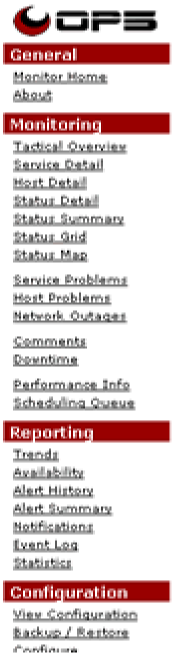
Users Manual

Monitor 2.2

By Patrik Brodin

Table of Contents

User Interface

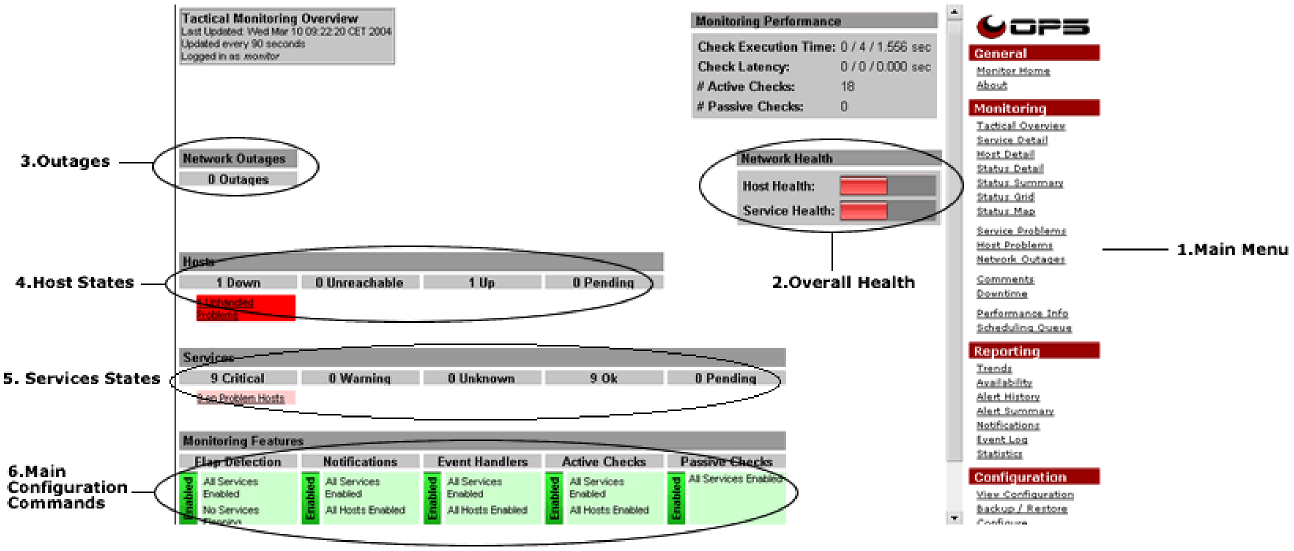


The web user interface is accessed through a standard web browser. The most common browsers as Opera, Mozilla, Explorer and Netscape have been tested. The start page is accessed by typing https://10.10.10.1/monitor. The IP address is unique for your system, 10.10.10.1 is just an example. The protocol used is to access is HTTP with SSL “Secure Socket Layer”. This enables a secure manner for accessing the web interface using encryption. The start page shows a main menu. This menu has three section, General, Monitoring, Reporting and Configuration. The general part links you to an About page which gives you the new functions and changes released in this version. Monitoring is related to Fault Management. Reporting has to do with reports and configuration is related to configuration of the system. The web user interface enables you to handle the whole Monitor system from a single point.

Lets go through the main menu choices.

Tactical Overview

The Tactical Overview window enables the user to get a summarized picture of the overall network health.



Tactical Monitoring Overview
Last Updated: Wed Mar 10 09:22:20 CET 2004
Updated every 90 seconds
Logged in as *monitor*

Monitoring Performance

Check Execution Time: 0 / 4 / 1.556 sec
Check Latency: 0 / 0 / 0.000 sec
Active Checks: 18
Passive Checks: 0

Network Outages
0 Outages

Hosts
1 Down | 0 Unreachable | 1 Up | 0 Pending
1 Unhandled Problems

Services
9 Critical | 0 Warning | 0 Unknown | 9 Ok | 0 Pending
9 on Problem Hosts

Monitoring Features

Flap Detection	Notifications	Event Handlers	Active Checks	Passive Checks
Enabled All Services Enabled No Services Flapping	Enabled All Services Enabled All Hosts Enabled	Enabled All Services Enabled All Hosts Enabled	Enabled All Services Enabled All Hosts Enabled	Enabled All Services Enabled

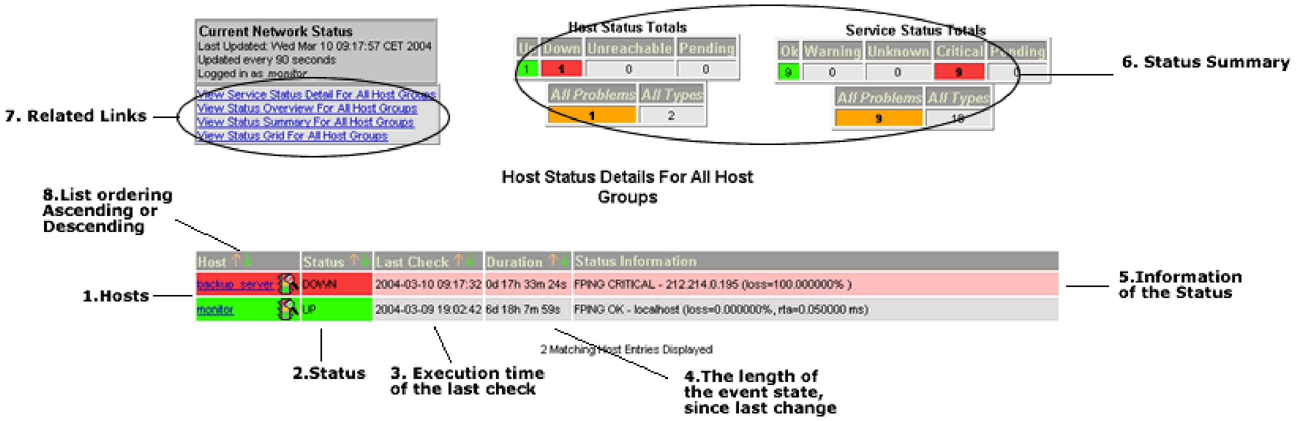
1. Main Menu, The main menu is accessible at all times no matter what window your in. This enables you make choices faster.
2. Overall Health, gives you an overall health view. The bars represent a percentage view of the status in the network.
3. Outages, shows if a central host is faulty and cusing hosts that are located below to be

unreachable. As an example, if a switch goes down causing connected hosts to be unreachable the switch will be listed as an network outage.

4. Host States, Gives you a summarized view of the host and their status. There are four different states:
    1. Down, the host is not responding to a check.
    2. Unreachable. The host is unreachable to the system due to a network outage (see network outage)
    3. Up, the host is working fine.
    4. Pending, the host has not been checked yet, the check of the host is in a queue about to be executed.
5. Services States, gives you a summarized view of the service status. There are five different states:
    1. Critical, the service check responds with a value that is within the configured critical level.
    2. Warning, the service check responds with a value that is within the configured warning level.
    3. Unknown, the service of a host does not respond correctly to a service check, or the service check is misconfigured.
    4. Ok, the service is working fine.
    5. Pending, the service has not been checked yet. The check is queued about to be executed.
6. Main configuration Commands. You have the possibility to enable and disable Monitor wide functions. Just by clicking on the enabled icon you can change the configuration.
    1. Flap Detection. If a host or a service is changes state between an ok and a non-ok state with low interval, the host or service is flapping and the alarms are suppressed. Monitor has the ability to detect flapping. Flap Detection can be enabled or disabled in this menu.
    2. Notifications. All status changes, from an ok to a non ok and vice versa is an event change. All event changes can cause a notification to the configured contacts via email or sms. In this menu the notifications can enabled or disabled for the whole system.
    3. Event Handlers. Event handler is a function that enables the execution of commands whenever a state change occurs, one possible use for this is to automatically restart a process that has died, this is normally not used in OP5 Monitor. These can be enabled or disabled in this menu.
    4. Active Checks. When determining if a host or a service is ok Monitor performs an active check is. i.e a plug in is executed for that host or service. This menu choice enables or disables that function.
    5. Passive Check. Monitor has the possibility to receive results from the outside where the check initially was not performed by Monitor. An example is traps which are executed from a host. This menu choice enables to enable or disable the reception of these checks.

Host and Service Detail

The Host and Service Detail window gives you a detailed list of the status of all host and service (Service Detail) or a detailed list of the status of all hosts (Host Detail). The list is sorted by clicking the listing icon either ascending or descending order (see nr 8 in picture). The list can sorted after host or services, last check or duration.


