m 31s'. The interface includes a navigation menu on the left with 'NetView' selected, and a top navigation bar with 'Home', 'Status', 'Reports', and 'Bookmarks'. The browser's address bar shows 'Groundwork Monitor Open Source - Mozilla Firefox'.

Groundwork Monitor Open Source - Mozilla Firefox

Home Status Reports Bookmarks

Overview NetView TroubleView FilterView Logout

NetView

- Hostgroups
 - Exchange
 - Linux_Servers
 - NYC_Servers
 - Hosts
 - demoexchange
 - demoweb
 - demoweb02
 - mail
 - Netbios_Osaz
 - Oracle_Apps
 - SF_Servers
 - Web_Apps
 - Windows_Servers

demoweb: demoweb

Disable Checks On This Host Process

Host Status: DOWN
Since: 2006-03-11 00:36:59
Last Status Check: 2006-03-12 00:48:48
Identifications: localhost

Status Information:
CRITICAL - 192.168.2.236: rta nan, lost 100%

Status Data Age:
0d 0h 0m 31s

Percent State Change: 0%

Current Notification Number: 4

State Durations:
1d 0h 14m 27s

Last Notifications:
2006-03-12 00:38:59

Is Host Flapping: No

Add A New Host Comment

There Are No Comments For This Host

Hide Information

Services

PING on demoweb

Schedule Downtime For This Service Process

Service Status:
CRITICAL Since 2006-03-11 00:35:55

Status Information:
CRITICAL - 192.168.2.236: rta nan, lost 100%

Last Status Check:
2006-03-12 00:45:55

Status Data Age:
0d 0h 0m 31s

Show More Information

Done

ホストグループ、ホストとサービスのコマンド説明

下表で、ステータスビューアで使用できる異なるホストグループ、ホストとサービスのコマンドをリストし、違いを説明します。

表 2.6.1. ホストグループのコマンド

ホストグループのコマンド	
Schedule Downtime for all Hosts (全ホストの計画停止)	このコマンドは、指定されたホストグループ内の全ホストの停止時間をスケジュール(計画停止)するために使います。指定された停止時間の間は、Nagiosはそれらのホストに関する通知を送出しません。スケジュールされた停止時間が切れると、Nagiosはそれらのホストに関する通知を通常どおり送じます。計画停止時間は、プログラムのシャットダウンやリスタートでも保持されます。開始と終了時間は、mm/dd/yyyy hh:mm:ssの形式で指定します。固定(fixed)オプションを選ぶと、停止時間は指定した開始と終了時間の間となります。固定(fixed)オプションを選ばない場合、Nagiosは、フレキシブルな停止時間として扱います。フレキシブル停止時間は、(指定した開始と停止時間の間に)ホストが停止して、到達しなくなった時点から始まり、指定した経過時間(Duration)が経過すると終了します。経過時間(Duration)フィールドは、固定(Fixed)の場合は適用されません。
Schedule Downtime for all Services (全サービスの計画停止)	このコマンドは、指定されたホストグループ内の全サービスの停止時間をスケジュール(計画停止)するために使います。指定された停止時間の間は、Nagiosはそれらのサービスに関する通知を送出しません。スケジュールされた停止時間が切れると、Nagiosはそれらのサービスに関する通知を通常どおり送じます。計画停止時間は、プログラムのシャットダウンやリスタートでも保持されます。開始と終了時間は、mm/dd/yyyy hh:mm:ssの形式で指定します。固定(fixed)オプションを選ぶと、停止時間は指定した開始と終了時間の間となります。固定(fixed)オプションを選ばない場合、Nagiosは、フレキシブルな停止時間として扱います。フレキシブル停止時間は、(指定した開始と停止時間の間に)サービスが正常でない(non-OK)になった時点から始まり、指定した経過時間(Duration)が経過すると終了します。経過時間(Duration)フィールドは、固定(Fixed)の場合は適用されません。サービスの計画停止時間は、自動的にそのサービスと関連するホストの停止時間をスケジュールしません。もし、全てのホストについての停止をスケジュールしたい場合は、Schedule Downtime for all Hosts (全ホストの計画停止)をチェックしてください。
Enable Notifications for all Hosts (全ホストの通知を可能にする)	このコマンドは、指定されたホストグループ内の全ホストの通知を可能にするために使います。通知は、ホスト定義の中で定義したホスト状態でのみ送出されます。
Disable Notifications for all Hosts (全ホストの通知を不可にする)	このコマンドは、指定されたホストグループ内の全ホストの通知を抑制するために使います。将来、何らかの通知を送れるようにするには、ホストグループの全ホストの通知を再度、可能にする必要があります。
Enable Notifications for all Services (全サービスの通知を可能にする)	このコマンドは、指定されたホストグループ内の全サービスの通知を可能にするために使います。通知は、ホスト定義の中で定義したサービス状態でのみ送出されます。Enable for Hostsオプションをチェックしない限り、これのみでは、ホストグループ内のホストの通知は可能にはなりません。
Disable Notifications for all Services (全サービスの通知を不可にする)	このコマンドは、指定されたホストグループ内の全サービスの通知を抑制するために使います。将来、何らかの通知を送れるようにするには、ホストグループの全サービスの通知を再度、可能にする必要があります。Disable for Hostsオプションをチェックしない限り、これのみでは、ホストグループ内のホストに関する通知は抑制されません。
Enable Checks for all Services (全サービスのチェックを実施する)	このコマンドは、指定されたホストグループ内の全サービスのアクティブチェックを実施させるために使います。Enable for Hostsオプションをチェックしない限り、これのみでは、ホストグループ内のホストのアクティブチェックを行うようにはなりません。
Disable Checks for all Services (全サービスのチェックを停止する)	このコマンドは、指定されたホストグループ内の全サービスのアクティブチェックを停止させるために使います。'Disable for Hosts'オプションをチェックしない限り、これのみでは、ホストグループ内のホストのアクティブチェックを停止しません。

表 2.6.2. ホストのコマンド

ホストのコマンド	
Disable Checks on this Host (本ホストのチェック停止)	このコマンドはNagiosからの特定ホストにアクティブに行うのステータスチェックを一時的に停止します。Nagiosがこのホストのステータスチェックを必要とした場合、チェックを停止する前の状態と同じ状態と仮定します。
Enable Checks on this Host (本ホストのチェック実施)	このコマンドはこのホストへのアクティブチェックを可能にするのに使用します。
Re-schedule the Next Check (次回チェックの再スケジュール)	このコマンドは、特定のホストの次回チェックをスケジュールするのに使います。Nagiosは、指定された時間にホストのチェックを行うよう再キューイングします。強制チェック (force check) オプションを選んだ場合、Nagiosはいつそのチェックがスケジュールされているかやそのホストに対してチェックが可能になっているかどうかに関わらず、ホストのチェックを強行します。
Schedule Check for all Services of this Host (本ホストの全サービスのチェックをスケジュール)	このコマンドは、特定のホストの全サービスの次回チェックをスケジュールするのに使います。強制チェック (force check) オプションを選んだ場合、Nagiosはいつスケジュールされているチェックが起こるかや、それらのサービスがのチェックが可能になっているかどうかに関わらず、全てのサービスのチェックを強行します。
Submit Passive Check Result (パッシブチェックの結果提供)	このコマンドは、特定のホストのパッシブチェックの結果を提供させるのに使います。
Enable Passive Checks (パッシブチェック可能)	このコマンドは、特定のホストの外部コマンドファイルの中にあるパッシブホストチェックの結果をNagiosが受けとることを可能にするのに使います。
Disable Passive Checks (パッシブチェック不可)	このコマンドは、特定のホストの外部コマンドファイルの中にあるパッシブホストチェックの結果をNagiosが受けとることを停止するのに使います。このホスト上に見つかった全てのパッシブチェック結果は、無視されます。
Start Obsessing over this Host (本ホストへのObsessing over開始)	このコマンドは、Nagiosが特定のホストにobsessing overを開始させるのに使います。
Stop Obsessing over this Host (本ホストへのObsessing over停止)	このコマンドは、Nagiosが特定のホストにobsessing overを停止させるのに使います。
Enable Event Handler (イベントハンドラ実施可)	このコマンドは、Nagiosに必要なとき(それが定義されていれば)、特定のサービスに対するホストイベントハンドラを実行できるようにするのに使います。
Disable Event Handler (イベントハンドラ不可)	このコマンドは、Nagiosが特定のサービスに対するホストイベントハンドラ実行するのを一時的に抑止するのに使います。
Acknowledge this Host Problem (ホスト問題の承認)	このコマンドは、ホストの問題を承認(acknowledge)するのに使います。ホストの問題を承認すると、その問題に対する通知は、ホスト状態が変化(例:回復)するまで一時的に停止されます。このホストに対するコンタクト(連絡先)は、承認の通知を受けるので、彼らは誰かがこの問題に対処していることが分かります。さらに、ホストに対するコメントを追加します。コメントフィールドには、あなたの名前とあなたが何をやっているかの短い説明を入力するようにしましょう。もし、ホストコメントをNagiosの再起動後も保持したいのであれば、'Persistent'(持続) チェックボックスをチェックします。承認の通知を適当なコンタクト(連絡先)に送りたくない場合は、'Send Notification' (通知送出)チェックボックスのチェックをはずします。
Remove Acknowledgment of Problem (問題承認の解除)	このコマンドは、特定のホスト問題の承認(Acknowledgmen)を取り除くのに使います。一度、承認が取り除かれると、そのホスト問題に関する通知が送出されるでしょう。注意:承認の解除は、元々承認に関連つけられていたホストコメントを削除しません。もしそうしたいのであれば、それを削除する必要があります。
Disable Notifications (通知停止)	このコマンドは、特定ホストについての通知送出を抑止するのに使います。将来、何らかのアラートを送出する前には、通知を再度実施(Enable)にする必要があります。注意:このコマンドは、このホストに関連するサービスについての通知は、停止しません。
Enable Notifications (通知実施)	このコマンドは、特定ホストについての通知送出を可能にするのに使います。通知は、ホスト定義の中で定義したホスト状態についてのみ送出されます。注意:このコマンドは、このホストに関連するサービスについては、通知を可能にはし

ホストのコマンド	
	ません。
Delay Next Notification (次回通知の延期)	このコマンドは、特定ホストについて、次回の問題通知の送出手を遅らせるのに使います。通知の延期は、次の通知が送出されるスケジュールの前にホスト状態が変化したら、無視されます。このコマンドは、現在稼動(UP)状態にあるホストでは、なんの影響もありません。
Enable Flap Detection (フラッピング検出を実施する)	このコマンドは、特定ホストについてのフラッピング検出を実施するのに使います。フラッピング検出がプログラム全体で停止されていれば、これは効果がありません。
Disable Flap Detection (フラッピング検出を停止する)	このコマンドは、特定ホストについてのフラッピング検出を停止するのに使います。
Schedule Downtime (停止時間スケジュール)	このコマンドは、特定ホストについての停止時間をスケジュールするのに使います。指定された停止時間の間、Nagiosはそのホストに関する通知を送出しません。スケジュールされた停止時間が満了したら、Nagiosはこのホストに対する通知を、通常どおり送出手します。計画停止時間は、プログラムのシャットダウンやリスタートでも保持されます。開始と終了時間は、mm/dd/yyyy hh:mm:ssの形式で指定します。固定(fixed)オプションを選ぶと、停止時間は指定した開始と終了時間の間となります。固定(fixed)オプションを選ばない場合、Nagiosは、“フレキシブル”な停止時間として扱います。フレキシブル停止時間は、(指定した開始と停止時間の間に)ホストが停止して、到達しなくなった時点から始まり、指定した経過時間(Duration)が経過すると終了します。経過時間(Duration)フィールドは、固定(Fixed)の場合は適用されません。

表 2.6.3. サービスのコマンド

サービスのコマンド	
Schedule downtime for this Service (サービス停止時間をスケジュール)	このコマンドは、特定サービスについての停止時間をスケジュールするのに使います。指定された停止時間の間、Nagiosはそのサービスに関する通知を送出しません。スケジュールされた停止時間が満了したら、Nagiosはこのサービスに対する通知を、通常どおり送じます。計画停止時間は、プログラムのシャットダウンやリスタートでも保持されます。開始と終了時間は、mm/dd/yyyy hh:mm:ssの形式で指定します。固定(fixed)オプションを選ぶと、停止時間は指定した開始と終了時間の間となります。固定(fixed)オプションを選ばない場合、Nagiosは、“フレキシブル”な停止時間として扱います。フレキシブル停止時間は、(指定した開始と停止時間の間に)サービスが正常でない(non-OK)になった時点から始まり、指定した経過時間(Duration)が経過すると終了します。経過時間(Duration)フィールドは、固定の場合は適用されません。
Disable Checks on this Service (サービスのチェックを停止)	このコマンドは、サービスのアクティブチェックを停止するのに使います。
Reschedule Next Check (次回チェックの再スケジュール)	このコマンドは、特定のサービスの次回のチェックをスケジュールするのに使います。Nagiosは、あなたが指定した時間にサービスをチェックするよう再キューイングします。強制チェック(force check)オプションを選んだ場合、Nagiosはいつスケジュールされているチェックが起こるかや、それらのサービスがのチェックが可能になっているかどうかに関わらず、全てのサービスのチェックを強行します。
Enable Checks (チェックを可能にする)	このコマンドは、サービスのアクティブチェックを実施可能するのに使います。
Submit Passive Check Result (パッシブチェックの結果提供)	このコマンドは、特定のサービスのパッシブチェックの結果を提供させるのに使います。それは、収束したセキュリティ関連のサービスを一度OK状態にリセットするのに、特に便利です。
Disable Passive Checks (パッシブチェック不可)	このコマンドは、特定のサービスのための外部コマンドファイルの中にあるパッシブサービスチェックの結果をNagiosが受けとることを停止するのに使います。見つかったこのサービスのための全てのパッシブチェック結果は、無視されます。
Enable Passive Checks (パッシブチェック可能)	このコマンドは、特定のサービスのための外部コマンドファイルの中にあるパッシブサービスチェックの結果をNagiosが受けれるようにするのに使います。
Acknowledge Problem (問題の承認)	このコマンドは、サービスの問題を承認(acknowledge)するのに使います。サービスの問題を承認すると、その問題に対する通知は、サービス状態が変化(例:回復)するまで一時的に停止されます。このサービスに対するコンタクト(連絡先)は承認の通知を受けられるので、彼らは誰かがこの問題に対処していることが分かります。さらに、サービスに対するコメントを追加します。コメントフィールドには、あなたの名前とあなたが何をやっているかの短い説明を入力するようにしましょう。もし、サービスコメントをNagiosの再起動後も保持したいのであれば、'Persistent'(持続)チェックボックスをチェックします。承認の通知を適当なコンタクト(連絡先)に送りたいくない場合は、'Send Notification'(通知送出)チェックボックスのチェックをはずします。
Remove Problem Acknowledgment (問題承認の解除)	このコマンドは、特定のサービス問題の承認(Acknowledgmen)を取り除くのに使います。一度、承認が取り除かれると、そのサービス問題に関する通知が送出されるでしょう。注意:承認の解除は、元々承認に関連つけられていたサービスコメントを削除しません。もしそうしたいのであれば、それを削除する必要があります。
Disable Notifications (通知停止)	このコマンドは、特定サービスについての通知送出を抑制するのに使います。将来、何らかのアラートを送出する前には、このサービスに対する通知を再度実施(Enable)にする必要があります。
Delay Next Notification (次回通知の延期)	このコマンドは、特定サービスについて、次回の問題通知の送出を遅らせるのに使います。通知の延期は、次の通知が送出されるスケジュールの前にサービス状態が変化したら、無視されます。このコマンドは、現在OK状態にあるサービスでは、なんの影響もありません。
Enable Notifications (通知実施)	このコマンドは、特定サービスについての通知送出を可能にするのに使います。通知は、サービス定義の中で定義したサービス状態タイプについてのみ送出されます。
Disable Event Handler	このコマンドは、一時的にNagiosが特定サービスについてのサービスイベントハンドラを実行するのを抑制するのに使います。

サービスのコマンド	
(イベントハンドラ不可)	
Enable Event Handler (イベントハンドラ実施可)	このコマンドは、Nagiosに必要なとき(それが定義されていれば)、特定のサービスに対するサービスイベントハンドラを実行できるようにするのに使います。
Disable Flap Detection (フラッピング検出を停止する)	このコマンドは、特定サービスについてのフラッピング検出を停止するのに使います。
Enable Flap Detection (フラッピング検出を実施する)	このコマンドは、特定サービスについてのフラッピング検出を実施するのに使います。フラッピング検出がプログラム全体で停止されていれば、これは効果がありません。

第7章 ステータスビューアの使い方ノウハウ

本章では、OverView、NetView、TroubleViewとFilterViewについて、「何々するにはどうするか」のシナリオを使って、GroundWork Monitor Open Sourceのステータスビューアの操作について復習します。

- ホスト/サービスのコメントを見たり追加するにはどうするか?
- 監視対象ホストグループ、ホストとサービスの拡張ビューを表示するにはどうするか?
- ホストグループ、ホストとサービスの情報を独立したObjectViewウィンドウに表示するにはどうするか?
- ホストやサービスコマンドを開始するにはどうするか?
- ステータスフィルタを使うにはどうするか?
- フィルタを編集したり、削除するにはどうするか?

