



---

Network Management + Monitoring Solutions  
ネットワークの管理 と 監視へのソリューション

## ネットワークディレクターの特徴

アプリケーション配信の非効率、遅延、障害は、管理コストの増大ばかりか、業務と信用に悪影響を及ぼす恐れもあります。ネットワークディレクターの製品は、ネットワーク管理者が前述の影響を最小限に抑え、アプリケーションの配信および稼働に対し簡略かつ戦略的管理を可能にします。

- ・ 市販ソフトウェアに比較して大幅に割安な費用で、無理のないTCO(総使用コスト)を実現
- ・ 弊社の技術者とオープンソースコミュニティによるフルサポート
- ・ 広範囲のネットワーク、ホスト、アプリケーション、サービスを監視する設定が可能
- ・ 拡張性の高いプラグイン構築によって容易な追加とユーザーニーズの監視の実行が可能
- ・ システム、ネットワーク担当者への電子メール、SMS、インスタントメッセージを使用した事前通告サービスによるアラート送信
- ・ 停電や故障の際に直ちに対処するように構成されるエスカレーション
- ・ MRTG2とSmoke pingの機能を組み込んだ次世代のネットワーク監視
- ・ ネットワークの認識がすべてできるコンソールの集中化
- ・ 設定可能なwebベースのレポートによって、ネットワーク管理者は可用性レポートの分析、パフォーマンスのグラフ表示、統計レポートの作成が瞬時に可能
- ・ フェイルオーバー機能を持つ高可用性マスター/スレーブにネットワークディレクターをインストール
- ・ SSHまたはVPN経由のリモートネットワーク監視
- ・ Windowsのホストとサービスのエージェントレス監視はWMIプロキシの利用で入手可能
- ・ 標準範囲(CPU、ディスク、メモリー)のパフォーマンスグラフは全ホストとデバイスに対して使用可能
- ・ テキストベースの設定ファイルではなく、ホスト、ホストグループ、サービス、サービスグループ、担当者、担当者グループ、リソースのWebベース管理
- ・ サービスの依存関係の機能によって、担当者はネットワークまたはアプリケーションの故障の際詳細の通知を受けるため、問題の追跡に無駄な時間を費やす必要がない
- ・ アクティブなステータスマップによって、ステータスとネットワークの依存関係をグラフ形状で表示

## 概要

ネットワークディレクターとは、ネットワークの監視及び管理を行うシステムで、個人向けや中小企業から大企業まで取り扱い可能なシステムです。70もの完成度の高いプロジェクトから成り、弊社のサポートチームやプロジェクト開発者によってサポートされています。以下は、プロジェクトの一部を一覧にしたものです。

- ADODB
- Apache
- CGI.pm
- Crypt-DES
- DBD-MySQL
- DBI
- Digest-HMAC
- Digest-MD5
- Digest-SHA
- Expat
- FontConfig
- Fping
- FreeTDS
- FreeType2
- Fruity
- GD2
- LibNet
- ModSSL
- NRPE
- NSCA
- NTP
- Nagios-Plugins
- Nagios2.0
- Net-SNMP
- Nmap
- Nuvola
- OpenLDAP
- OpenRadius
- OpenSSH
- OpenSSL
- PHP5
- Perl5.8
- SendEmail
- SleepyCatDB
- Smokeping
- T1lib
- TIME-HiRes
- XPM
- Bison
- cgilib
- Gawk
- Gdbm
- gettext
- glib
- GNU-findutils
- jpegsrc
- libart\_lgpl
- libol
- libpng
- PostgreSQL
- Qstat
- readline
- RRDTool
- sendEmail
- syslog-ng
- tcl8
- tk8
- zlib

## ネットワークディレクターのプラグイン

ネットワークディレクターのNagios Coreによってプラグインが実行されます。プラグインは多くの場合2つの目的を達成するように記述されています。1つ目は、サービスのステータスを検証するため、2つ目はそのサービスのパフォーマンスをネットワークディレクターに返信するためです。通常使用されるプラグインの一覧は以下のとおりです。



### Unix ベースプラグイン

check_dhcp	check_nrpe
check_dig	check_ntp
check_disk	check_oracle
check_dns	check_novell
check_file_age	check_mssql
check_fping	check_pgsql
check_ftp	check_ping
check_ftpj	check_pop
check_hpjd	check_procs
check_http	check_rpc
check_icmp	check_sensors
check_ifoperstatus	check_simap
check_ifstatus	check_smtp
check_imap	check_snmp
check_linux_disk_io	check_spop
check_linux_memory	check_ssh
check_linux_net_io	check_ssntp
check_load	check_swap
check_log	check_tcp
check_mailq	check_time
check_mysql	check_udp
check_net_connstate	check_udp2
check_nntp	check_unix_open_fh
check_nntp	

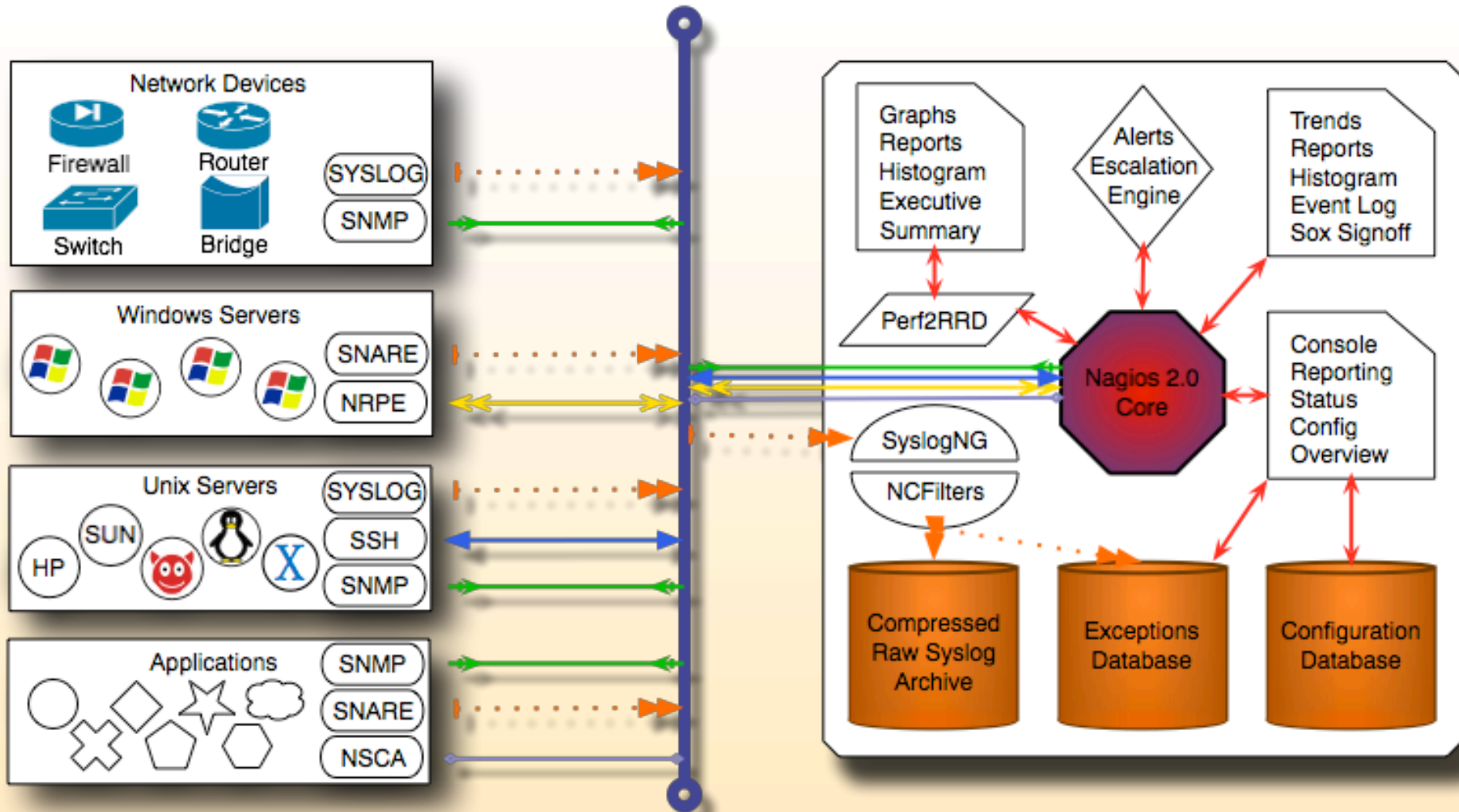


### Windows ベースプラグイン

check_counter.vbs	wmi_exchange_mailbox_size.vbs
check_counter2.vbs	wmi_exchange_mta_workq.vbs
check_counter2_rate.vbs	wmi_exchange_public_receiveq.vbs
check_counter_rate.vbs	wmi_exchange_public_sendq.vbs
check_printque.vbs	wmi_mem.vbs
check_process.vbs	wmi_mssql_buf_cache_hit.vbs
check_process2.vbs	wmi_mssql_latch_waits.vbs
check_service.vbs	wmi_mssql_lock_wait_time.vbs
check_service2.vbs	wmi_mssql_log_growth.vbs
mssql_buf_cache_hit.vbs	wmi_mssql_log_used.vbs
mssql_latch_waits.vbs	wmi_mssql_transactions.vbs
mssql_lock_wait_time.vbs	wmi_printqueue.vbs
mssql_log_growth.vbs	wmi_process.vbs
mssql_log_growth1.vbs	wmi_service.vbs
mssql_log_used.vbs	wmi_swap.vbs
mssql_log_used1.vbs	
mssql_transactions.vbs	
wmi_cpu.vbs	
wmi_disks.vbs	
wmi_drive.vbs	
wmi_exchange_diskfile.vbs	
wmi_exchange_mailbox_receiveq.vbs	
wmi_exchange_mailbox_sendq.vbs	

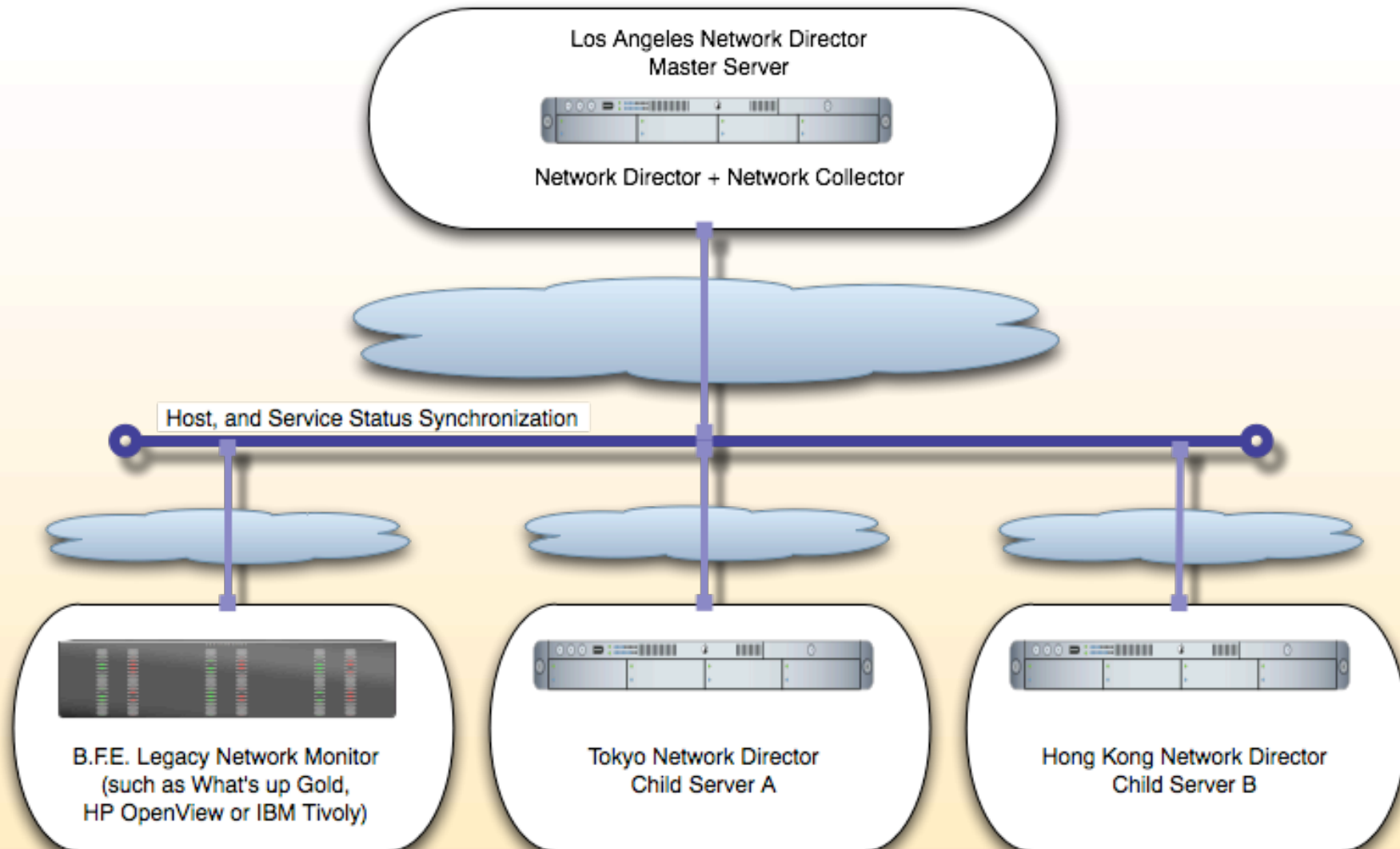
## 監視フローと相关性

ネットワーク装置、ホスト、アプリケーションはNagios 2.0 core によって探索され、処理されます。次にそのパフォーマンスデータは、グラフ化およびレポートのためにRR Database内に書き込まれ、処理されます。SyslogNGサーバーログはNetwork Collectorによって選別され、ネットワークディレクターによって処理およびアーカイブされます。スラッシュホールド値を超えるプラグイン値は、Alerts Engineに転送されます。Configuration DatabaseにWebベース構成を格納します。このように多様な技術を使用して、多岐にわたるアプリケーションを監視できます。



## 分散型監視と高汎用性監視を実現

ネットワークディレクターは安全なネットワーク通信経路で分散型監視を可能にします。アクティブなスレイブサーバーは、ホストとサービスのステータス情報をマスターサーバーに送信します。また、マスターサーバーとスレイブサーバーはCisco Works、Dell Open ManageまたはSmartsなどの他の市販の監視ソリューションのステータス情報を取り込み、受け入れるように設定することも可能です。



## 定義

### ホスト:

ホストとは、汎用性ステータスが監視される必要のあるコンピューターを指します。このコンピューターはIPアドレスを持っていることもあれば、持っていないこともあります。サーバー、ルーター、スイッチ、ファイアウォール、PBX、負荷分散装置、SAN、アプリケーションまたはクラスターなどのデバイスまたはソフトウェアである場合もあります。

### ホスト グループ:

レポートおよび表示を目的とする1つ以上のホストのグループのことです。

### サービス:

ホストオブジェクトに関連するパラメーター、ステータス、または要求のことです。

### サービス グループ:

レポートおよび表示を目的とする1つ以上のサービスのグループのことです。

### 担当者:

担当者とは、ネットワーク上に問題が発生した場合に通知される人物のことです。

### 時間帯:

時間帯とは、サービスの点検並びに担当者への連絡が行なわれる時間帯を指します。

### コマンド:

コマンドは特定の機能のために定義、実行され、さらに、サービスの検証、サービスの通知、サービスイベントハンドラー、ホストの検証、ホストイベントハンドラー用に定義されます。

### サービスの依存関係:

複数のサービスのステータスに基づき、アクティブサービスの検証を抑制することです。

[次のページへ続く](#)

## 定義

### サービス エスカレーション:

担当者が問題があるサービスの通知を受け取れなかった場合、他のネットワーク管理者またはネットワーク マネージャーに通知を自動変更することです。

### ホストの依存関係:

複数のホストのステータスに基づき、アクティブなホストの検証を抑制することです。

### ホスト エスカレーション:

担当者が問題があるホストの通知を受け取れなかった場合、他のネットワーク管理者またはネットワーク マネージャーに通知を自動変更することです。

### 拡張ホスト情報:

拡張ホスト情報とは、CGIに伝えるために使用される情報で、検知可能なホストに関する追加の情報です。ネットワークディレクターでは、通常、ICMPの待ち時間やパケットロスをもとめてグラフ化するSmokepingを示します。

### 拡張サービス情報:

拡張サービス情報とは、CGIに伝えるために使用される情報で、検知可能なサービスに関する追加の情報です。ネットワークディレクターでは、通常、パフォーマンスデータまたはサービス点検後のサービス出力から作成されたグラフを示しています。

### サービス出力情報:

サービス出力情報とはCPU使用率、メモリ使用率、毎秒ランザクション回数、またはサーバールームの室温水準等に関して、OK、WARNING、CRITICAL、またはUNKOWNといった4種類のステータス等も含む、サービス点検に関連する情報のことです。

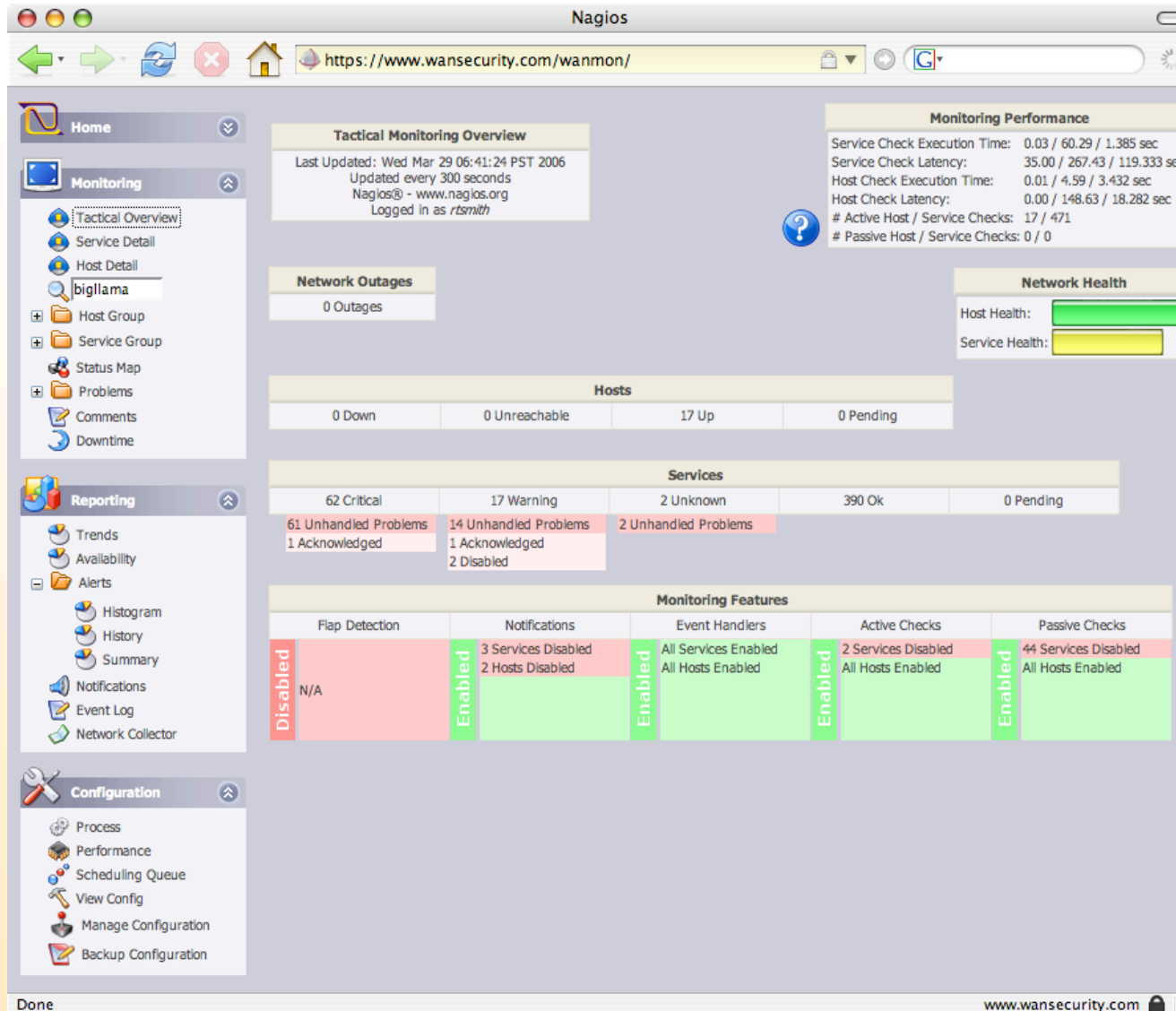
### パフォーマンスデータ:

パフォーマンスデータとは、監視されているサービスおよびホストのパフォーマンスの統計情報を収集、格納、レポートするために使用されます。パフォーマンスデータもまた、CPU使用率、メモリ使用率、毎秒ランザクション回数、またはサーバールームの湿度水準等に関するの情報となります。



## タクティカル オーバービュー (Tactical Overview)

タクティカルオーバービュー画面は、ネットワークや監視しているサーバーの状態を示す全体図です。アクティブホスト数とサービスチェック数、それらの実行回数、ネットワーク、ホスト、サービス障害数に関する情報を示しています。



The screenshot shows the Nagios Tactical Monitoring Overview dashboard. The browser address bar indicates the URL is <https://www.wansecurity.com/wanmon/>. The dashboard is divided into several sections:

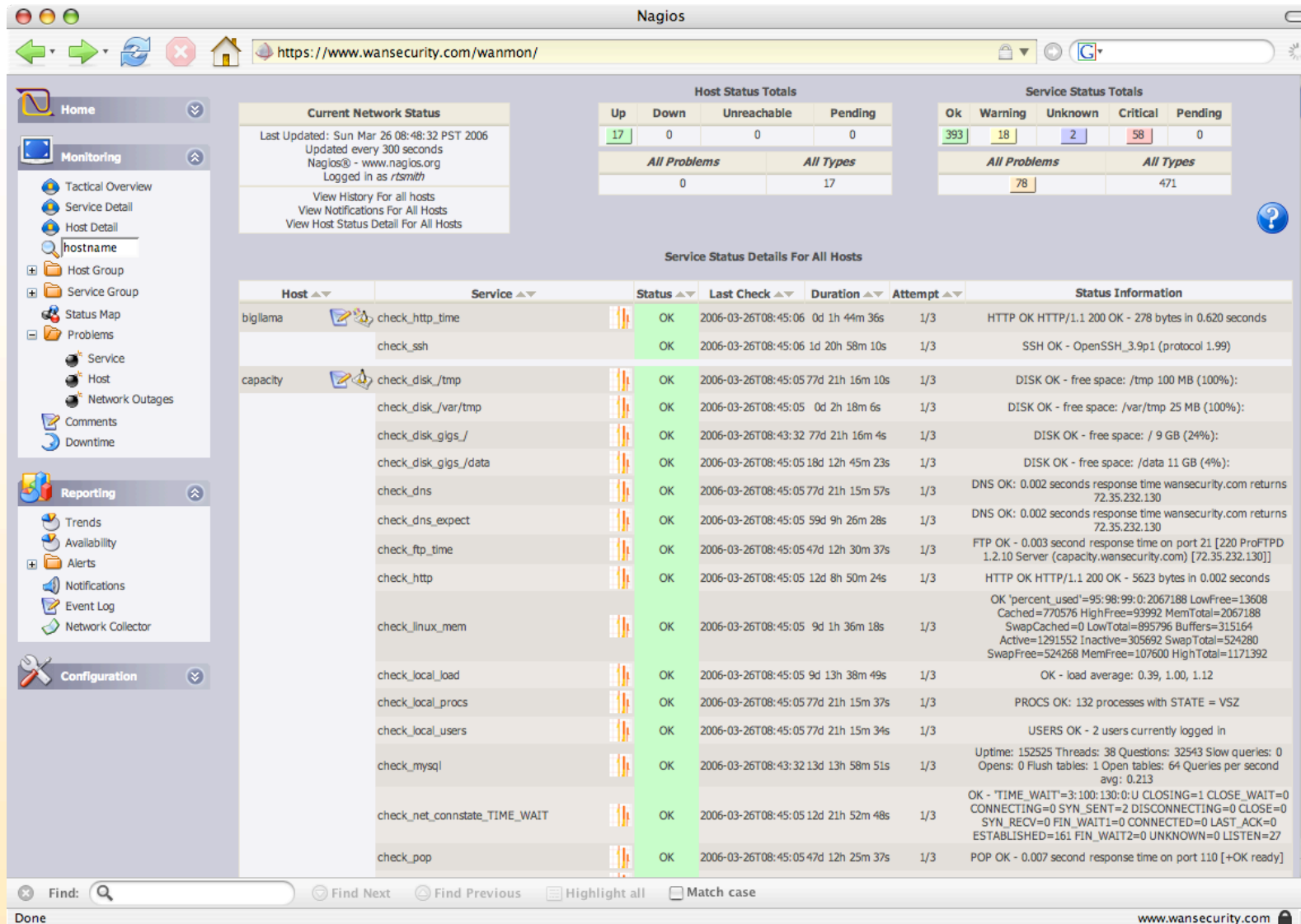
- Tactical Monitoring Overview:** Last Updated: Wed Mar 29 06:41:24 PST 2006, Updated every 300 seconds, Nagios@ - www.nagios.org, Logged in as rtsmith.
- Monitoring Performance:**
  - Service Check Execution Time: 0.03 / 60.29 / 1.385 sec
  - Service Check Latency: 35.00 / 267.43 / 119.333 sec
  - Host Check Execution Time: 0.01 / 4.59 / 3.432 sec
  - Host Check Latency: 0.00 / 148.63 / 18.282 sec
  - # Active Host / Service Checks: 17 / 471
  - # Passive Host / Service Checks: 0 / 0
- Network Outages:** 0 Outages
- Network Health:** Host Health: █, Service Health: █
- Hosts:** 0 Down, 0 Unreachable, 17 Up, 0 Pending
- Services:**
  - 62 Critical, 17 Warning, 2 Unknown, 390 Ok, 0 Pending
  - 61 Unhandled Problems (1 Acknowledged), 14 Unhandled Problems (1 Acknowledged, 2 Disabled), 2 Unhandled Problems
- Monitoring Features:**

	Flap Detection	Notifications	Event Handlers	Active Checks	Passive Checks
Disabled	N/A	Enabled	Enabled	Enabled	Enabled
		3 Services Disabled 2 Hosts Disabled	All Services Enabled All Hosts Enabled	2 Services Disabled All Hosts Enabled	44 Services Disabled All Hosts Enabled

The left sidebar contains navigation menus for Home, Monitoring (Tactical Overview, Service Detail, Host Detail, bigllama, Host Group, Service Group, Status Map, Problems, Comments, Downtime), Reporting (Trends, Availability, Alerts, Histogram, History, Summary, Notifications, Event Log, Network Collector), and Configuration (Process, Performance, Scheduling Queue, View Config, Manage Configuration, Backup Configuration).