7. Related Links
6. Status Summary
8.List ordering Ascending or Descending
1.Hosts
5.Information of the Status
2.Status
3. Execution time of the last check
4.The length of the event state, since last change

Current Network Status
Last Updated: Wed Mar 10 09:17:57 CET 2004
Updated every 90 seconds
Logged in as monitor

View Service Status Detail For All Host Groups
View Status Overview For All Host Groups
View Status Summary For All Host Groups
View Status Grid For All Host Groups

Host Status Totals

Up	Down	Unreachable	Pending
1	1	0	0

All Problems	All Types
1	2

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
9	0	0	9	0

All Problems	All Types
9	18

Host Status Details For All Host Groups

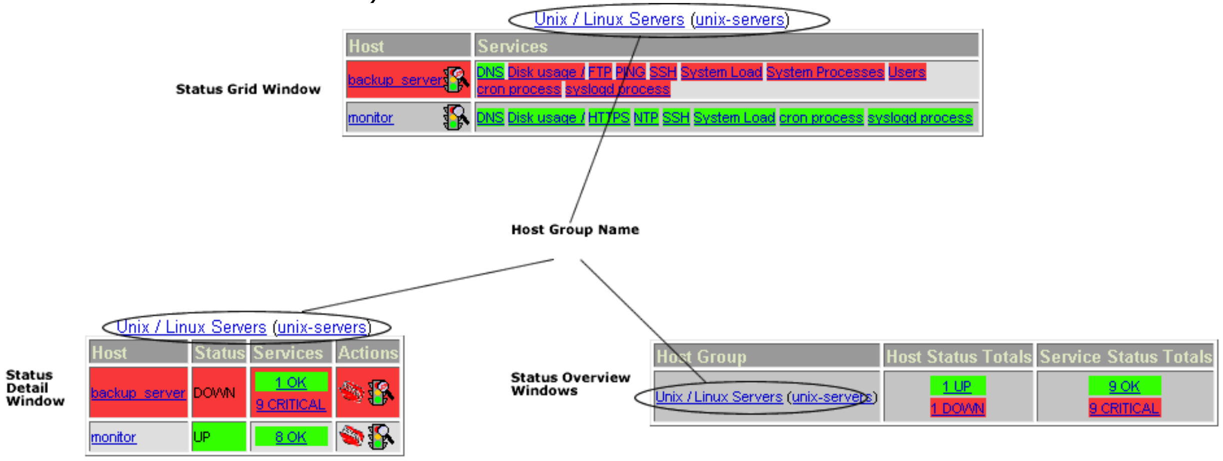
Host ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Status Information
backup_server	DOWN	2004-03-10 09:17:32	0d 17h 33m 24s	FPING CRITICAL - 212.214.0.195 (loss=100.000000%)
monitor	UP	2004-03-09 19:02:42	6d 18h 7m 59s	FPING OK - localhost (loss=0.000000%, rta=0.050000 ms)

2 Matching Host Entries Displayed

1. Hosts. Shows you the name of the host. This is the name configured for a certain host or service.
2. 2. Status. Shows the current status of the host or service.
3. Last Check. Lists the date and time when the last check was executed.
4. Duration. Shows you the amount of time the host or service has been in the current state.
5. Status Information. Shows you the response of the check on a host or a service. This information corresponds the status of the device.
6. Status Summary. A Summary of the status for all hosts and services.
7. Related links. Enables you to shortcut to Service detail if you are in the Host detail windows or vice versa. It also enables you to shortcut host group informational windows: Status Summary, Status Grid and the Status Overview.

Status Detail, Status Grid, Status Summary

These three windows gives you a Status view of the network where the hosts and services are grouped into host groups. Host groups is a way of grouping elements in the network and connect these to a group of contacts. By doing this larger corporations with large networks can let the administrator manage only a part of the network. Example: A company can divide there network in geographical instances, like Sweden, Finland and Norway. The administrators for these sites can then utilize the Status windows and only see their portion of the network (hosts and services and their status).



Unix / Linux Servers (unix-servers)

Host	Services
backup_server	DNS Disk usage / FTP PING SSH System Load System Processes Users cron process syslogd process
monitor	DNS Disk usage / HTTPS NTP SSH System Load cron process syslogd process

Unix / Linux Servers (unix-servers)

Host	Status	Services	Actions
backup_server	DOWN	1 OK 9 CRITICAL	
monitor	UP	8 OK	

Host Group	Host Status Totals	Service Status Totals
Unix / Linux Servers (unix-servers)	1 UP 1 DOWN	9 OK 9 CRITICAL

Status Grid Window

Lists all hosts and their services and the status of the hosts and services. You'll get one table per host group. The hosts and services can be clicked. They are linked to the host or service information window.

Status Detail Window

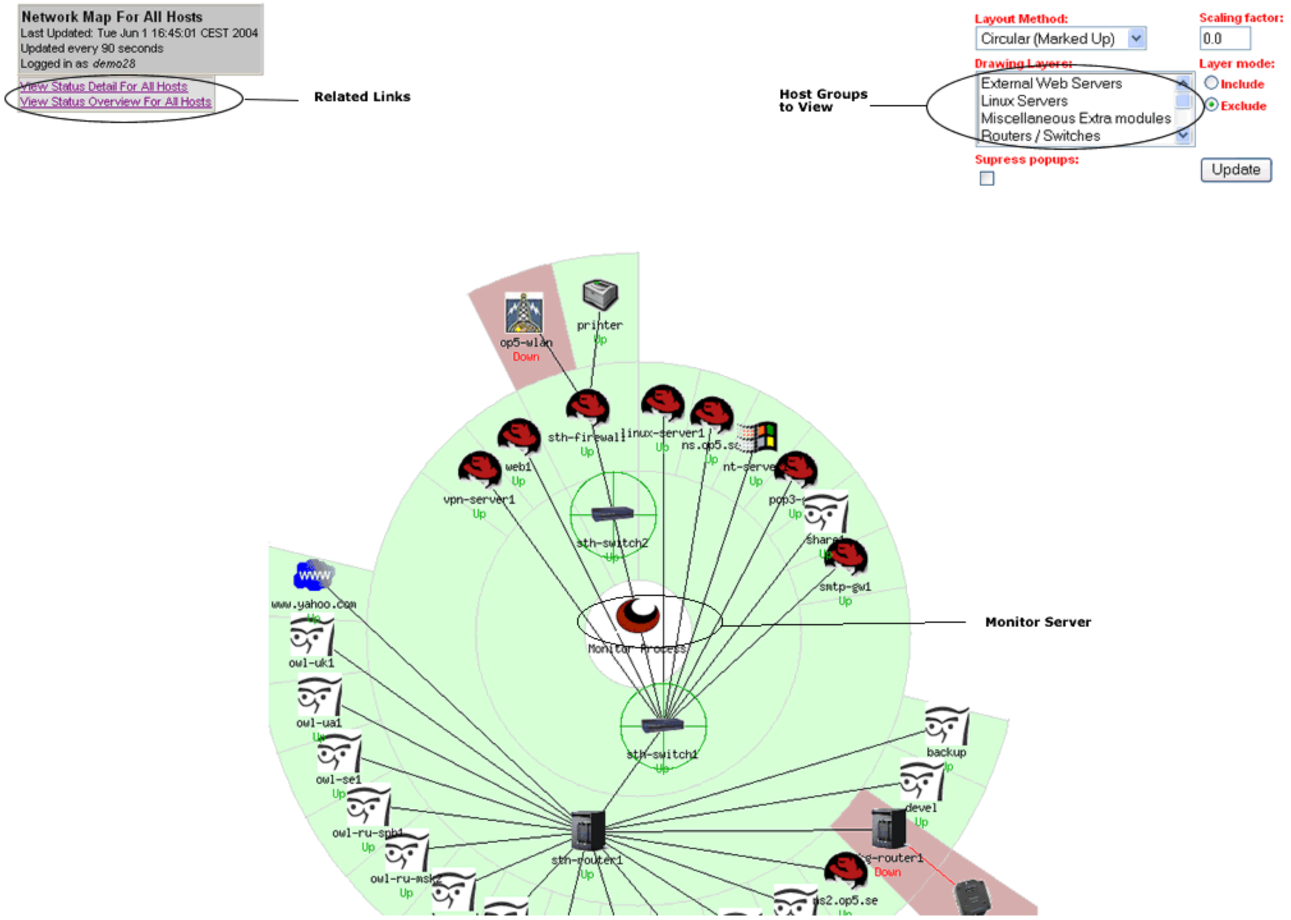
Lists all hosts and their states. You'll also get a summarized status picture of the services per host. All taken actions are also listed per host. (Comments, Acknowledgments, enabled and disabled functions.)The hosts and services can be clicked. They are linked to the host or services information window.

Status Over View Window

Lists all host groups and the states of all hosts and services connected to it. The host and service status can be clicked. If you click the host status link you will end up in the Status Detail Window. If you click on the service status link you'll end up in the Status Grid window.

Status Map

The Status Map gives you geographical view of the network including the relations between the hosts. The Map also shows what parts of the network that are functional, nonfunctional and out aged.



Network Map For All Hosts
Last Updated: Tue Jun 1 16:45:01 CEST 2004
Updated every 90 seconds
Logged in as *demo28*

View Status Detail For All Hosts
View Status Overview For All Hosts

Layout Method: Circular (Marked Up)

Scaling factor: 0.0

Drawing Layers:
External Web Servers
Linux Servers
Miscellaneous Extra modules
Routers / Switches

Layer mode: ○ Include ● Exclude

Supress popups: □

Update

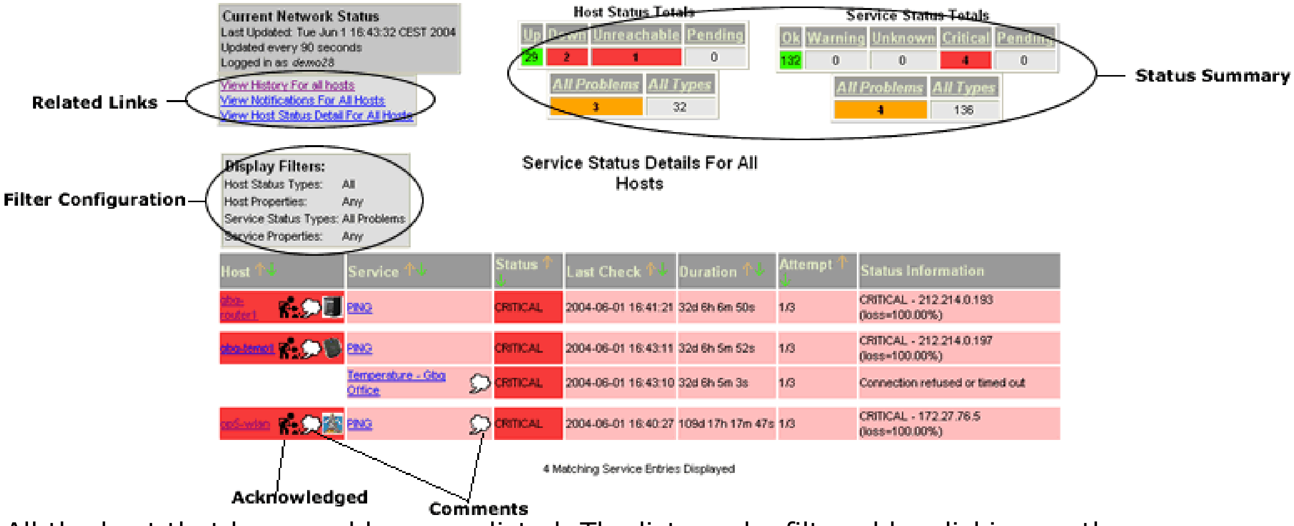
Furthermore the Status Map can be configured with a background to show a map as an example. All the icons enables you to find your hosts quickly further pinpoint the location of the problem. The icons can be replaced by your choice.