ホスト/サービスのコメントを見たり追加するにはどうするか?

コメントは、問題のあるホスト/サービスについて管理者がコミュニケーションするのに良い手段です。もし継続(Persistent)オプションをチェックしなければ、そのコメントは、Nagiosが再起動されたときに自動的に削除されます。


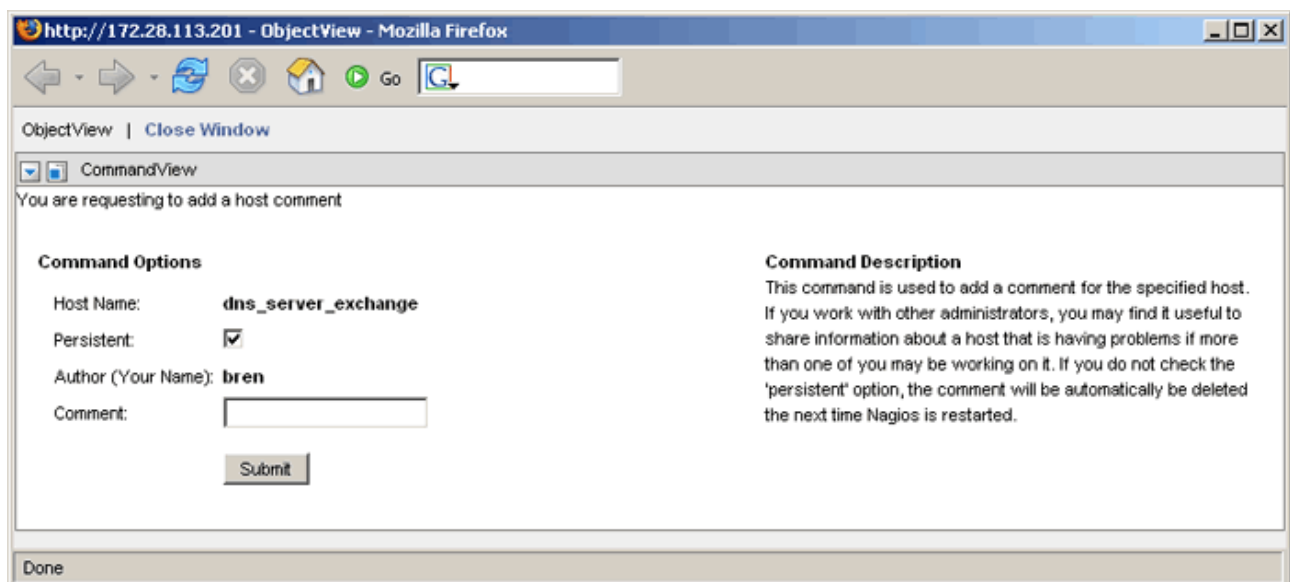
1. OverView、NetViewとTroubleViewにおいて、ObjectView ウィンドウに入るために、アイコンをクリックします。ObjectView内では、ホストやサービスのために前に入力したコメントを見ることができ、新しいホストやサービスのコメントを追加することができます。画面で詳細なビューを表示しない場合、**Show More Information** を選びます。元に戻すためには、**Hide Information** を選びます。
2. 新しいコメントを追加するには、**Add a new Host/Service Comment** を選びます。下に示す**CommandView**画面で、提供されているスペースにコメントを追加し、Submitを選びます。

図 2.7.1. ステータスビューアでのコメントの参照と追加



ObjectView | Close Window

CommandView

You are requesting to add a host comment

Command Options	Command Description
Host Name: dns_server_exchange	This command is used to add a comment for the specified host. If you work with other administrators, you may find it useful to share information about a host that is having problems if more than one of you may be working on it. If you do not check the 'persistent' option, the comment will be automatically be deleted the next time Nagios is restarted.
Persistent: <input checked="" type="checkbox"/>	
Author (Your Name): bren	
Comment: <input type="text"/>	

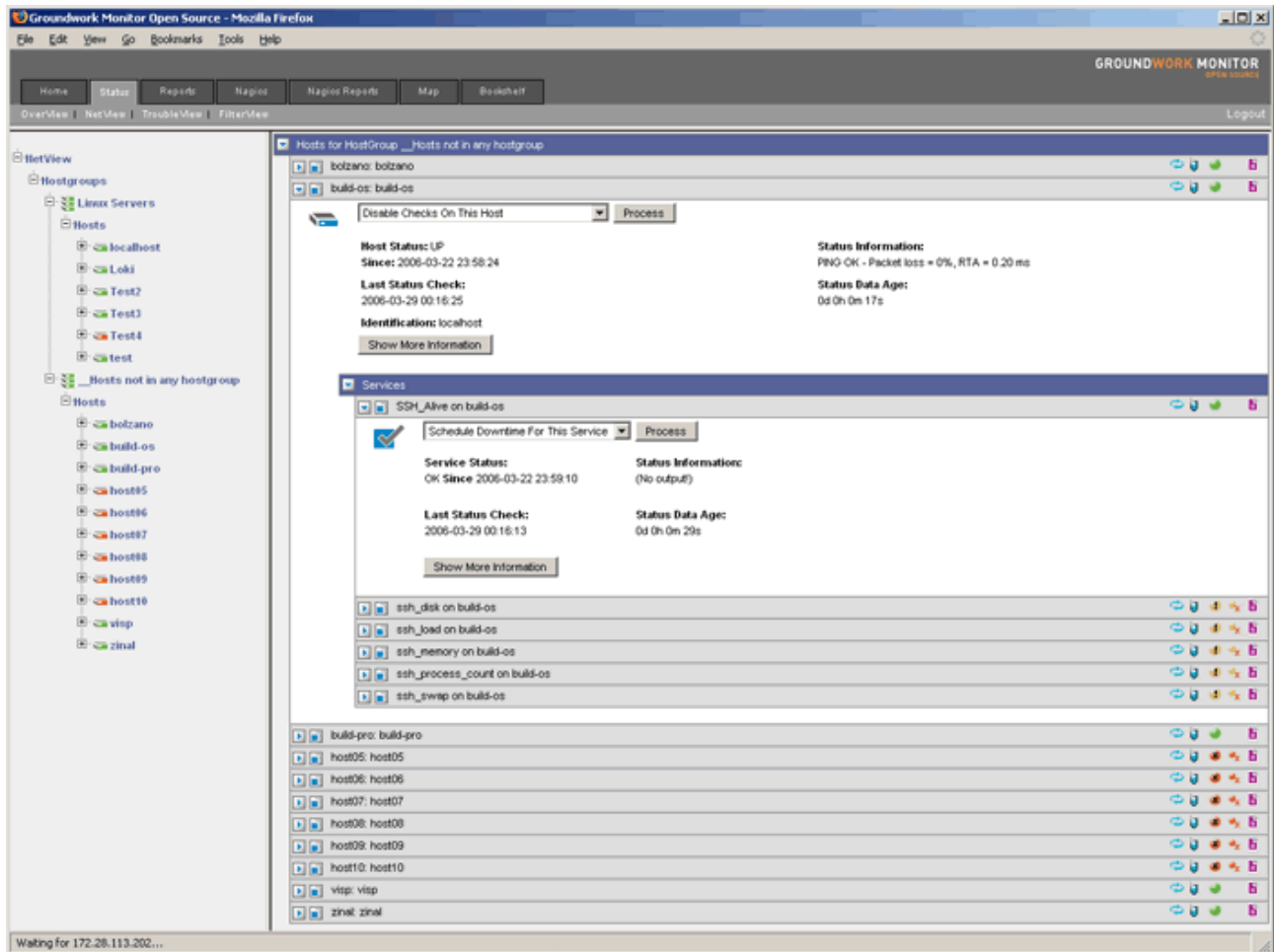
Submit

Done


監視対象ホストグループ、ホストとサービスの拡張ビューを表示するにはどうするか？

1. NetViewで、拡張することのできる監視対象のホストグループのビューを開き、続けてホストとサービスを開くためには、左枠のナビゲーションツリーを使います。📁 のように色分けされたアイコンは、各モニターの状態を表します、このアイコンは緑なのでOKです。NetViewの右枠も使うことができます。
▶ アイコンを選んで、ホストグループを拡張してホストとサービスにします。これらの二つやり方が下の図 2.7.2に表示されています。

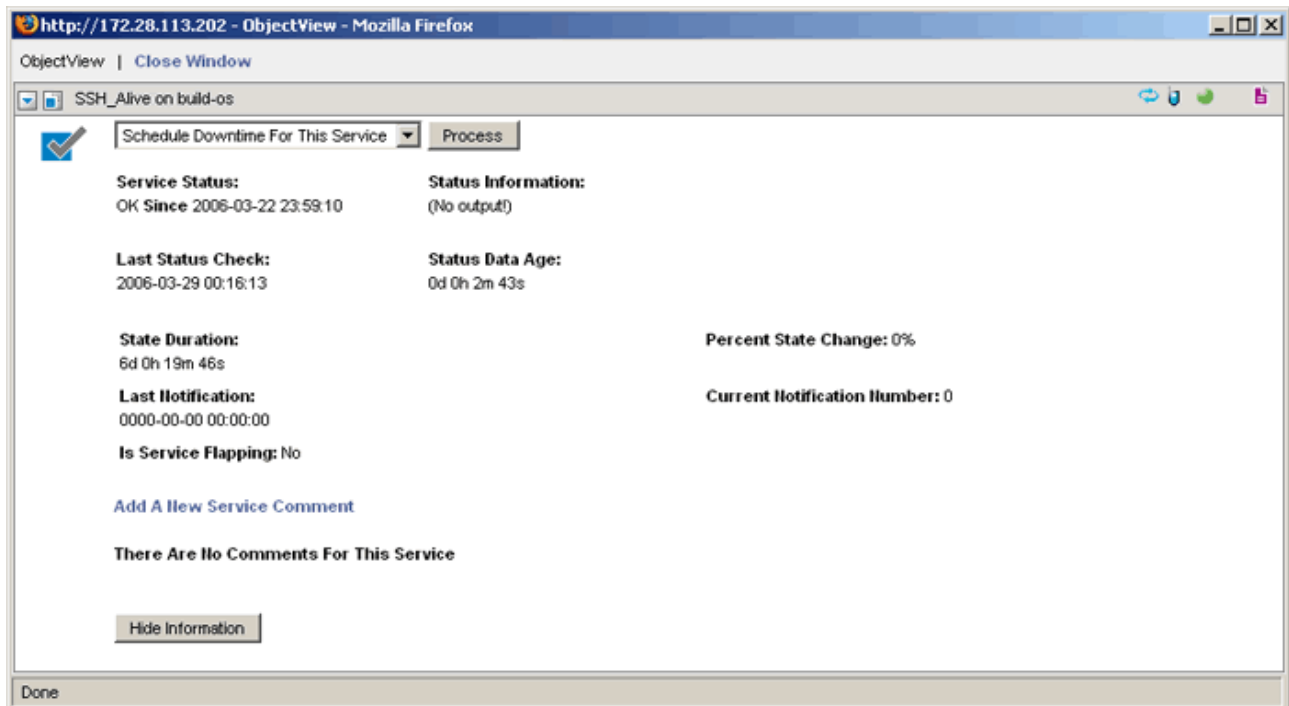
図 2.7.2. 監視対象ホストグループの拡張可能なビュー



ホストグループ、ホストとサービスの情報を独立したObjectViewウィンドウに表示するにはどうするか？

1. NetView内で、ホストグループ、ホストやサービスの下で、独立したObjectViewウィンドウ内にホストグループ、ホストとサービス情報を表示できるようにするために、クローンアイコン  を選びます。ObjectViewウィンドウによって、NetViewや他のビューのデータの参照を続けながら、あなたが選んだモニタに眼を光らせることができます。ObjectViewウィンドウは、ステータスビューアの全てのビューからアクセスすることができます。

2.7.3. ObjectView

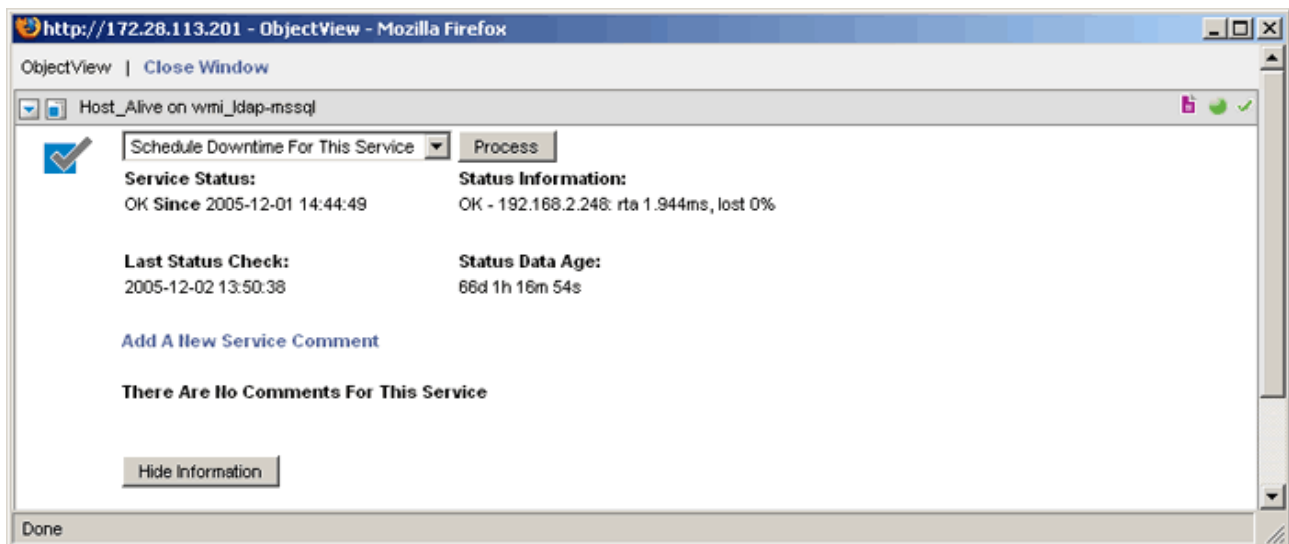


ホストやサービスコマンドを開始するにはどうするか？

ObjectView、NetView、TroubleViewやFilterViewで、ホストやサービスのコマンドを開始できます。

1. 下記のイメージで表示するように、ドロップダウン・ボックスを選びホストやサービスのために適切なコマンドを選んで、**Process** を選択します。
2. **CommandView** 画面が、コマンドとオプションおよび説明を表示します。要求された情報を入力し、コマンドを実行するため **Submit** を選びます。