## サービスの詳細

この画面では、各ホストのサービスステータスの詳細および全ホスト上のサービスすべてに対するサービス点検出力情報を確認できます。下の画面は、メニュー検索機能を使用してホストを検索する際に表示されるデフォルトの画面です。



The screenshot displays the Nagios web interface. At the top, there are summary tables for Host Status Totals and Service Status Totals. Below these is a table titled 'Service Status Details For All Hosts' which lists various services for two hosts: 'bigilama' and 'capacity'.

**Host Status Totals**

Up	Down	Unreachable	Pending
17	0	0	0
<b>All Problems</b>		<b>All Types</b>	
0		17	

**Service Status Totals**

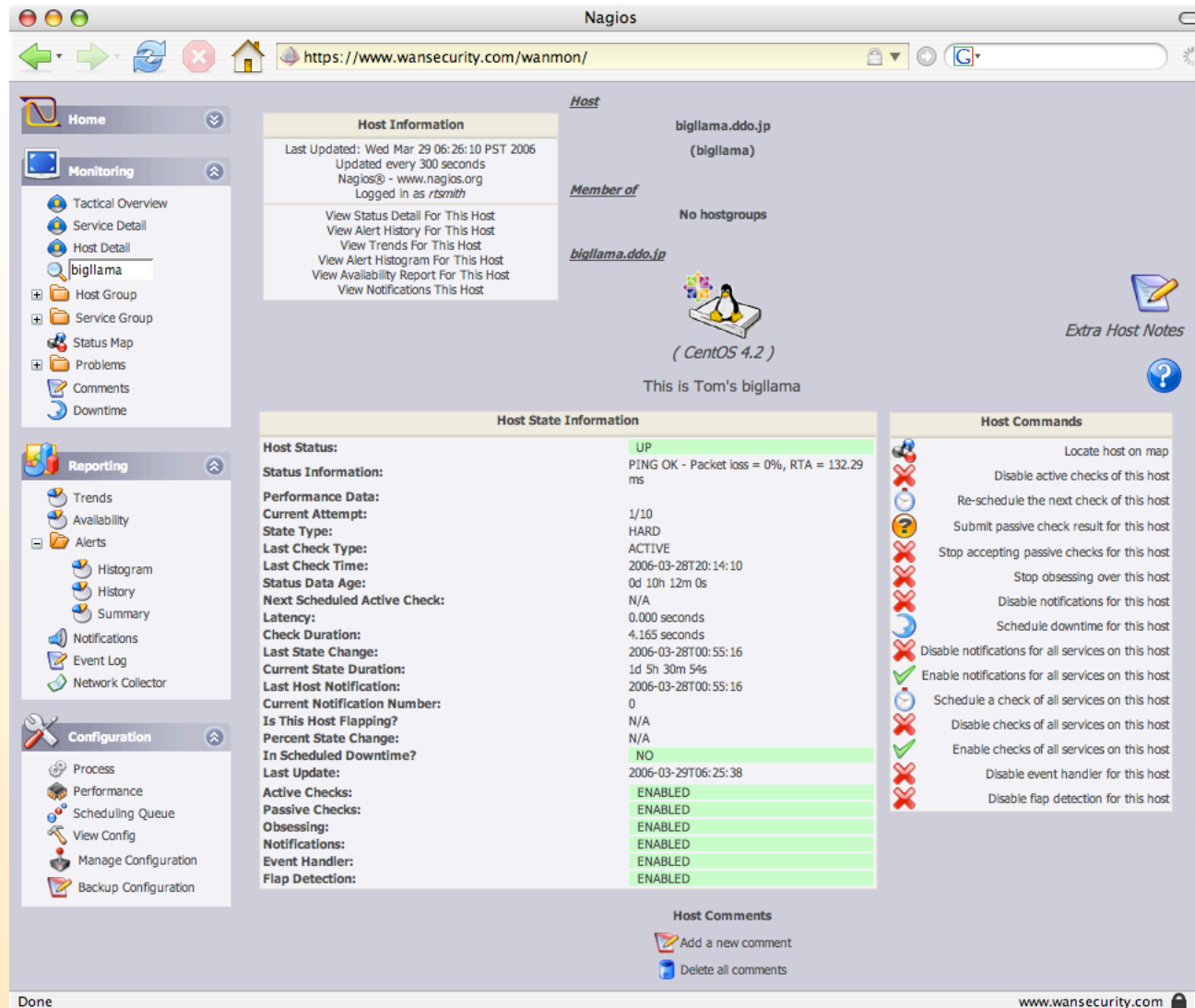
Ok	Warning	Unknown	Critical	Pending
393	18	2	58	0
<b>All Problems</b>		<b>All Types</b>		
78		471		

**Service Status Details For All Hosts**

Host	Service	Status	Last Check	Duration	Attempt	Status Information
bigilama	check_http_time	OK	2006-03-26T08:45:06	0d 1h 44m 36s	1/3	HTTP OK HTTP/1.1 200 OK - 278 bytes in 0.620 seconds
	check_ssh	OK	2006-03-26T08:45:06	1d 20h 58m 10s	1/3	SSH OK - OpenSSH_3.9p1 (protocol 1.99)
capacity	check_disk_/tmp	OK	2006-03-26T08:45:05	77d 21h 16m 10s	1/3	DISK OK - free space: /tmp 100 MB (100%):
	check_disk_/var/tmp	OK	2006-03-26T08:45:05	0d 2h 18m 6s	1/3	DISK OK - free space: /var/tmp 25 MB (100%):
	check_disk_gigs_/	OK	2006-03-26T08:43:32	77d 21h 16m 4s	1/3	DISK OK - free space: / 9 GB (24%):
	check_disk_gigs_/data	OK	2006-03-26T08:45:05	18d 12h 45m 23s	1/3	DISK OK - free space: /data 11 GB (4%):
	check_dns	OK	2006-03-26T08:45:05	77d 21h 15m 57s	1/3	DNS OK: 0.002 seconds response time wansecurity.com returns 72.35.232.130
	check_dns_expect	OK	2006-03-26T08:45:05	59d 9h 26m 28s	1/3	DNS OK: 0.002 seconds response time wansecurity.com returns 72.35.232.130
	check_ftp_time	OK	2006-03-26T08:45:05	47d 12h 30m 37s	1/3	FTP OK - 0.003 second response time on port 21 [220 ProFTPD 1.2.10 Server (capacity.wansecurity.com) [72.35.232.130]]
	check_http	OK	2006-03-26T08:45:05	12d 8h 50m 24s	1/3	HTTP OK HTTP/1.1 200 OK - 5623 bytes in 0.002 seconds
	check_linux_mem	OK	2006-03-26T08:45:05	9d 1h 36m 18s	1/3	OK 'percent_used'=95:98:99:0:2067188 LowFree=13608 Cached=770576 HighFree=93992 MemTotal=2067188 SwapCached=0 LowTotal=895796 Buffers=315164 Active=1291552 Inactive=305692 SwapTotal=524280 SwapFree=524268 MemFree=107600 HighTotal=1171392
	check_local_load	OK	2006-03-26T08:45:05	9d 13h 38m 49s	1/3	OK - load average: 0.39, 1.00, 1.12
	check_local_procs	OK	2006-03-26T08:45:05	77d 21h 15m 37s	1/3	PROCS OK: 132 processes with STATE = VSZ
	check_local_users	OK	2006-03-26T08:45:05	77d 21h 15m 34s	1/3	USERS OK - 2 users currently logged in
	check_mysql	OK	2006-03-26T08:43:32	13d 13h 58m 51s	1/3	Uptime: 152525 Threads: 38 Questions: 32543 Slow queries: 0 Opens: 0 Flush tables: 1 Open tables: 64 Queries per second avg: 0.213
check_net_connstate_TIME_WAIT	OK	2006-03-26T08:45:05	12d 21h 52m 48s	1/3	OK - 'TIME_WAIT'=3:100:130:0:U CLOSING=1 CLOSE_WAIT=0 CONNECTING=0 SYN_SENT=2 DISCONNECTING=0 CLOSE=0 SYN_RECV=0 FIN_WAIT1=0 CONNECTED=0 LAST_ACK=0 ESTABLISHED=161 FIN_WAIT2=0 UNKNOWN=0 LISTEN=27	
check_pop	OK	2006-03-26T08:45:05	47d 12h 25m 37s	1/3	POP OK - 0.007 second response time on port 110 [+OK ready]	

## ホスト情報

ホスト情報の画面では、ホストに関する情報を確認でき、ホストコマンドを多数実行できます。図中のこのホストには、関連のあるメモを掲載した「Extra Host Notes」(画面右上隅のメモ帳のアイコン)があります。この場合、ホストのICMPの待ち時間やパケットロスのチェックをまとめたSmokepingスタイルのグラフになりますが、拡張ホスト情報であればメモとして掲載されます。



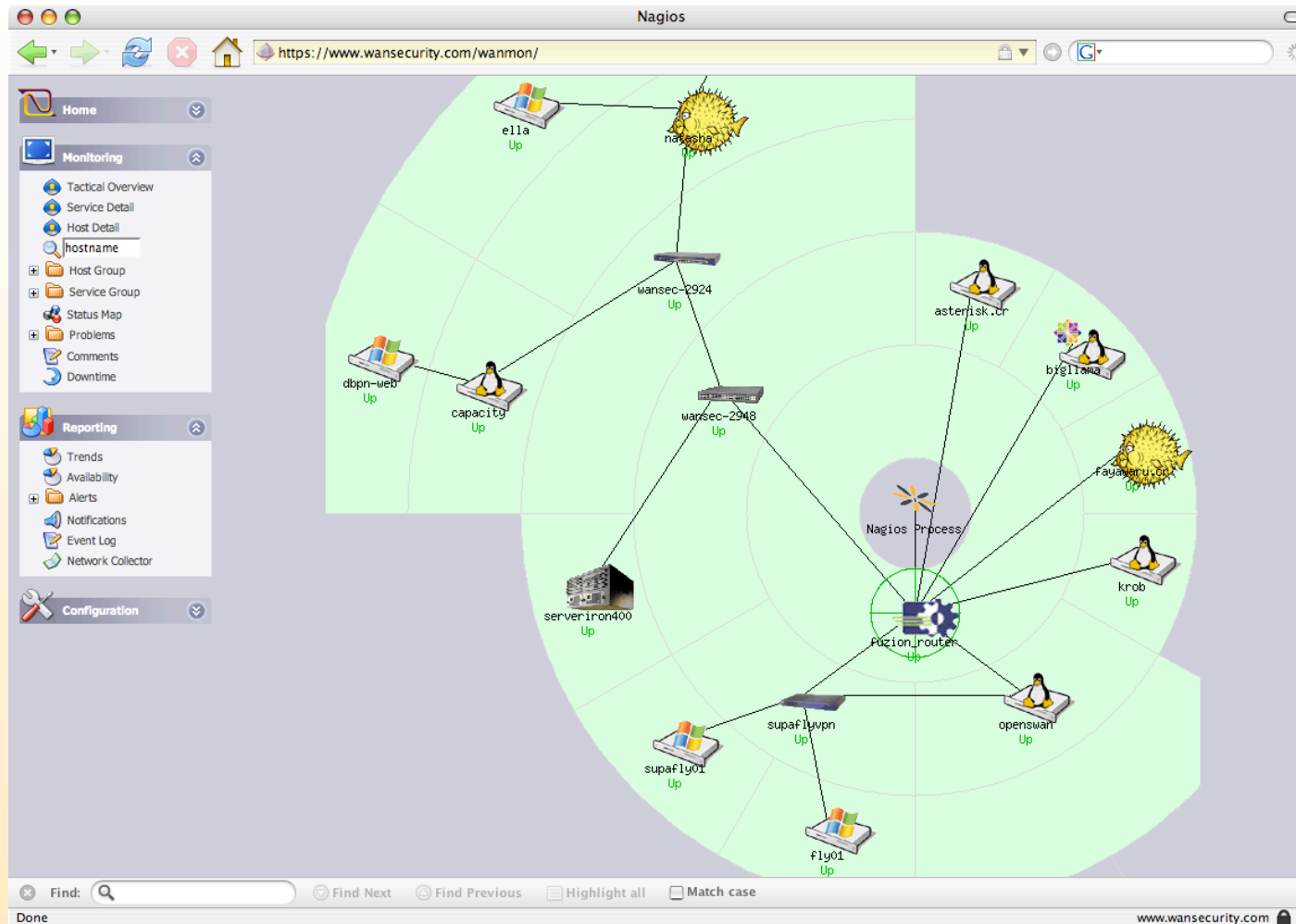
The screenshot shows the Nagios web interface for a host named 'bigllama.ddo.jp'. The interface is divided into several sections:

- Host Information:**
  - Host: bigllama.ddo.jp (bigllama)
  - Last Updated: Wed Mar 29 06:26:10 PST 2006
  - Updated every 300 seconds
  - Nagios® - www.nagios.org
  - Logged in as rtsmith
  - Member of: No hostgroups
  - Operating System: (CentOS 4.2)
  - Extra Host Notes icon is visible.
- Host State Information:**
  - Host Status: UP
  - Status Information: PING OK - Packet loss = 0%, RTA = 132.29 ms
  - Performance Data: 1/10
  - Current Attempt: HARD
  - State Type: ACTIVE
  - Last Check Type: 2006-03-28T20:14:10
  - Last Check Time: 0d 10h 12m 0s
  - Status Data Age: N/A
  - Next Scheduled Active Check: 0.000 seconds
  - Latency: 4.165 seconds
  - Check Duration: 2006-03-28T00:55:16
  - Last State Change: 1d 5h 30m 54s
  - Current State Duration: 2006-03-28T00:55:16
  - Last Host Notification: 0
  - Current Notification Number: N/A
  - Is This Host Flapping?: N/A
  - Percent State Change: N/A
  - In Scheduled Downtime?: NO
  - Last Update: 2006-03-29T06:25:38
  - Active Checks: ENABLED
  - Passive Checks: ENABLED
  - Obsessing: ENABLED
  - Notifications: ENABLED
  - Event Handler: ENABLED
  - Flap Detection: ENABLED
- Host Commands:**
  - Locate host on map
  - Disable active checks of this host
  - Re-schedule the next check of this host
  - Submit passive check result for this host
  - Stop accepting passive checks for this host
  - Stop obsessing over this host
  - Disable notifications for this host
  - Schedule downtime for this host
  - Disable notifications for all services on this host
  - Enable notifications for all services on this host
  - Schedule a check of all services on this host
  - Disable checks of all services on this host
  - Enable checks of all services on this host
  - Disable event handler for this host
  - Disable flap detection for this host
- Host Comments:**
  - Add a new comment
  - Delete all comments

The left sidebar contains navigation menus for Home, Monitoring (Tactical Overview, Service Detail, Host Detail, Host Group, Service Group, Status Map, Problems, Comments, Downtime), Reporting (Trends, Availability, Alerts, Histogram, History, Summary, Notifications, Event Log, Network Collector), and Configuration (Process, Performance, Scheduling Queue, View Config, Manage Configuration, Backup Configuration).

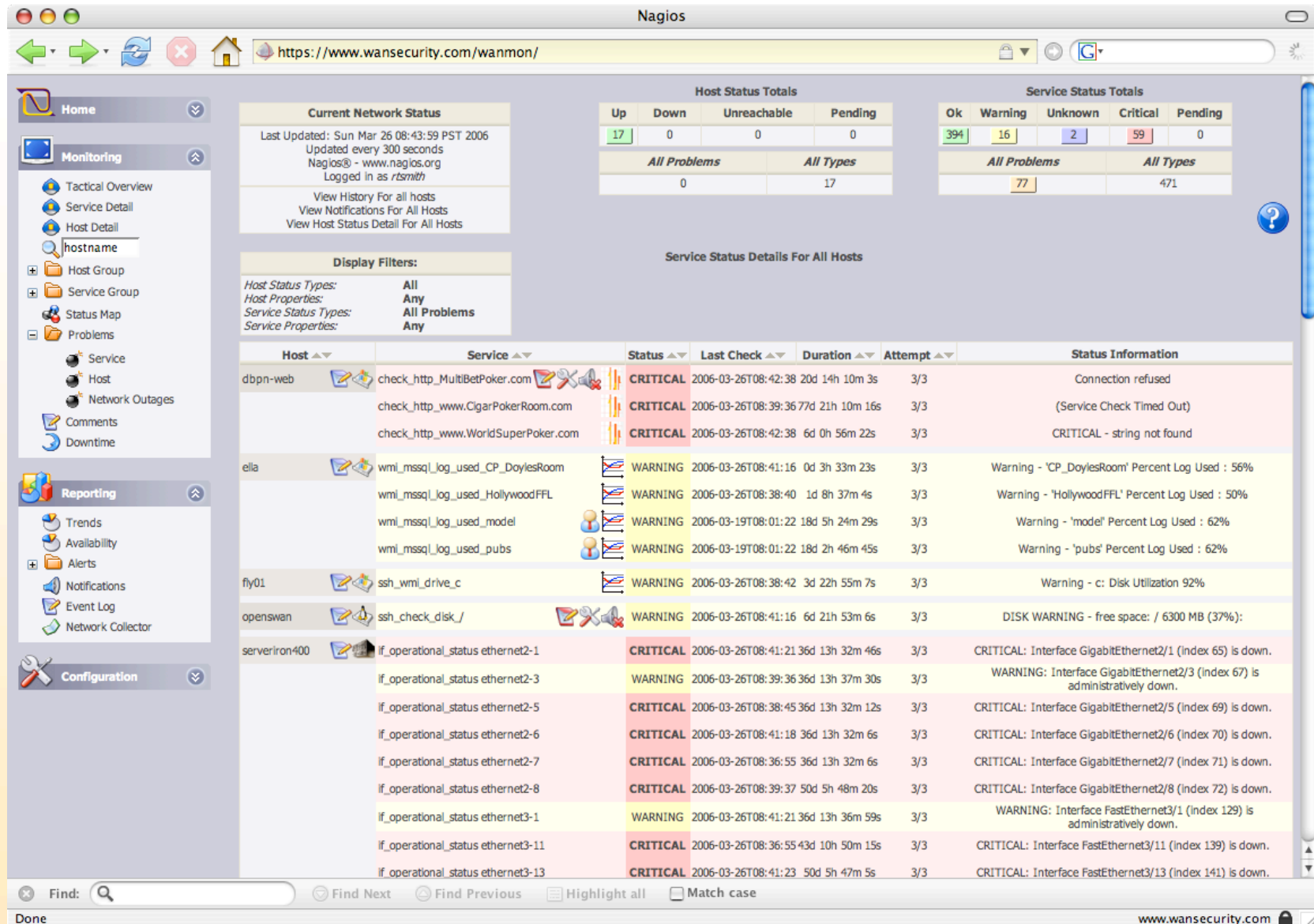
## ステータスマップ

アクティブなステータスマップでは、ホストの動向、タイプ、ステータス、マスターとスレーブの関係をすべてグラフィカルな表示で確認できます。このマップはcgi.cfgで指定した間隔で更新されます。この間隔の指定は、ネットワークディレクター設定のユーティリティで設定できます。マップ上では、SupaflyVPN (Cisco PIX 515E)とIPSecのVPN集線装置としてのOpenSwan2.4 (Linux搭載のホスト)間の相互の依存関係が確認できます。ホストの依存関係としては、Fly01とSupafly01はSupaflyVPN (Cisco PIX 515E)に依存しています。



## Problem ビュー

ProblemまたはTroubleビュー画面は、問題のあるホスト、問題のあるサービスと関連のあるホスト、ネットワーク障害のすべてを確認できます。



**Current Network Status**

Last Updated: Sun Mar 26 08:43:59 PST 2006  
 Updated every 300 seconds  
 Nagios® - www.nagios.org  
 Logged in as rsmith

View History For all hosts  
 View Notifications For All Hosts  
 View Host Status Detail For All Hosts

**Host Status Totals**

Up	Down	Unreachable	Pending
17	0	0	0
<b>All Problems</b>		<b>All Types</b>	
0		17	

**Service Status Totals**

Ok	Warning	Unknown	Critical	Pending
394	16	2	59	0
<b>All Problems</b>		<b>All Types</b>		
77		471		

**Display Filters:**

Host Status Types: All  
 Host Properties: Any  
 Service Status Types: All Problems  
 Service Properties: Any