The Status Map can filter out all hosts that are related to a certain host group and show or exclude these. This is done choosing the drawing layers. The map can be scaled, zoomed in or out.

For more information about the status you can choose the related links that sends you to the status detail and overview window.

Service and Host Problems

The Service and Host Problem Windows are similar to the Host and Service Detail windows. The real difference is the display of status. The Service and Host Problem windows only shows problems. Service Problem window shows all hosts and services with problems. The Host Problems window show all hosts that have problems.



Current Network Status
Last Updated: Tue Jun 1 16:43:32 CEST 2004
Updated every 90 seconds
Logged in as demo28

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

Host Status Totals

Up	Down	Unreachable	Pending
29	2	1	0

All Problems	All Types
3	32

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
132	0	0	4	0

All Problems	All Types
4	136

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
gbg-router1	PING	CRITICAL	2004-06-01 16:41:21	32d 6h 6m 50s	1/3	CRITICAL - 212.214.0.193 (loss=100.00%)
gbg-temp1	PING	CRITICAL	2004-06-01 16:43:11	32d 6h 5m 52s	1/3	CRITICAL - 212.214.0.197 (loss=100.00%)
	Temperature - Gbg Office	CRITICAL	2004-06-01 16:43:10	32d 6h 5m 3s	1/3	Connection refused or timed out
op5-wlan	PING	CRITICAL	2004-06-01 16:40:27	109d 17h 17m 47s	1/3	CRITICAL - 172.27.76.5 (loss=100.00%)

4 Matching Service Entries Displayed

All the host that have problems are listed. The list can be filtered by clicking on the arrows (see host and service details). All problem can be acknowledged. The problem will be associated with a pink color in Tactical Overview window. Acknowledged problems are recognized by the working man icon. All host and services can be commented. The comments looks like in the picture above. Detailed information on who is working on the problem, information about the host and services and so on can be stored.

The Display filter table shows if the list is filtered.

Related links are connected to:

History for Hosts (View all event history for hosts)

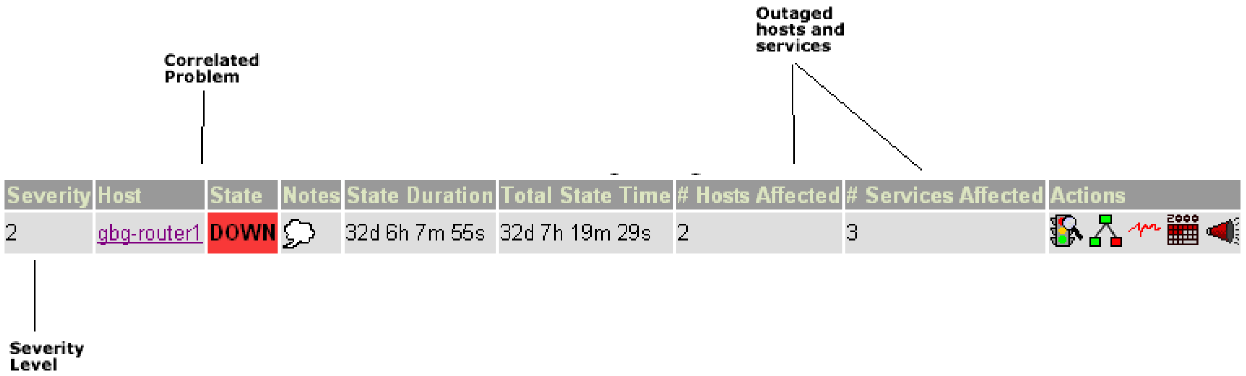
Notifications for Hosts (Shows all previous notifications for hosts)

Status Detail (Status of all hosts and services per host group)

Status Summary shows a summary of all hosts and services in the network divided by state.

Network Outages

By using event correlation Monitor will suppress all host alarms that comes from hosts behind a faulty host. Monitor is preconfigured with knowledge of the physichal structure of the network and creates a notification of which host that is causing the outage. Digging into the problem at a deeper level is left to the user, as there are any number of things which might actually be the cause of the problem.

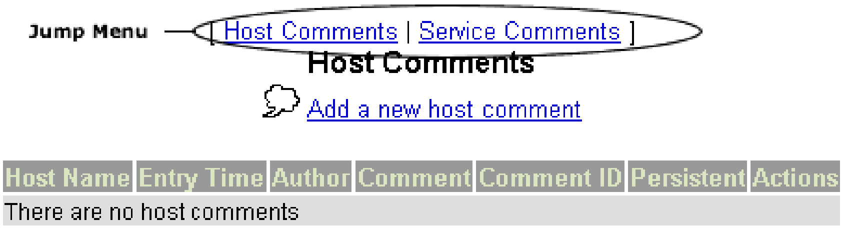


Severity	Host	State	Notes	State Duration	Total State Time	# Hosts Affected	# Services Affected	Actions
2	gbg-router1	DOWN	💬	32d 6h 7m 55s	32d 7h 19m 29s	2	3	

In order to display the problem hosts in a somewhat useful manner, they are sorted by the severity of the effect they are having on the network. The severity level is determined by two things: The number of hosts which are affected by problem host and the number of services which are affected. Hosts hold a higher weight than services when it comes to calculating severity. The current code sets this weight ratio at 4:1 (i.e. hosts are 4 times more important than individual services).

Host and Service Comments

All hosts and Services can have one or more comments related to it. Top of the window display a jump menu. If there is a long list of comments this jump menu will guide you to the services or host comments.

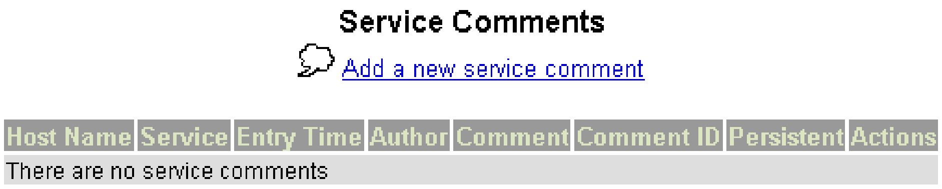


[Host Comments | Service Comments]

Host Comments

Add a new host comment

Host Name	Entry Time	Author	Comment	Comment ID	Persistent	Actions
There are no host comments						



Service Comments

Add a new service comment

Host Name	Service	Entry Time	Author	Comment	Comment ID	Persistent	Actions
There are no service comments							

Host name: Is The host name the comment is related to.

Entry Time: Date and time for the comment entry.

Author: The name of the author of the comment.

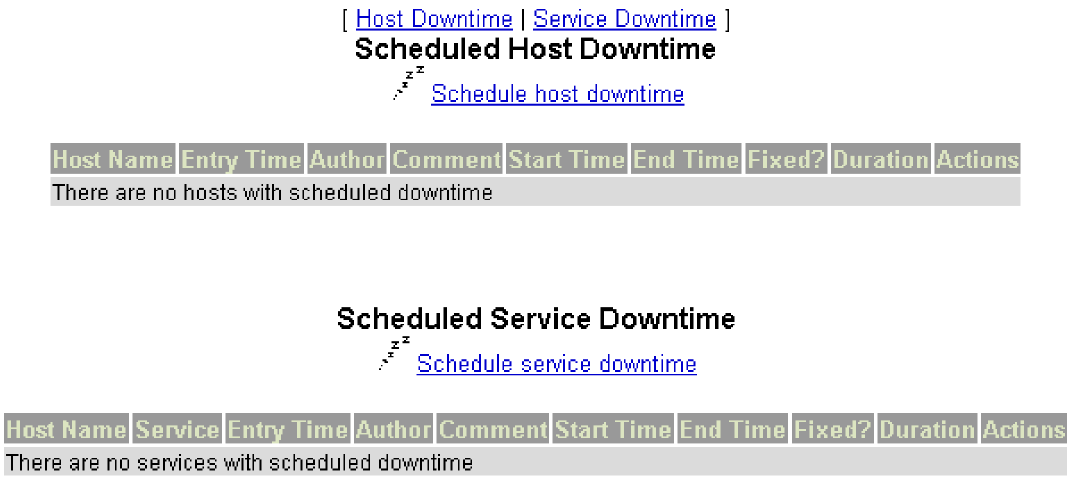
Comment. The comment itself.

Comment ID: A Unique ID number for the comment. Can be used as a reference number.

Persistent: If the comment is persistent or not. Comments that are not persistent will be removed if the OP5 Monitor system is restarted.

Scheduled Downtime

Using scheduled downtime enables you to plan for system work ahead. When a host or service is scheduled for downtime OP5 Monitor suppresses alarms for that host or service. Furthermore Monitor informs you about what host or service is scheduled for downtime through the web interface. Information about the scheduled downtime are also stored in the logs so that planned system work does not affect availability reports.



[Host Downtime | Service Downtime]

Scheduled Host Downtime

Schedule host downtime

Host Name	Entry Time	Author	Comment	Start Time	End Time	Fixed?	Duration	Actions
There are no hosts with scheduled downtime								

Scheduled Service Downtime

Schedule service downtime

Host Name	Service	Entry Time	Author	Comment	Start Time	End Time	Fixed?	Duration	Actions
There are no services with scheduled downtime									

Basically the window consists of a jump menu to Scheduled Host and Service downtime. There is also a link to schedule the downtime itself. One link for hosts (Schedule Host downtime) and one for services (Schedule service downtime)

The rest is a listing of all scheduled downtime.

Host name: Host name which the downtime affects.

Service: Service which the downtime affects.

Entry Time: Time for creation of the scheduled downtime.

Author: The name of the author of the scheduled downtime.

Comment: Comments to the scheduled downtime.

Start time: Start time and date of the scheduled downtime.