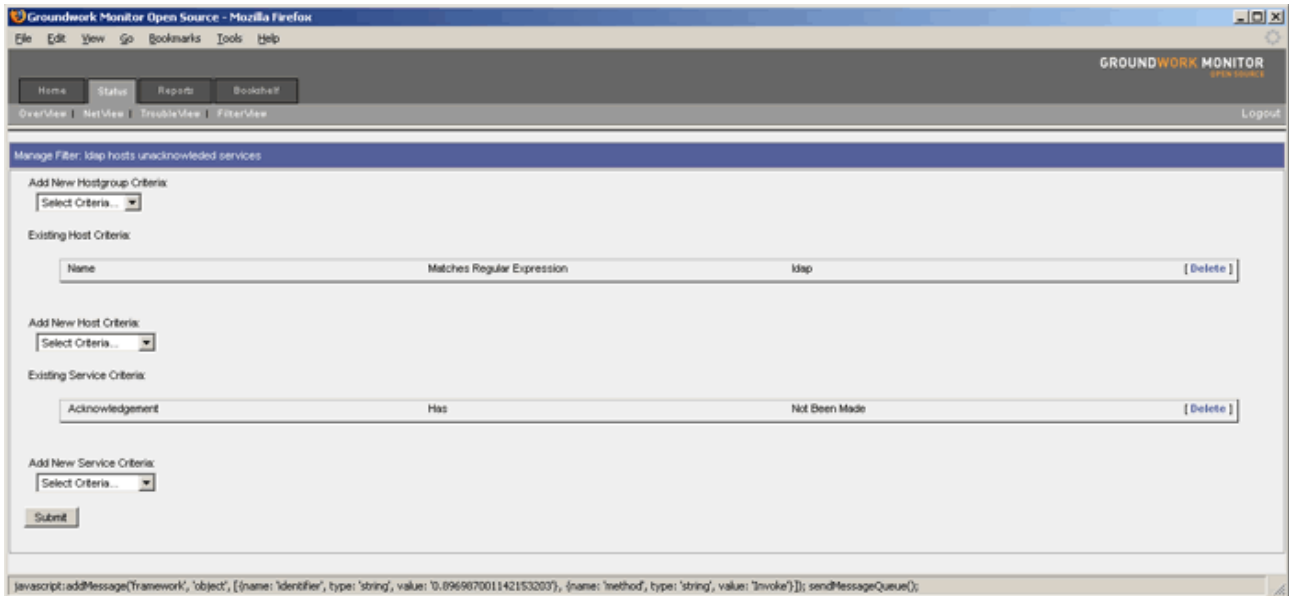
図 2.7.4. コマンドの開始



ステータスフィルタを使うにはどうするか？

1. FilterViewにおいて、Manage Filtersのリストから定義されたフィルタを選びます；ここでは **ldap** が表示されています。定義された判断基準に適合した全てのホストとサービスが表示されるでしょう。フィルタの名称が、次の画面で挿入される左枠に表示されるでしょう。

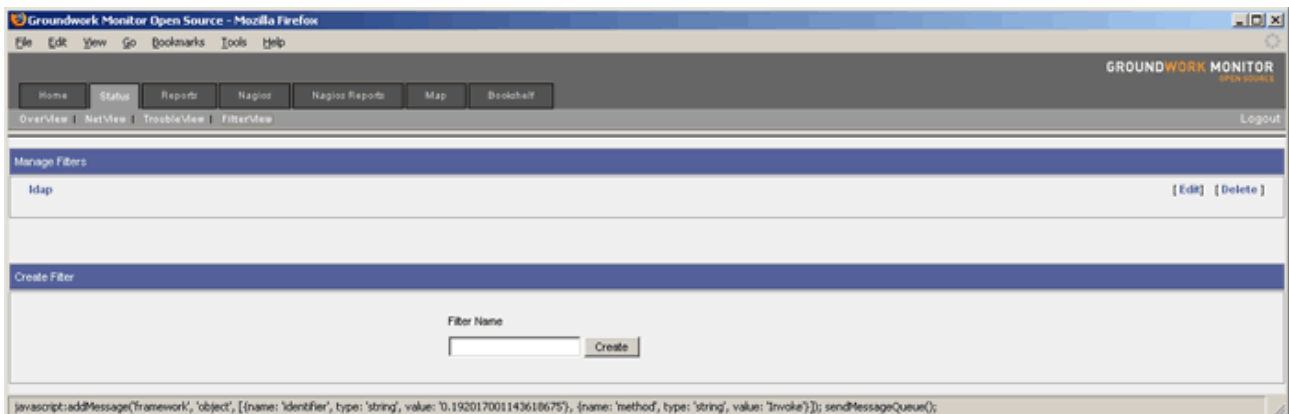
図 2.7.5. フィルターの実行



フィルタを編集したり、削除するにはどうするか？

1. FilterViewにおいて、フィルタを編集する場合は **Edit** を選び、削除する場合は **Delete** を選びます。
2. 編集する場合は、ホストグループ、ホストおよびサービス判断基準のどのような変更でも行えます。先に定義した全ての判断基準を削除するために **Delete** を選ぶこともできます。
3. 変更を実施するため、**Submit** を選択します。これで、Manage Filtersのリストからフィルターを実行することができます。

図 2.7.6. フィルタの編集と削除



第3部 インサイトレポートの作成

本セクションでは、アラーム、通知と停止を含む、さまざまなGroundWork のインサイトレポートの使い方について詳しく説明します。

第1章 概要

インサイトレポート(Insight Reports)について

第2章 アラームレポート

アラームレポートのタイプ

アラームレポートの作成

第3章 通知レポート

通知レポートのタイプ

通知レポートの作成

第4章 停止レポート

停止レポートのタイプ

停止レポートの作成

第5章 レポートの詳細

第1章 概要

インサイトレポート(Insight Reports)について

GroundWorkのインサイトレポートは、システムの可用性とパフォーマンスについてのリアルタイムと履歴データを記録し、詳細な運用ビューに提供します。これらのレポートには、アラーム、通知と停止を含み、企業のITインフラストラクチャ運用の踏み込んだ情報を提供します。履歴レポートは、長期傾向を識別して追跡するのを支援します。データは、ひと目で理解できるよう、グラフィカルで提供され、IT要員とリソースのよりよい管理のために必要なエグゼクティブ情報を提供します。

機能

- ヒストリカル傾向レポート
 - アラーム、ワーニングと通知の活動
- アラームアクティビティ
 - 最も多くのアラーム活動を生じさせている要素のレポート
- 記述的なレポートフォーマット
 - 各インターバルでの正確な計測値を示す表
 - 時系列の変化を見せるヒストグラム図
 - 多数のサンプルの時系列変化を見せる折れ線グラフ
- ユーザ選択可能なオプション
 - 開始と終了日
 - レポーティングの間隔
 - アラーム、ワーニング、通知についての要素の詳細さのレベル
- Nagios監視システムからのデータ
- Nagiosの監視ログをレポートシステムにインポート
- Webアクセス可能
 - GroundWorkのインサイトマネージャは、どのようなブラウザからもアクセスできる
- 他のソースからのデータ
 - インサイトレポートは、他のモニタリングツール、サービスデスク製品、アプリケーションログとコンフィギュレーションデータベースなど、他のソースからのデータを取り込める。

利点

- 可用性向上
 - 処が必要な、インフラストラクチャ内の長期にわたる問題領域を見つけ出すことによって、可用性を向上
- 知的な判断
 - 期間の停止やアラームと通知の傾向を調べることで、リソースの配置や購買について、より知的な判断ができるようにする
- インフラストラクチャの適正化
 - 使用率統計を提供することで、現在のインフラストラクチャの正当性評価をする
- 効率の向上
 - ツールのコンフィギュレーションを最適化するためにレポートを使って監視ツールの効率を向上する

第2章 アラームレポート

アラームレポートのタイプ

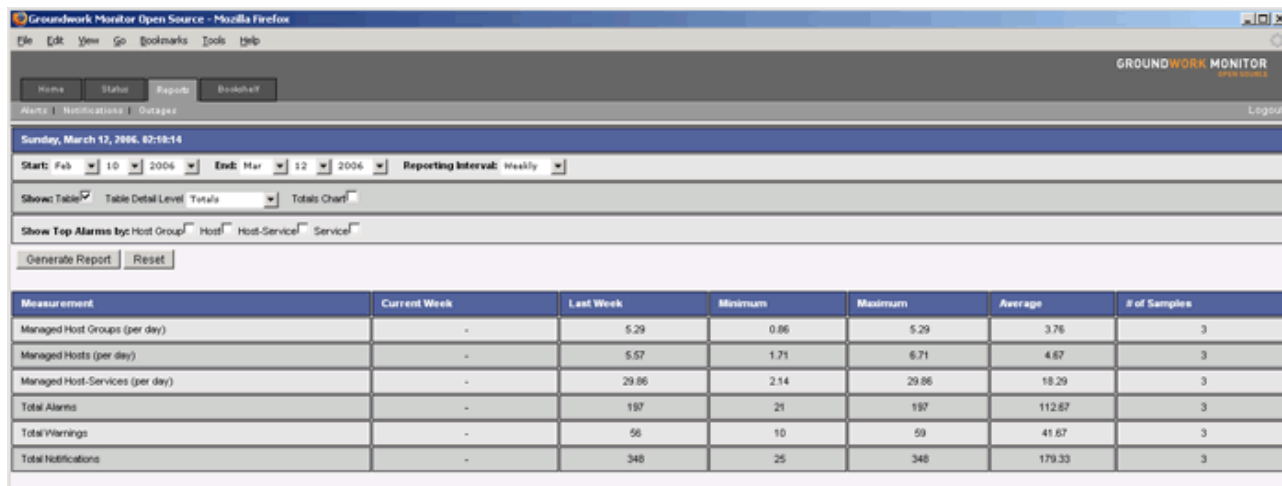
GroundWorkのインサイトレポートは、6種類の監視アラームレポートを提供します。下記にそれぞれのタイプを説明します。

- 表
- 総合チャート
- アラーム数の多いホストグループ
- アラーム数の多いホスト
- アラーム数の多いホスト/サービス
- アラーム数の多いサービス

表

表レポートのオプションは、選択されたレポート間隔での、管理要素のトータル(ホストグループ、ホスト、ホスト-サービス)とアラーム、ワーニング、通知のトータルを表示します。詳しいデータもDetail Level オプションを選ぶことで図に表すことができます。監視対象のホストグループ、ホストとホスト/サービスは、監視されているエレメントの数として表され、インフラストラクチャの大きさの指標となります。ホストとホストグループに対するアラームは、ハードダウン状態のホストチェックとして定義されます。ホスト/サービスとサービス要素に対するアラームは、ハードクリティカル状態のサービスチェックとして定義されます。ホストグループの計測値は、そのホストグループ内の全ホストのカウントを集計して計算されます。

図 3.2.1. アラーム - 表レポート

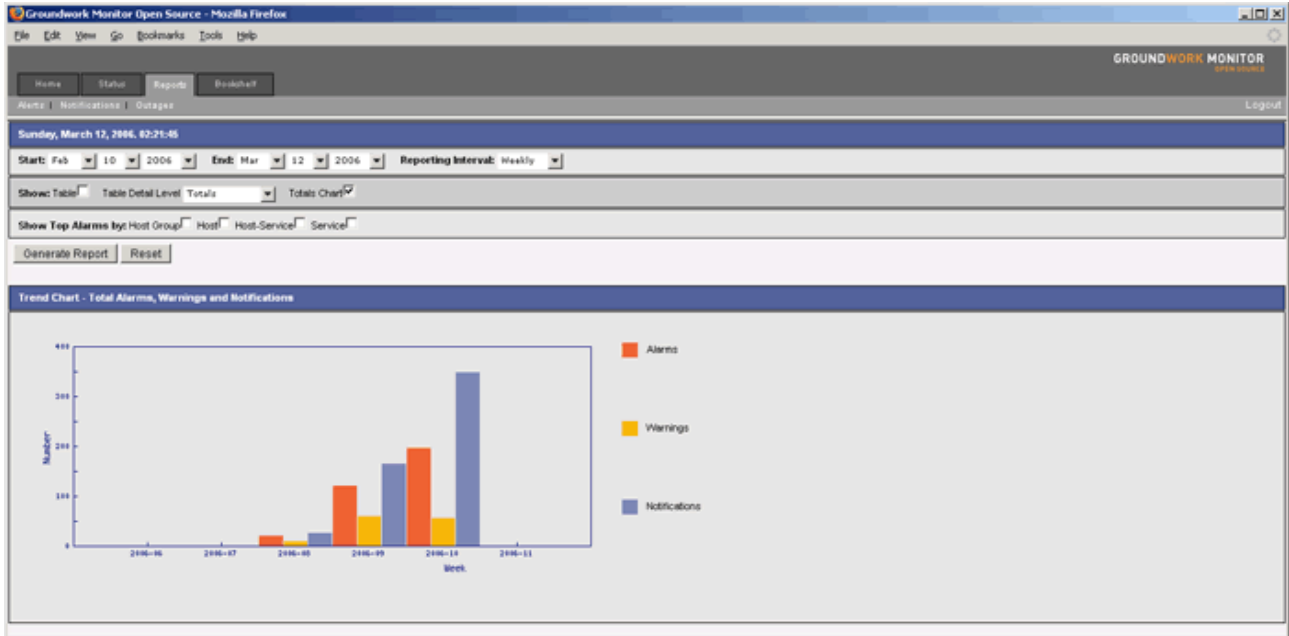


Measurement	Current Week	Last Week	Minimum	Maximum	Average	# of Samples
Managed Host Groups (per day)	-	5.29	0.86	5.29	3.76	3
Managed Hosts (per day)	-	5.57	1.71	6.71	4.67	3
Managed Host-Services (per day)	-	29.86	2.14	29.86	18.29	3
Total Alarms	-	197	21	197	112.67	3
Total Warnings	-	56	10	59	41.67	3
Total Notifications	-	348	25	348	179.33	3

総合チャート

総合チャートは指定されたレポート期間のアラーム、ワーニング、通知の合計を表示します。各インターバルと計測値をバーで示す棒グラフが作られます。標本化する間隔数が棒グラフで表示できるよりも多い場合、代わりに折れ線グラフが作成されます。

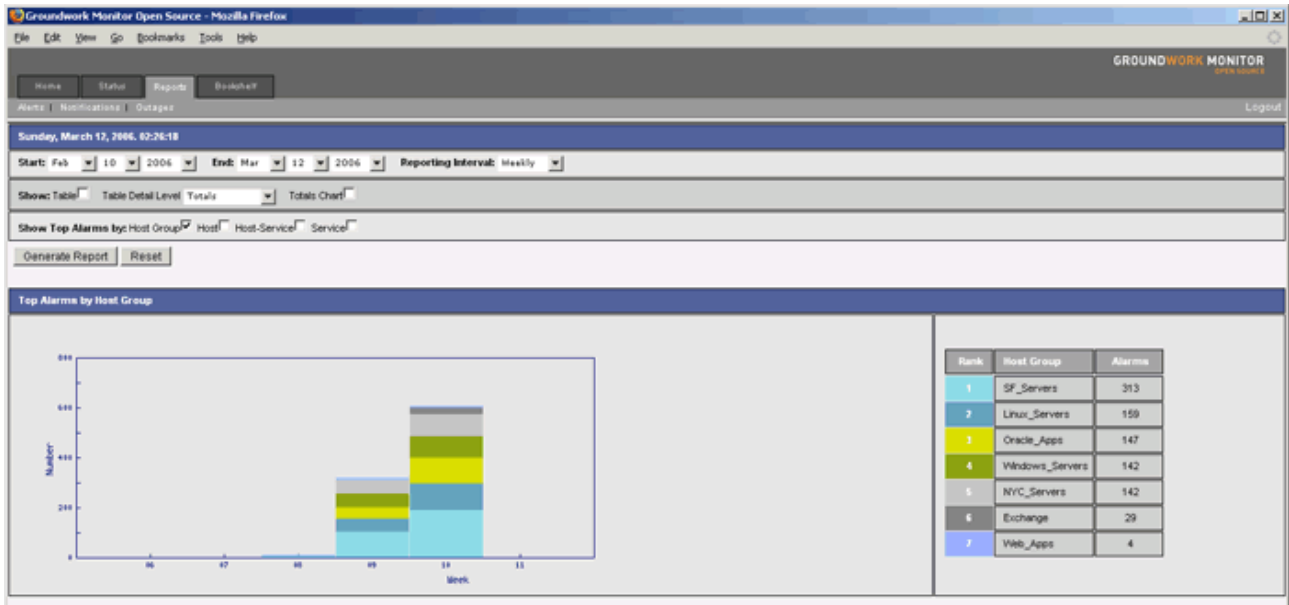
図 3.2.2. アラーム - 総合チャート



アラーム数の多いホストグループ

このレポートングオプションは、アラーム数の多い順にホストグループをリストします。ホストグループは、たとえば技術グループによってWindowsやUnixなどに;運用ヘルプデスクなどの組織ごとに、SFやNYなどの地理的サイト毎にまとめられます。傾向チャートは、特定の日付の幅でホストグループのアラーム数をグラフ化して表示します。各インターバルで積み重なったバーが、各ホストグループのアラームの割合を示します。各バーの色は、上位リスト(右側の表)の色と対応します。