**Service Status Details For All Hosts**

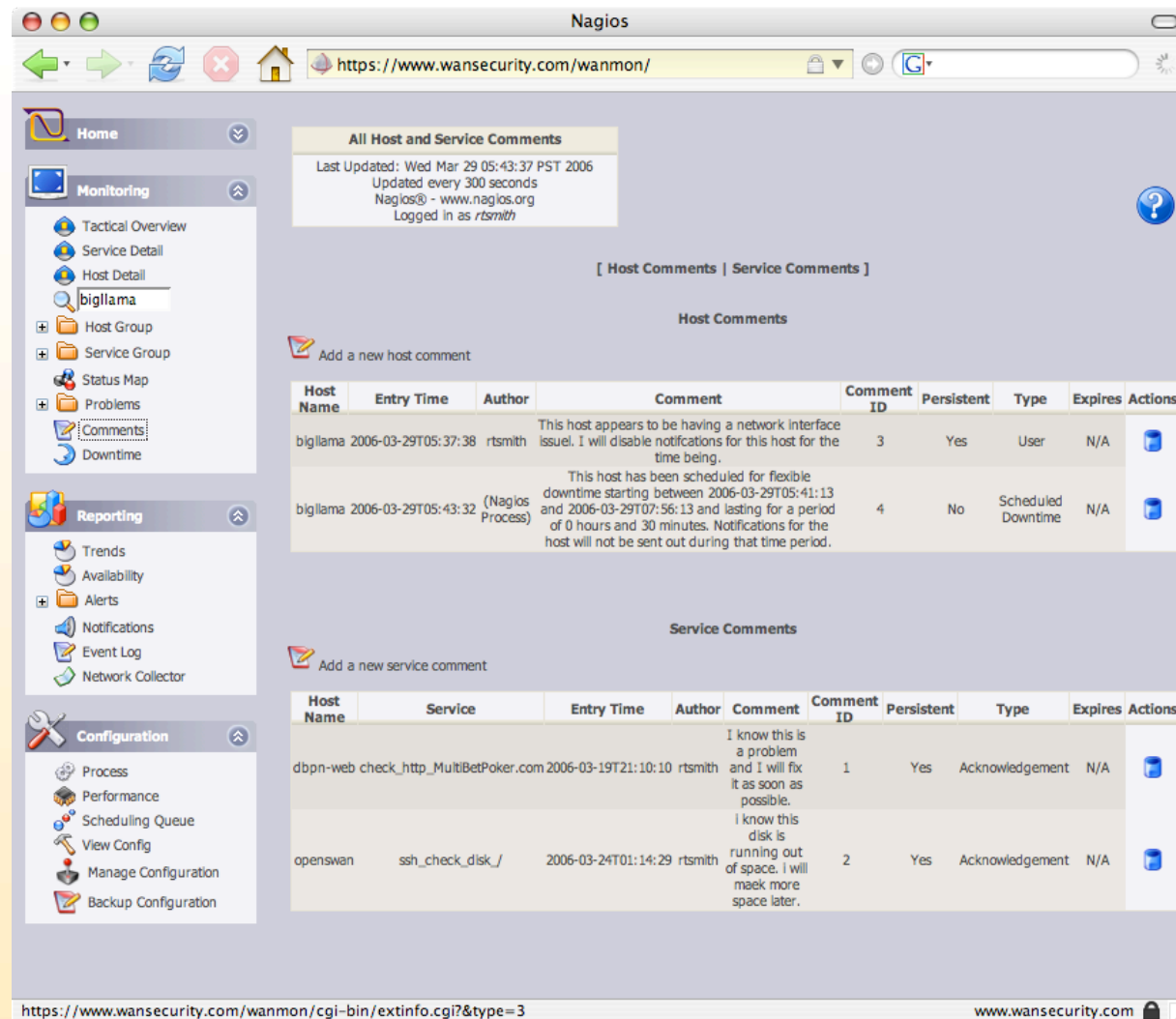
Host	Service	Status	Last Check	Duration	Attempt	Status Information
dbpn-web	check_http_MultiBetPoker.com	CRITICAL	2006-03-26T08:42:38	20d 14h 10m 3s	3/3	Connection refused
	check_http_www.CigarPokerRoom.com	CRITICAL	2006-03-26T08:39:36	77d 21h 10m 16s	3/3	(Service Check Timed Out)
	check_http_www.WorldSuperPoker.com	CRITICAL	2006-03-26T08:42:38	6d 0h 56m 22s	3/3	CRITICAL - string not found
ella	wmi_mssql_log_used_CP_DoylesRoom	WARNING	2006-03-26T08:41:16	0d 3h 33m 23s	3/3	Warning - 'CP_DoylesRoom' Percent Log Used : 56%
	wmi_mssql_log_used_HollywoodFFL	WARNING	2006-03-26T08:38:40	1d 8h 37m 4s	3/3	Warning - 'HollywoodFFL' Percent Log Used : 50%
	wmi_mssql_log_used_model	WARNING	2006-03-19T08:01:22	18d 5h 24m 29s	3/3	Warning - 'model' Percent Log Used : 62%
	wmi_mssql_log_used_pubs	WARNING	2006-03-19T08:01:22	18d 2h 46m 45s	3/3	Warning - 'pubs' Percent Log Used : 62%
fly01	ssh_wmi_drive_c	WARNING	2006-03-26T08:38:42	3d 22h 55m 7s	3/3	Warning - c: Disk Utilization 92%
openswan	ssh_check_disk_/_	WARNING	2006-03-26T08:41:16	6d 21h 53m 6s	3/3	DISK WARNING - free space: / 6300 MB (37%):
serveriron400	if_operational_status ethernet2-1	CRITICAL	2006-03-26T08:41:21	36d 13h 32m 46s	3/3	CRITICAL: Interface GigabitEthernet2/1 (index 65) is down.
	if_operational_status ethernet2-3	WARNING	2006-03-26T08:39:36	36d 13h 37m 30s	3/3	WARNING: Interface GigabitEthernet2/3 (index 67) is administratively down.
	if_operational_status ethernet2-5	CRITICAL	2006-03-26T08:38:45	36d 13h 32m 12s	3/3	CRITICAL: Interface GigabitEthernet2/5 (index 69) is down.
	if_operational_status ethernet2-6	CRITICAL	2006-03-26T08:41:18	36d 13h 32m 6s	3/3	CRITICAL: Interface GigabitEthernet2/6 (index 70) is down.
	if_operational_status ethernet2-7	CRITICAL	2006-03-26T08:36:55	36d 13h 32m 6s	3/3	CRITICAL: Interface GigabitEthernet2/7 (index 71) is down.
	if_operational_status ethernet2-8	CRITICAL	2006-03-26T08:39:37	50d 5h 48m 20s	3/3	CRITICAL: Interface GigabitEthernet2/8 (index 72) is down.
	if_operational_status ethernet3-1	WARNING	2006-03-26T08:41:21	36d 13h 36m 59s	3/3	WARNING: Interface FastEthernet3/1 (index 129) is administratively down.
	if_operational_status ethernet3-11	CRITICAL	2006-03-26T08:36:55	43d 10h 50m 15s	3/3	CRITICAL: Interface FastEthernet3/11 (index 139) is down.
	if_operational_status ethernet3-13	CRITICAL	2006-03-26T08:41:23	50d 5h 47m 5s	3/3	CRITICAL: Interface FastEthernet3/13 (index 141) is down.

Find:  Find Next Find Previous Highlight all Match case

Done www.wansecurity.com

## ホスト コメントとサービス コメント

ホストコメントとサービスコメントの入力によって、ネットワーク管理者は、サービスとホストの問題を認識し、ホストまたはサービス通知の拡大を防ぎ、関連のある問題に関する注記を残すことができます。さらに、他のネットワーク管理者が問題解決の現在の進行状況を確認できます。



The screenshot shows the Nagios web interface with the following components:

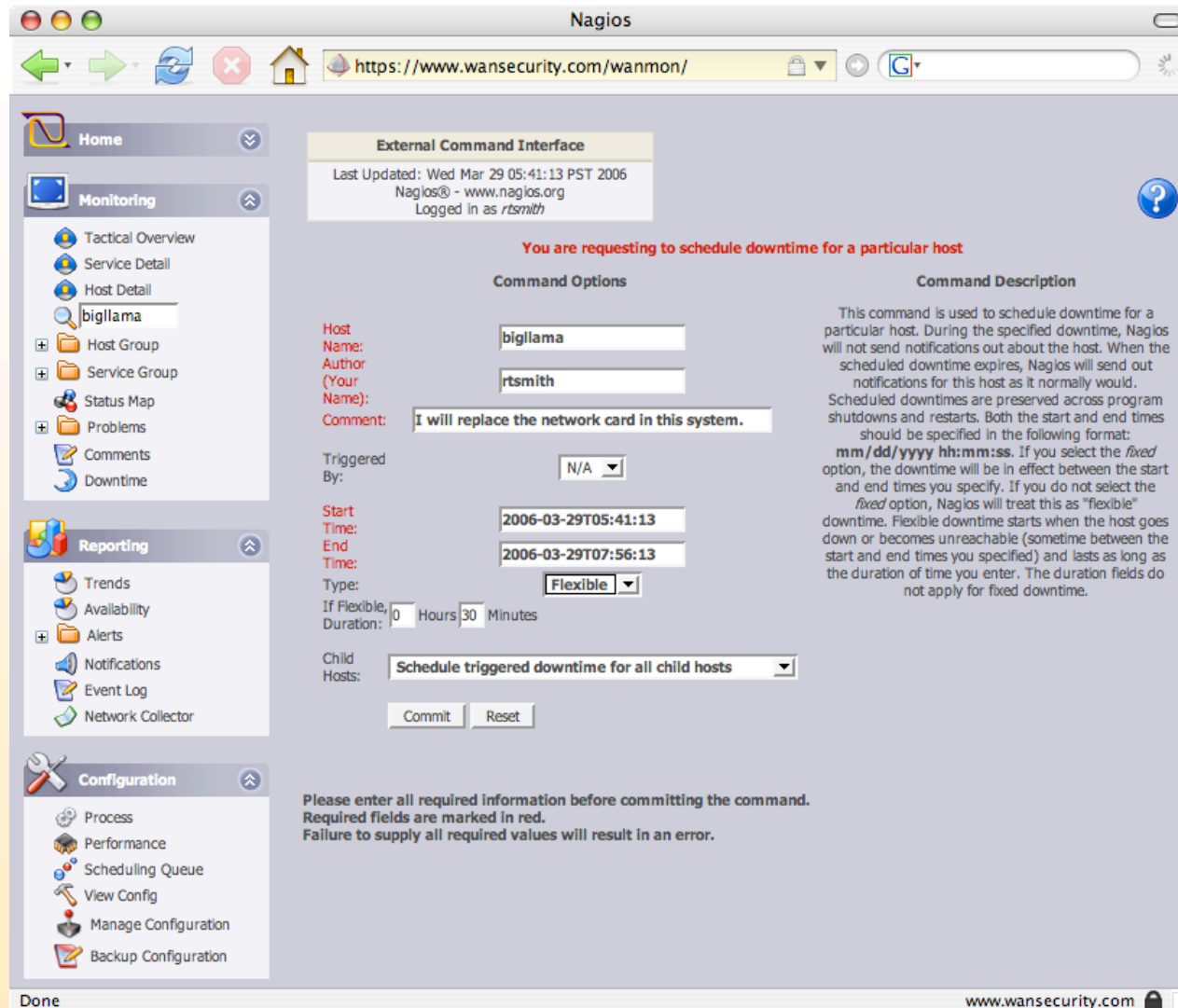
- Navigation Menu:** Home, Monitoring (Tactical Overview, Service Detail, Host Detail, bigllama, Host Group, Service Group, Status Map, Problems, Comments, Downtime), Reporting (Trends, Availability, Alerts, Notifications, Event Log, Network Collector), Configuration (Process, Performance, Scheduling Queue, View Config, Manage Configuration, Backup Configuration).
- Page Header:** Nagios, Last Updated: Wed Mar 29 05:43:37 PST 2006, Updated every 300 seconds, Nagios® - www.nagios.org, Logged in as rtsmith.
- Host Comments Table:**

Host Name	Entry Time	Author	Comment	Comment ID	Persistent	Type	Expires	Actions
bigllama	2006-03-29T05:37:38	rtsmith	This host appears to be having a network interface issue. I will disable notifications for this host for the time being.	3	Yes	User	N/A	[Action]
bigllama	2006-03-29T05:43:32	(Nagios Process)	This host has been scheduled for flexible downtime starting between 2006-03-29T05:41:13 and 2006-03-29T07:56:13 and lasting for a period of 0 hours and 30 minutes. Notifications for the host will not be sent out during that time period.	4	No	Scheduled Downtime	N/A	[Action]
- Service Comments Table:**

Host Name	Service	Entry Time	Author	Comment	Comment ID	Persistent	Type	Expires	Actions
dbpn-web	check_http_MultiBetPoker.com	2006-03-19T21:10:10	rtsmith	I know this is a problem and I will fix it as soon as possible.	1	Yes	Acknowledgement	N/A	[Action]
openswan	ssh_check_disk_	2006-03-24T01:14:29	rtsmith	I know this disk is running out of space. I will make more space later.	2	Yes	Acknowledgement	N/A	[Action]

## ダウンタイムのスケジュール化

ダウンタイムのスケジュール化は、より正確なレポートを提供し、変化の監視を強化します。アラームに振り回されることなく、より正確なレポートを提供し、制御変更の規律を強化します。ダウンタイムは、修理や設定の変更が行われる際に、固定の時間枠または多様な時間枠に設定できます。



The screenshot shows the Nagios External Command Interface in a web browser. The browser address bar shows `https://www.wansecurity.com/wanmon/`. The page title is "Nagios".

At the top, there is a status bar: "Last Updated: Wed Mar 29 05:41:13 PST 2006", "Nagios® - www.nagios.org", and "Logged in as rtsmith".

The main content area is titled "External Command Interface" and contains a red warning: "You are requesting to schedule downtime for a particular host".

The form is divided into two columns: "Command Options" and "Command Description".

**Command Options:**

- Host Name:
- Author (Your Name):
- Comment:
- Triggered By:
- Start Time:
- End Time:
- Type:
- If Flexible, Duration:  Hours  Minutes
- Child Hosts:

**Command Description:**

This command is used to schedule downtime for a particular host. During the specified downtime, Nagios will not send notifications out about the host. When the scheduled downtime expires, Nagios will send out notifications for this host as it normally would. Scheduled downtimes are preserved across program shutdowns and restarts. Both the start and end times should be specified in the following format: **mm/dd/yyyy hh:mm:ss**. If you select the *fixed* option, the downtime will be in effect between the start and end times you specify. If you do not select the *fixed* option, Nagios will treat this as "flexible" downtime. Flexible downtime starts when the host goes down or becomes unreachable (sometime between the start and end times you specified) and lasts as long as the duration of time you enter. The duration fields do not apply for fixed downtime.

At the bottom of the form are "Commit" and "Reset" buttons.

A warning message at the bottom of the form reads: "Please enter all required information before committing the command. Required fields are marked in red. Failure to supply all required values will result in an error."

The left sidebar contains navigation menus for "Home", "Monitoring" (with sub-items: Tactical Overview, Service Detail, Host Detail, bigllama, Host Group, Service Group, Status Map, Problems, Comments, Downtime), "Reporting" (with sub-items: Trends, Availability, Alerts, Notifications, Event Log, Network Collector), and "Configuration" (with sub-items: Process, Performance, Scheduling Queue, View Config, Manage Configuration, Backup Configuration).

The status bar at the bottom left says "Done" and the bottom right shows the URL `www.wansecurity.com`.

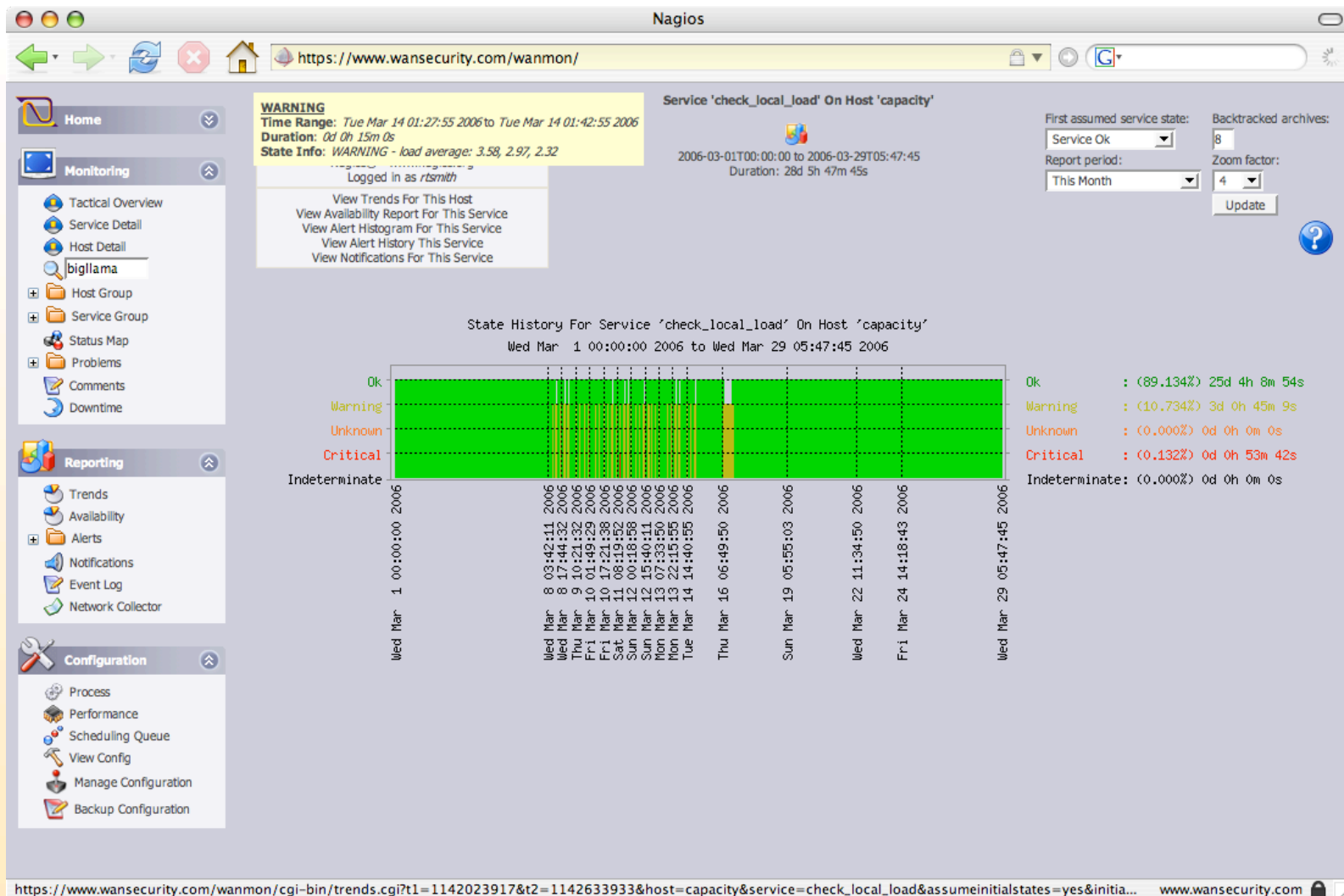
## ネットワークディレクターのレポートと傾向

- 傾向
- 汎用性
- アラート ヒストグラム
- アラート サマリー
- 通知
- イベント ログ
- サービスのグラフ
- ホストのグラフ



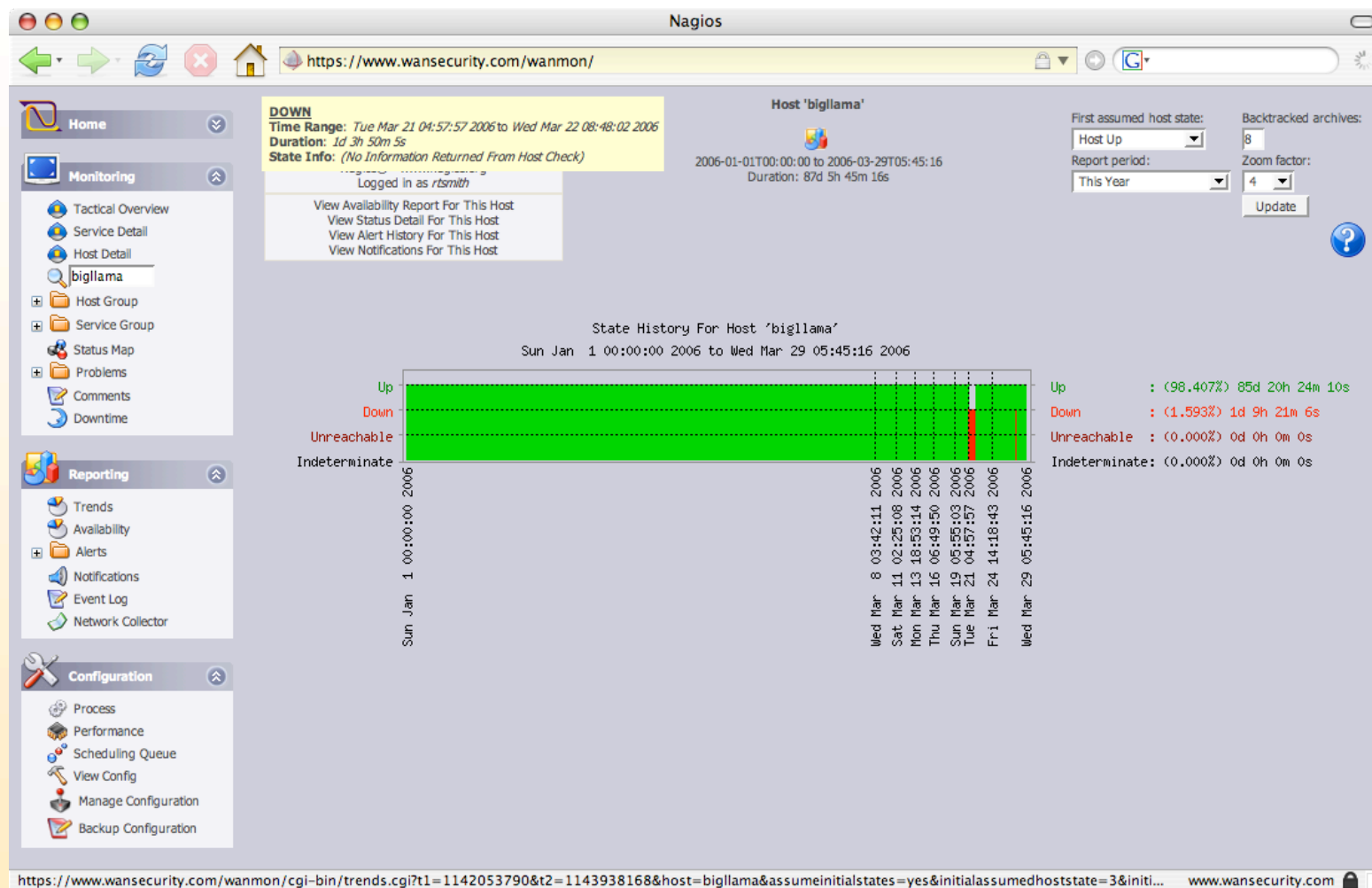
## サービスステートの履歴

下のグラフに示されるように、サービスステートの履歴のグラフによって、ネットワーク管理者は特定のホスト上にある特定のサービスの履歴で傾向を確認することが可能になります。下のグラフは、OK、WARNING、CRITICAL状態であった時間の割合(%)を示しています。なお、期間内に未知の時間が見られる場合、UNKNOWNと表示します。このグラフは、[Reporting]タブの下にある[Trends]ツールを使用して作成されます。



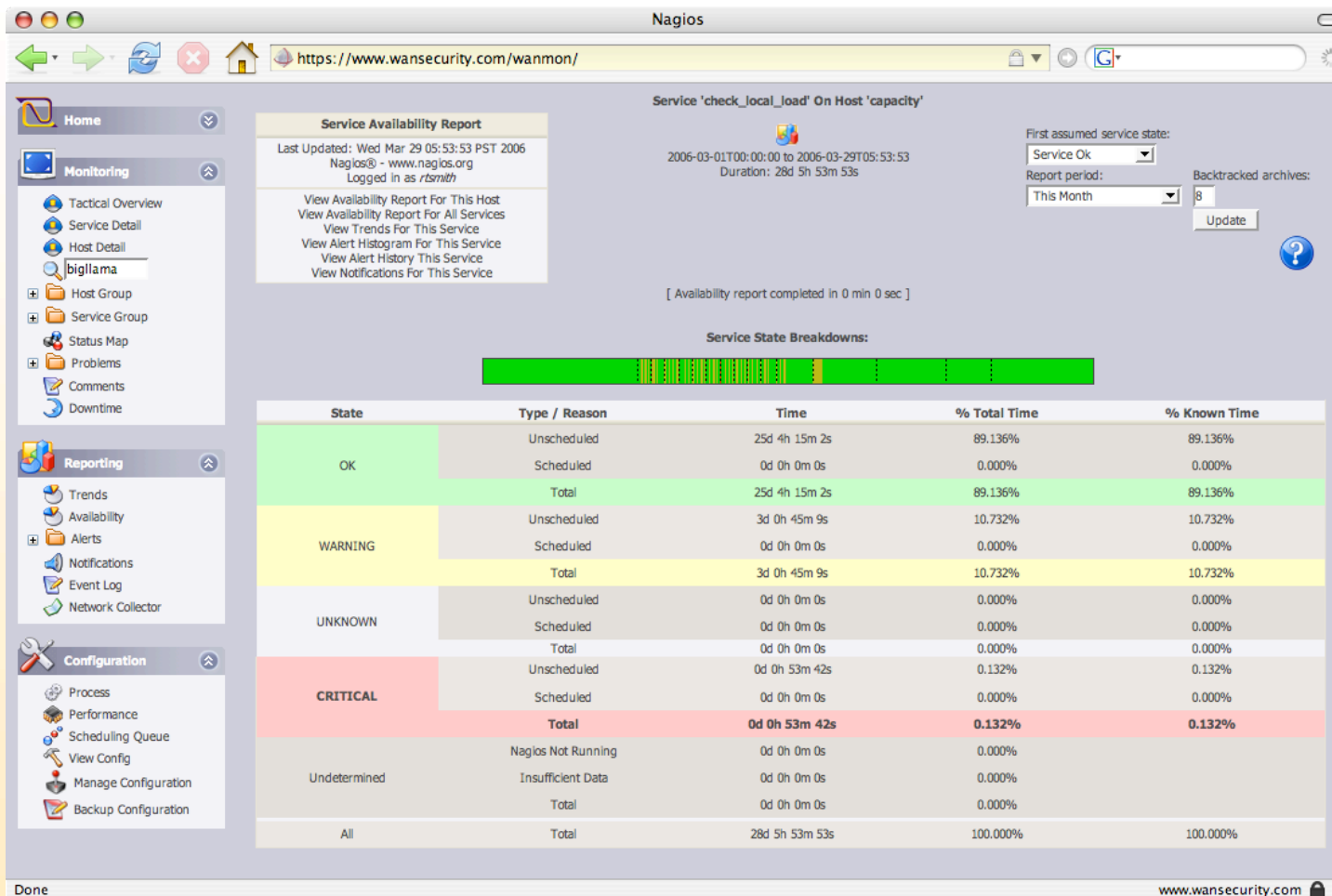
## ホストステートの履歴

ホストステートの履歴を示すグラフでは、ネットワーク管理者が、以下のグラフで示すように特定のホストの有用な履歴を見て傾向を捉えることができます。以下のグラフは、UP、DOWN、UNREACHABLEの状態であった時間の割合(%)を示しています。なお、期間内に未知の時間が見られる場合、UNKNOWNと表示します。このグラフは、[Reporting]タブの下にある[Trends]ツールを使用して作成されます。