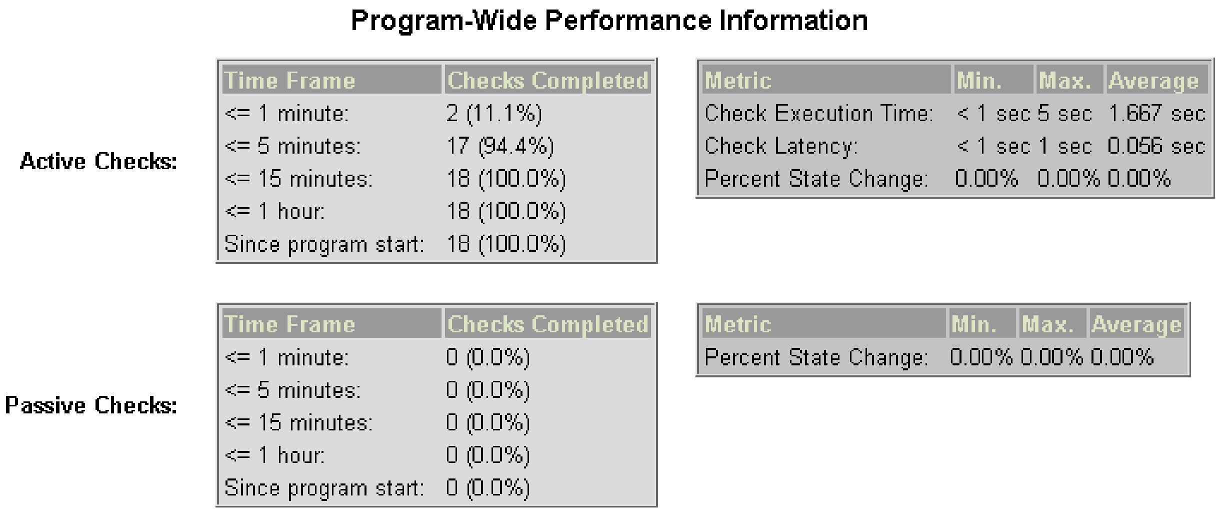
End Time: End time and date for the scheduled downtime.

Fixed?: If the downtime is a fixed entry, it starts at the “Start Time” and ends at the “End Time”. If the schedule isn't fixed then it starts when the host or service goes down and stops when the service goes up (very useful for system restarts)

Duration: Is the duration of the scheduled downtime.

Performance Information

Monitor gives you detailed information about the performance of executed checks.



Program-Wide Performance Information

Active Checks:

Time Frame	Checks Completed
<= 1 minute:	2 (11.1%)
<= 5 minutes:	17 (94.4%)
<= 15 minutes:	18 (100.0%)
<= 1 hour:	18 (100.0%)
Since program start:	18 (100.0%)

Metric	Min.	Max.	Average
Check Execution Time:	< 1 sec	5 sec	1.667 sec
Check Latency:	< 1 sec	1 sec	0.056 sec
Percent State Change:	0.00%	0.00%	0.00%

Passive Checks:

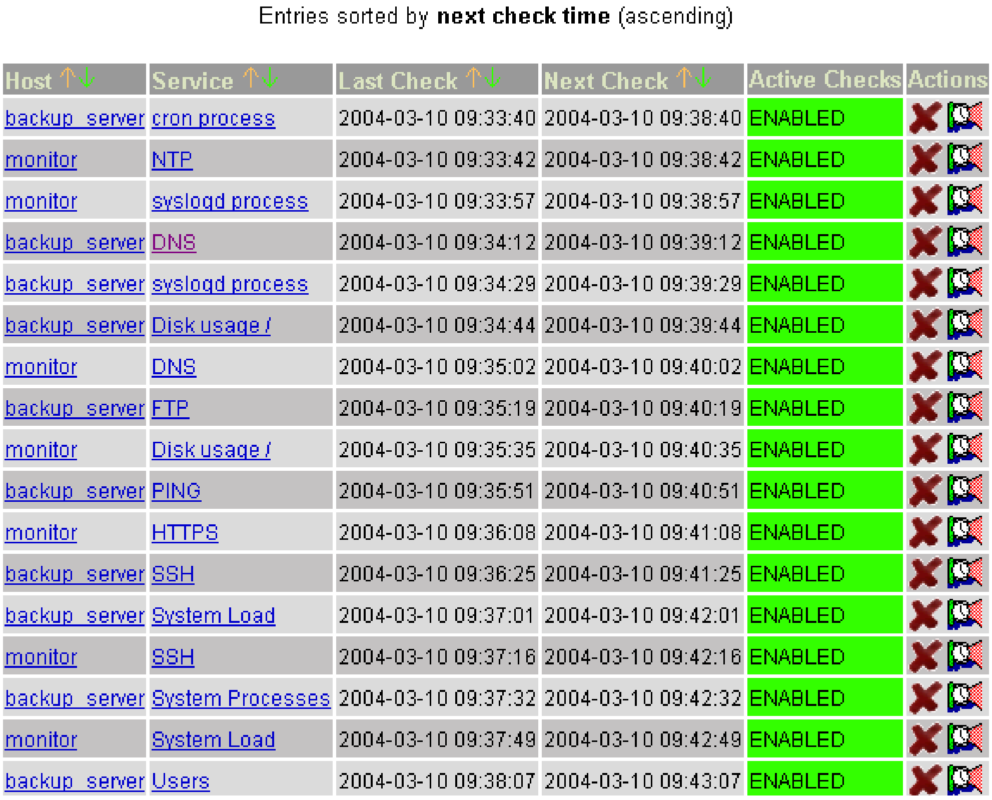
Time Frame	Checks Completed
<= 1 minute:	0 (0.0%)
<= 5 minutes:	0 (0.0%)
<= 15 minutes:	0 (0.0%)
<= 1 hour:	0 (0.0%)
Since program start:	0 (0.0%)

Metric	Min.	Max.	Average
Percent State Change:	0.00%	0.00%	0.00%

The information is divided in Active checks, passive checks and metrics. The performance is showed for checks completed within a certain time frame. 11,1% of all active checks where performed within 1 minute time frame. 94,4% where performed within a 5 minute time frame. 100% where performed within a 15 minute time frame and so on. The Metric is calculated on execution time, latency and state changes. The figures should be read as an interval with an average. Check Execution time had an interval between 1 and 5 seconds and the average was 1,667 seconds.

Scheduling Queue

Scheduling queue is a list of all checks that have been executed and when they are about to be executed.



Entries sorted by **next check time** (ascending)

Host ↑↓	Service ↑↓	Last Check ↑↓	Next Check ↑↓	Active Checks	Actions
backup_server	cron process	2004-03-10 09:33:40	2004-03-10 09:38:40	ENABLED	✗ ⏲
monitor	NTP	2004-03-10 09:33:42	2004-03-10 09:38:42	ENABLED	✗ ⏲
monitor	syslogd process	2004-03-10 09:33:57	2004-03-10 09:38:57	ENABLED	✗ ⏲
backup_server	DNS	2004-03-10 09:34:12	2004-03-10 09:39:12	ENABLED	✗ ⏲
backup_server	syslogd process	2004-03-10 09:34:29	2004-03-10 09:39:29	ENABLED	✗ ⏲
backup_server	Disk usage /	2004-03-10 09:34:44	2004-03-10 09:39:44	ENABLED	✗ ⏲
monitor	DNS	2004-03-10 09:35:02	2004-03-10 09:40:02	ENABLED	✗ ⏲
backup_server	FTP	2004-03-10 09:35:19	2004-03-10 09:40:19	ENABLED	✗ ⏲
monitor	Disk usage /	2004-03-10 09:35:35	2004-03-10 09:40:35	ENABLED	✗ ⏲
backup_server	PING	2004-03-10 09:35:51	2004-03-10 09:40:51	ENABLED	✗ ⏲
monitor	HTTPS	2004-03-10 09:36:08	2004-03-10 09:41:08	ENABLED	✗ ⏲
backup_server	SSH	2004-03-10 09:36:25	2004-03-10 09:41:25	ENABLED	✗ ⏲
backup_server	System Load	2004-03-10 09:37:01	2004-03-10 09:42:01	ENABLED	✗ ⏲
monitor	SSH	2004-03-10 09:37:16	2004-03-10 09:42:16	ENABLED	✗ ⏲
backup_server	System Processes	2004-03-10 09:37:32	2004-03-10 09:42:32	ENABLED	✗ ⏲
monitor	System Load	2004-03-10 09:37:49	2004-03-10 09:42:49	ENABLED	✗ ⏲
backup_server	Users	2004-03-10 09:38:07	2004-03-10 09:43:07	ENABLED	✗ ⏲

The list can be sorted as with the host and service detail by clicking the arrows next to the name host, service, last check or next check. The list will be sorted in ascending or descending order.

Host: The host name for which the check is to be executed.

Service: The Service name for which the check is to be executed.

Last Check: When the check was last performed.

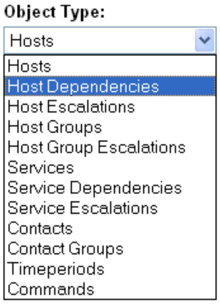
Next Check: When the next check will be performed.

Active Checks: If active checks is enabled or disabled.

Actions: The clock links you to specify a new time for check execution. The X disables an active check for that service and host.

View Configuration

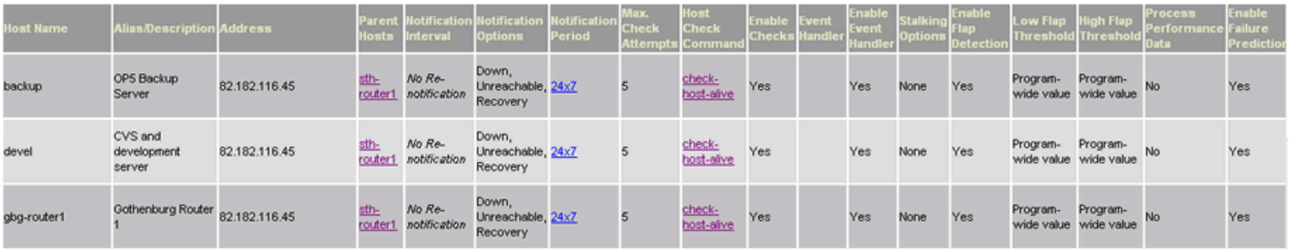
The View Configuration menu option enables you to view all your configuration. You can choose from viewing the configuration for; Hosts, Host Dependencies, Host Escalations, Host Groups, Host Group Escalations, Services, Service Dependencies, Service Escalations, Contacts, Contact Groups, Time periods and Commands.