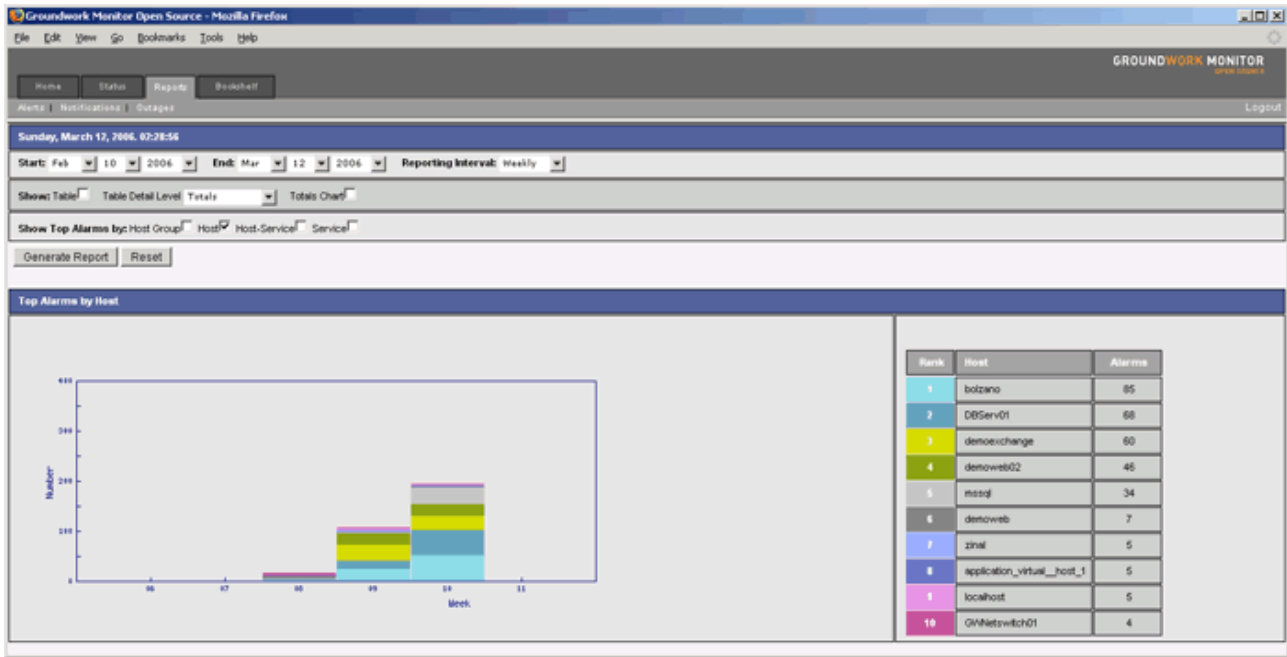
図 3.2.3. アラーム - ホストグループ



アラーム数の多いホスト

このレポートングオプションは、アラーム数の多い順にホストをリストします。ホストは、たとえば、サーバやルータなどの物理デバイス毎やアプリケーションなどの仮想的なエンティティ毎に組織化され、名称付与されます。傾向チャートは、特定の日付の幅でホストのアラーム数をグラフ化して表示します。各インターバルで積み重なったバーが、各ホストのアラームの割合を示します。各バーの色は、上位リスト(右側の表)の色と対応します。

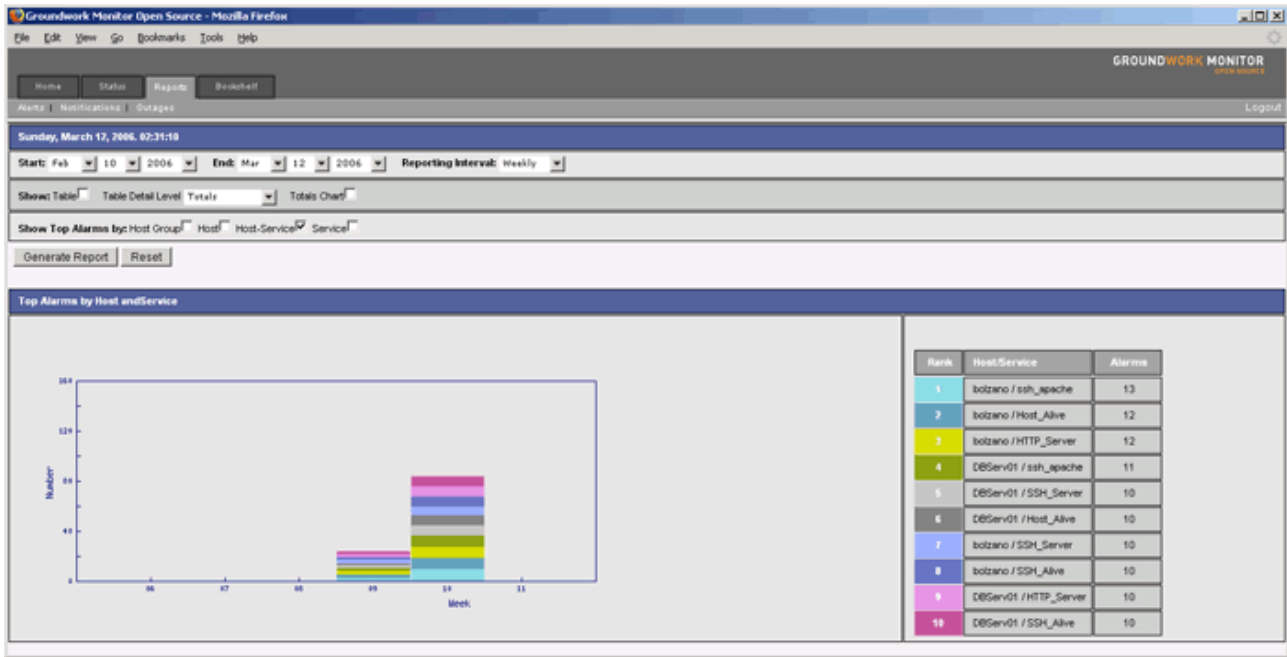
図 3.2.4. アラーム - ホスト



アラーム数の多いホスト/サービス

このレポートングオプションは、アラーム数の多い順にホスト/サービスをリストします。ホスト/サービスとは、ホストとその詳細なサービスのことで、傾向チャートは、特定の日付の幅でホスト/サービスのアラーム数をグラフ化して表示します。各インターバルで積み重なったバーが、各ホスト/サービスのアラームの割合を示します。各バーの色は、上位リスト(右側の表)の色と対応します。

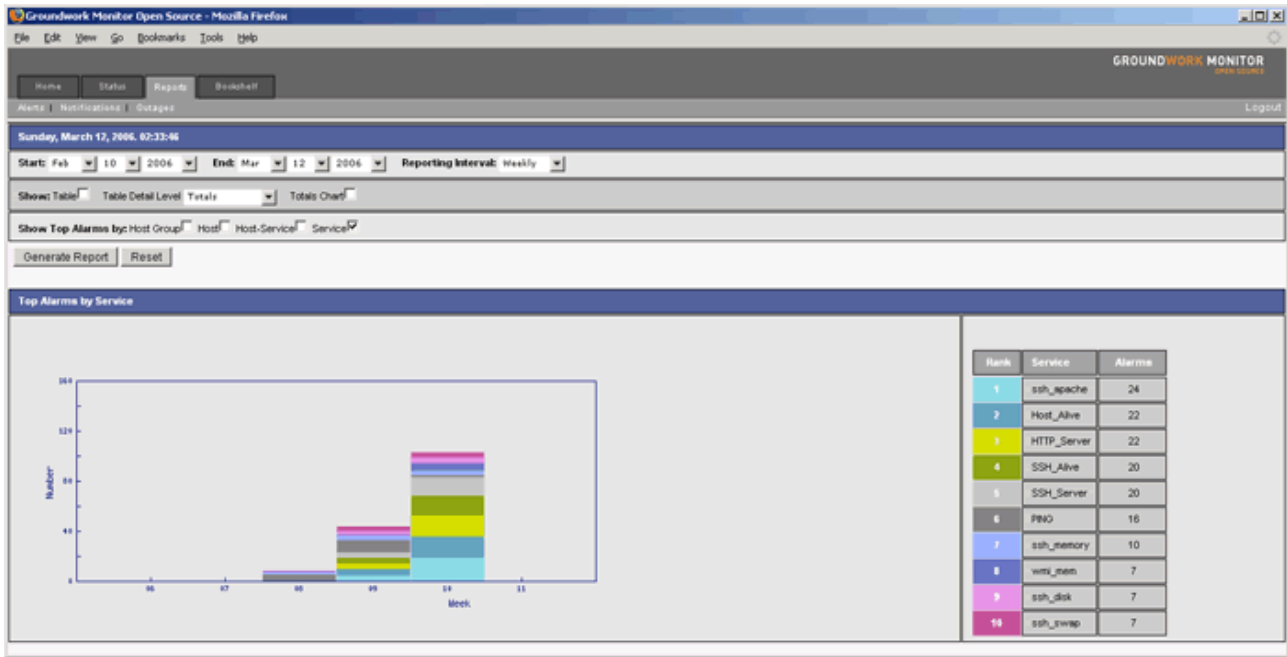
図 3.2.5 アラーム - ホスト/サービスレポート



アラーム数の多いサービス

このレポートングオプションは、アラーム数の多い順にサービスをリストします。サービスは、ホストから独立して、プロトコルやモニタのタイプでグルーピングしたものです。傾向チャートは、特定の日付の幅でサービスのアラーム数をグラフ化して表示します。各インターバルで積み重なったバーが、各サービスのアラームの割合を示します。各バーの色は、上位リスト(右側の表)の色と対応します。

図 3.2.6. アラーム - サービスレポート



アラームレポートの作成

アラームレポートを作成するには、下記のレポートングのオプションを選んでから、Generate Reportを選びます。

図 3.2.7. アラーム - Reportの作成

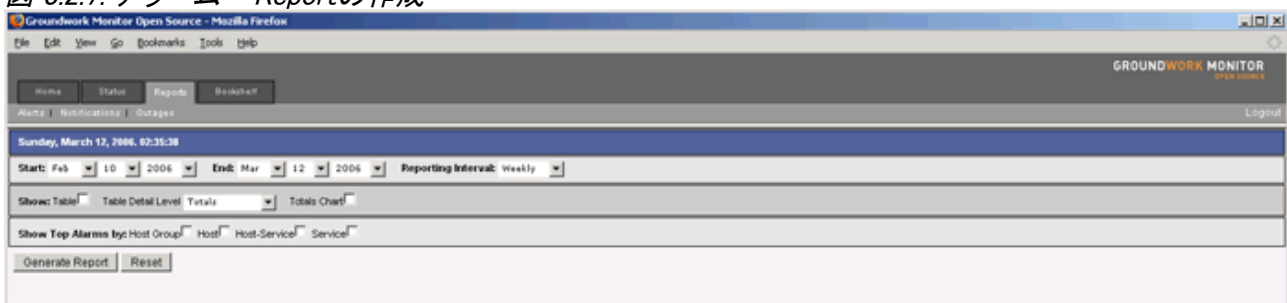


表 3.2.1. アラーム - Reportの作成

フィールド	説明
Start(開始)	作成するレポートの開始日付を選びます.
End(終了)	作成するレポートの終了日付を選びます.
Reporting Interval (レポート間隔)	データをレポートする間隔(日次、週次、月次、年次)を指示します.
Table (表)	作成したレポートの中に計測値の表を表示します.
Table Detail Level (詳細レベルの表)	アラーム、ワーニング、通知についての各ホストグループ、ホスト、ホスト/サービスやサービス毎の詳細データを計測値の表の中にリストします.
Totals Chart (総合チャート)	トータルのアラーム、ワーニングおよび通報の傾向チャートを表示します
Top Alarms by: Host Group (アラーム数の多いホストグループ)	レポート中にホストグループのチャートを作成します.
Top Alarms by: Host (アラーム数の多いホスト)	レポート中にホストのチャートを作成します.
Top Alarms by: Host/Service (アラーム数の多いホスト/サービス)	レポート中にホスト/サービスのチャートを作成します.
Top Alarms by: Service (アラーム数の多いサービス)	レポート中にサービスのチャートを作成します.

第3章 通知レポート

通知レポートのタイプ

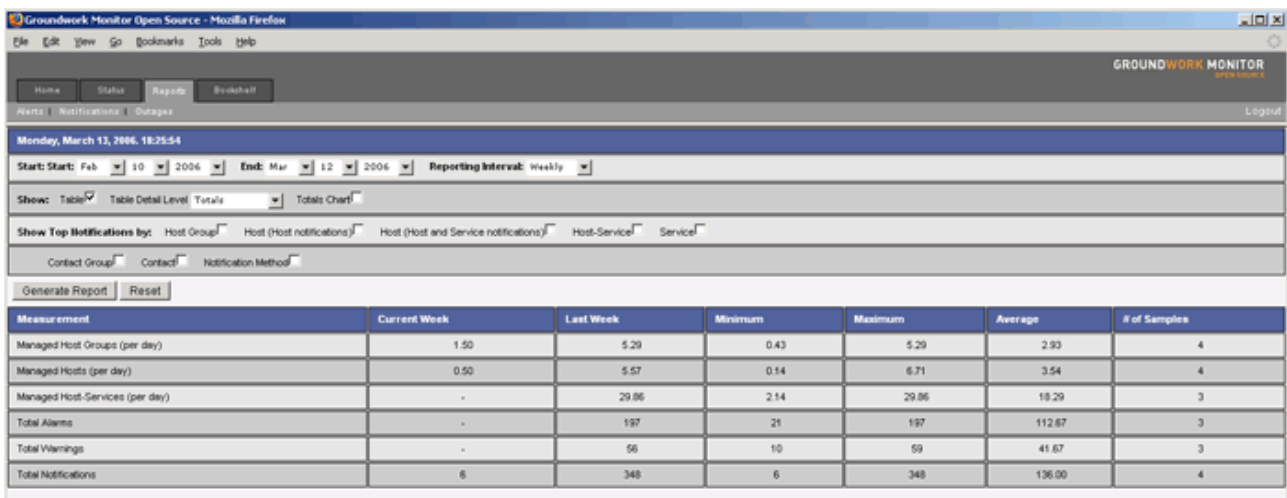
GroundWorkのインサイトレポートは、11種類の監視通知レポートを提供します。下記にそれぞれのタイプを説明します。

- 表
- 総合チャート
- 通知数の多いホストグループ
- 通知数の多いホスト(ホスト通知)
- 通知数の多いホスト(ホストとサービス通知)
- 通知数の多いホスト-サービス
- 通知数の多いサービス
- コンタクトグループ
- コンタクト
- 通知方法

表

表レポートのオプションは、選択されたレポート間隔での、管理要素のトータル(ホストグループ、ホスト、ホスト-サービス)とアラーム、ワーニング、通知のトータルを表示します。詳しいデータもDetail Level オプションを選ぶことで図に表すことができます。この表は、アラームと停止レポートからも作成することができます。