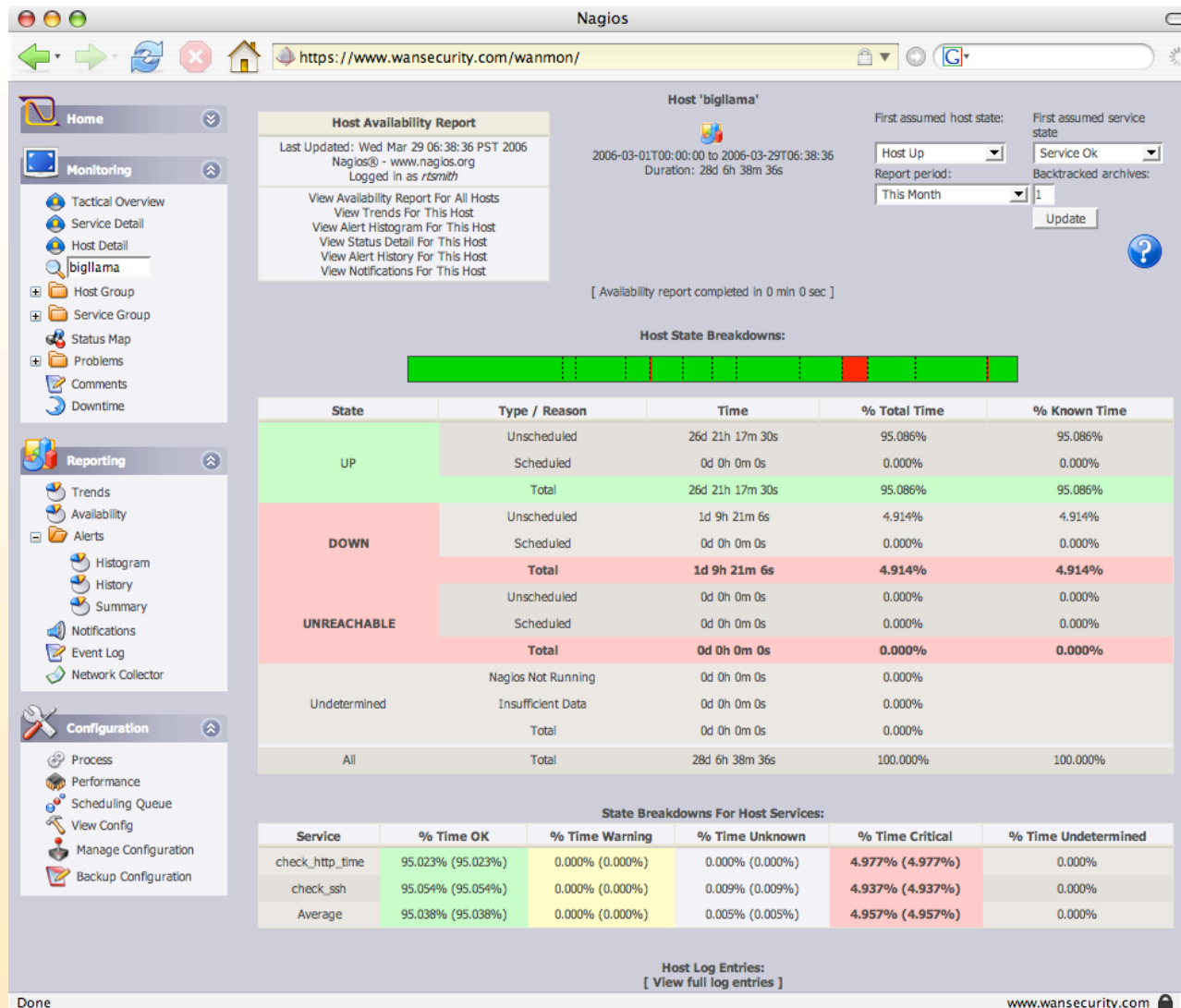
## サービスの汎用性

サービスの可用性レポートは、サービス状況の履歴とは異なり、OK、WARNING、CRITICALの状態にあるサービスが実際には何時間スケジュールされていたのかを示します。ダウンタイムのスケジュール化が全体の可用性に影響を及ぼすことはありません。なお、期間内に未知の時間が見られる場合、UNKNOWNと表示します。このグラフは、Nagiosログの[Reporting]タブの下にある[Availability]ツールを使用して作成されます。



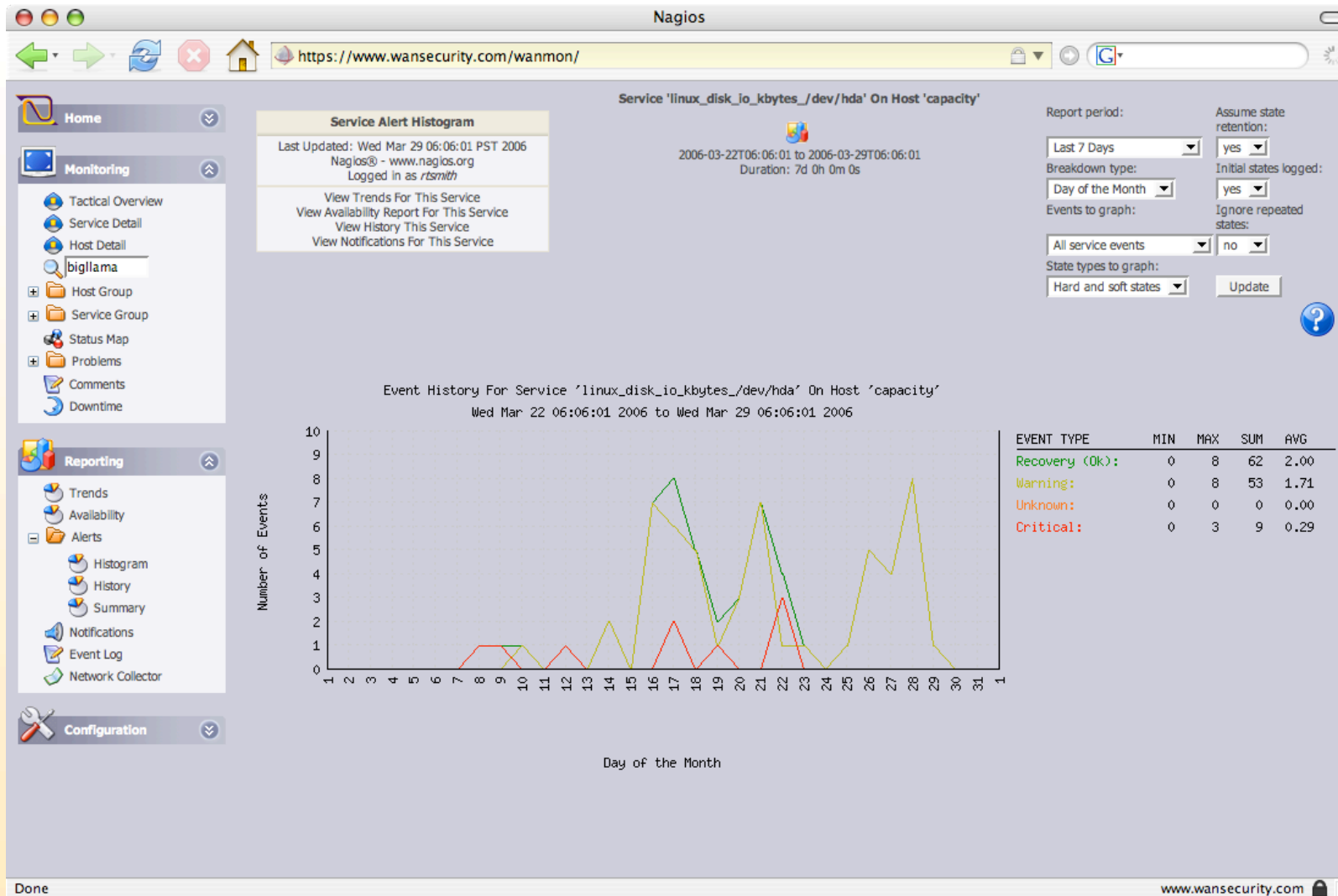
## ホストの汎用性

ホストの可用性レポートは、ホスト状況の履歴とは異なり、可用性を何時間でスケジュールしたのかを示します。ダウンタイムのスケジュール化は、可用性レポートに影響を及ぼすことはありません。そのため、メンテナンス時にダウンタイムのスケジュールを組むことが非常に重要です。そのようにすることで、ネットワーク、ホスト、サービスのある期間の状態に関する可用性レポート全体が改善されます。



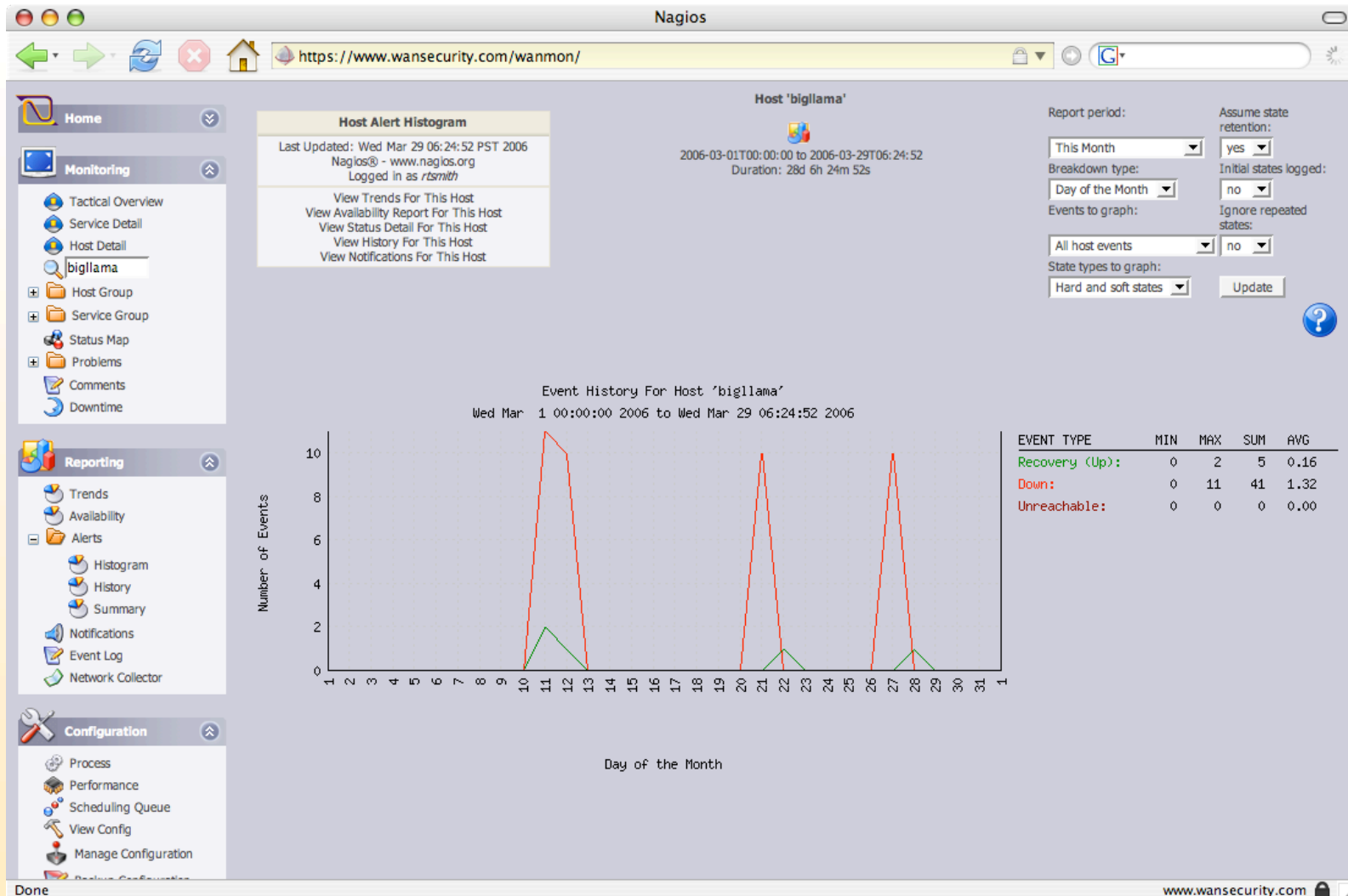
## サービスイベントのヒストグラム

サービスイベントのヒストグラムは、特定期間内でサービスに関係していたイベント数を示しています。下のヒストグラムは、期間が7日間で、linux\_disk\_io\_kbytesにイベント数を、/dev/hdaに毎秒を示しています。このレポートは[Alerts]の下にある[Reporting]タブ内の[Histogram]ツールを使用して生成されます。



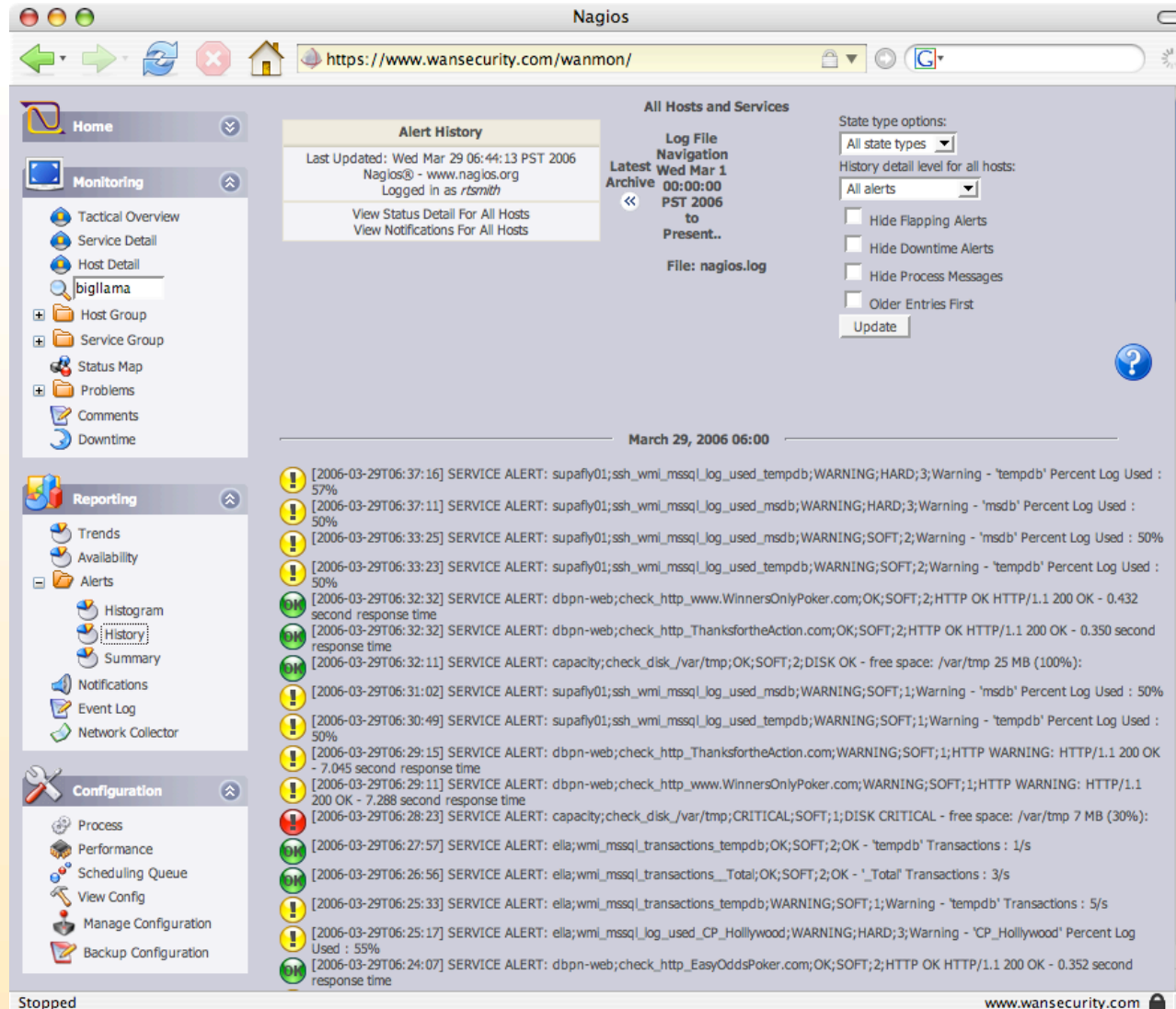
## ホストイベントのヒストグラム

ホストイベントのヒストグラムは、特定期間内でホストに関係していたイベント数を示しています。下のヒストグラムは、最近7日間のホストbigllamaに関するホストイベント数を示しています。このレポートは[Alerts]の下にある[Reporting]タブ内の[Histogram]ツールを使用して作成されます。



## アラート履歴

アラート履歴ツールは、監視システムから生成されたアラートの全一覧を示します。アラートは、時間、アラートの種類(ホスト、サービス、ネットワーク)、サービス、サービスステート、アラートに関連するホスト、ハードステートまたはソフトステートのどちらの状態か、サービス出力情報の項目に分けられています。

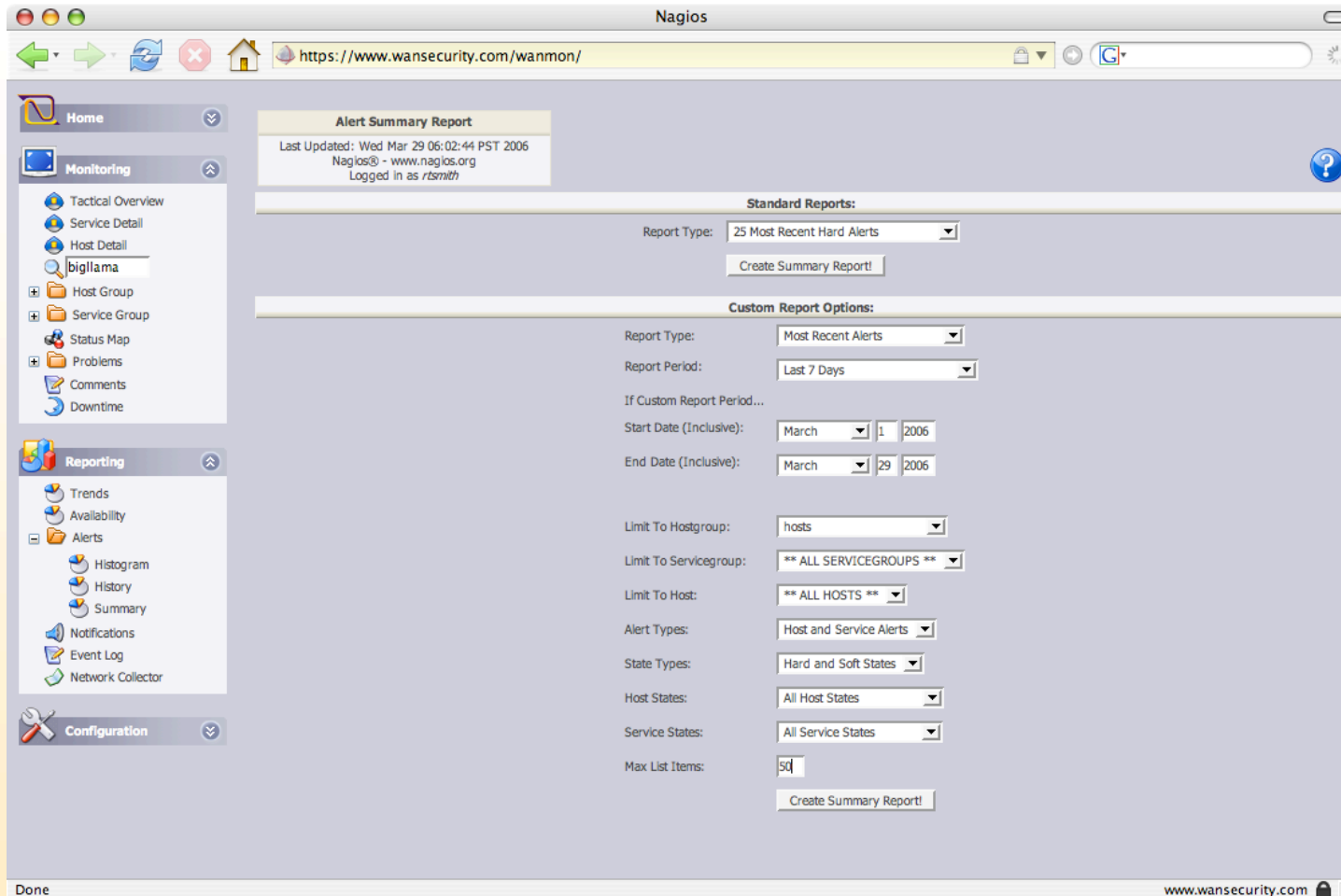


The screenshot shows the Nagios web interface with the following components:

- Alert History:**
  - Last Updated: Wed Mar 29 06:44:13 PST 2006
  - Nagios® - www.nagios.org
  - Logged in as *rtsmth*
  - View Status Detail For All Hosts
  - View Notifications For All Hosts
- All Hosts and Services:**
  - Log File Navigation: Wed Mar 1 00:00:00 PST 2006 to Present..
  - File: nagios.log
- State type options:**
  - All state types
  - History detail level for all hosts: All alerts
  - Hide Flapping Alerts
  - Hide Downtime Alerts
  - Hide Process Messages
  - Older Entries First
  - Update
- Alert Log (March 29, 2006 06:00):**
  - [2006-03-29T06:37:16] SERVICE ALERT: supafly01;ssh\_wmi\_mssql\_log\_used\_tempdb;WARNING;HARD;3;Warning - 'tempdb' Percent Log Used : 57%
  - [2006-03-29T06:37:11] SERVICE ALERT: supafly01;ssh\_wmi\_mssql\_log\_used\_msdb;WARNING;HARD;3;Warning - 'msdb' Percent Log Used : 50%
  - [2006-03-29T06:33:25] SERVICE ALERT: supafly01;ssh\_wmi\_mssql\_log\_used\_msdb;WARNING;SOFT;2;Warning - 'msdb' Percent Log Used : 50%
  - [2006-03-29T06:33:23] SERVICE ALERT: supafly01;ssh\_wmi\_mssql\_log\_used\_tempdb;WARNING;SOFT;2;Warning - 'tempdb' Percent Log Used : 50%
  - [2006-03-29T06:32:32] SERVICE ALERT: dbpn-web;check\_http\_www.WinnersOnlyPoker.com;OK;SOFT;2;HTTP OK HTTP/1.1 200 OK - 0.432 second response time
  - [2006-03-29T06:32:32] SERVICE ALERT: dbpn-web;check\_http\_ThanksfortheAction.com;OK;SOFT;2;HTTP OK HTTP/1.1 200 OK - 0.350 second response time
  - [2006-03-29T06:32:11] SERVICE ALERT: capacity;check\_disk\_/var/tmp;OK;SOFT;2;DISK OK - free space: /var/tmp 25 MB (100%):
  - [2006-03-29T06:31:02] SERVICE ALERT: supafly01;ssh\_wmi\_mssql\_log\_used\_msdb;WARNING;SOFT;1;Warning - 'msdb' Percent Log Used : 50%
  - [2006-03-29T06:30:49] SERVICE ALERT: supafly01;ssh\_wmi\_mssql\_log\_used\_tempdb;WARNING;SOFT;1;Warning - 'tempdb' Percent Log Used : 50%
  - [2006-03-29T06:29:15] SERVICE ALERT: dbpn-web;check\_http\_ThanksfortheAction.com;WARNING;SOFT;1;HTTP WARNING: HTTP/1.1 200 OK - 7.045 second response time
  - [2006-03-29T06:29:11] SERVICE ALERT: dbpn-web;check\_http\_www.WinnersOnlyPoker.com;WARNING;SOFT;1;HTTP WARNING: HTTP/1.1 200 OK - 7.288 second response time
  - [2006-03-29T06:28:23] SERVICE ALERT: capacity;check\_disk\_/var/tmp;CRITICAL;SOFT;1;DISK CRITICAL - free space: /var/tmp 7 MB (30%):
  - [2006-03-29T06:27:57] SERVICE ALERT: ella;wmi\_mssql\_transactions\_tempdb;OK;SOFT;2;OK - 'tempdb' Transactions : 1/s
  - [2006-03-29T06:26:56] SERVICE ALERT: ella;wmi\_mssql\_transactions\_Total;OK;SOFT;2;OK - '\_Total' Transactions : 3/s
  - [2006-03-29T06:25:33] SERVICE ALERT: ella;wmi\_mssql\_transactions\_tempdb;WARNING;SOFT;1;Warning - 'tempdb' Transactions : 5/s
  - [2006-03-29T06:25:17] SERVICE ALERT: ella;wmi\_mssql\_log\_used\_CP\_Hollywood;WARNING;HARD;3;Warning - 'CP\_Hollywood' Percent Log Used : 55%
  - [2006-03-29T06:24:07] SERVICE ALERT: dbpn-web;check\_http\_EasyOddsPoker.com;OK;SOFT;2;HTTP OK HTTP/1.1 200 OK - 0.352 second response time

## アラート サマリーレポート

アラートサマリーレポートの生成では、ネットワーク管理者が特定期間内のホストまたはサービスに対して作成されたアラートすべてを確認することができます。以下は、ステートの履歴、可用性やヒストグラムレポート生成ユーティリティと同様のアラートサマリーのレポート作成画面です。



The screenshot shows the Nagios web interface for generating an Alert Summary Report. The browser address bar shows <https://www.wansecurity.com/wanmon/>. The interface is divided into a left sidebar and a main content area.