Hosts

The view configuration selection for hosts basically gives you the configuration information about:

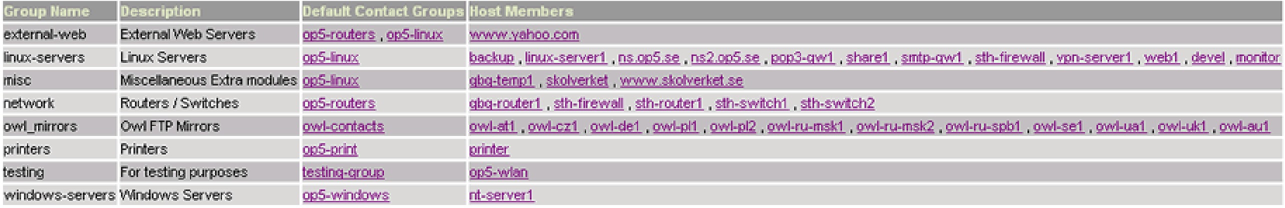
- Host name,
- Alias (Descriptive name of host),
- IP Address, Parent host (The host that this host is related or connected to),
- Notification Interval (The interval between the notifications sent to a contact),
- Notification Options (What type of state changes that will be notified),
- Notification Period (The timescope within notifications are sent),
- Max Check Attempts (The number of checks that will be performed before the state changes from soft to hard),
- Host Check Command (The macro that will be executed to perform the check),
- Enable Checks (If checks are enabled or not),
- Enable Event Handler (If event handlers shall be used or not),
- Stalking Options (log the results of the host/service check if the output from the check differs from the output from the previous check),
- Enable Flap Detection (If a host or service is pending between to states, i.e flapping, Monitor will suppress the alarm saying it is a flap detection. This option is either enabled or disabled).
- Low and High Flap Threshold (Threshold for Flap Detection to react to), Process Performance Data, Failure Prediction.
- Process Performance Data
- Failure Prediction



Host Name	Alias/Description	Address	Parent Hosts	Notification Interval	Notification Options	Notification Period	Max. Check Attempts	Host Check Command	Enable Checks	Event Handler	Enable Event Handler	Stalking Options	Enable Flap Detection	Low Flap Threshold	High Flap Threshold	Process Performance Data	Enable Failure Prediction
backup	OP5 Backup Server	82.182.116.45	sth-router1	*No Re-notification*	Down, Unreachable, Recovery	24x7	5	check-host-alive	Yes		Yes	None	Yes	Program-wide value	Program-wide value	No	Yes
devel	CVS and development server	82.182.116.45	sth-router1	*No Re-notification*	Down, Unreachable, Recovery	24x7	5	check-host-alive	Yes		Yes	None	Yes	Program-wide value	Program-wide value	No	Yes
gbg-router1	Gothenburg Router 1	82.182.116.45	sth-router1	*No Re-notification*	Down, Unreachable, Recovery	24x7	5	check-host-alive	Yes		Yes	None	Yes	Program-wide value	Program-wide value	No	Yes

Hostgroups

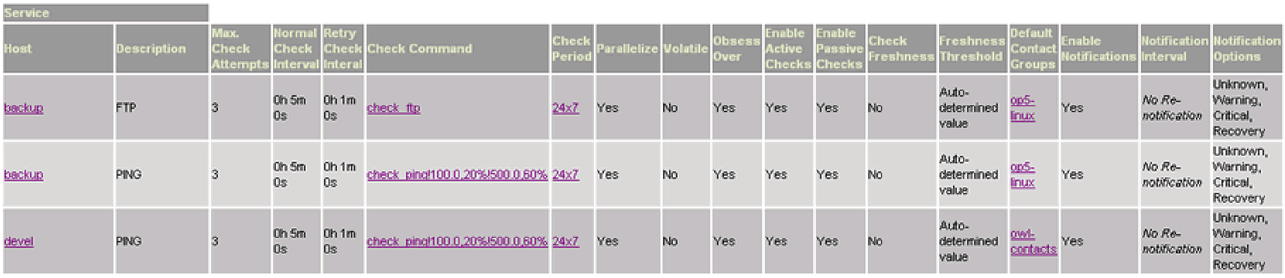
The View Configuration selection for host groups shows you the relations between the contact group and the hosts.



Group Name	Description	Default Contact Groups	Host Members
external-web	External Web Servers	op5-routers , op5-linux	www.yahoo.com
linux-servers	Linux Servers	op5-linux	backup , linux-server1 , ns.op5.se , ns2.op5.se , pop3-gw1 , share1 , smtp-gw1 , sth-firewall , vpn-server1 , web1 , devel , monitor
misc	Miscellaneous Extra modules	op5-linux	gbg-temp1 , skolverket , www.skolverket.se
network	Routers / Switches	op5-routers	gbg-router1 , sth-firewall , sth-router1 , sth-switch1 , sth-switch2
owl_mirrors	Owl FTP Mirrors	owl-contacts	owl-at1 , owl-cz1 , owl-de1 , owl-pl1 , owl-pl2 , owl-ru-msk1 , owl-ru-msk2 , owl-ru-spb1 , owl-se1 , owl-ua1 , owl-uk1 , owl-au1
printers	Printers	op5-print	printer
testing	For testing purposes	testing-group	op5-wlan
windows-servers	Windows Servers	op5-windows	nt-server1

Services

The view configuration selection for services shows you the details about services.



Service

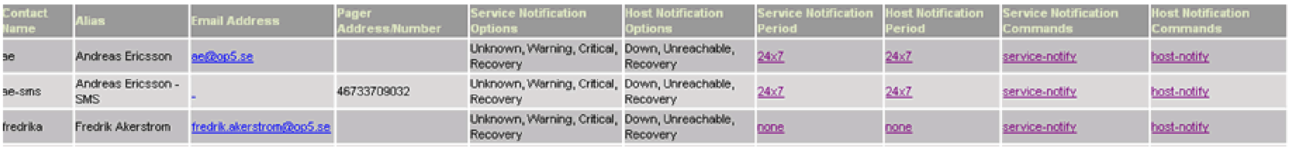
Host	Description	Max. Check Attempts	Normal Check Interval	Retry Check Interal	Check Command	Check Period	Parallelize	Volatile	Obsess Over	Enable Active Checks	Enable Passive Checks	Check Freshness	Freshness Threshold	Default Contact Groups	Enable Notifications	Notification Interval	Notification Options
backup	FTP	3	0h 5m 0s	0h 1m 0s	check_ftp	24x7	Yes	No	Yes	Yes	Yes	No	Auto-determined value	op5-linux	Yes	*No Re-notification*	Unknown, Warning, Critical, Recovery
backup	PING	3	0h 5m 0s	0h 1m 0s	check_ping!100.0,20%!500.0,60%	24x7	Yes	No	Yes	Yes	Yes	No	Auto-determined value	op5-linux	Yes	*No Re-notification*	Unknown, Warning, Critical, Recovery
devel	PING	3	0h 5m 0s	0h 1m 0s	check_ping!100.0,20%!500.0,60%	24x7	Yes	No	Yes	Yes	Yes	No	Auto-determined value	owl-contacts	Yes	*No Re-notification*	Unknown, Warning, Critical, Recovery

- Host (Name of the Host)
- Description (Name of the Service)
- Max Check Attempts (Number of Attempts before changing states from soft to hard)
- Normal Check Interval (Interval between checks when everything is normal, i.e no state change)
- Retry Check Interval (Interval between checks when not in normal environment, i.e state change)
- Check Command (the macro to execute to perform the check)
- Check Period (The time period for the check to be executed)
- Parallelized (Either yes or no depending on if the check can be executed in parallel with other checks, normally this is yes for performance reasons)
- Volatile (Either yes or no, hosts which services automatically reset themselves to an "OK" state each time they are checked)

- Obsess over (When in the server sits in a distributed Monitor network, obsess over is used to determine relations between Monitor servers, All checks are reported to a server that obsess another server).
- Enable Active Checks (If checks from the Monitor server are enabled or disabled)
- Enable Passive Checks (If checks performed outside Monitor should be received by Monitor)
- Check Freshness (ensure that passive checks are being received as frequently as you want)
- Freshness Threshold (The threshold in which the Freshness interval should reside)
- Default Contact Group (Contact group related to service)
- Enable Notifications (If notifications going out to a contact is enabled or not)
- Notification Interval (The interval between the notifications going out to a contact)
- Notification Options (Which state changes that will cause a notification to be sent)

Contacts

The view configuration selection for contacts lets you view the relation between contacts, email and SMS addresses.

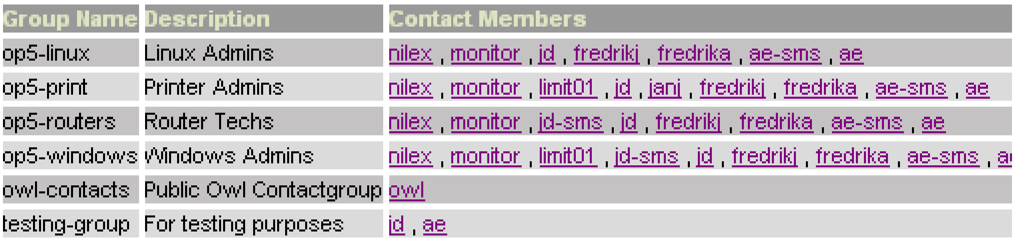


Contact Name	Alias	Email Address	Pager Address/Number	Service Notification Options	Host Notification Options	Service Notification Period	Host Notification Period	Service Notification Commands	Host Notification Commands
ae	Andreas Ericsson	ae@op5.se		Unknown, Warning, Critical, Recovery	Down, Unreachable, Recovery	24x7	24x7	service-notify	host-notify
ae-sms	Andreas Ericsson - SMS	-	46733709032	Unknown, Warning, Critical, Recovery	Down, Unreachable, Recovery	24x7	24x7	service-notify	host-notify
fredrika	Fredrik Akerstrom	fredrik.akerstrom@op5.se		Unknown, Warning, Critical, Recovery	Down, Unreachable, Recovery	none	none	service-notify	host-notify

- Contact Name (Short name of contact)
- Alias (Full name of contact)
- Email Address
- Pager Address number (Cell phone number)
- Service Notification Options (Which state changes of services that shall be notified)
- Host Notification Options (Which state changes of Hosts that shall be notified)
- Service Notification Period (The time period for the contacts to be notified when services change state)
- Host Notification Period (The time period for the contacts to be notified when hosts change state)
- Service Notification Commands (The macro that will be executed when a service change state to send a notification)
- Host Notification Commands (The macro that will be executed when a host change state to send a notification)

Contact groups

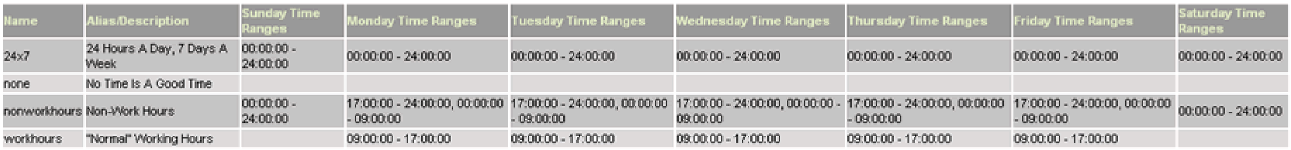
Information regarding which contact groups the contacts belongs to.