図 3.3.1. 通知 - 表レポート

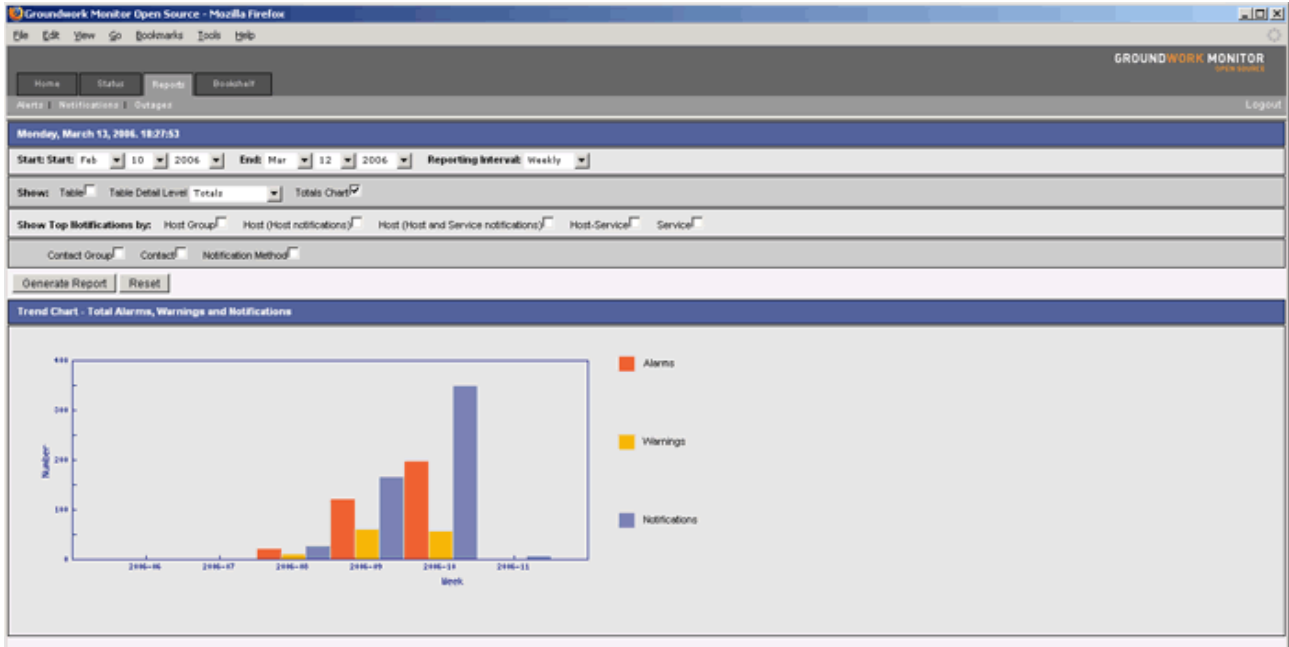


Measurement	Current Week	Last Week	Minimum	Maximum	Average	# of Samples
Managed Host Groups (per day)	1.50	5.29	0.43	5.29	2.93	4
Managed Hosts (per day)	0.50	5.57	0.14	6.71	3.54	4
Managed Host-Services (per day)	-	29.86	2.14	29.86	18.29	3
Total Alarms	-	197	21	197	112.67	3
Total Warnings	-	56	10	59	41.67	3
Total Notifications	6	348	6	348	136.00	4

総合チャート

総合チャートのレポートオプションは、指定されたレポート期間のアラーム、ワーニング、通知の合計を表示します。各インターバルと計測値をバーで示す棒グラフが作られます。標準化する間隔数が棒グラフで表示できるよりも多い場合、代わりに折れ線グラフが作成されます。

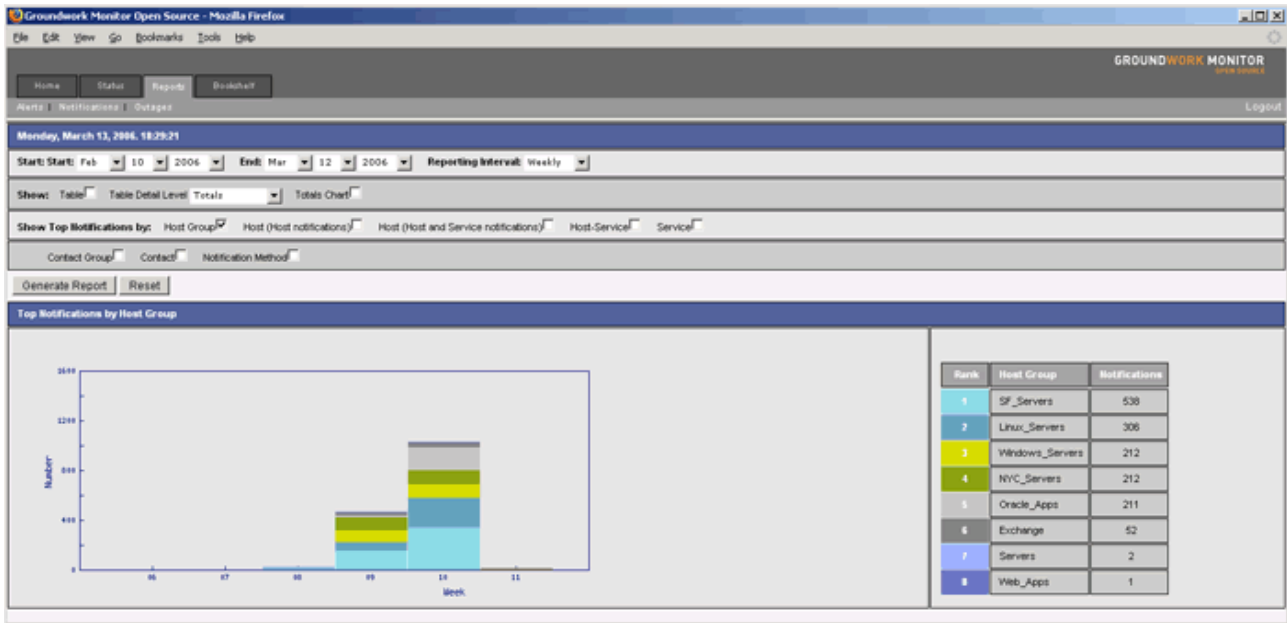
図 3.3.2. 通知 - 総合レポート



通知数の多いホストグループ

ホストグループのレポートオプションは、通知数の多い順にホストグループをリストします。ホストグループは、たとえば技術グループによってWindowsやUnixなどに;運用ヘルプデスクなどの組織ごとに、SFやNYなどの地理的サイト毎にまとめられます。傾向チャートは、特定の日付の幅でホストグループの通知数をグラフ化して表示します。各インターバルで積み重なったバーが、各ホストグループの通知数の割合を示します。各バーの色は、上位リスト(右側の表)の色と対応します。

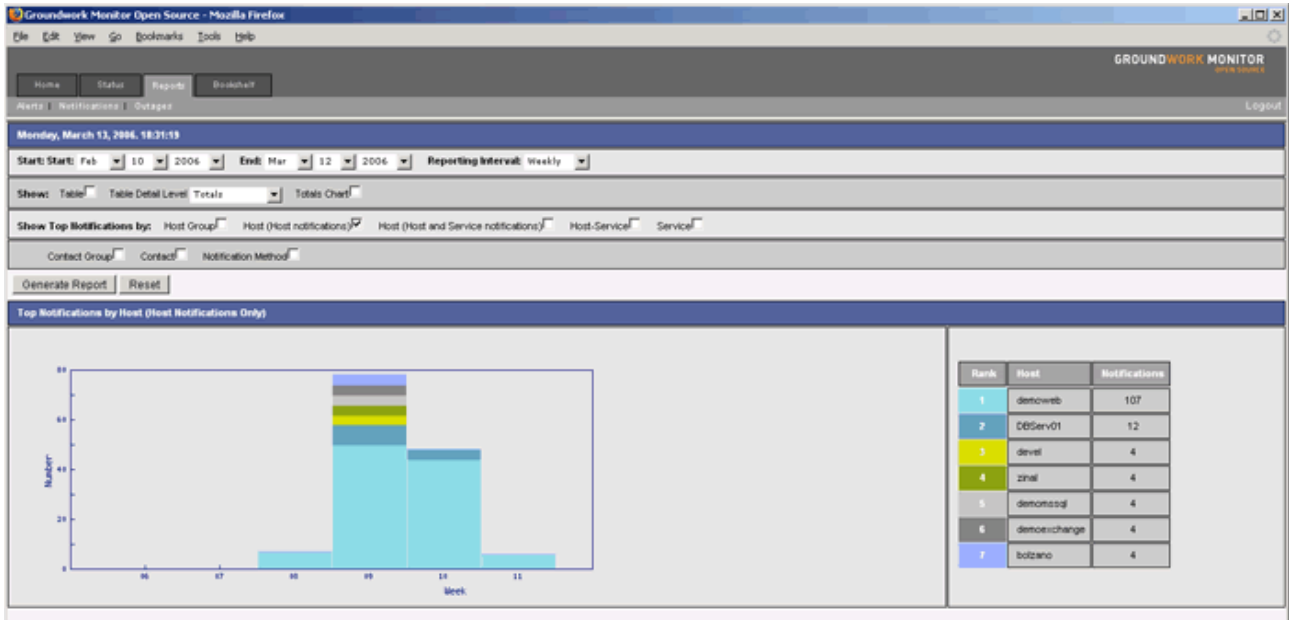
図 3.3.3. 通知 - ホストグループレポート



通知数の多いホスト(ホスト通知のみ)

このレポートングオプションは、通知数の多い順にホストをリストします。ホストは、たとえば、サーバやルータなどの物理デバイス毎やアプリケーションなどの仮想的なエンティティ毎に組織化され、名称付与されます。傾向チャートは、特定の日付の幅でホストの通知数をグラフ化して表示します。各インターバルで積み重なったバーが、各ホストの通知の割合を示します。各バーの色は、上位リスト(右側の表)の色と対応します。

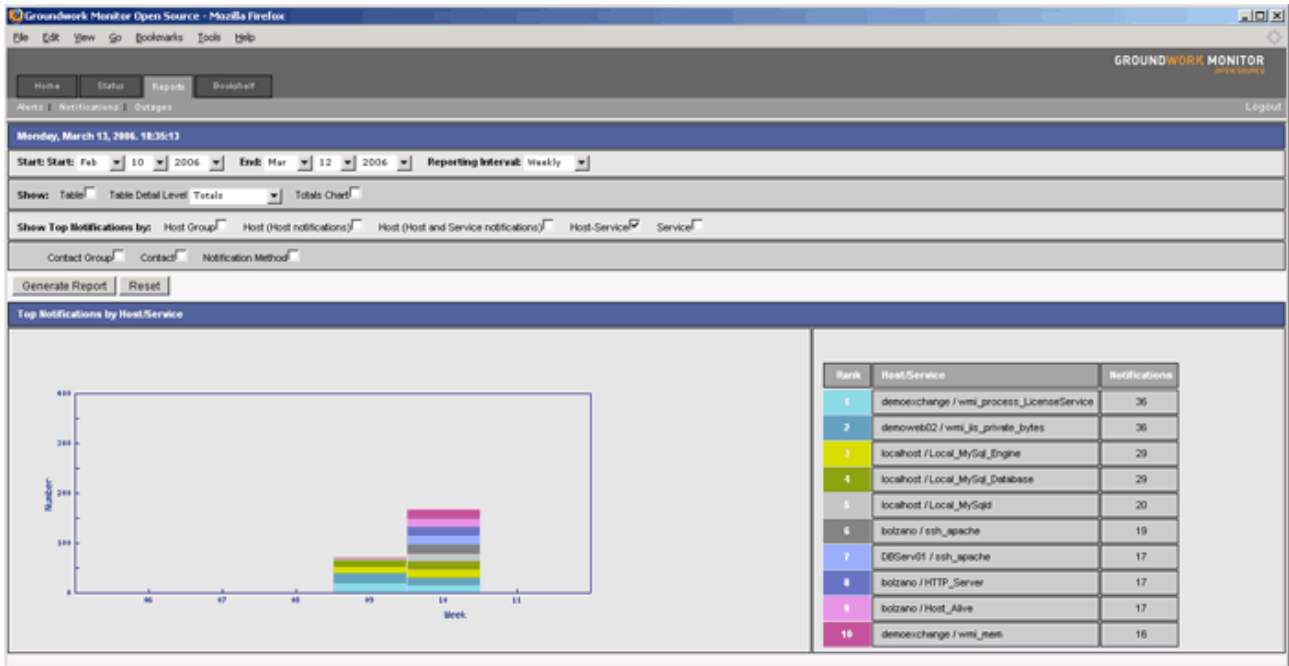
図 3.3.4. 通知 - ホスト(通知のみ) レポート



通知数の多いホスト (ホストとサービス通知)

このレポートングオプションは、通知数の多い順にホストをリストします。ホストは、たとえば、サーバやルータなどの物理デバイス毎やアプリケーションなどの仮想的なエンティティ毎に組織化され、名称付与されます。傾向チャートは、特定の日付の幅でホストとサービスの通知数をグラフ化して表示します。各インターバルで積み重なったバーが、各ホストとサービスの通知数の割合を示します。各バーの色は、上位リスト(右側の表)の色と対応します。

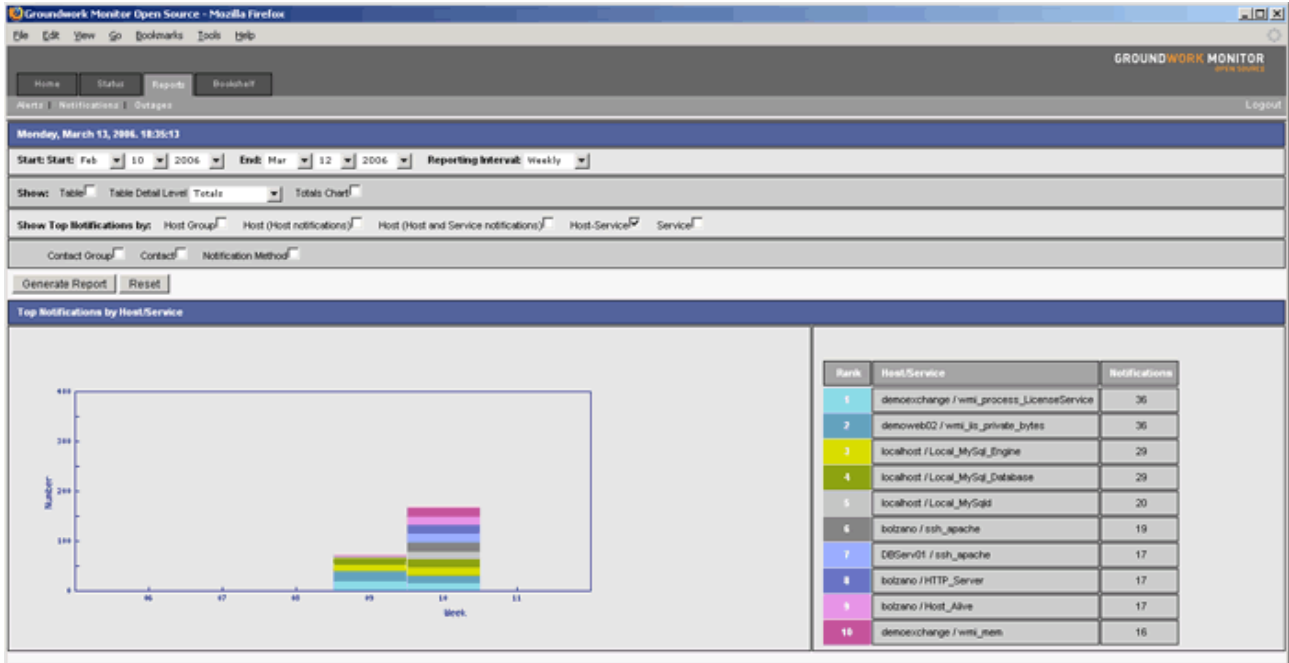
図 3.3.5. 通知 - ホスト (ホストとサービス) レポート



通知数の多いホスト/サービス (ホストと詳細サービス)

このレポートングオプションは、通知数の多い順にホスト/サービスをリストします。傾向チャートは、特定の日付の幅でホストとサービスの通知数をグラフ化して表示します。各インターバルで積み重なったバーが、各ホストとサービスの通知数の割合を示します。各バーの色は、上位リスト(右側の表)の色と対応します。