**Left Sidebar:**

- Home
- Monitoring
  - Tactical Overview
  - Service Detail
  - Host Detail
  - bigllama
  - Host Group
  - Service Group
  - Status Map
  - Problems
  - Comments
  - Downtime
- Reporting
  - Trends
  - Availability
  - Alerts
    - Histogram
    - History
    - Summary
  - Notifications
  - Event Log
  - Network Collector
- Configuration

**Main Content Area:**

**Alert Summary Report**  
 Last Updated: Wed Mar 29 06:02:44 PST 2006  
 Nagios® - www.nagios.org  
 Logged in as rsmith

**Standard Reports:**

Report Type: 25 Most Recent Hard Alerts

**Custom Report Options:**

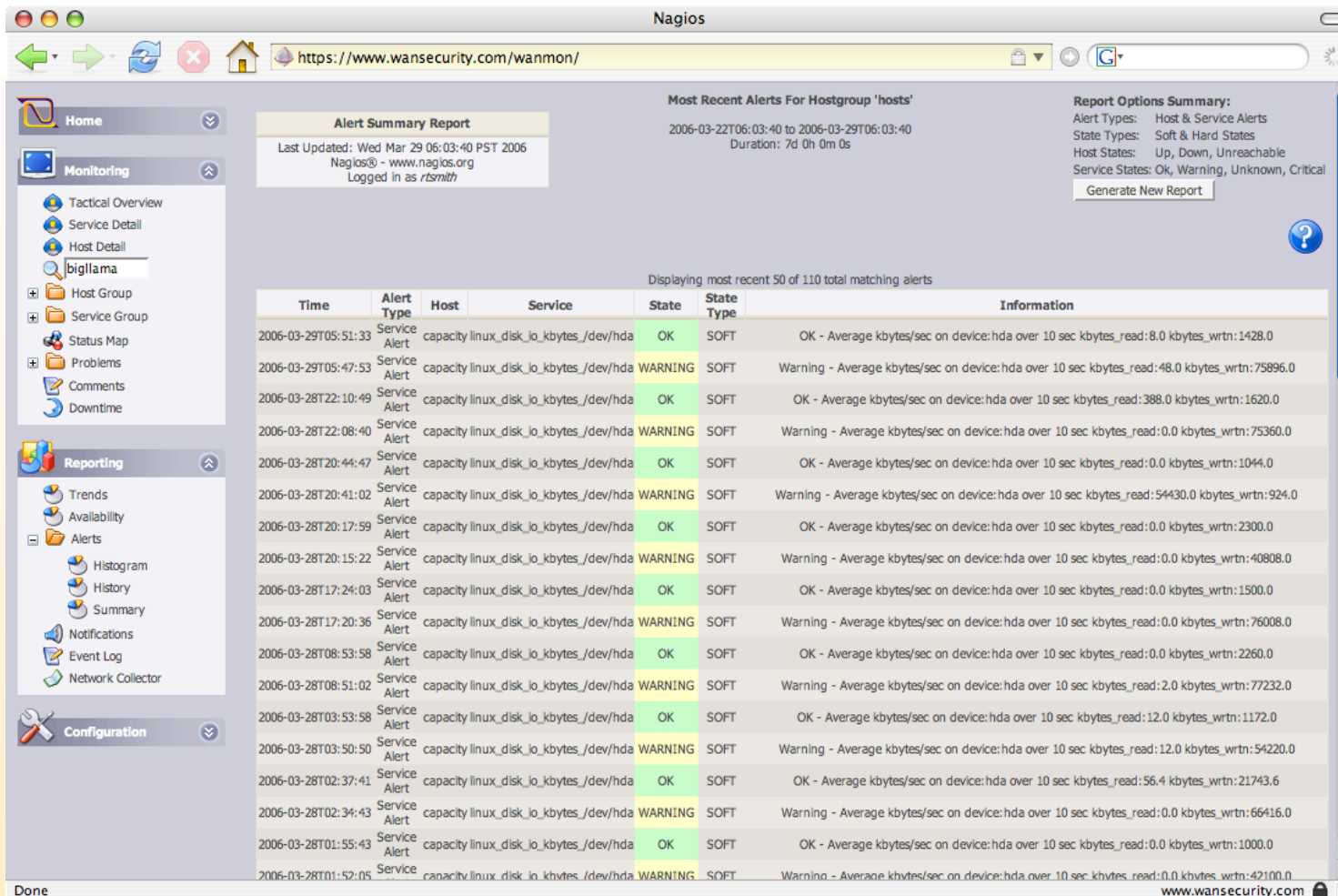
Report Type: Most Recent Alerts  
 Report Period: Last 7 Days  
 If Custom Report Period...  
 Start Date (Inclusive): March 1 2006  
 End Date (Inclusive): March 29 2006  
 Limit To Hostgroup: hosts  
 Limit To Servicegroup: \*\* ALL SERVICEGROUPS \*\*  
 Limit To Host: \*\* ALL HOSTS \*\*  
 Alert Types: Host and Service Alerts  
 State Types: Hard and Soft States  
 Host States: All Host States  
 Service States: All Service States  
 Max List Items: 50

Done www.wansecurity.com



## アラートサマリーのレポート

アラート履歴同様、レポートは、時間、アラートの種類、サービス、ステート、ステートの種類、サービス出力情報の項目に分けられています。アラートサマリーのレポートは特定のサービスまたはホストに対して作成されます。以下は、生成された最新25のサービスアラートを一覧にしています。今回の場合は、問題のあるサービスに対して同じ種類のアラートを発信しています



The screenshot shows the Nagios web interface. The main content area displays an "Alert Summary Report" for the hostgroup 'hosts'. The report includes a table of the most recent alerts, showing columns for Time, Alert Type, Host, Service, State, State Type, and Information. The table lists 25 alerts, with alternating rows of OK and WARNING states for the service 'capacity linux\_disk\_io\_kbytes /dev/hda'.

**Alert Summary Report**  
 Last Updated: Wed Mar 29 06:03:40 PST 2006  
 Nagios® - www.nagios.org  
 Logged in as *rtsmith*

**Most Recent Alerts For Hostgroup 'hosts'**  
 2006-03-22T06:03:40 to 2006-03-29T06:03:40  
 Duration: 7d 0h 0m 0s

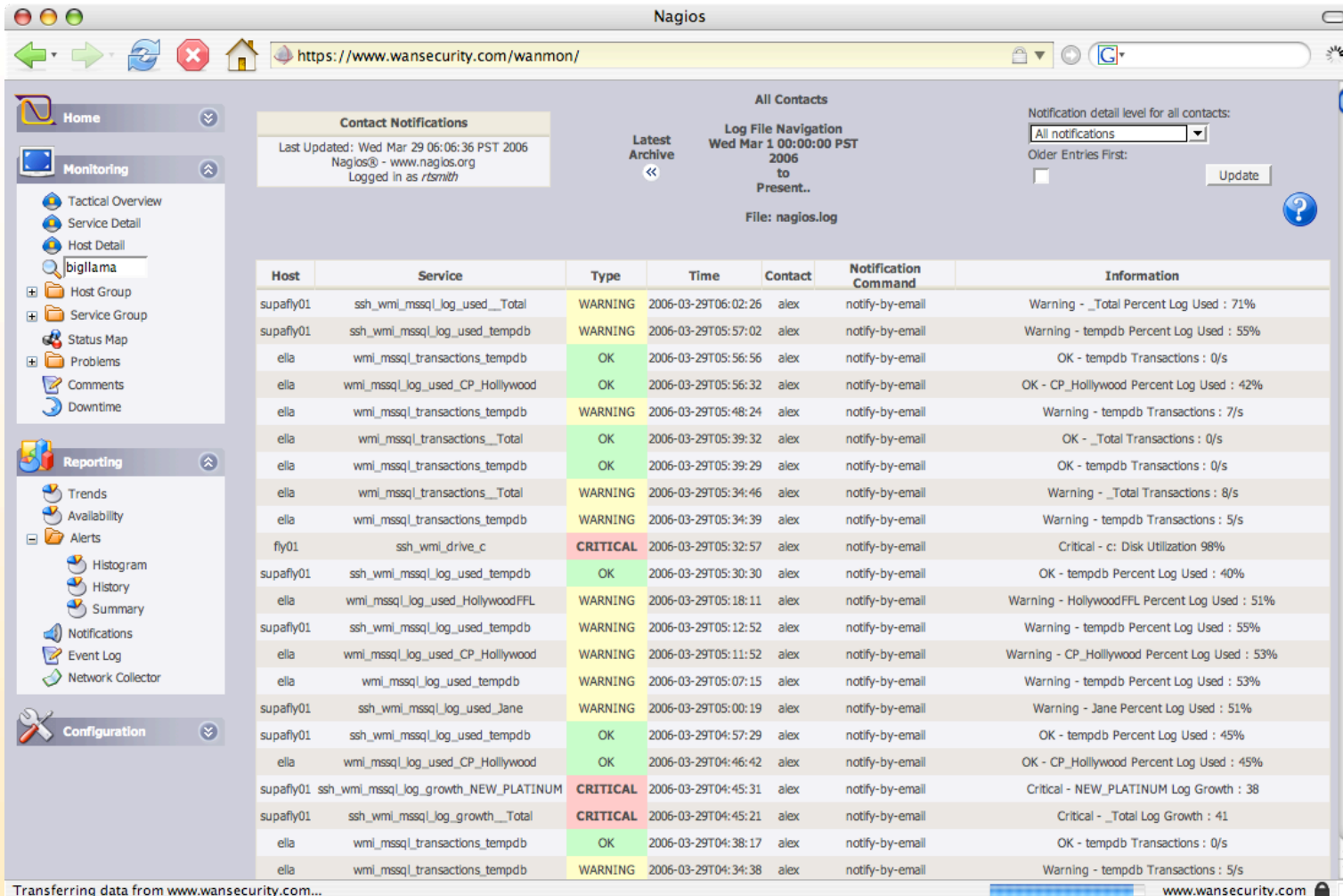
**Report Options Summary:**  
 Alert Types: Host & Service Alerts  
 State Types: Soft & Hard States  
 Host States: Up, Down, Unreachable  
 Service States: Ok, Warning, Unknown, Critical  
 Generate New Report

Displaying most recent 50 of 110 total matching alerts

Time	Alert Type	Host	Service	State	State Type	Information
2006-03-29T05:51:33	Service Alert	capacity	linux_disk_io_kbytes /dev/hda	OK	SOFT	OK - Average kbytes/sec on device:hda over 10 sec kbytes_read:8.0 kbytes_wrtn:1428.0
2006-03-29T05:47:53	Service Alert	capacity	linux_disk_io_kbytes /dev/hda	WARNING	SOFT	Warning - Average kbytes/sec on device:hda over 10 sec kbytes_read:48.0 kbytes_wrtn:75896.0
2006-03-28T22:10:49	Service Alert	capacity	linux_disk_io_kbytes /dev/hda	OK	SOFT	OK - Average kbytes/sec on device:hda over 10 sec kbytes_read:388.0 kbytes_wrtn:1620.0
2006-03-28T22:08:40	Service Alert	capacity	linux_disk_io_kbytes /dev/hda	WARNING	SOFT	Warning - Average kbytes/sec on device:hda over 10 sec kbytes_read:0.0 kbytes_wrtn:75360.0
2006-03-28T20:44:47	Service Alert	capacity	linux_disk_io_kbytes /dev/hda	OK	SOFT	OK - Average kbytes/sec on device:hda over 10 sec kbytes_read:0.0 kbytes_wrtn:1044.0
2006-03-28T20:41:02	Service Alert	capacity	linux_disk_io_kbytes /dev/hda	WARNING	SOFT	Warning - Average kbytes/sec on device:hda over 10 sec kbytes_read:54430.0 kbytes_wrtn:924.0
2006-03-28T20:17:59	Service Alert	capacity	linux_disk_io_kbytes /dev/hda	OK	SOFT	OK - Average kbytes/sec on device:hda over 10 sec kbytes_read:0.0 kbytes_wrtn:2300.0
2006-03-28T20:15:22	Service Alert	capacity	linux_disk_io_kbytes /dev/hda	WARNING	SOFT	Warning - Average kbytes/sec on device:hda over 10 sec kbytes_read:0.0 kbytes_wrtn:40808.0
2006-03-28T17:24:03	Service Alert	capacity	linux_disk_io_kbytes /dev/hda	OK	SOFT	OK - Average kbytes/sec on device:hda over 10 sec kbytes_read:0.0 kbytes_wrtn:1500.0
2006-03-28T17:20:36	Service Alert	capacity	linux_disk_io_kbytes /dev/hda	WARNING	SOFT	Warning - Average kbytes/sec on device:hda over 10 sec kbytes_read:0.0 kbytes_wrtn:76008.0
2006-03-28T08:53:58	Service Alert	capacity	linux_disk_io_kbytes /dev/hda	OK	SOFT	OK - Average kbytes/sec on device:hda over 10 sec kbytes_read:0.0 kbytes_wrtn:2260.0
2006-03-28T08:51:02	Service Alert	capacity	linux_disk_io_kbytes /dev/hda	WARNING	SOFT	Warning - Average kbytes/sec on device:hda over 10 sec kbytes_read:2.0 kbytes_wrtn:77232.0
2006-03-28T03:53:58	Service Alert	capacity	linux_disk_io_kbytes /dev/hda	OK	SOFT	OK - Average kbytes/sec on device:hda over 10 sec kbytes_read:12.0 kbytes_wrtn:1172.0
2006-03-28T03:50:50	Service Alert	capacity	linux_disk_io_kbytes /dev/hda	WARNING	SOFT	Warning - Average kbytes/sec on device:hda over 10 sec kbytes_read:12.0 kbytes_wrtn:54220.0
2006-03-28T02:37:41	Service Alert	capacity	linux_disk_io_kbytes /dev/hda	OK	SOFT	OK - Average kbytes/sec on device:hda over 10 sec kbytes_read:56.4 kbytes_wrtn:21743.6
2006-03-28T02:34:43	Service Alert	capacity	linux_disk_io_kbytes /dev/hda	WARNING	SOFT	Warning - Average kbytes/sec on device:hda over 10 sec kbytes_read:0.0 kbytes_wrtn:66416.0
2006-03-28T01:55:43	Service Alert	capacity	linux_disk_io_kbytes /dev/hda	OK	SOFT	OK - Average kbytes/sec on device:hda over 10 sec kbytes_read:0.0 kbytes_wrtn:1000.0
2006-03-28T01:52:05	Service Alert	capacity	linux_disk_io_kbytes /dev/hda	WARNING	SOFT	Warning - Average kbytes/sec on device:hda over 10 sec kbytes_read:0.0 kbytes_wrtn:42100.0

## ログ通知

[Reporting]タブの下にある[Notifications]をクリックすると、過去に送られた通知の一覧をすべて表示することができます。通知は、ホスト、サービス、種類、時間、担当者、通知コマンド、サービス出力情報の項目に分かれています。通知コマンドはプログラムで、ネットワークディレクターによって実行され、問題を担当者に通知するスクリプトです。

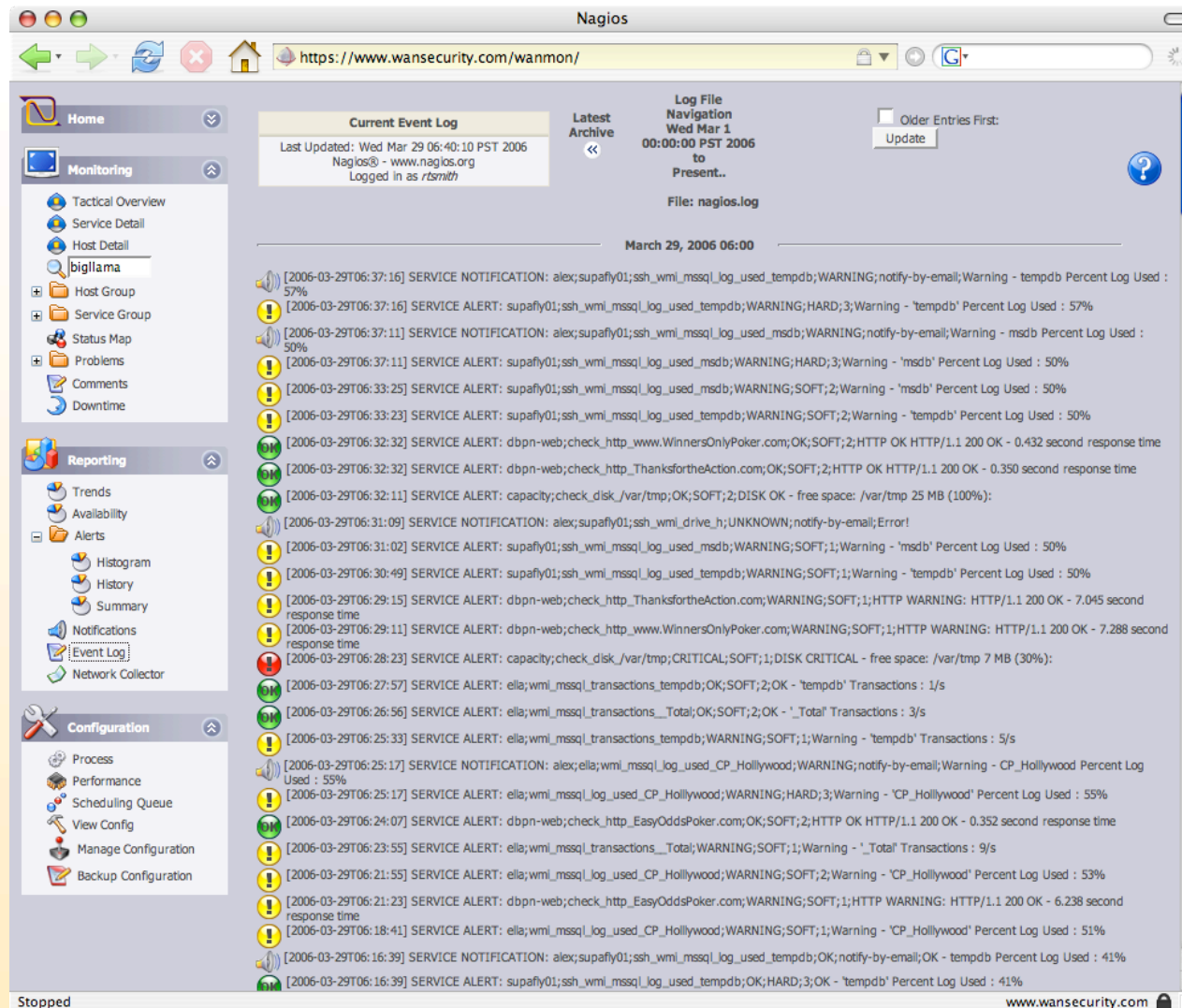


The screenshot shows the Nagios web interface with the 'Reporting' tab selected. The 'Notifications' section is active, displaying a table of recent notifications. The table columns are Host, Service, Type, Time, Contact, Notification Command, and Information. The notifications are sorted by time, showing various warning and critical alerts for different services and hosts.

Host	Service	Type	Time	Contact	Notification Command	Information
supafly01	ssh_wmi_mssql_log_used__Total	WARNING	2006-03-29T06:02:26	alex	notify-by-email	Warning - __Total Percent Log Used : 71%
supafly01	ssh_wmi_mssql_log_used_tempdb	WARNING	2006-03-29T05:57:02	alex	notify-by-email	Warning - tempdb Percent Log Used : 55%
ella	wmi_mssql_transactions_tempdb	OK	2006-03-29T05:56:56	alex	notify-by-email	OK - tempdb Transactions : 0/s
ella	wmi_mssql_log_used_CP_Hollywood	OK	2006-03-29T05:56:32	alex	notify-by-email	OK - CP_Hollywood Percent Log Used : 42%
ella	wmi_mssql_transactions_tempdb	WARNING	2006-03-29T05:48:24	alex	notify-by-email	Warning - tempdb Transactions : 7/s
ella	wmi_mssql_transactions__Total	OK	2006-03-29T05:39:32	alex	notify-by-email	OK - __Total Transactions : 0/s
ella	wmi_mssql_transactions_tempdb	OK	2006-03-29T05:39:29	alex	notify-by-email	OK - tempdb Transactions : 0/s
ella	wmi_mssql_transactions__Total	WARNING	2006-03-29T05:34:46	alex	notify-by-email	Warning - __Total Transactions : 8/s
ella	wmi_mssql_transactions_tempdb	WARNING	2006-03-29T05:34:39	alex	notify-by-email	Warning - tempdb Transactions : 5/s
fly01	ssh_wmi_drive_c	CRITICAL	2006-03-29T05:32:57	alex	notify-by-email	Critical - c: Disk Utilization 98%
supafly01	ssh_wmi_mssql_log_used_tempdb	OK	2006-03-29T05:30:30	alex	notify-by-email	OK - tempdb Percent Log Used : 40%
ella	wmi_mssql_log_used_HollywoodFFL	WARNING	2006-03-29T05:18:11	alex	notify-by-email	Warning - HollywoodFFL Percent Log Used : 51%
supafly01	ssh_wmi_mssql_log_used_tempdb	WARNING	2006-03-29T05:12:52	alex	notify-by-email	Warning - tempdb Percent Log Used : 55%
ella	wmi_mssql_log_used_CP_Hollywood	WARNING	2006-03-29T05:11:52	alex	notify-by-email	Warning - CP_Hollywood Percent Log Used : 53%
ella	wmi_mssql_log_used_tempdb	WARNING	2006-03-29T05:07:15	alex	notify-by-email	Warning - tempdb Percent Log Used : 53%
supafly01	ssh_wmi_mssql_log_used_Jane	WARNING	2006-03-29T05:00:19	alex	notify-by-email	Warning - Jane Percent Log Used : 51%
supafly01	ssh_wmi_mssql_log_used_tempdb	OK	2006-03-29T04:57:29	alex	notify-by-email	OK - tempdb Percent Log Used : 45%
ella	wmi_mssql_log_used_CP_Hollywood	OK	2006-03-29T04:46:42	alex	notify-by-email	OK - CP_Hollywood Percent Log Used : 45%
supafly01	ssh_wmi_mssql_log_growth_NEW_PLATINUM	CRITICAL	2006-03-29T04:45:31	alex	notify-by-email	Critical - NEW_PLATINUM Log Growth : 38
supafly01	ssh_wmi_mssql_log_growth__Total	CRITICAL	2006-03-29T04:45:21	alex	notify-by-email	Critical - __Total Log Growth : 41
ella	wmi_mssql_transactions_tempdb	OK	2006-03-29T04:38:17	alex	notify-by-email	OK - tempdb Transactions : 0/s
ella	wmi_mssql_transactions_tempdb	WARNING	2006-03-29T04:34:38	alex	notify-by-email	Warning - tempdb Transactions : 5/s

## イベント ログ

イベントログは、Nagiosログファイル内にイベントをすべて一覧表示します。イベントには、通知、アラート、プログラムの再起動、変更の設定、保持値の保管、受動サービスチェックから取得したイベントデータなどを含んでいます。



The screenshot shows the Nagios web interface at <https://www.wansecurity.com/wanmon/>. The interface is divided into several sections:

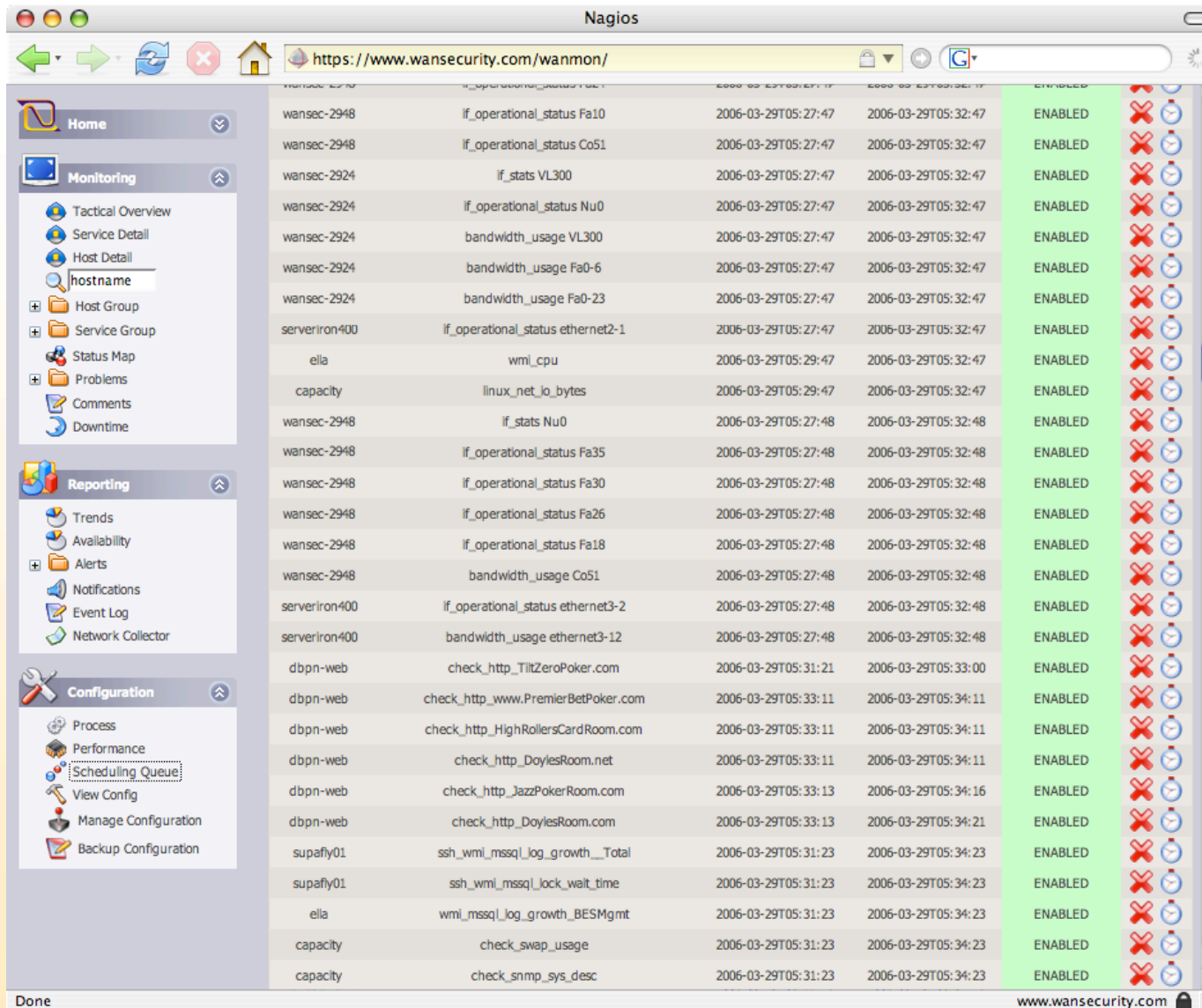
- Home:** Includes links for Tactical Overview, Service Detail, Host Detail, and a search bar for 'bigllama'.
- Monitoring:** Contains links for Host Group, Service Group, Status Map, Problems, Comments, and Downtime.
- Reporting:** Contains links for Trends, Availability, Alerts, Histogram, History, Summary, Notifications, and Network Collector.
- Configuration:** Contains links for Process, Performance, Scheduling Queue, View Config, Manage Configuration, and Backup Configuration.