Group Name	Description	Contact Members
op5-linux	Linux Admins	nilex , monitor , jd , fredrikj , fredrika , ae-sms , ae
op5-print	Printer Admins	nilex , monitor , limit01 , jd , janj , fredrikj , fredrika , ae-sms , ae
op5-routers	Router Techs	nilex , monitor , jd-sms , jd , fredrikj , fredrika , ae-sms , ae
op5-windows	Windows Admins	nilex , monitor , limit01 , jd-sms , jd , fredrikj , fredrika , ae-sms , a
owl-contacts	Public Owl Contactgroup	owl
testing-group	For testing purposes	jd , ae

Time Periods

Information of time period configuration. Time periods are used to specify when to do things, for example execute service checks or send notifications.



Name	Alias/Description	Sunday Time Ranges	Monday Time Ranges	Tuesday Time Ranges	Wednesday Time Ranges	Thursday Time Ranges	Friday Time Ranges	Saturday Time Ranges
24x7	24 Hours A Day, 7 Days A Week	00:00:00 - 24:00:00	00:00:00 - 24:00:00	00:00:00 - 24:00:00	00:00:00 - 24:00:00	00:00:00 - 24:00:00	00:00:00 - 24:00:00	00:00:00 - 24:00:00
none	No Time Is A Good Time							
nonworkhours	Non-Work Hours	00:00:00 - 24:00:00	17:00:00 - 24:00:00, 00:00:00 - 09:00:00	17:00:00 - 24:00:00, 00:00:00 - 09:00:00	17:00:00 - 24:00:00, 00:00:00 - 09:00:00	17:00:00 - 24:00:00, 00:00:00 - 09:00:00	17:00:00 - 24:00:00, 00:00:00 - 09:00:00	00:00:00 - 24:00:00
workhours	"Normal" Working Hours		09:00:00 - 17:00:00	09:00:00 - 17:00:00	09:00:00 - 17:00:00	09:00:00 - 17:00:00	09:00:00 - 17:00:00	

Commands (Plug ins)

A list of the macros for the plug ins that are executed when a check is performed.

check-host-alive	$USER2$/check_fping -H $HOSTADDRESS$ -w 5000,100% -c 5000,100% -n 1
check-host-alive-http	$USER2$/check_tcp -H $HOSTADDRESS$ -p 80 -w 4 -c 5 -t 6
check-host-alive-icmp	$USER2$/check_fping -H $HOSTADDRESS$ -w 5000,80% -c 5000,100% -n 1
check-host-alive-telnet	$USER2$/check_tcp -H $HOSTADDRESS$ -p 23 -w 4 -c 5 -t 6
check_citrix	$USER1$/check_citrix -C $HOSTADDRESS$ -P "$ARG1$"
check_dig	$USER1$/check_dig -H $HOSTADDRESS$ -l $ARG2$
check_dns	$USER1$/check_dns -H $ARG1$ -s $HOSTADDRESS$ -a $ARG2$
check_ftp	$USER1$/check_ftp -H $HOSTADDRESS$
check_hpjd	$USER1$/check_hpjd -H $HOSTADDRESS$ -C $ARG1$
check_hpjd_public	$USER1$/check_hpjd -H $HOSTADDRESS$ -C public
check_http	$USER1$/check_http -H $HOSTADDRESS$
check_http_auth	$USER1$/check_http -H $HOSTADDRESS$ -a $ARG1$:$ARG2$
check_http_auth_url	$USER1$/check_http -H $HOSTADDRESS$ -a $ARG1$:$ARG2$ -u $ARG3$
check_http_port	$USER1$/check_http -H $HOSTADDRESS$ -p $ARG1$
check_http_port_url	$USER1$/check_http -H $HOSTADDRESS$ -p $ARG1$ -u $ARG2$
check_http_url	$USER1$/check_http -H $HOSTADDRESS$ -u $ARG1$ -s $ARG2$
check_http_url_regex	$USER1$/check_http -H $HOSTADDRESS$ -u $ARG1$ -r $ARG2$
check_http_url_string	$USER1$/check_http -H $HOSTADDRESS$ -u $ARG1$ -s $ARG2$
check_http_vhost	$USER1$/check_http -H $ARG1$

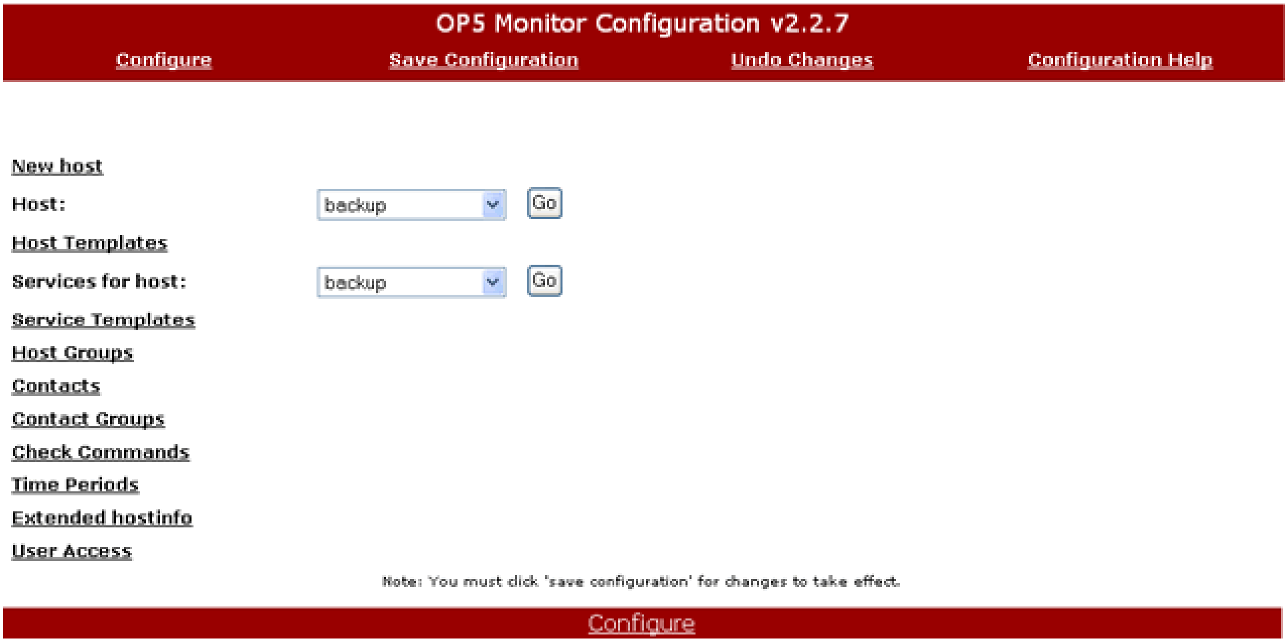
check_http_vhost_port_url	$USER1$/check_http -I $HOSTADDRESS$ -H $ARG1$ -p $ARG2$ -u $ARG3$
check_https	$USER1$/check_http -H $HOSTADDRESS$ -S
check_https_auth	$USER1$/check_http -H $HOSTADDRESS$ -a $ARG1$:$ARG2$ -S
check_https_auth_url	$USER1$/check_http -H $HOSTADDRESS$ -a $ARG1$:$ARG2$ -S -u $ARG3$
check_https_port	$USER1$/check_http -H $HOSTADDRESS$ -p $ARG1$ -S
check_https_port_url	$USER1$/check_http -H $HOSTADDRESS$ -p $ARG1$ -u $ARG2$ -S
check_https_url	$USER1$/check_http -H $HOSTADDRESS$ -u $ARG1$ -s $ARG2$ -S
check_https_url_regex	$USER1$/check_http -H $HOSTADDRESS$ -u $ARG1$ -r $ARG2$ -S
check_https_url_string	$USER1$/check_http -H $HOSTADDRESS$ -u $ARG1$ -s $ARG2$ -S
check_https_vhost	$USER1$/check_http -H $ARG1$ -S
check_ifoperstatus	$USER1$/check_ifoperstatus -H $HOSTADDRESS$ -C $ARG1$ -v 1 -k $ARG2$
check_imap	$USER1$/check_imap -H $HOSTADDRESS$
check_imap3	$USER1$/check_tcp -H $HOSTADDRESS$ -p 220
check_imaps	$USER1$/check_tcp -H $HOSTADDRESS$ -p 993
check_log	$USER1$/check_log2.pl -l $ARG1$ -s /opt/monitor/var/$ARG2$ -p $HOSTADDRESS$
check_mysql	$USER1$/check_mysql -H $HOSTADDRESS$ -u $ARG1$ -p $ARG2$
check_nntp	$USER1$/check_nntp -H $HOSTADDRESS$
check_nrpe	$USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$
check_nrpe_disk_root	$USER1$/check_nrpe -H $HOSTADDRESS$ -c check_disk_root
check_nrpe_disk_var	$USER1$/check_nrpe -H $HOSTADDRESS$ -c check_disk_var
check_nrpe_load	$USER1$/check_nrpe -H $HOSTADDRESS$ -c check_load
check_nrpe_proc_crond	$USER1$/check_nrpe -H $HOSTADDRESS$ -c check_proc_crond
check_nrpe_proc_named	$USER1$/check_nrpe -H $HOSTADDRESS$ -c check_proc_named
check_nrpe_proc_syslogd	$USER1$/check_nrpe -H $HOSTADDRESS$ -c check_proc_syslogd
check_nrpe_proc_total	$USER1$/check_nrpe -H $HOSTADDRESS$ -c check_proc_total
check_nrpe_proc_zombie	$USER1$/check_nrpe -H $HOSTADDRESS$ -c check_proc_zombie
check_nrpe_swap	$USER1$/check_nrpe -H $HOSTADDRESS$ -c check_swap
check_nrpe_users	$USER1$/check_nrpe -H $HOSTADDRESS$ -c check_users
check_nt_clientversion	$USER1$/check_nt -H $HOSTADDRESS$ -p 1248 -v CLIENTVERSION
check_nt_cpuload	$USER1$/check_nt -H $HOSTADDRESS$ -p 1248 -v CPULOAD -l$ARG1$
check_nt_disk	$USER1$/check_nt -H $HOSTADDRESS$ -p 1248 -v USEDDISKSPACE -l $ARG1$ -w $ARG2$ -c $ARG3$
check_nt_memuse	$USER1$/check_nt -H $HOSTADDRESS$ -p 1248 -v MEMUSE -w $ARG1$ -c $ARG2$