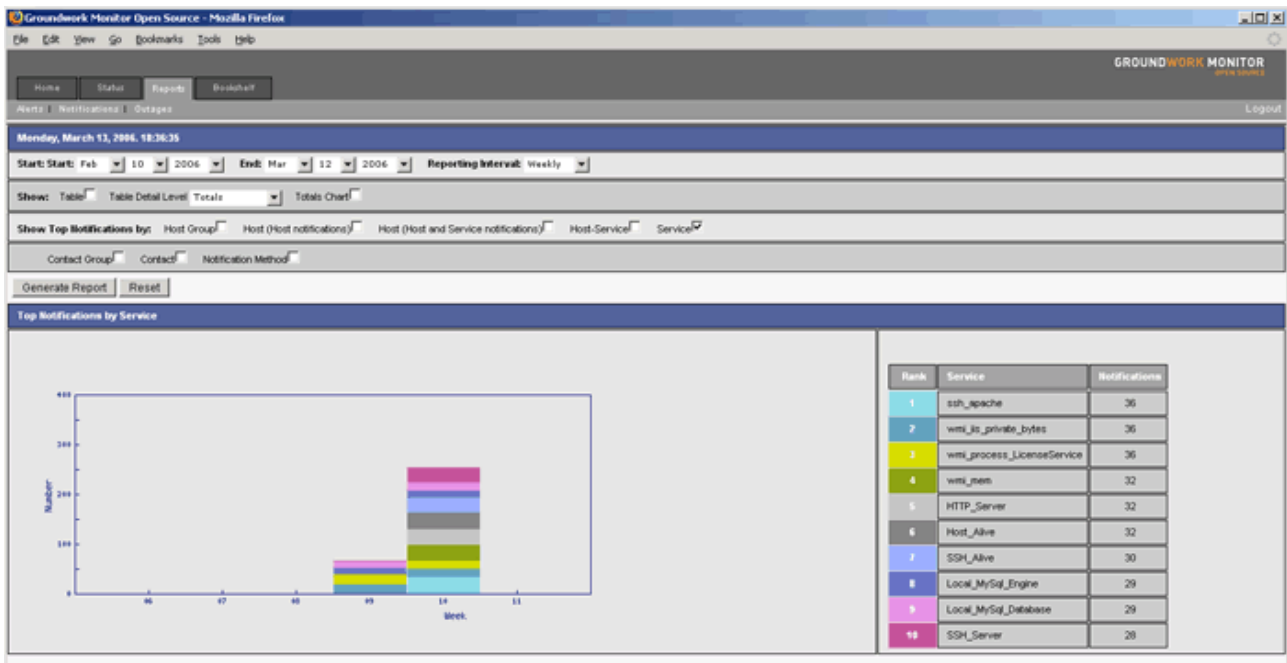
図 3.3.6. 通知 - ホスト/サービスレポート



通知数の多いサービス (ホストから独立したサービス、プロトコルやモニタのタイプでグループ化)

このレポートングオプションは、通知数の多い順にサービスをリストします。傾向チャートは、特定の日付の幅でサービスの通知数をグラフ化して表示します。各インターバルで積み重なったバーが、各サービスの通知数の割合を示します。各バーの色は、上位リスト(右側の表)の色と対応します。

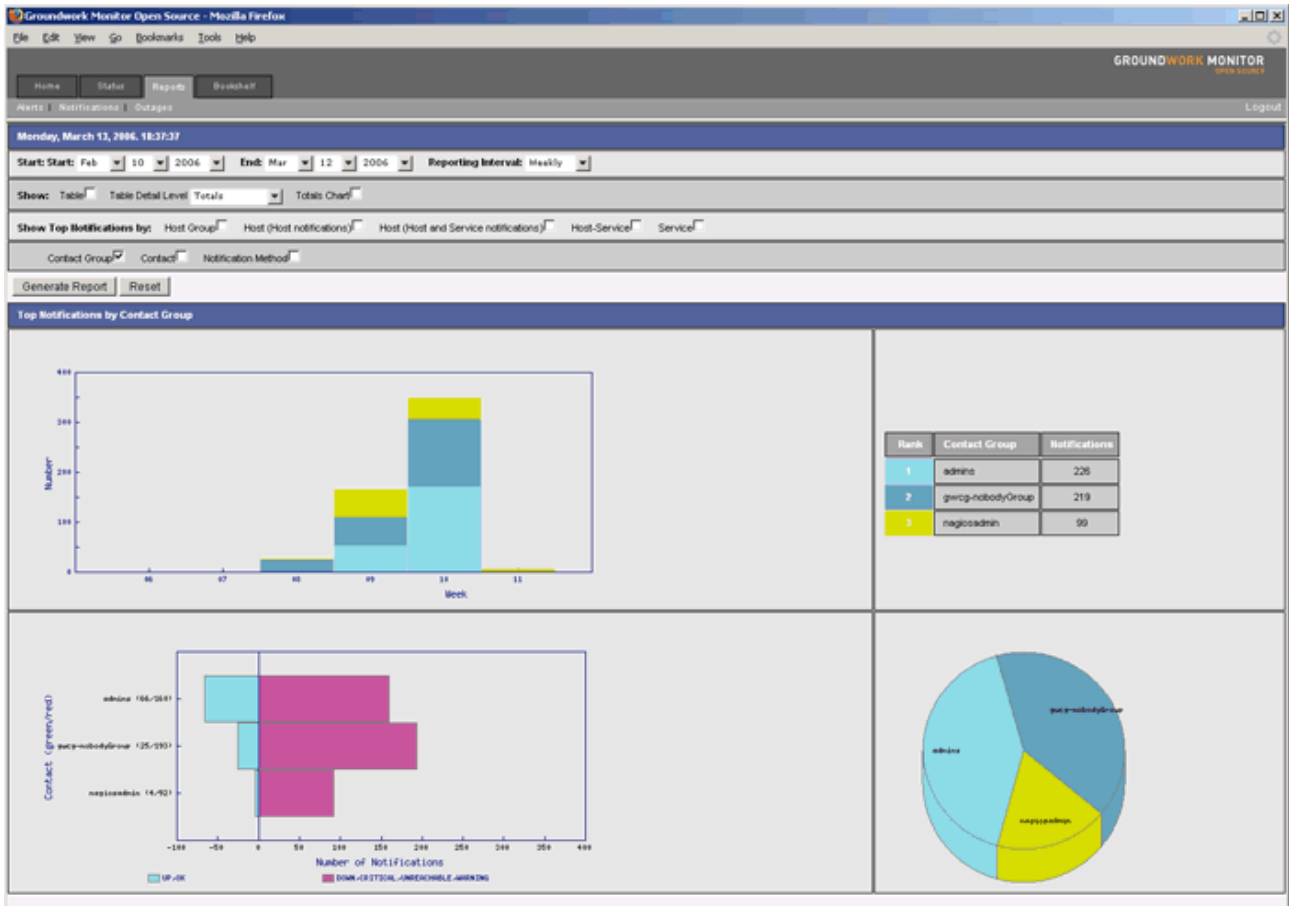
図 3.3.7. 通知 - サービスレポート



通知数の多いコンタクトグループ

このレポートングオプションは、通知数の多い順にコンタクトグループをリストします。傾向チャートは、特定の日付の幅でコンタクトグループの通知数をグラフ化して表示します。各インターバルで積み重なったバーが、各コンタクトグループの通知数の割合を示します。各バーの色は、上位リスト(右側の表)の色と対応します。このオプションは、また、コンタクトグループ毎に、各コンタクトグループ内のコンタクト(連絡先)の比率を示す円グラフおよび、コンタクトグループ毎のOK対ダウンの通知種別を示す、コンタクトグループ毎通報グラフを表示します。

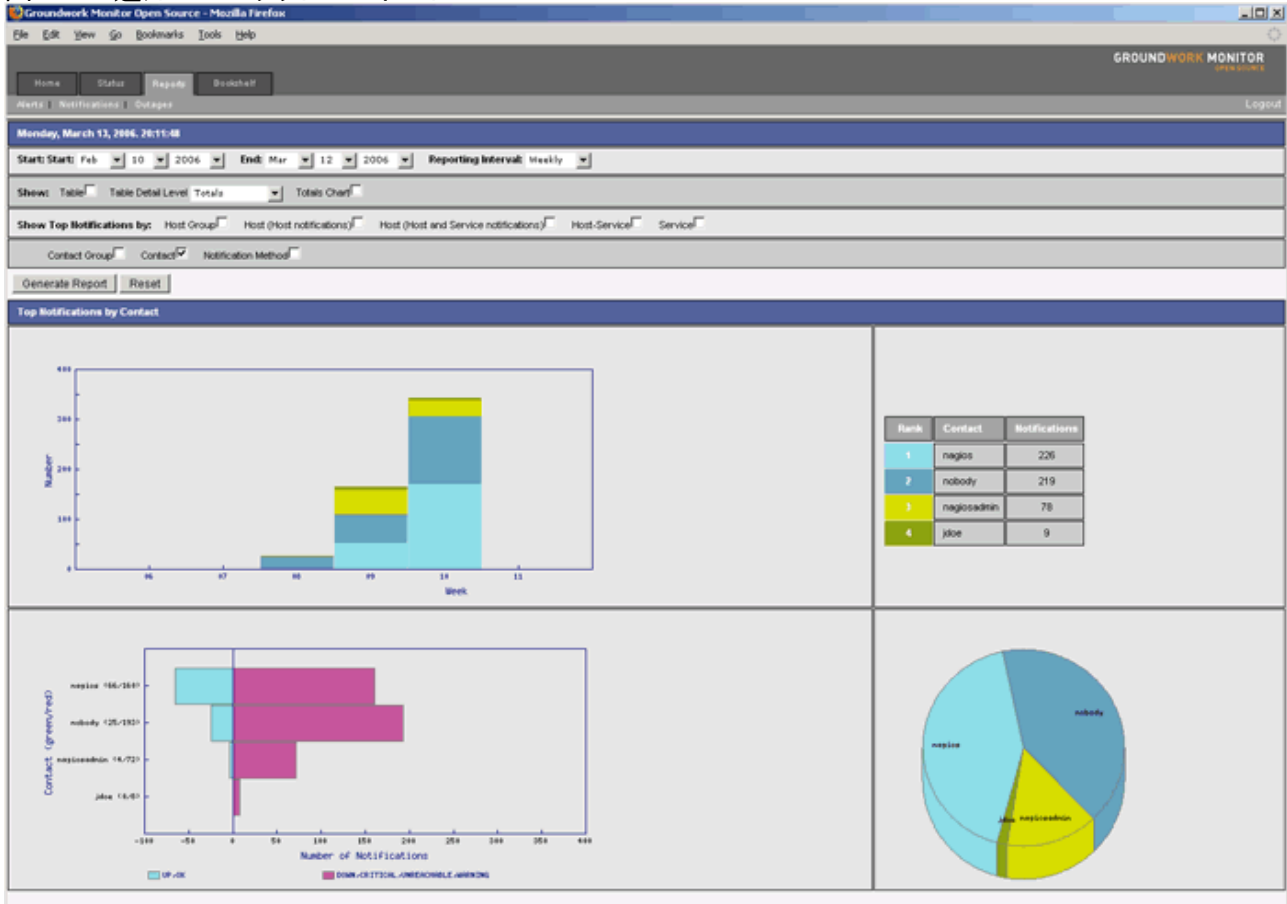
図 3.3.8. 通知 - コンタクトグループレポート



通知数の多いコンタクト

このレポートオプションは、通知数の多い順にコンタクト(連絡先)をリストします。傾向チャートは、特定の日付の幅でコンタクトの通知数をグラフ化して表示します。各インターバルで積み重なったバーが、各コンタクトの通知数の割合を示します。各バーの色は、上位リスト(右側の表)の色と対応します。このオプションは、また、コンタクトグループ毎に、各コンタクトグループ内のコンタクト(連絡先)の比率を示す円グラフを表示します。また、コンタクト毎のOK対ダウンの通知種別を示す、コンタクト毎通報グラフを表示します。

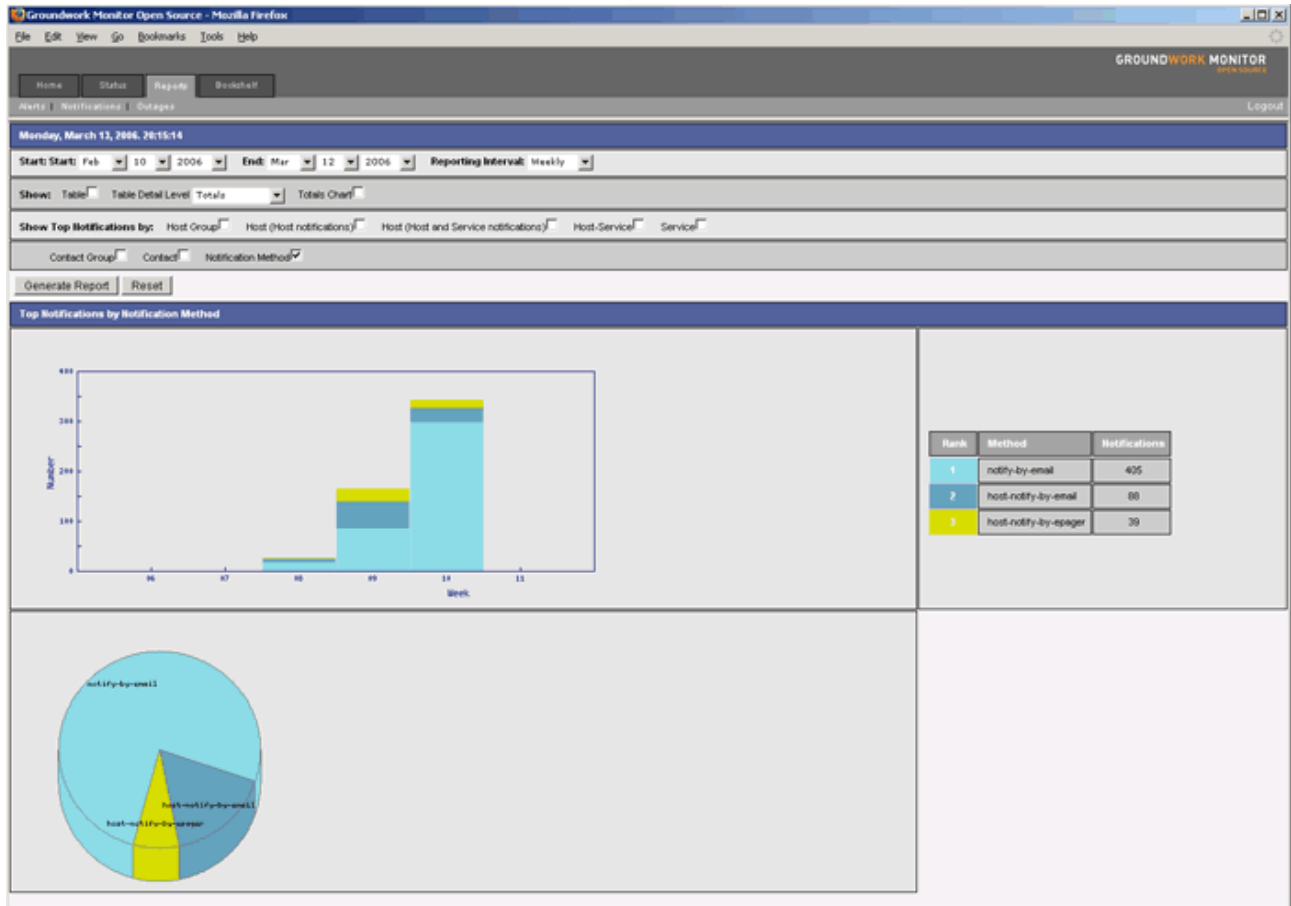
図 3.3.9. 通知 - コンタクトのレポート



通知数の多い通知方式

このレポートングオプションは、通知数の多い順に通知方式をリストします。傾向チャートは、特定の日付の幅で通知方式毎の通知数をグラフ化して表示します。各インターバルで積み重なったバーが、各通知方式での通知数の割合を示します。各バーの色は、上位リスト(右側の表)の色と対応します。このオプションは、各通知方式毎ののコンタクト(連絡先)の比率を示す、通知方式による通報グラフを表示します。