The main content area displays the 'Current Event Log' for the file 'nagios.log', updated on 'Wed Mar 29 06:40:10 PST 2006'. The log entries are listed with their timestamps and details:

- [2006-03-29T06:37:16] SERVICE NOTIFICATION: alex;supafly01;ssh\_wmi\_mssql\_log\_used\_tempdb;WARNING;notify-by-email;Warning - tempdb Percent Log Used : 57%
- [2006-03-29T06:37:16] SERVICE ALERT: supafly01;ssh\_wmi\_mssql\_log\_used\_tempdb;WARNING;HARD;3;Warning - 'tempdb' Percent Log Used : 57%
- [2006-03-29T06:37:11] SERVICE NOTIFICATION: alex;supafly01;ssh\_wmi\_mssql\_log\_used\_msdb;WARNING;notify-by-email;Warning - msdb Percent Log Used : 50%
- [2006-03-29T06:37:11] SERVICE ALERT: supafly01;ssh\_wmi\_mssql\_log\_used\_msdb;WARNING;HARD;3;Warning - 'msdb' Percent Log Used : 50%
- [2006-03-29T06:33:25] SERVICE ALERT: supafly01;ssh\_wmi\_mssql\_log\_used\_msdb;WARNING;SOFT;2;Warning - 'msdb' Percent Log Used : 50%
- [2006-03-29T06:33:23] SERVICE ALERT: supafly01;ssh\_wmi\_mssql\_log\_used\_tempdb;WARNING;SOFT;2;Warning - 'tempdb' Percent Log Used : 50%
- [2006-03-29T06:32:32] SERVICE ALERT: dbpn-web;check\_http\_www.WinnersOnlyPoker.com;OK;SOFT;2;HTTP OK HTTP/1.1 200 OK - 0.432 second response time
- [2006-03-29T06:32:32] SERVICE ALERT: dbpn-web;check\_http\_ThanksfortheAction.com;OK;SOFT;2;HTTP OK HTTP/1.1 200 OK - 0.350 second response time
- [2006-03-29T06:32:11] SERVICE ALERT: capacity;check\_disk\_/var/tmp;OK;SOFT;2;DISK OK - free space: /var/tmp 25 MB (100%):
- [2006-03-29T06:31:09] SERVICE NOTIFICATION: alex;supafly01;ssh\_wmi\_drive\_h;UNKNOWN;notify-by-email;Error!
- [2006-03-29T06:31:02] SERVICE ALERT: supafly01;ssh\_wmi\_mssql\_log\_used\_msdb;WARNING;SOFT;1;Warning - 'msdb' Percent Log Used : 50%
- [2006-03-29T06:30:49] SERVICE ALERT: supafly01;ssh\_wmi\_mssql\_log\_used\_tempdb;WARNING;SOFT;1;Warning - 'tempdb' Percent Log Used : 50%
- [2006-03-29T06:29:15] SERVICE ALERT: dbpn-web;check\_http\_ThanksfortheAction.com;WARNING;SOFT;1;HTTP WARNING: HTTP/1.1 200 OK - 7.045 second response time
- [2006-03-29T06:29:11] SERVICE ALERT: dbpn-web;check\_http\_www.WinnersOnlyPoker.com;WARNING;SOFT;1;HTTP WARNING: HTTP/1.1 200 OK - 7.288 second response time
- [2006-03-29T06:28:23] SERVICE ALERT: capacity;check\_disk\_/var/tmp;CRITICAL;SOFT;1;DISK CRITICAL - free space: /var/tmp 7 MB (30%):
- [2006-03-29T06:27:57] SERVICE ALERT: ella;wmi\_mssql\_transactions\_tempdb;OK;SOFT;2;OK - 'tempdb' Transactions : 1/s
- [2006-03-29T06:26:56] SERVICE ALERT: ella;wmi\_mssql\_transactions\_\_Total;OK;SOFT;2;OK - '\_Total' Transactions : 3/s
- [2006-03-29T06:25:33] SERVICE ALERT: ella;wmi\_mssql\_transactions\_tempdb;WARNING;SOFT;1;Warning - 'tempdb' Transactions : 5/s
- [2006-03-29T06:25:17] SERVICE NOTIFICATION: alex;ella;wmi\_mssql\_log\_used\_CP\_Hollywood;WARNING;notify-by-email;Warning - CP\_Hollywood Percent Log Used : 53%
- [2006-03-29T06:25:17] SERVICE ALERT: ella;wmi\_mssql\_log\_used\_CP\_Hollywood;WARNING;HARD;3;Warning - 'CP\_Hollywood' Percent Log Used : 55%
- [2006-03-29T06:24:07] SERVICE ALERT: dbpn-web;check\_http\_EasyOddsPoker.com;OK;SOFT;2;HTTP OK HTTP/1.1 200 OK - 0.352 second response time
- [2006-03-29T06:23:55] SERVICE ALERT: ella;wmi\_mssql\_transactions\_\_Total;WARNING;SOFT;1;Warning - '\_Total' Transactions : 9/s
- [2006-03-29T06:21:55] SERVICE ALERT: ella;wmi\_mssql\_log\_used\_CP\_Hollywood;WARNING;SOFT;2;Warning - 'CP\_Hollywood' Percent Log Used : 53%
- [2006-03-29T06:21:23] SERVICE ALERT: dbpn-web;check\_http\_EasyOddsPoker.com;WARNING;SOFT;1;HTTP WARNING: HTTP/1.1 200 OK - 6.238 second response time
- [2006-03-29T06:18:41] SERVICE ALERT: ella;wmi\_mssql\_log\_used\_CP\_Hollywood;WARNING;SOFT;1;Warning - 'CP\_Hollywood' Percent Log Used : 51%
- [2006-03-29T06:16:39] SERVICE NOTIFICATION: alex;supafly01;ssh\_wmi\_mssql\_log\_used\_tempdb;OK;notify-by-email;OK - tempdb Percent Log Used : 41%
- [2006-03-29T06:16:39] SERVICE ALERT: supafly01;ssh\_wmi\_mssql\_log\_used\_tempdb;OK;HARD;3;OK - 'tempdb' Percent Log Used : 41%

## キューのスケジュール化

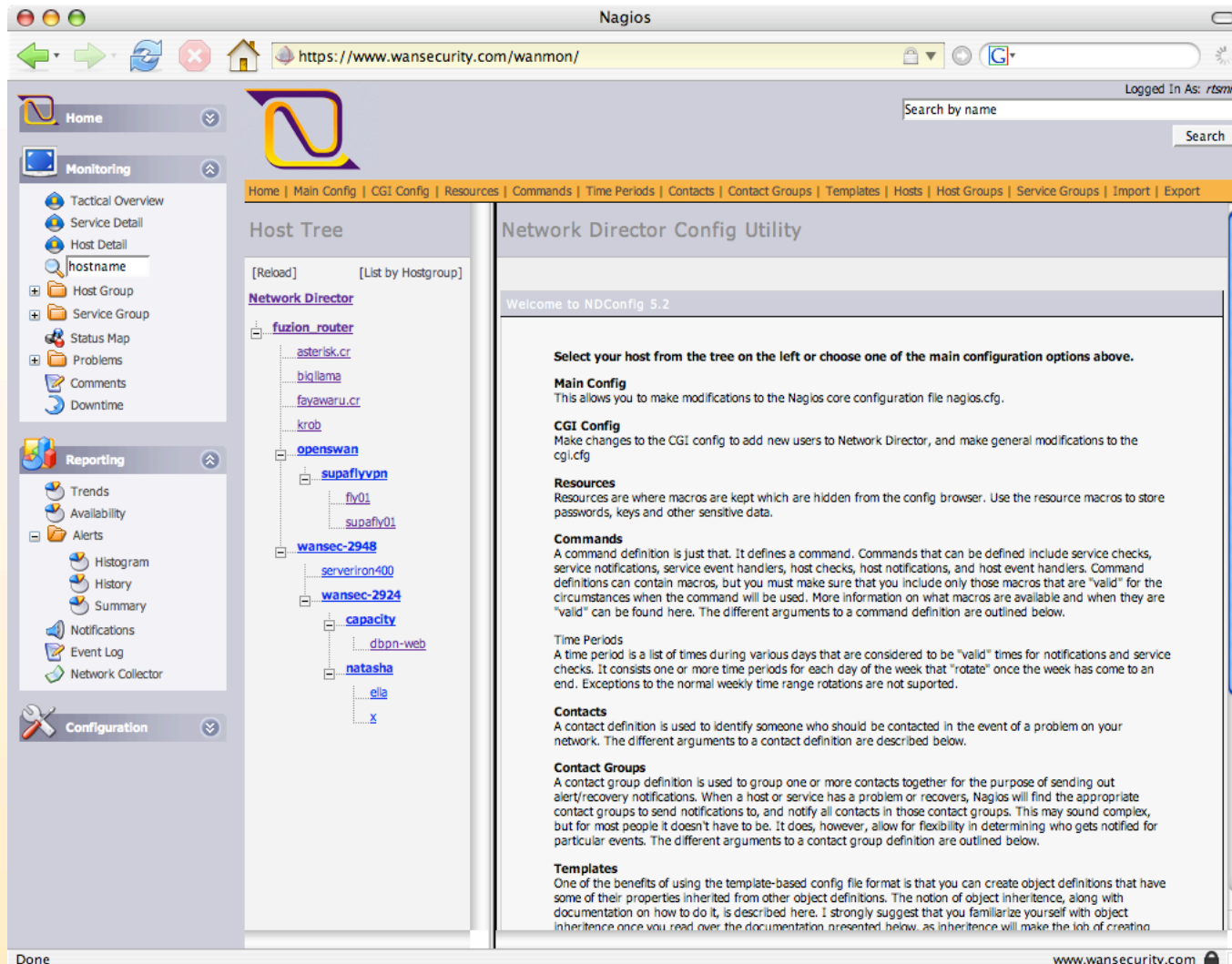
スケジューリング キューは実行するようにスケジュールされたサービスとホストのチェックをすべて一覧にします。指定したチェック時間をスケジュールから修正または削除できます。



Service	Check Name	Host	Next Scheduled	Last Scheduled	Status	Actions
wansec-2948	if_operational_status Fa10		2006-03-29T05:27:47	2006-03-29T05:32:47	ENABLED	⊗ ⌚
wansec-2948	if_operational_status Co51		2006-03-29T05:27:47	2006-03-29T05:32:47	ENABLED	⊗ ⌚
wansec-2924	if_stats VL300		2006-03-29T05:27:47	2006-03-29T05:32:47	ENABLED	⊗ ⌚
wansec-2924	if_operational_status Nu0		2006-03-29T05:27:47	2006-03-29T05:32:47	ENABLED	⊗ ⌚
wansec-2924	bandwidth_usage VL300		2006-03-29T05:27:47	2006-03-29T05:32:47	ENABLED	⊗ ⌚
wansec-2924	bandwidth_usage Fa0-6		2006-03-29T05:27:47	2006-03-29T05:32:47	ENABLED	⊗ ⌚
wansec-2924	bandwidth_usage Fa0-23		2006-03-29T05:27:47	2006-03-29T05:32:47	ENABLED	⊗ ⌚
serveriron400	if_operational_status ethernet2-1		2006-03-29T05:27:47	2006-03-29T05:32:47	ENABLED	⊗ ⌚
ella	wmi_cpu		2006-03-29T05:29:47	2006-03-29T05:32:47	ENABLED	⊗ ⌚
capacity	linux_net_io_bytes		2006-03-29T05:29:47	2006-03-29T05:32:47	ENABLED	⊗ ⌚
wansec-2948	if_stats Nu0		2006-03-29T05:27:48	2006-03-29T05:32:48	ENABLED	⊗ ⌚
wansec-2948	if_operational_status Fa35		2006-03-29T05:27:48	2006-03-29T05:32:48	ENABLED	⊗ ⌚
wansec-2948	if_operational_status Fa30		2006-03-29T05:27:48	2006-03-29T05:32:48	ENABLED	⊗ ⌚
wansec-2948	if_operational_status Fa26		2006-03-29T05:27:48	2006-03-29T05:32:48	ENABLED	⊗ ⌚
wansec-2948	if_operational_status Fa18		2006-03-29T05:27:48	2006-03-29T05:32:48	ENABLED	⊗ ⌚
wansec-2948	bandwidth_usage Co51		2006-03-29T05:27:48	2006-03-29T05:32:48	ENABLED	⊗ ⌚
serveriron400	if_operational_status ethernet3-2		2006-03-29T05:27:48	2006-03-29T05:32:48	ENABLED	⊗ ⌚
serveriron400	bandwidth_usage ethernet3-12		2006-03-29T05:27:48	2006-03-29T05:32:48	ENABLED	⊗ ⌚
dbpn-web	check_http_TiltZeroPoker.com		2006-03-29T05:31:21	2006-03-29T05:33:00	ENABLED	⊗ ⌚
dbpn-web	check_http_www.PremierBetPoker.com		2006-03-29T05:33:11	2006-03-29T05:34:11	ENABLED	⊗ ⌚
dbpn-web	check_http_HighRollersCardRoom.com		2006-03-29T05:33:11	2006-03-29T05:34:11	ENABLED	⊗ ⌚
dbpn-web	check_http_DoylesRoom.net		2006-03-29T05:33:11	2006-03-29T05:34:11	ENABLED	⊗ ⌚
dbpn-web	check_http_JazzPokerRoom.com		2006-03-29T05:33:13	2006-03-29T05:34:16	ENABLED	⊗ ⌚
dbpn-web	check_http_DoylesRoom.com		2006-03-29T05:33:13	2006-03-29T05:34:21	ENABLED	⊗ ⌚
supafly01	ssh_wmi_mssql_log_growth_Total		2006-03-29T05:31:23	2006-03-29T05:34:23	ENABLED	⊗ ⌚
supafly01	ssh_wmi_mssql_lock_wait_time		2006-03-29T05:31:23	2006-03-29T05:34:23	ENABLED	⊗ ⌚
ella	wmi_mssql_log_growth_BESMgmt		2006-03-29T05:31:23	2006-03-29T05:34:23	ENABLED	⊗ ⌚
capacity	check_swap_usage		2006-03-29T05:31:23	2006-03-29T05:34:23	ENABLED	⊗ ⌚
capacity	check_snmp_sys_desc		2006-03-29T05:31:23	2006-03-29T05:34:23	ENABLED	⊗ ⌚

## ネットワークディレクターの設定

ネットワークディレクターの設定は、Fruityプロジェクトに基づいています。Fruityとは、Nagiosを設定するオープンソースPHP/MySQLベースのアプリケーションです。ネットワークディレクターに統合するように構成されています。



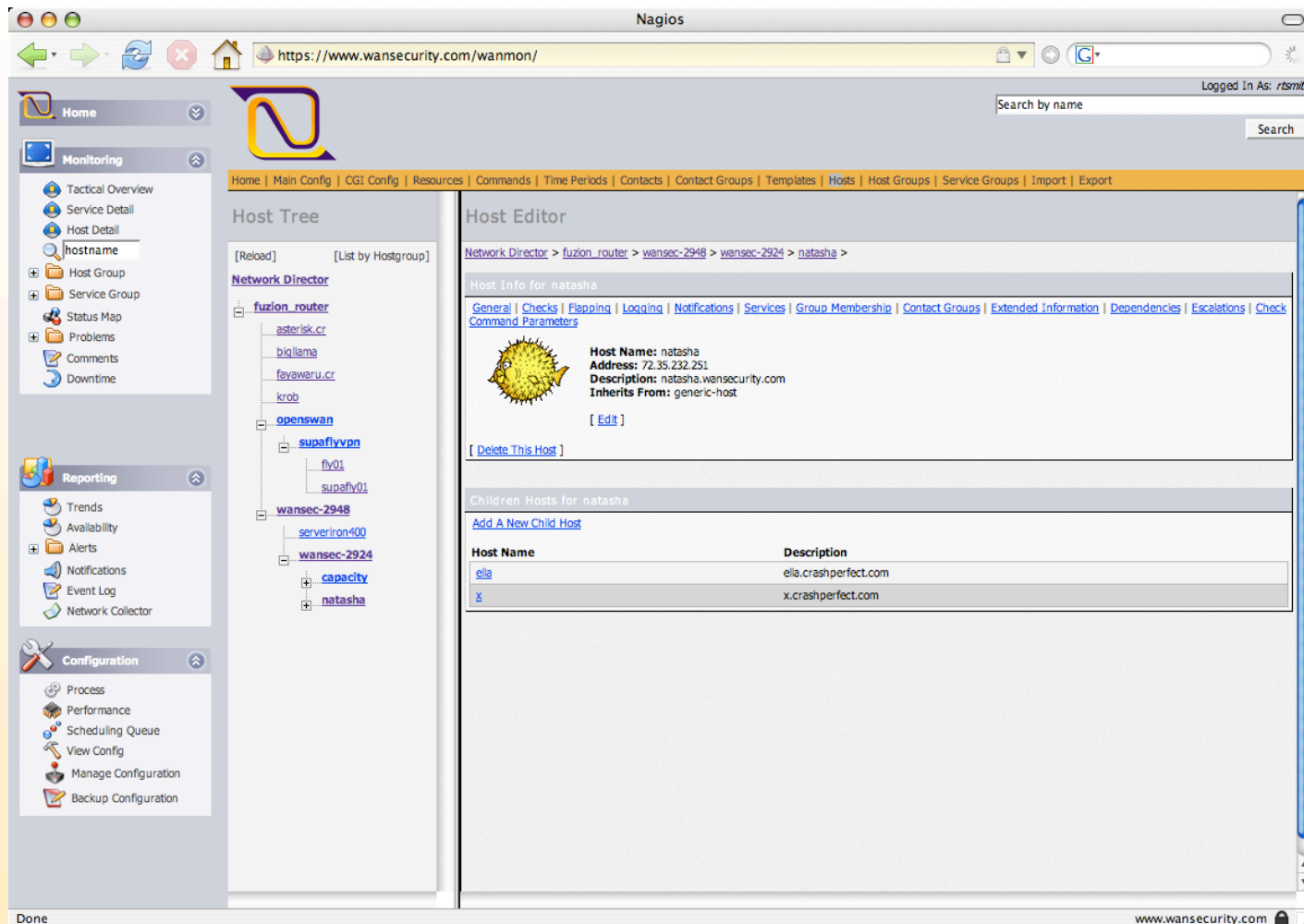
The screenshot displays the Nagios Network Director Config Utility interface. The browser address bar shows the URL `https://www.wansecurity.com/wanmon/`. The page is titled "Network Director Config Utility" and includes a search bar and a navigation menu. The main content area is split into two panes: "Host Tree" on the left and "Network Director Config Utility" on the right.

The "Host Tree" pane shows a hierarchical view of hosts, including:

- Network Director
  - fuzion\_router
    - asterisk.cr
    - bigllama
    - favawaru.cr
    - krob
  - openswan
    - supaflyvpn
      - fly01
      - supafly01
  - wansec-2948
    - serveriron400
  - wansec-2924
    - capacity
      - dbpn-web
    - natasha
      - ella
      - x

## ネットワークディレクターのホスト設定

ホスト設定のセクションは、ロギング[logging]、チェック[checks]、フラッピング[flapping]、サービス[services]、グループメンバーシップ[group membership]、担当者グループ[contact groups]、拡張インフォメーション[extended information](グラフ、ノート、アクション)、依存関係[dependencies]、エスカレーション[escalations]、チェックコマンドのパラメータ[check\_command parameters]などのホストプロパティのすべての面をユーザが設定することができます。以下はOpenBSDホスト(natasha)の例です。



The screenshot shows the Nagios Network Director web interface. The browser address bar displays `https://www.wansecurity.com/wanmon/`. The interface includes a navigation menu on the left with sections for Monitoring, Reporting, and Configuration. The main content area is split into two panes: 'Host Tree' and 'Host Editor'.

**Host Tree:** A hierarchical tree view showing the network structure. The path is: Network Director > fuzion\_router > openswan > supaflyvpn > wansec-2948 > natasha.