check_nt_pagingfile	$USER1$/check_nt -H $HOSTADDRESS$ -p 1248 -v COUNTER -l "\\Paging File(_Total)\\% Usage","Paging File usage is %.2f %%" -w $ARG1$ -c $ARG2$
check_nt_process	$USER1$/check_nt -H $HOSTADDRESS$ -p 1248 -v PROCSTATE -l $ARG1$
check_nt_service	$USER1$/check_nt -H $HOSTADDRESS$ -p 1248 -v SERVICESTATE -l $ARG1$
check_nt_uptime	$USER1$/check_nt -H $HOSTADDRESS$ -p 1248 -v UPTIME
check_ntp	$USER1$/check_ntp -H $HOSTADDRESS$ -w 60 -c 120 -j 5000 -k 10000
check_nwstat	$USER1$/check_nwstat -H $HOSTADDRESS$ -v $ARG1$ -w $ARG2$ -c $ARG4$
check_nwstat_conns	$USER1$/check_nwstat -H $HOSTADDRESS$ -v CONNS -w $ARG1$ -c $ARG2$
check_nwstat_load1	$USER1$/check_nwstat -H $HOSTADDRESS$ -v LOAD1 -w $ARG1$ -c $ARG2$
check_nwstat_load15	$USER1$/check_nwstat -H $HOSTADDRESS$ -v LOAD15 -w $ARG1$ -c $ARG2$
check_nwstat_load5	$USER1$/check_nwstat -H $HOSTADDRESS$ -v LOAD5 -w $ARG1$ -c $ARG2$
check_nwstat_uprb	$USER1$/check_nwstat -H $HOSTADDRESS$ -v UPRB -w $ARG1$ -c $ARG2$
check_ping	$USER2$/check_fping -H $HOSTADDRESS$ -w $ARG1$ -c $ARG2$ -n 5
check_ping_critical	$USER2$/check_fping -H $HOSTADDRESS$ -w 20,20% -c 100,60% -n 5
check_ping_normal	$USER2$/check_fping -H $HOSTADDRESS$ -w 100,20% -c 500,60% -n 5
check_pop	$USER1$/check_pop -H $HOSTADDRESS$
check_smtp	$USER1$/check_smtp -H $HOSTADDRESS$
check_snmp	$USER1$/check_snmp -H $HOSTADDRESS$ -P 1 -o $ARG1$ -w $ARG2$ -c $ARG3$ -C$ARG4$ -m :
check_snmp_cisco_cpu	$USER1$/check_snmp -H $HOSTADDRESS$ -P 1 -o .1.3.6.1.4.1.9.2.1.58.0 -w $ARG1$ -c $ARG2$ -C$ARG3$ -u % -l "CPU load is" -m :
check_snmp_cisco_mem	$USER1$/check_snmp -H $HOSTADDRESS$ -P 1 -o .1.3.6.1.4.1.9.9.48.1.1.1.5.1 -w $ARG1$ -c $ARG2$ -C$ARG3$ -u b -l "Memory usage is" -m :
check_snmp_ups_batterysec	$USER1$/check_snmp -H $HOSTADDRESS$ -o .1.3.6.1.2.1.33.1.2.2.0 -C $ARG1$ -u sec -P 1 -l "Second on Battery is" --string="INTEGER: 0" -m :
check_snmp_ups_batterystatus	$USER1$/check_snmp -H $HOSTADDRESS$ -o .1.3.6.1.2.1.33.1.2.1.0 -C $ARG1$ -P 1 -l "Battery Status is" --string="INTEGER: 2" -m :
check_snmp_ups_minremain	$USER1$/check_snmp -H $HOSTADDRESS$ -o .1.3.6.1.2.1.33.1.2.3.0 -w $ARG1$ -c $ARG2$ -C $ARG3$ -u min -P 1 -l "Minutes Remaining is" -m :
check_snmp_ups_percentload	$USER1$/check_snmp -H $HOSTADDRESS$ -o .1.3.6.1.2.1.33.1.4.4.1.5.1 -w $ARG1$ -c $ARG2$ -C $ARG3$ -u % -P 1 -l "UPS Load is" -m :
check_snmp_ups_temp	$USER1$/check_snmp -H $HOSTADDRESS$ -o .1.3.6.1.2.1.33.1.2.7.0 -w $ARG1$ -c $ARG2$ -C $ARG3$ -u c -P 1 -l "Battery Temp is" -m :
check_ssh	$USER1$/check_ssh -t $ARG1$ $HOSTADDRESS$
check_ssh_10	$USER1$/check_ssh -t 10 $HOSTADDRESS$
check_ssh_5	$USER1$/check_ssh -t 5 $HOSTADDRESS$
check_tcp	$USER1$/check_tcp -H $HOSTADDRESS$ -p $ARG1$
check_telnet	$USER1$/check_tcp -H $HOSTADDRESS$ -p 23
check_temptracker_e	$USER1$/check_temptraxe --celsius -H $HOSTADDRESS$ -w $ARG1$ -c $ARG2$

check_traffic	$USER1$/check_traffic -H $HOSTADDRESS$ -C $ARG1$ -i $ARG2$ -b $ARG3$ -w $ARG4$ -c $ARG5$
check_udp	$USER1$/check_udp -H $HOSTADDRESS$ -p $ARG1$
host-notify	$USER3$/notify/notify.sh "$CONTACTNAME$" "$CONTACTEMAIL$" "$CONTACTPAGER$" "$host name$" "$HOSTALIAS$" "$HOSTADDRESS$" "$HOSTSTATE$" "$OUTPUT$" "$EXECUTIONTIME$" "$DATE$" "$TIME$" "$NOTIFICATIONTYPE$" "$NOTIFICATIONNUMBER$"
service-notify	$USER3$/notify/notify.sh "$CONTACTNAME$" "$CONTACTEMAIL$" "$CONTACTPAGER$" "$host name$" "$HOSTALIAS$" "$HOSTADDRESS$" "$HOSTSTATE$" "$OUTPUT$" "$EXECUTIONTIME$" "$DATE$" "$TIME$" "$NOTIFICATIONTYPE$" "$NOTIFICATIONNUMBER$" "$SERVICEDESC$" "$SERVICESTATE$" "$LATENCY$"

Configure

Configure is a module within Monitor to configure what the system shall monitor.



Host: backup

Services for host: backup

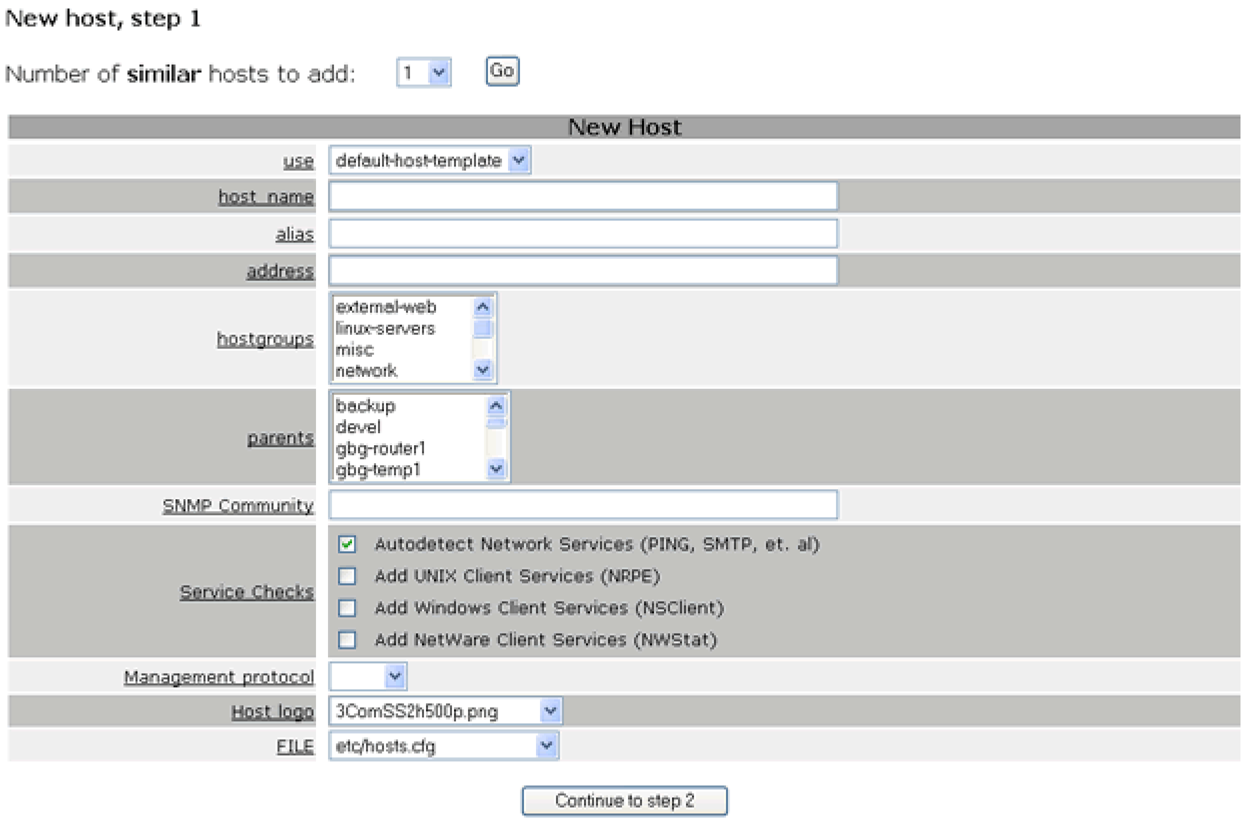
Note: You must click 'save configuration' for changes to take effect.