図 3.3.11. 通知 - 方式のレポート



通知レポートの作成

通知レポートを作成するには、下記に説明するレポートングオプションを選んでから、Generate Reportを選択します。

図 3.3.12. 通知 - レポートの作成

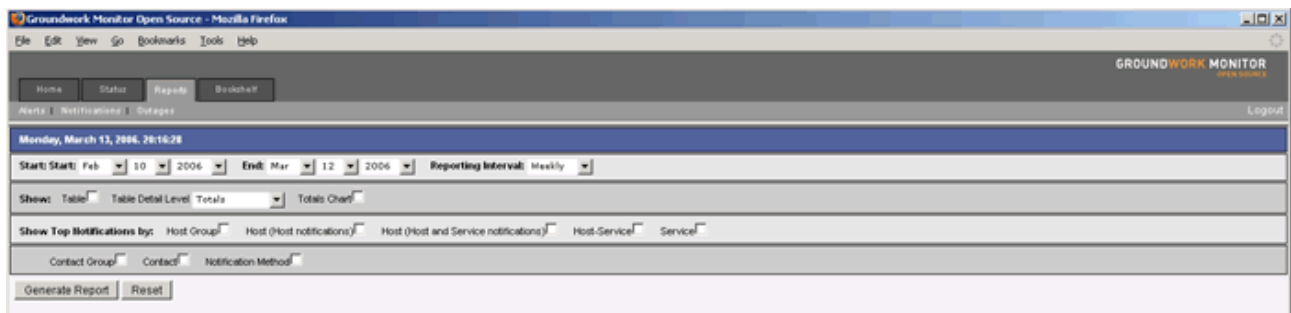


表 3.3.1. 通知 - レポートの作成

フィールド	説明
Start (開始)	作成するレポートの開始日付を選びます。
End (終了)	作成するレポートの終了日付を選びます。
Reporting Interval (レポート間隔)	データをレポートする間隔 (日次、週次、月次、年次) を指示します。
Table (表)	作成したレポートの中に計測値の表を表示します。
Table Detail Level (詳細レベルの表)	アラーム、ワーニング、通知についての各ホストグループ、ホスト、ホスト/サービスやサービス毎の詳細データを計測値の表の中にリストします。
Totals Chart (総合チャート)	トータルのアラーム、ワーニングおよび通報の傾向チャートを表示します
Top Notifications by: Host Group (通知数の多いホストグループ)	レポート中にホストグループのチャートを作成します
Top Notifications by: Host (通知数の多いホスト)	レポート中にホストのチャートを作成します
Top Notifications by: Host/Service (通知数の多いホスト/サービス)	レポート中にホスト/サービスのチャートを作成します
Top Notifications by: Service (通知数の多いサービス)	レポート中にサービスのチャートを作成します
Top Notifications by: Contact Group (通知数の多いコンタクトグループ)	レポート中にコンタクトグループのチャートを作成します
Top Notifications by: Contact (通知数の多いコンタクト)	レポート中にコンタクトのチャートを作成します
Top Notifications by: Contact (Outage Only) (通知数の多いコンタクト-停止のみ)	レポート中にコンタクト(停止通知のみ)のチャートを作成します
Top Notifications by: Notification Method (通知数の多い通知方式)	レポート中に通知方式のチャートを作成します

第4章 停止レポート

停止レポートのタイプ

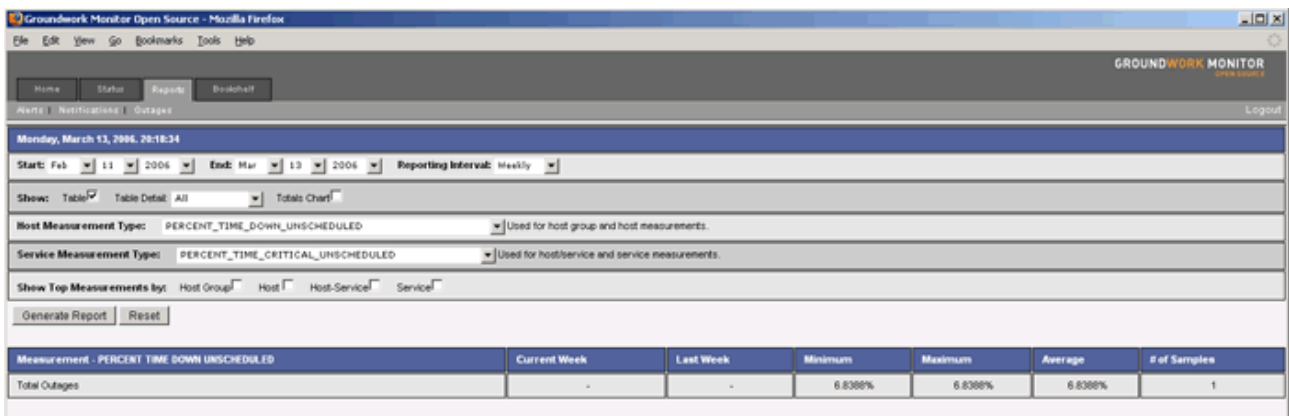
GroundWorkのインサイトレポートは、6種類の停止レポートを提供します。下記にそれぞれのタイプを説明します。

- 表
- 総合チャート
- 停止回数の多いホストグループ
- 停止回数の多いホスト
- 停止回数の多いホスト/サービス
- 停止回数の多いサービス

表

このレポートのオプションは、今週と前週の計画外停止の時間比率を表示します。さらに、指定されたレポート期間での総停止パーセンテージの最小値、最大値、平均値を表示します。下記は、6週間の例を示しています。

図 3.4.1. 停止 - 表レポート



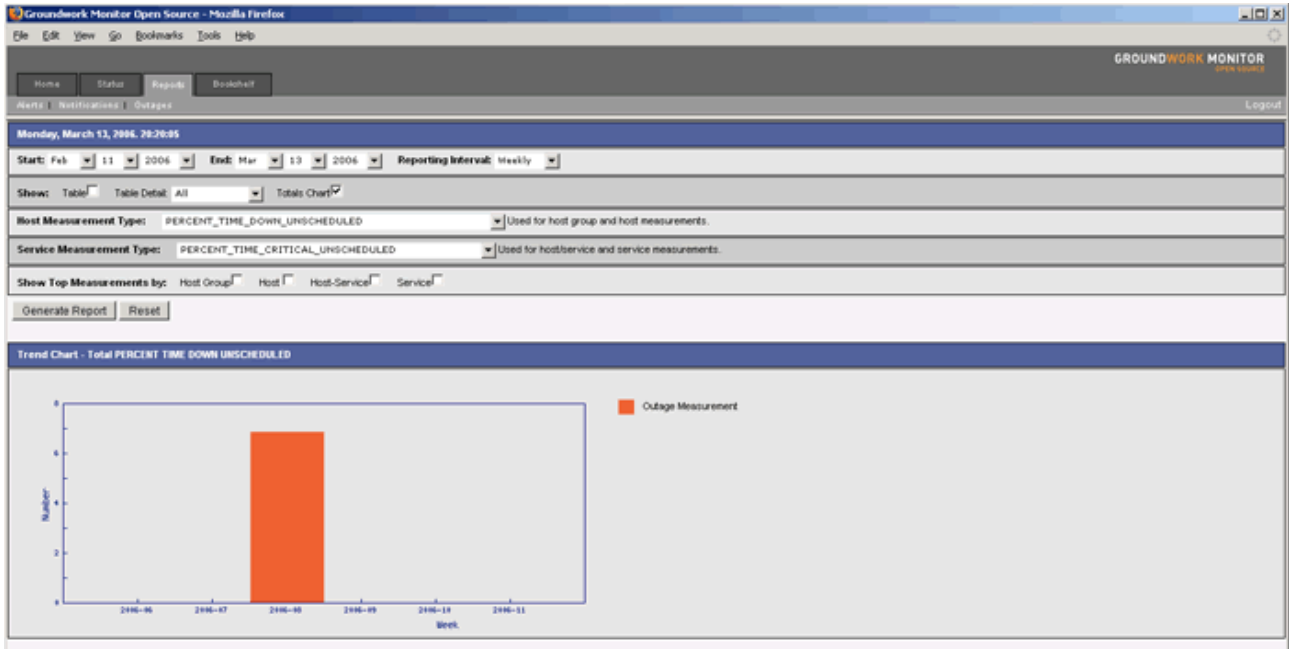
The screenshot shows the GroundWork Monitor web interface. The main content area displays a table report for 'PERCENT TIME DOWN UNSCHEDULED'. The table has columns for 'Current Week', 'Last Week', 'Minimum', 'Maximum', 'Average', and '# of Samples'. The data row shows 'Total Outages' with values: Current Week: -, Last Week: -, Minimum: 6.8388%, Maximum: 6.8388%, Average: 6.8388%, # of Samples: 1.

Measurement - PERCENT TIME DOWN UNSCHEDULED	Current Week	Last Week	Minimum	Maximum	Average	# of Samples
Total Outages	-	-	6.8388%	6.8388%	6.8388%	1

総合チャート

このレポートのオプションは、指定されたレポート日付の範囲での停止計測値を表示します。各インターバルと計測値を示すグラフが作成されます。

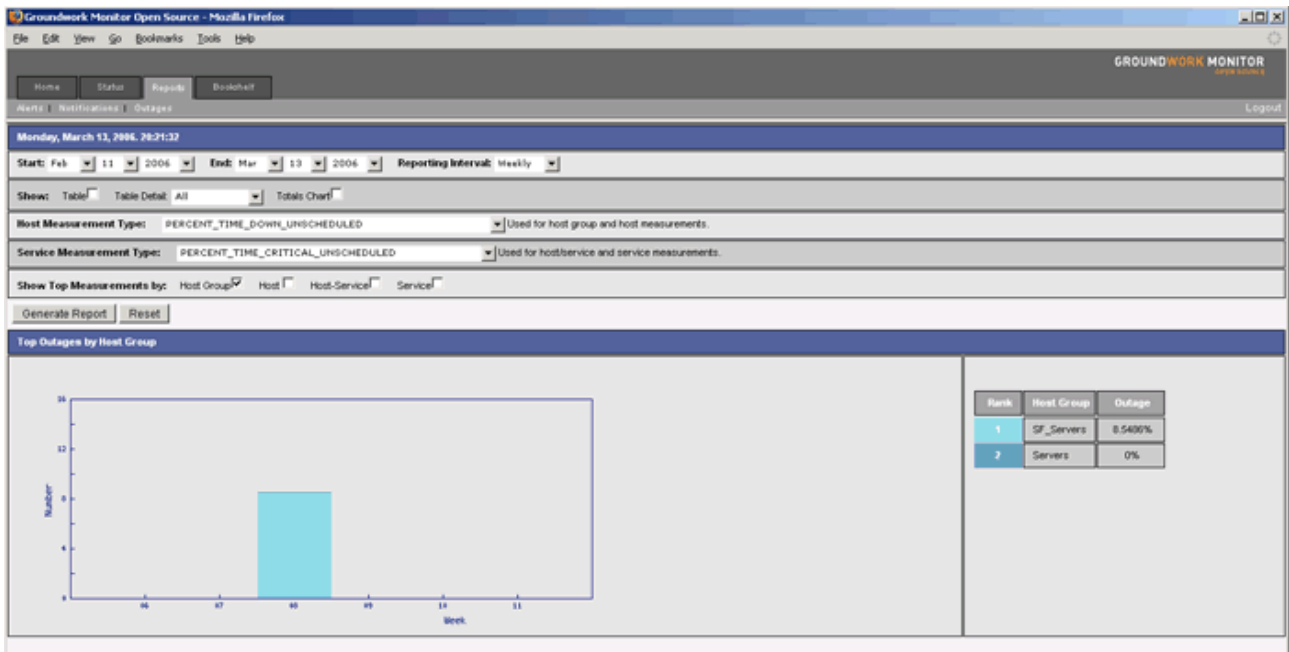
図 3.4.2. 停止 - 総合チャート



停止回数の多いホストグループ

このレポートのオプションは、停止回数の多い順にホストグループをリストします。傾向チャートは、特定の日付の幅でホストグループの停止数をグラフ化して表示します。各インターバルで積み重なったバーが、各ホストグループの停止数の割合を示します。各バーの色は、上位リスト(右側の表)の色と対応します。

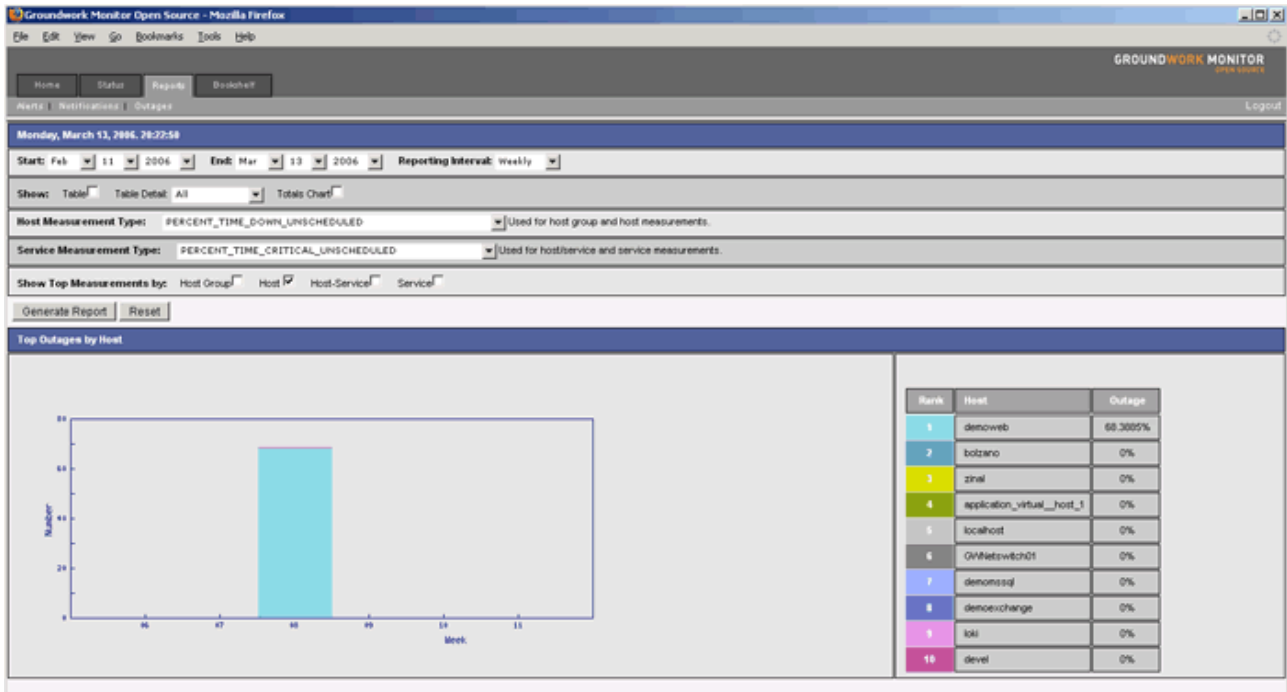
図 3.4.3. 停止 - ホストグループReport



停止回数の多いホスト

このレポートのオプションは、停止回数の多い順にホストをリストします。傾向チャートは、特定の日付の幅でホストの停止数をグラフ化して表示します。各インターバルで積み重なったバーが、各ホストの停止数の割合を示します。各バーの色は、上位リスト(右側の表)の色と対応します。

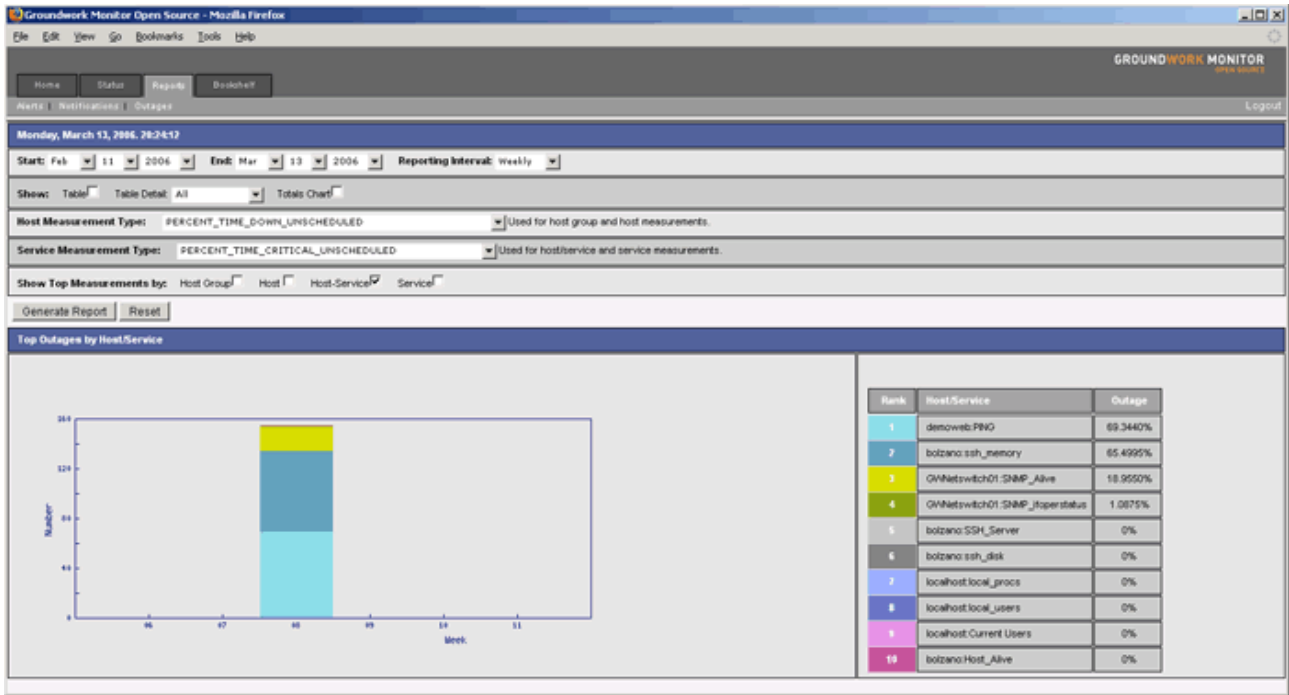
図 3.4.4. 停止 - ホスト Report



停止回数の多いホスト/サービス

このレポートのオプションは、停止回数の多い順にホスト/サービスをリストします。傾向チャートは、特定の日付の幅でホスト/サービスの停止数をグラフ化して表示します。各インターバルで積み重なったバーが、各ホスト/サービスの停止数の割合を示します。各バーの色は、上位リスト(右側の表)の色と対応します。