**Host Editor:** The configuration page for the host 'natasha'. It includes a breadcrumb trail: Network Director > fuzion\_router > wansec-2948 > wansec-2924 > natasha >. The host information is as follows:

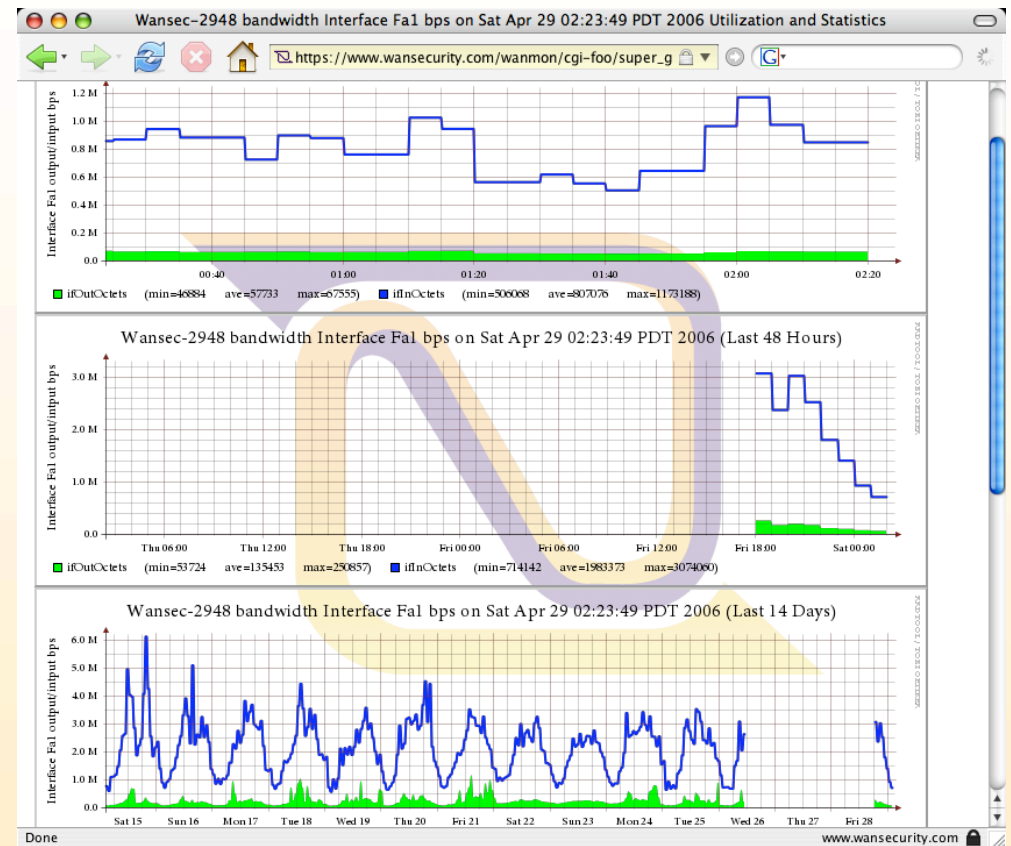
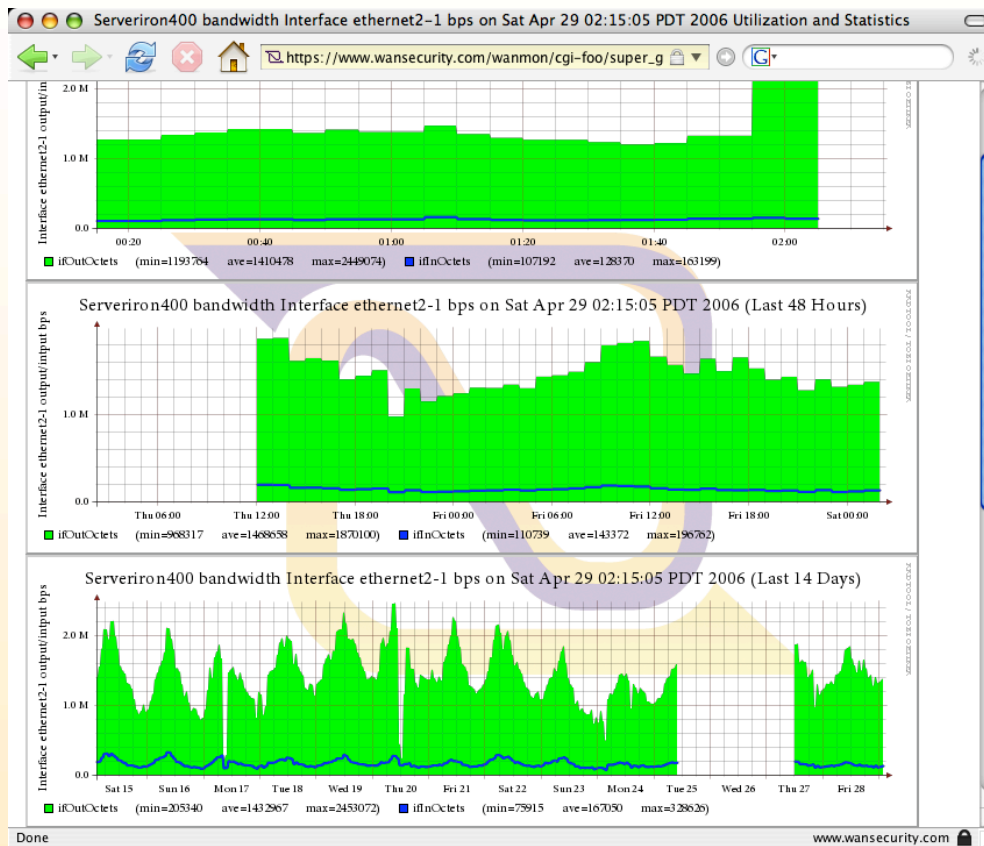
- Host Name: natasha
- Address: 72.35.232.251
- Description: natasha.wansecurity.com
- Inherits From: generic-host

Below the host information, there is a table for 'Children Hosts for natasha':

Host Name	Description
ella	ella.crashperfect.com
x	x.crashperfect.com

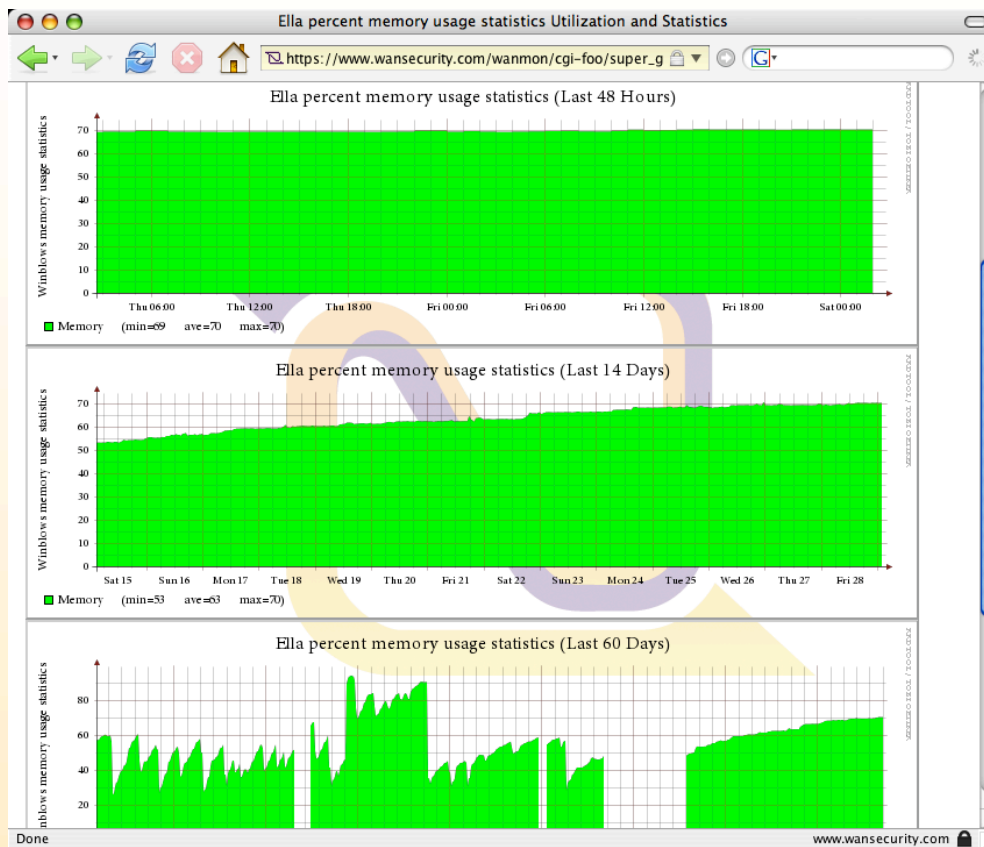
## バンド幅の使用

ネットワークディレクターは、事実上すべてのSNMPを認識するネットワーク装置からバンド幅使用量を探索しグラフ化することができます。下のグラフでは、Foundry ServerIron 400 Load BalancerとCisco 2948 Layer 3 switchのバンド幅の使用量を示しています。



## メモリ使用量

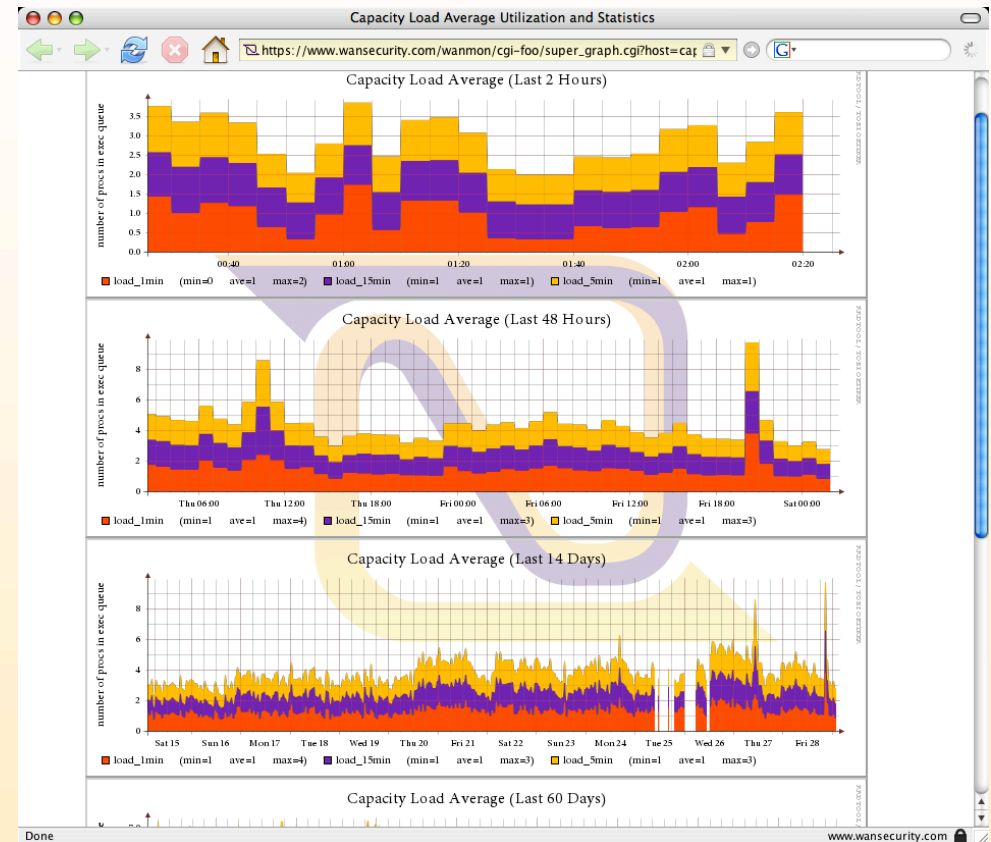
ネットワークディレクターは、事実上すべてのオペレーティングシステムとほぼすべてのSNMPを認識できるネットワーク装置からメモリとスワップの使用量を探索しグラフ化することができます。下のグラフではWindows Server 2003とLinux 2.6のメモリ使用量を示しています。





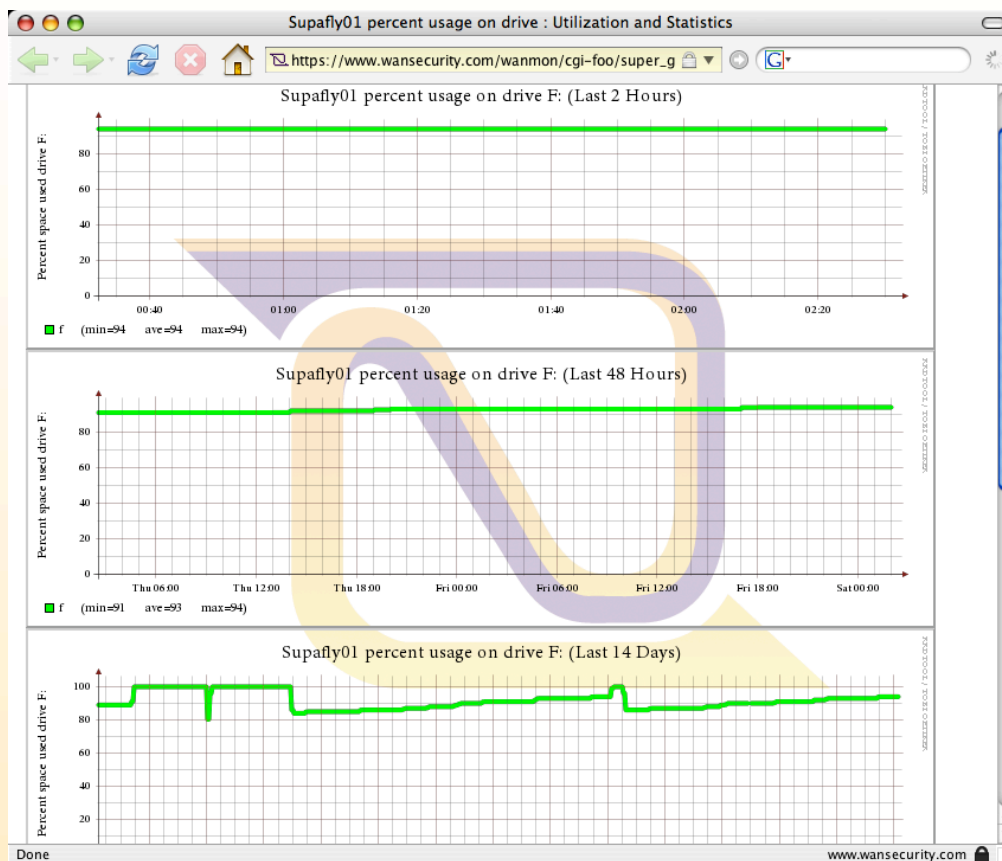
## CPUの使用量

ネットワークディレクターは、事実上すべてのオペレーティングシステムとほぼすべてのSNMPを認識できるネットワーク装置からCPU使用量とロードアベレージを探索し、グラフ化することができます。下のグラフでは、SQL Server 2000を稼動しているWindows 2000 ServerのCPU使用量とlinux Kernel 2.6. のLinuxロードアベレージを示しています。



## ディスクの使用状況

ネットワークディレクターは、事実上すべてのオペレーティングシステムとほぼすべてのSNMPを認識できるネットワーク装置からディスク使用量を探知しグラフ化することができます。下のグラフはMsSQLが稼動しているWindows 2003 ServerのFDドライブに対するディスク使用量と、Unixシステムの/var/tmp のディスク使用量を示しています。



# Network Collector

ネットワーク・コレクター

## 集中ログ機能

シスログシステムは、イベント通知メッセージをログ形式で転送するメカニズムと保存するメカニズムを備えています。シスログは、RFC3164によって定義されたシステムイベントのログGINGのデファクトスタンダードです。シスログは当初ソケットを介したUnixシステムおよびUnixのシスログデーモン(syslogd)で使用されていました。現在では、ルータ、スイッチ、ファイアウォール、さらにはカスタムアプリケーションなど、一般的なネットワーク装置すべてに使用されています。Windowsシステムではどうでしょう。WindowsのEventLogアプリケーションに直接接続するSnareソフトウェアが、リアルタイムにイベントログを変換、転送します。

ネットワークコレクターの構造は、膨大な数のシスログメッセージの処理に対し企業レベルの拡張性ソリューションを提供し、アドミニストレータとネットワーク管理者が規制遵守に適合するようにデータを分類し、分析する手助けをします。ネットワークコレクターは以下の問題のソリューションを提供します。

- ・ 企業内のシスログ情報の集中アーカイブと集中処理
- ・ 調査および承認のための詳細情報をネットワーク管理者に提供
- ・ SIM (Security Information Management)、政府および他の規制適合の支援(ただし必ずしも以下に限定されない):
  - ISO 17799
  - FFIEC (Federal Financial Institutions Examination Council)
  - SOX (Sarbanes-Oxley Act of 2002)
  - GLBA (Gramm-Leach Billey Financial Modernization)
  - HIPAA (Health Insurance Portability and Accountability Act of 1996)
- ・ ネットワーク管理者がリアルタイムでネットワーク上のアクティビティの概要を確認する方法
- ・ 不定期間のシスログデータのアーカイブとシスログデータへの瞬時アクセス
- ・ リモートネットワークからネットワークコレクターのマスタークラスターへシスログデータを安全性かつ信頼性の高い転送
- ・ ログの処理ロジックと顧客のニーズに合わせたログデータの統計分析
- ・ イベントアラームの設定

## ネットワークコレクターの説明

UDPシスログメッセージは、ネットワークコレクターのノード(NCNode)、またはネットワークコレクターのノードのクラスター(NCNodes)によってLANセグメントに集められます。NCNodesは、ネットワークコレクターマスタークラスター(NCMC)に届くリモートファシリティまたはネットワークからのログデータが重要である場合に実行されます。その後シスログデータは処理され、確實かつ安全にシスログデータを割り当てるNCMCに送信されます。そして割り当てられたNCMCサーバーの1つによって処理されます。高度なフィルターロジックを使用して、マスターサーバーは、ベンダーと製品のデータベースで設定済みのフィルタールールに対してシスログイベントメッセージを適合します。メッセージがフィルタールールに適合すると、イベント情報は分類され、アーカイブデータベースに送信されます。未処理のアーカイブログデータは、暗号化され、社外に転送することができます。

## フィルタールール

ネットワークコレクターは、多種多様なネットワーク装置、UNIX、Windowsサーバーなどからのログとイベントメッセージを認識します。フィルターロジックは、ネットワークコレクターのWebインターフェイスから拡張および設定が可能です。弊社はクライアントと共に協力し、求められる共通の例外一覧のフィルターロジックを策定しました。ネットワークコレクターは以下のシスログメッセージタイプのフィルターロジックを組み込んでいます。

## Windows Serverとワークステーション製品(Windows EventLog API)

- Logon failure reported by users
- User disabled report
- Logon Failure report by computers
- Software install/uninstall report
- Logon Access report by users and computers
- Critical service downtime time report
- Resource access success report
- User authentication granted
- Resource access denied report
- User authentication granted
- Resource access denied report
- User authentication denied
- Password reset by user
- Active directories: User added/deleted
- Access rights to shared, files and folders
- Active Directories: Computers added/deleted
- Group policy changed
- SQL Server: Logon failure
- User lockout report
- SQL Server: Logon

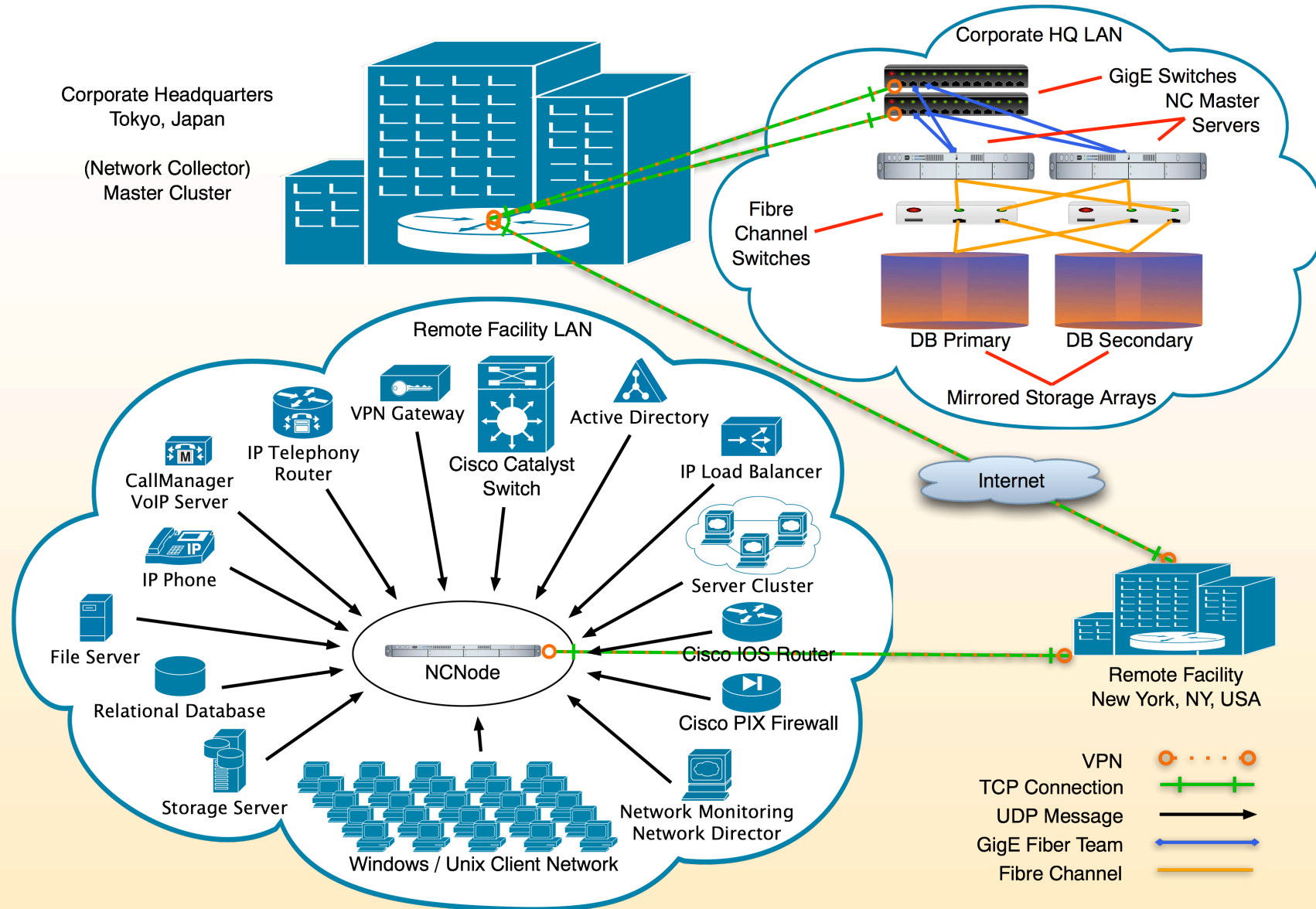
## UNIX、Linux、BSD、SolarisとUNIX系のシステム ネットワークディレクターのフィルタ ルール (続き)

- Logon failure report
- Intrusion Detection report
- Logon success report
- Root activity report
- Root (Administrative) logon report
- Audit Policy changed report
- Password change reports
- Privileged user activities
- Privilege escalation report (su or sudo)
- SSHD failed login
- FTP and (x)inetd activities
- Remote volume mounts
- Local Firewall logs
- PF Logs
- IPtables Logs
- IPFW Logs
- IPF Logs
- Local media mounts
- Mail messages (Postfix, Sendmail, Qmail)
- MySQL
- PostgreSQL

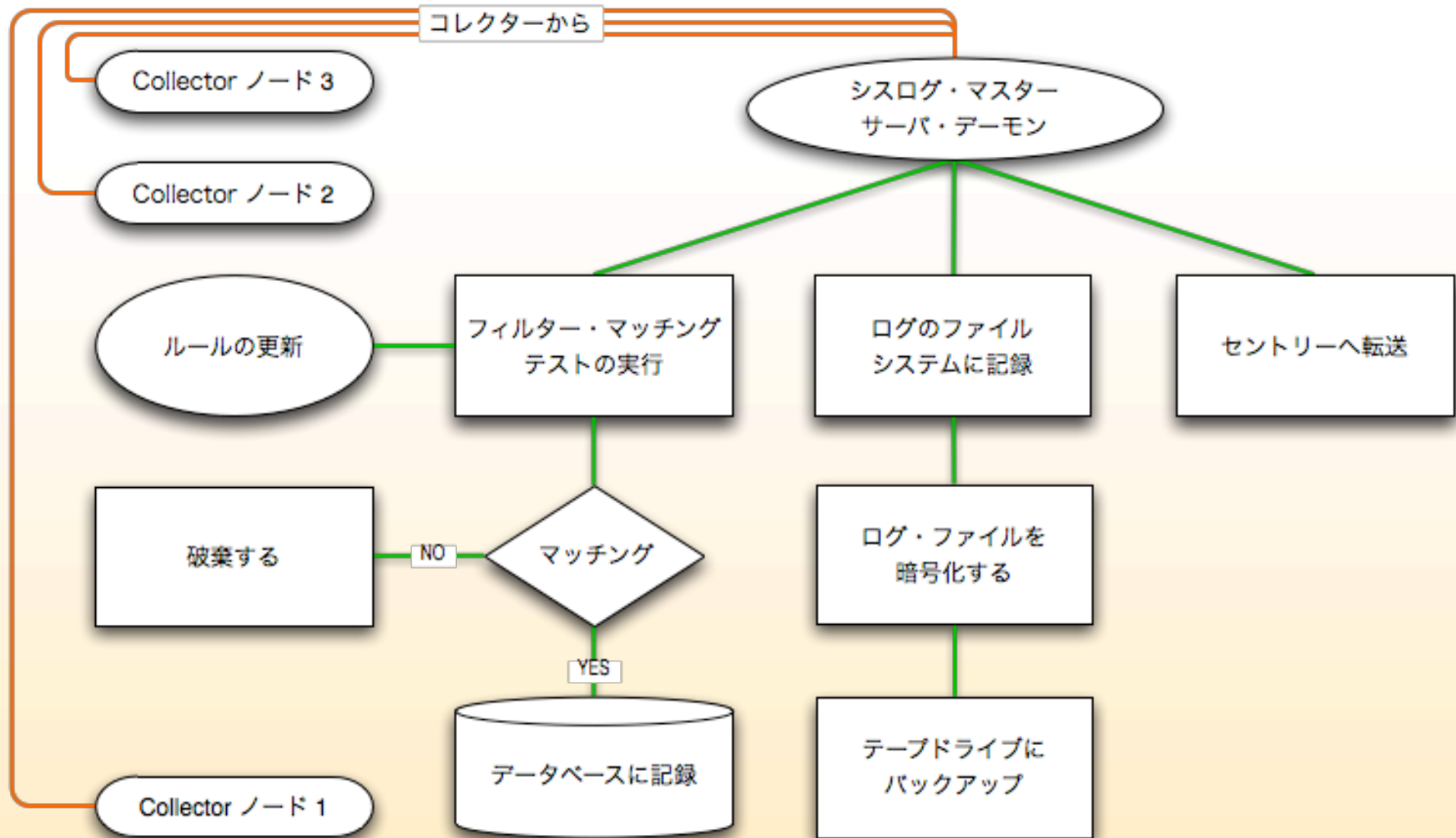
## Cisco、Foundry、Nokia、Checkpoint、FW1、IOS Routers、 Sourcefire IDS

- Login failures
- Intrusion Detection report
- Logon success report
- Configured changed
- MAC identity assumption
- Matching packet rules
- Packets passed
- Packets Dropped
- Packets Rejected
- Packets Returned
- TCP Checksum mismatches
- Mangled packets
- Fragmented packets
- Interface flapping errors
- Duplex errors
- Failed exploit attempts
- Connect resets by peer
- Successful exploit attempts
- Attempted exploit match
- Attempted DoS match
- ICMP floods
- Interface errors
- Interface discards
- VLAN Hops

## ネットワークコレクターの事例研究



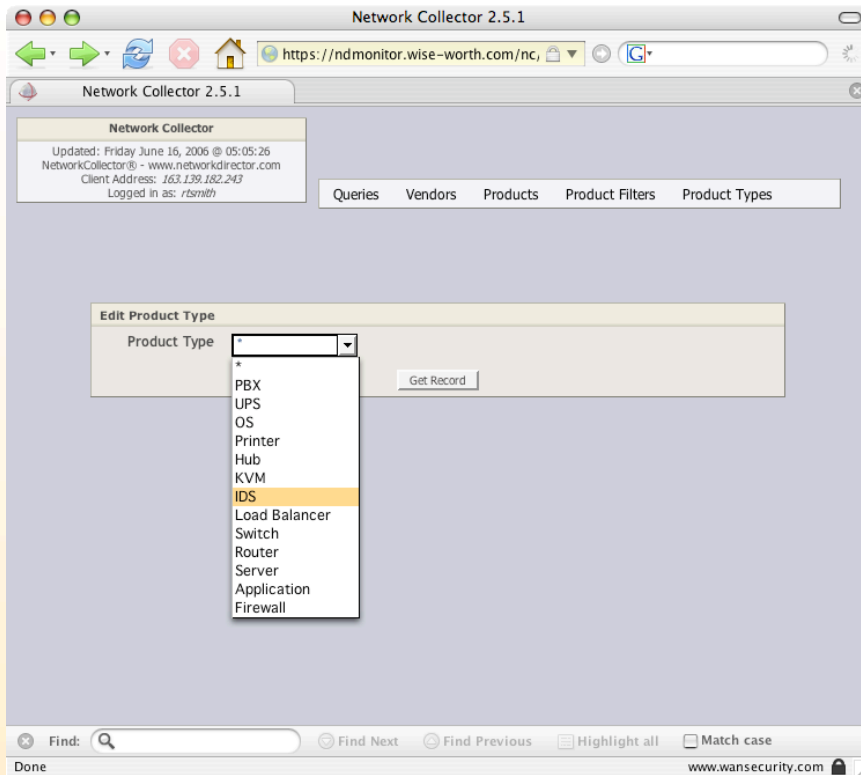
ネットワークコレクターのメッセージ処理





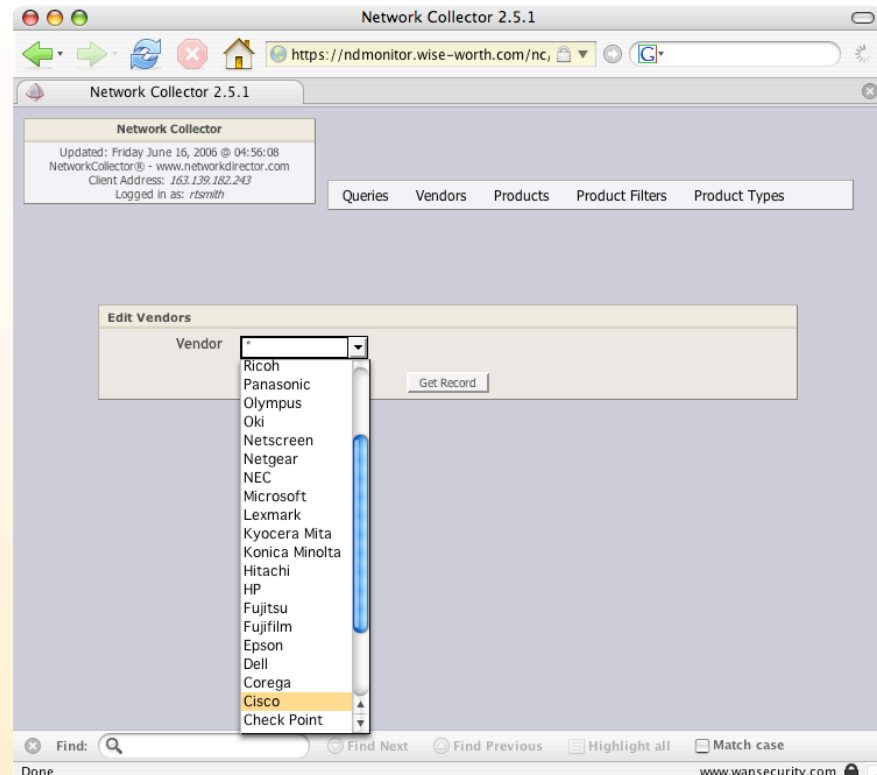
## ネットワークコレクターの画面キャプチャー

以下の画面キャプチャーでは、フィルター・マネージメント・インターフェースを使い、新しいフィルター・ルールを追加しています。



### ステップ 1

該当製品がリストにない場合は” Product Type” から追加（例：ファイアーウォール）

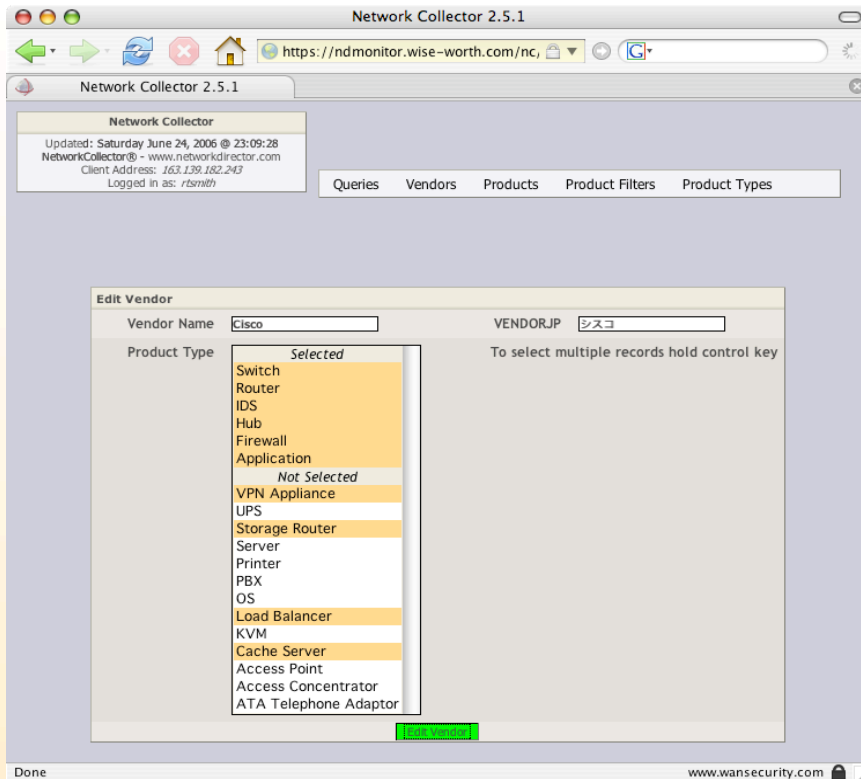


### ステップ 2

該当ベンダーがリストにない場合は”Vendor”から追加（例：Cisco）

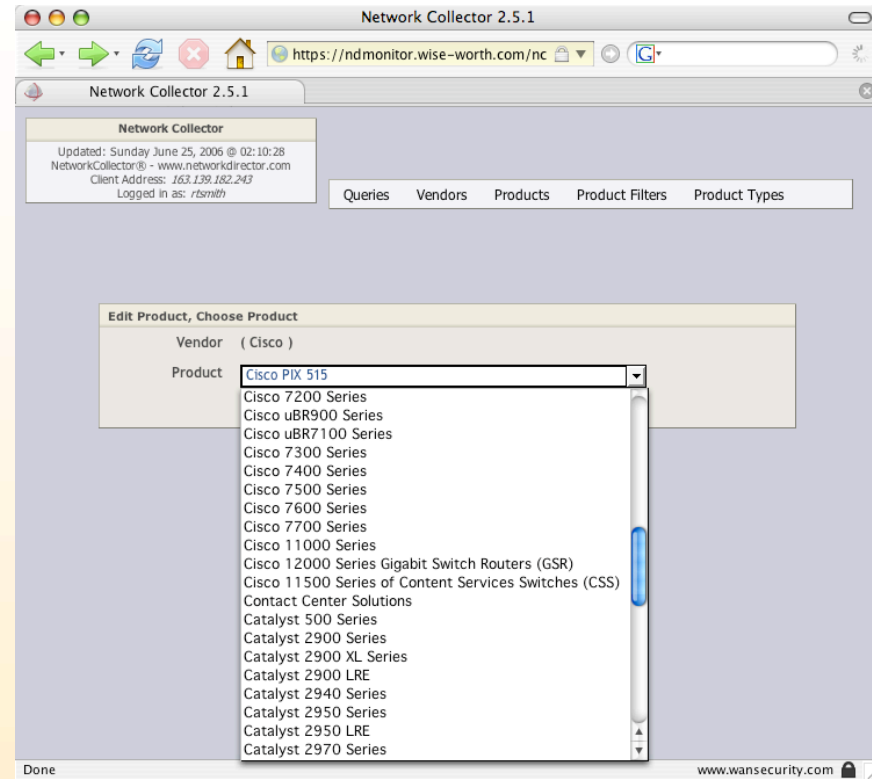
## ネットワークコレクターの画面キャプチャー

以下の画面キャプチャーでは、フィルター・マネージメント・インターフェースを使い、新しいフィルター・ルールを追加しています。



### ステップ 3

ベンダー (Vendor) を選択して、表示された製品タイプ (Product Types) と関連付けてください。

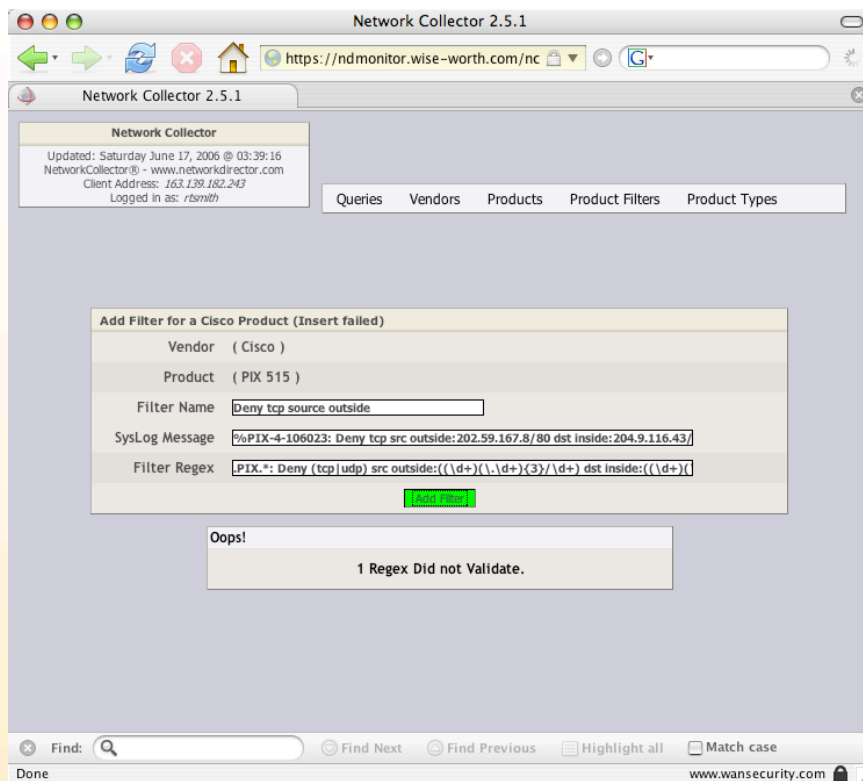


### ステップ 4

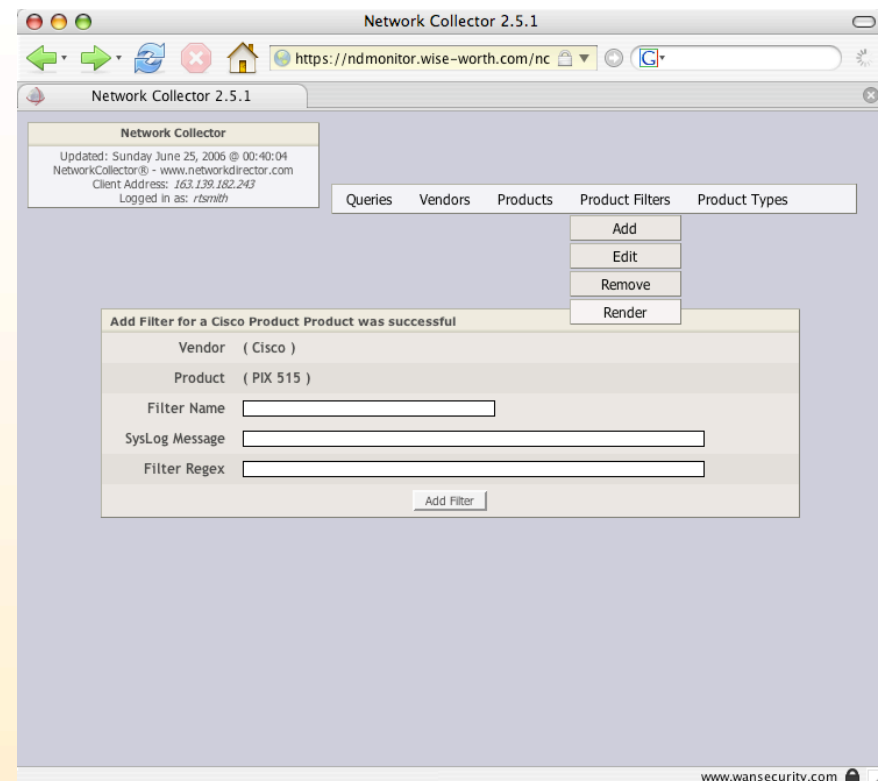
該当製品がリストにない場合は"Product"から追加 (例 : PIX515)

## ネットワークコレクターの画面キャプチャー

以下の画面キャプチャーでは、フィルター・マネージメント・インターフェースを使い、新しいフィルター・ルールを追加しています。



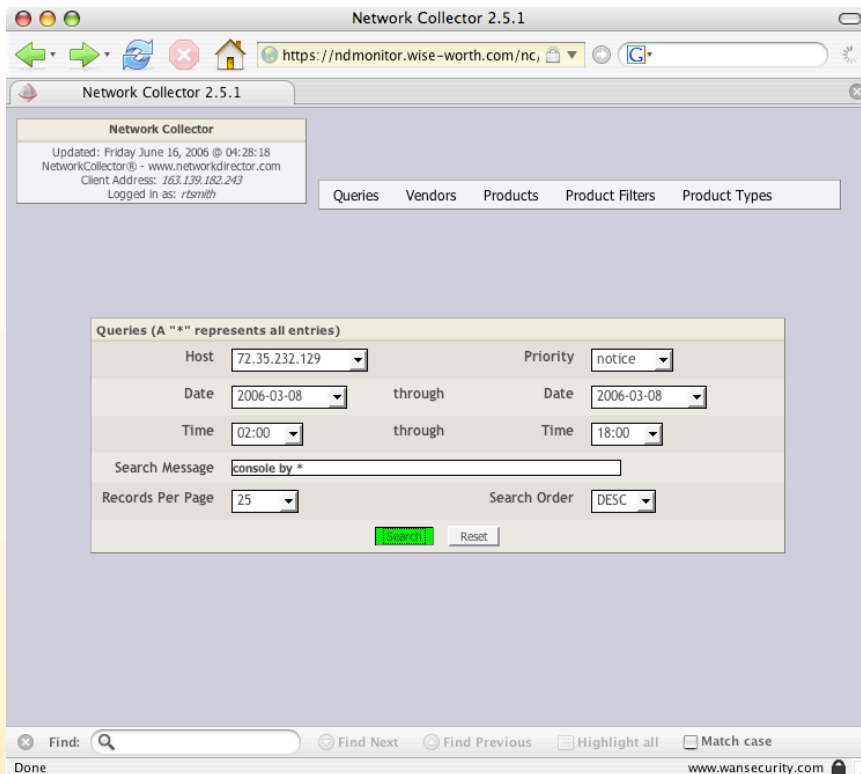
ステップ 5  
フィルター・ルールを” Filter Rule” から、  
フィルター管理DBへ追加 (例 : PIX515)



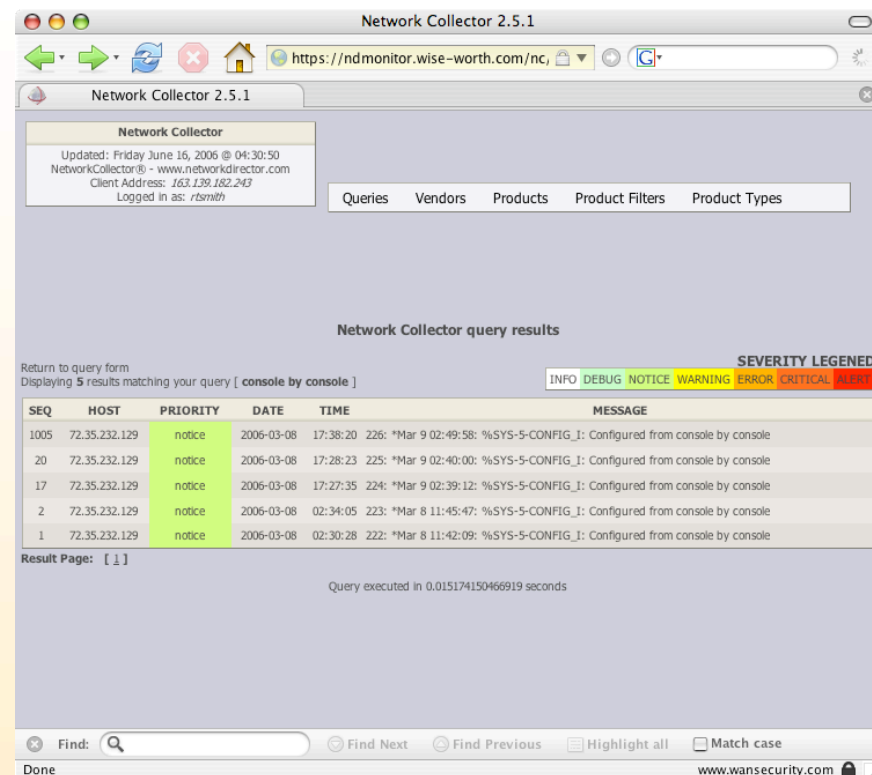
ステップ 6  
フィルター・ルールをフィルターエンジンに追加

# ネットワークコレクターの画面キャプチャー

以下の画面キャプチャーでは、フィルター・マネージメント・インターフェースを使い、新しいフィルター・ルールを追加しています。



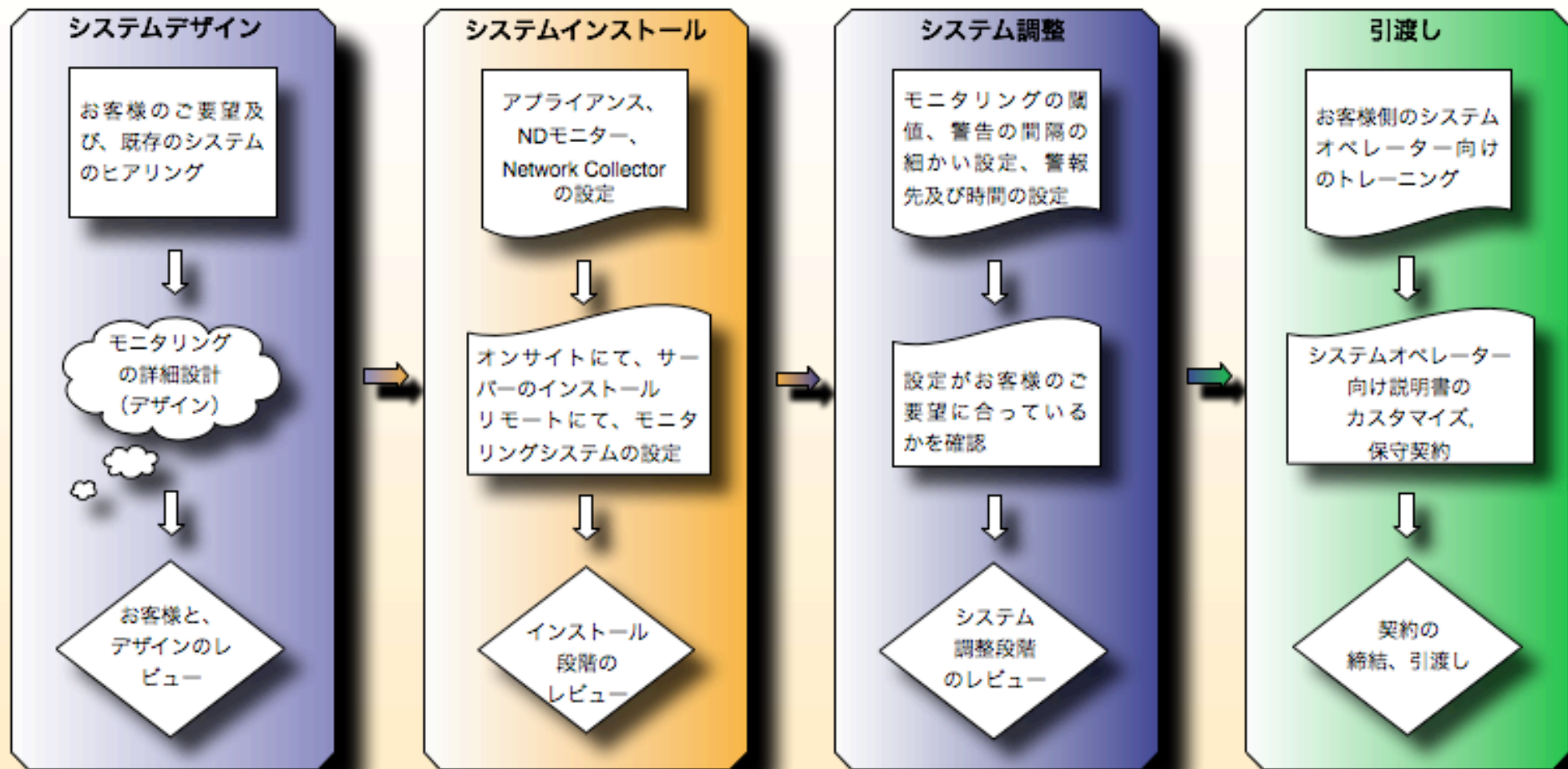
ステップ 7  
カスタム・クエリーを実行



ステップ 8  
カスタム・クエリーの結果

## 設置手順

設計段階で、お客様のネットワーク監視のニーズに関して打ち合わせを行います。弊社は、そのニーズおよび現在ご利用の監視システムを評価し、お客様のニーズに見合う監視システムを設計します。お客様の承認を頂きました後、ネットワークディレクターシステムをインストールし、設計を構成、調整し、お客様へお引渡しいたします。お客様は新しいシステムためのトレーニングへの出席が必要となります。トレーニングと設計仕様に基づく条件に見合った監視ソリューションのインストールが終了後、お客様はサインオフし、弊社からお客様へのハンドオフが行われます。



## カスタム監視ソリューション設計とインストール手順

これまでの多数の経験から、お客様が早急にかつ効果的に新しい監視システムを利用できるまでのプロセスを以下の手順のように効率的に行うことができます。このプロセスを円滑に進めるために、設計、調整、システム導入など各段階において綿密に打ち合わせを行います。

### 弊社

- お客様からの要望を収集
- 自動ディスカバリを実行
- 監視の仕様を設計
- 監視の仕様を提示
- ネットワークディレクターのインストール
- ネットワークディレクターを監視の仕様に基づいて設定
- システムの調整
- お客様にマニュアルの提供
- お客様に資料の提供
- トレーニングの実施
- お客様にシステムをハンドオフ

### お客様

- ネットワークディレクターのインストールの作業を支援するスタッフのアサイン
- 要請された情報の提供
- 自動ディスカバリの管理
- 既存の監視システムのデモ
- 監視の仕様の確認
- エージェントのインストール
- 誤ったアラームに関する情報の提供による調整処理のアシスト
- トレーニングへの出席
- 監視システムの設定終了後サインオフ

# ありがとうございました。

ご質問、詳細については下記までご連絡ください。宜しくお願い申し上げます。

ndmonitor-info@wise-worth.com

+81 (0)3.3505.2303