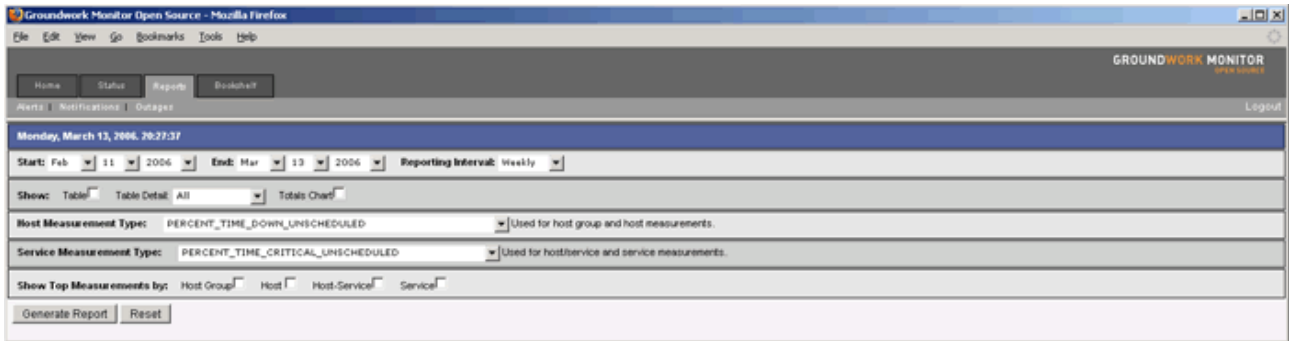
図 3.4.5. 停止 - ホスト/サービス Report



停止回数の多いサービス

このレポートのオプションは、停止回数の多い順にサービスをリストします。傾向チャートは、特定の日付の幅でサービスの停止数をグラフ化して表示します。各インターバルで積み重なったバーが、各ホストのサービス停止数の割合を示します。各バーの色は、上位リスト(右側の表)の色と対応します。

図 3.4.6. 停止 - サービス Report



停止レポートの作成

停止レポートを作成するには、下記に説明するレポートオプションを選んでから、Generate Reportを選択します。

図 3.4.7. 停止 - レポートの作成

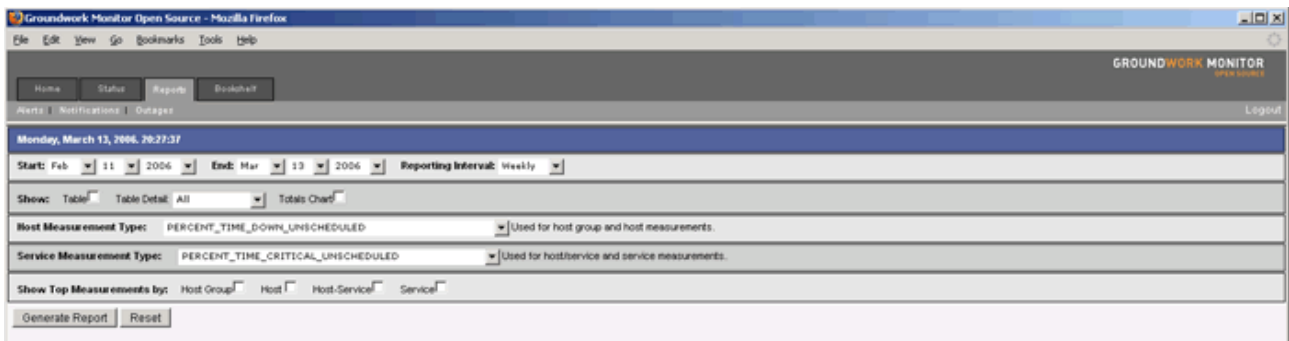


表 3.4.1. 停止 - レポートの作成

フィールド	説明
Start (開始)	作成するレポートの開始日付を選びます。
End (終了)	作成するレポートの終了日付を選びます。
Reporting Interval (レポート間隔)	データをレポートする間隔 (日次、週次、月次、年次) を指示します。
Table (表)	作成したレポートの中に計測値の表を表示します。
Table Detail Level (詳細レベルの表)	アラーム、ワーニング、通知についての各ホストグループ、ホスト、ホスト/サービスやサービス毎の詳細データを計測値の表の中にリストします。
Totals Chart (総合チャート)	トータルのアラーム、ワーニングおよび通報の傾向チャートを表示します
Host Measurement Type (ホストの計測タイプ)	選択されたパラメータは、ホストやホストグループに関連するすべての計算とチャートに使用されます。これらは、Nagios監視システムからの可用性の計測値です。
Service Measurement Type (サービスの計測タイプ)	選択されたパラメータは、ホスト/サービスやサービスに関連するすべての計算とチャートに使用されます。これらは、Nagios監視システムからの可用性の計測値です。
Top Measurements by: Host Group (計測値の大きいホストグループ)	レポート中にホストグループのチャートを作成します
Top Measurements by: Host (計測値の大きいホスト)	レポート中にホストのチャートを作成します
Top Measurements by: Host/Service (計測値の大きいホスト/サービス)	レポート中にホスト/サービスのチャートを作成します
Top Measurements by: Service (計測値の大きいサービス)	レポート中にサービスのチャートを作成します

第5章 レポートの詳細

Nagios監視システムは全てのホストとサービスチェックの結果を含むログを作成します。セットされる時間に、Ground Workのデータ収集プログラムは、このファイルを読み、結果をMySQLデータベースにロードします。ひとつのレコードが各計測値のタイプ、コンポーネントと日毎に生成されます。アラーム、ワーニングと通知データはこの方法で集められます。

停止レポートでは、GroundWorkのデータ収集プログラムは、NagiosのWebインタフェースを使って、Nagios可用性レポートを作成し、その結果をデータベースにロードします。データ収集プログラムは、Nagiosからのホストとサービス可用性の計測値を要求するため HTTPを使います。

インサイトレポートのCGIプログラムは、データベースに問い合わせるWebページとチャートを作成して、レポートページを作ります。

第4部 BOOKSHELFを使ってドキュメントをアクセスする

本セクションでは、GroundWork Monitor Open Source内のBookshelf(本棚)機能を説明します。Bookshelfは、GroundWork Monitor Open Sourceのインストレーションや Nagiosプラグインを含む、最新のGroundWork Monitor Open Sourceとオープンソースのリファレンス文献に容易にアクセスできるようにした、GroundWorkの製品ドキュメントライブラリです。また、Bookshelfは、あなたが固有のドキュメントや手順書を統合することができるよう構成設定(コンフィギュレーション)可能です。その情報は、GroundWork Monitor Open Source管理者 ガイドに記述されています。

第1章 概要

第2章 ブックシェルフ内をナビゲートする

第3章 ブックシェルフ内を検索する

第1章 概要

GroundWorkの製品ドキュメントとオープンソースのリファレンス文献は、GroundWork Monitor Open SourceのBookshelfオプションを介してアクセスできます。GroundWorkのリファレンスは、システムの主な3つのユーザ:管理者、開発者とオペレータ向けにまとめられています。それぞれのユーザ向けの関連ドキュメントは、それらの適切なディレクトリに収められています。オープンソースのリファレンスは、Nagios Pluginsのように、オープンソースのリファレンス文献のタイトルによって整理されています。

下表で、現在、本バージョンのGroundWork Monitor Open Sourceの中にある異なるカテゴリとドキュメントをリストアップします。

表 4.1.1. GroundWorkリファレンス

ADMINISTRATOR (管理者)	
GroundWork Monitor Open Source Administrator Guide	GroundWork Monitor Open Source Administrator Guide 1.0 には、GroundWork Monitor Open Source 4.5の管理の詳細が記述されています。このガイドは、システムの初期導入や管理の一環として、システムのインストール、構成設定、カスタマイズと保守をする必要がある、システム管理者向けの情報を提供します。
GroundWork Monitor Open Source Profiles	このプロファイルフォルダには、GroundWorkがGroundWork Monitor Open Source版のために配布するプロファイル定義、つまり、Service Ping、SNMP NetworkとSSH Unixを含んでいます。
Profiles Overview	このドキュメントはGroundWork Monitor Open Sourceのプロファイル、プロファイルのサイン、アップデートとプロファイルグラフについて説明します。
SSH Monitoring on UNIX	このドキュメントは、GroundWorkのNagios コンポーネントからプラグインを実行するために、SSHコネクションをセットアップするプロセスを説明します。一度このアクセスが整備されると、SSHを実行している限り、容易にUNIXホストをさまざま面から監視することができます。
DEVELOPER (開発者)	
GroundWork Monitor Open Source Developer Guide	GroundWork Monitor Open Source Developer Guide 1.0 には、GroundWork Foundation (GroundWork Monitor Open Sourceパッケージの基礎を成すデータにアクセスするもの)を含む、GroundWork Monitor Open Source 4.5の詳しい開発者リファレンスが記述されています。
OPERATOR(オペレータ)	
GroundWork Monitor Open Source Operator Guide	GroundWork Monitor Open Source Operator Guide 1.0 には、GroundWork Monitor Open Source 4.5のオペレーションの詳細が記述されています。このガイドは、GroundWork Monitor Open Sourceが始めてのユーザ向けにデザインされています。このガイドの中の情報は、どのようにアクセスし、使い、ユーザインタフェースを介してシステムや他のリソースとやり取りするかを説明します。それは、どうやって監視状態、詳細なコンポーネントビューを見、可用性とパフォーマンスレポートやアラート履歴を作成するかへのオペレータ指示を提供し、GroundWork Monitor Open Source ユーザのためのオペレーションリファレンスガイドとしても意図されています。読者は、プログラミングやソフトウェア開発の知識を必要としませんが、基本的な監視についての概ね慣れているべきでしょう。

表 4.1.2. オープンソースリファレンス

MySQL	MySQL概要は、MySQLの簡単な説明とMySQLのリソースへのリンクを提供します。
Nagios	Nagios概要は、Nagios と Nagiosプラグインの簡単な説明とさまざまな Nagios リソースへのリンクを提供します。 さらに、このホルダには GroundWork Monitor Open Sourceで配布するプラグインのための説明と利用法およびオプション情報が含まれています。
Perl	Perl概要は、Perlの簡単な説明とPerlのリソースへのリンクを提供します。
PHP	PHP概要は、PHPの簡単な説明とPHPのリソースへのリンクを提供します。
RRDtool	RRDtool概要は、Manページを含む、RRDtoolの説明を提供し、RRDtoolのリソースへのリンクを提供します。
WMI	WMI概要は、WMIの簡単な説明とWMIのリソースへのリンクを提供します。

第2章 Bookshelf 内のナビゲーション


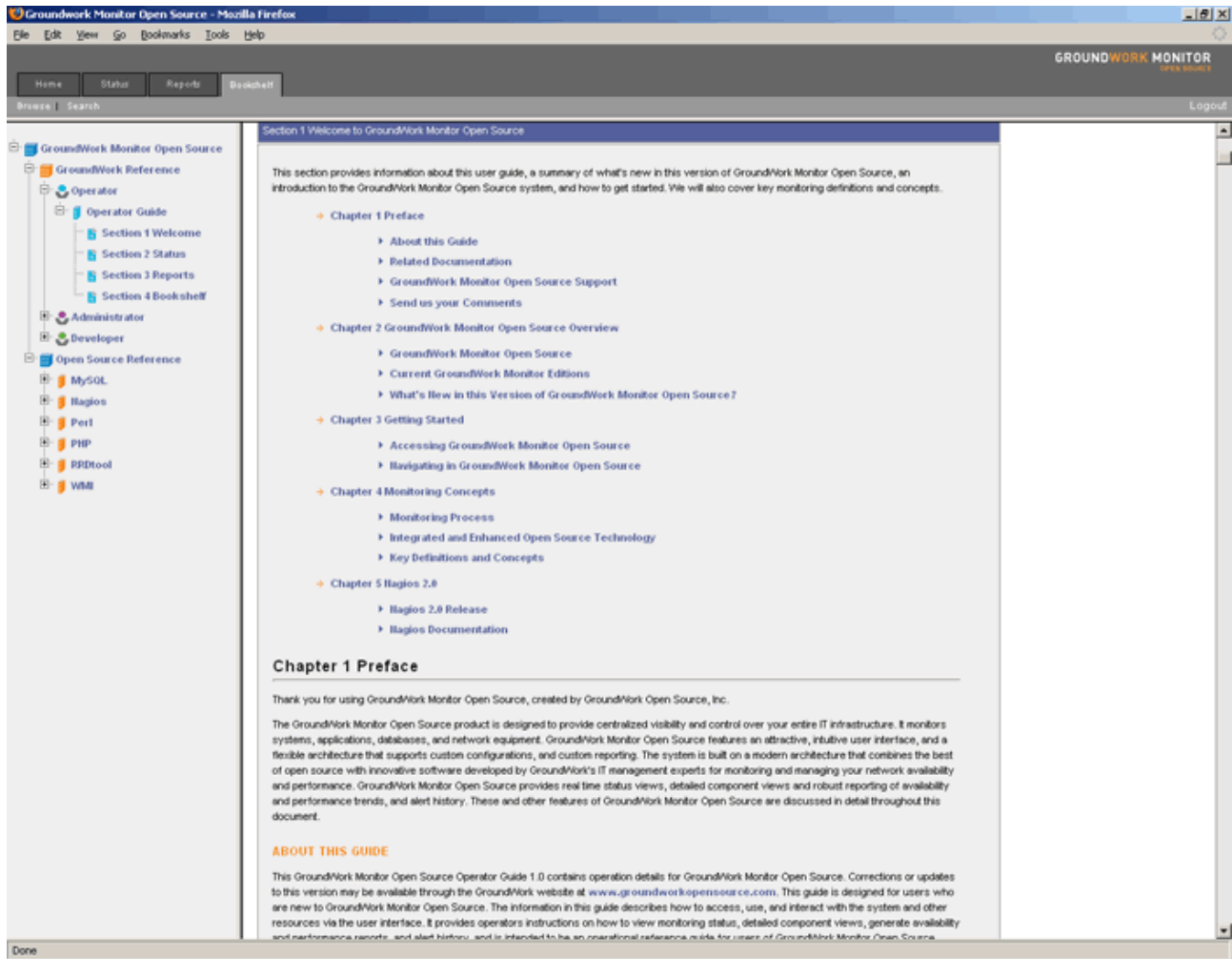
GroundWork Monitor Open SourceのBookshelfは、ツリーナビゲーションと一体になっています。Bookshelfに入ると、ツリーナビゲーションが左に表示されます。カテゴリの隣の  と、参照したいドキュメントを選びます。ドキュメントを選択すると、右側の枠に表示されます。本の中のセクションや章をナビゲートするのにドキュメントの中のリンクを使うことができます。また、左側の枠にもドキュメント内のナビゲーションが表示されます。

図 4.2.1. Bookshelf内のナビゲーション



第3章 Bookshelf内の検索 (Search)

Bookshelfオプションには、検索フィルタ機能が含まれています。下記のステップに従い、キーワードやフレーズでBookshelf内のドキュメントを検索します。

1. Bookshelf画面の上部にある **Search** を選びます。Search the Bookshelfのボックスが表示されるでしょう。
2. **Query** ボックスにキーワードやフレーズを入力します。
3. **Search** ボタンを選びます。
4. システムは、入力したキーワードやフレーズにマッチするすべてのコンテンツのリストを返すでしょう。また、検索でマッチした数も示されます。あなたが選んだ青色のリンクをクリックすることで、リストされたドキュメントのどれでも開くことができます。いつでも **Browse** を選ぶことで、検索機能を抜けることができます。

図 4.3.1. Bookshelf内の検索