The main menu consists of four menu selections:

- Configure (returns to the configure start page listed above)
- Save Configuration (Verifies the configuration made, saves the configuration and reloads the monitor process with the new configuration)
- Undo Changes (Goes back to the configuration you had before doing changes)
- Configuration Help (Help window)

Add a host

To add a host, click the 'New host' link. A new window appears that allows you to enter the data needed to add the host. By choosing 'number of similar host to add'wou'll have the possibility to add more than one host at the same time.



New host, step 1

Number of **similar** hosts to add: 1 Go

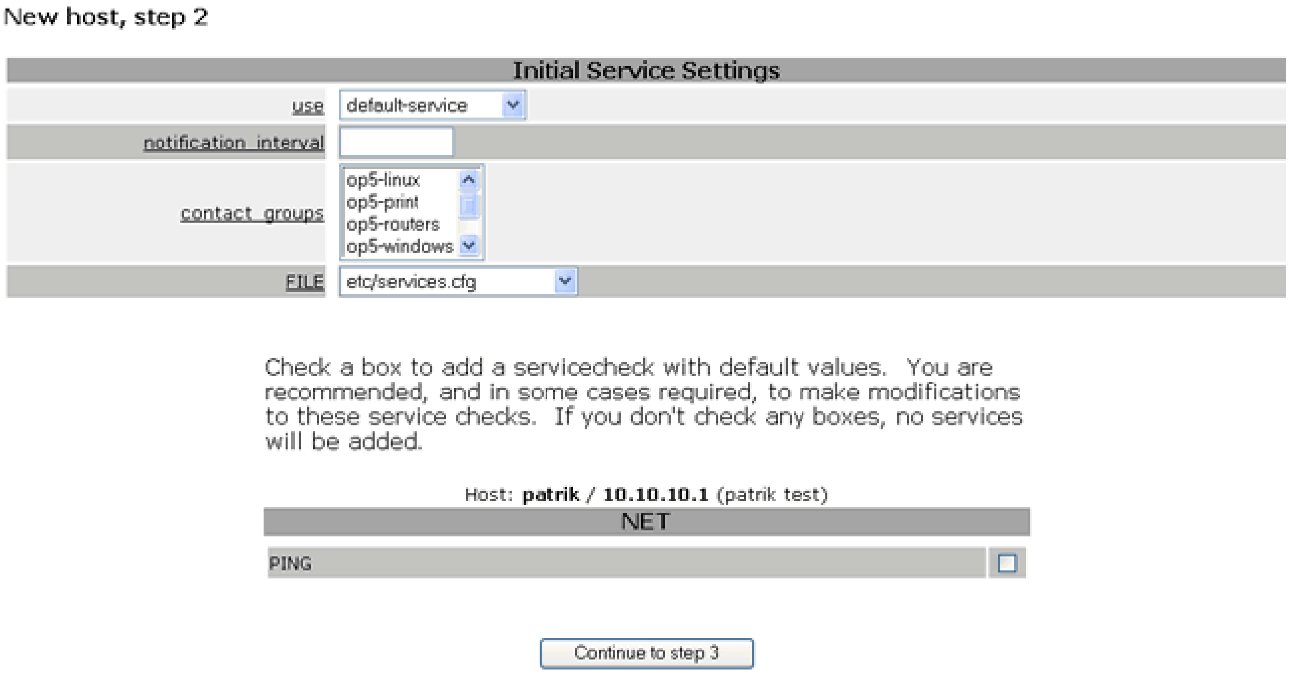
	New Host
use	default-host-template
host_name	
alias	
address	
hostgroups	external-web linux-servers misc network
parents	backup devel gbg-router1 gbg-temp1
SNMP Community	
Service Checks	☑ Autodetect Network Services (PING, SMTP, et. al) ☐ Add UNIX Client Services (NRPE) ☐ Add Windows Client Services (NSClient) ☐ Add NetWare Client Services (NWStat)
Management protocol	
Host logo	3ComSS2h500p.png
FILE	etc/hosts.cfg

Continue to step 2

The required fields to enter data in are: host name, alias, address, host groups and parents. If you fail to add information in this fields the configuration of the new host will fail. You can click on the names of the fields and get a detailed description of the field itself.

- Use (Specifies the template to use for this host. Many values are similar for each host, therefore the use of templates. Templates can be configured from the start page)
- host_name (The name of the host that you want to add)
- Alias (Full description of the host)
- Address (The IP address or host name of the host)
- Host groups (The host groups that the host will be a member of)
- Parents (The parents that this host will is physically connected to, can be one or more)
- SNMP Community (Community name if this host is using SNMP)
- Service Checks (Add the items that Monitor will scan for in the host. By default the Network services is checked. You can also check for clients that have been installed on hosts)
- Management Protocol (Choose the management protocol used to configure the host)
- Host Logo (Associate a logo to the host. This logo will appear in the status map)
- File (the configuration file that this data will be stored in, default is hosts.cfg)

Click the 'Continue to step 2'to continue to add a new host.



New host, step 2

Initial Service Settings

use: default-service

notification_interval:

contact_groups: op5-linux, op5-print, op5-routers, op5-windows

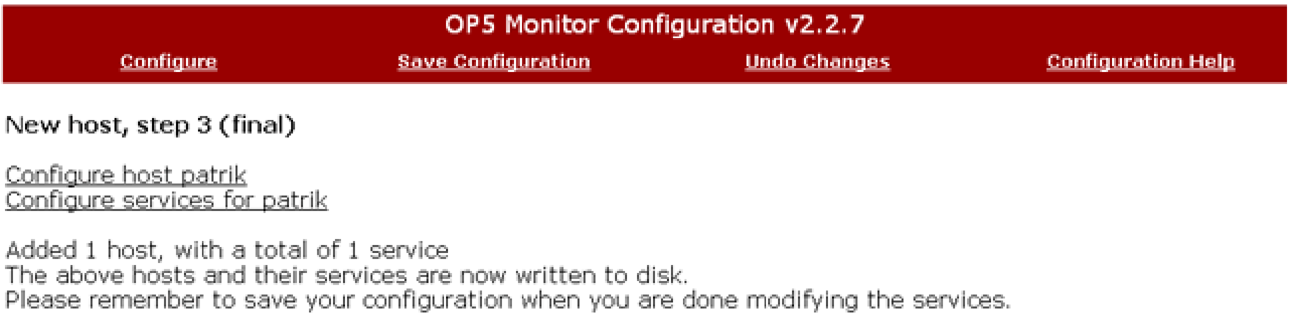
FILE: etc/services.cfg

Check a box to add a servicecheck with default values. You are recommended, and in some cases required, to make modifications to these service checks. If you don't check any boxes, no services will be added.

Host: **patrik** / **10.10.10.1** (patrik test)

NET	
PING	□

The second step window appears and asks you to specify the service template to use. In the bottom of the window all services appears that have been found whilst performing the scan of the host. Check the services you want to add and click 'Continue to step 3'.



New host, step 3 (final)

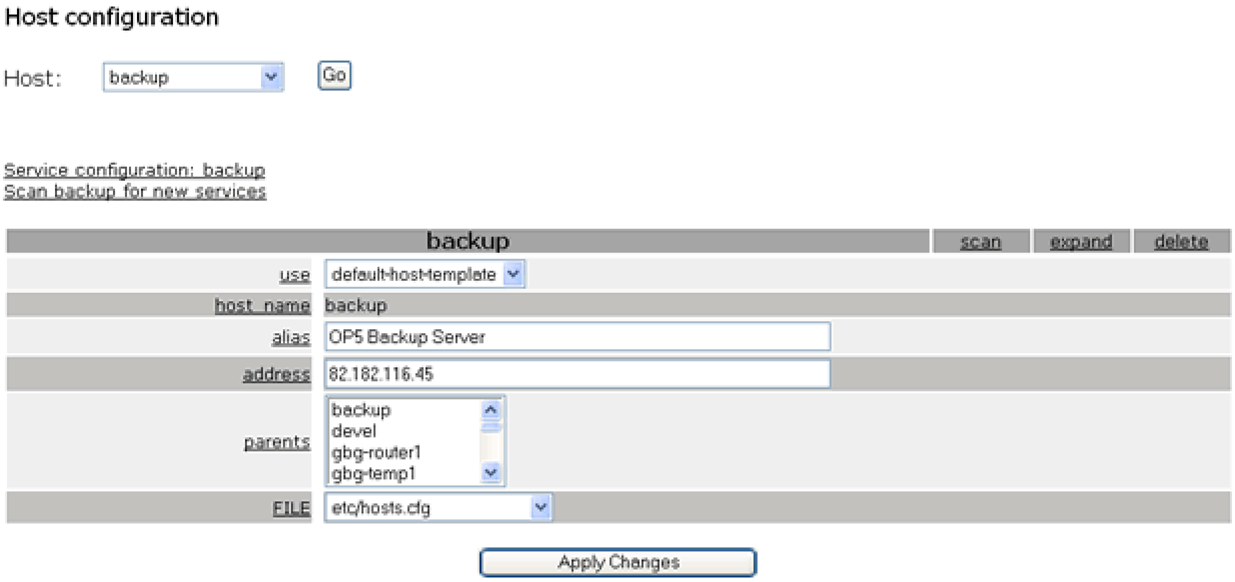
Configure host patrik
Configure services for patrik

Added 1 host, with a total of 1 service
The above hosts and their services are now written to disk.
Please remember to save your configuration when you are done modifying the services.

That's it you now added a new host to Monitor. You now have the options to go back and do configurations on the new host or it's services. If you feel you're done click save configuration. The verification is made , Monitor restarted and voila the new host is up and running. If you encounter problems with the 'Save Configuration' you probably didn't fill out the fields correctly or missed to enter data in the fields. For a complete reference of all field names and their purpose see Appendix A – Field names.

Change or Delete a Host

To change a host choose the start page and to the right of the text 'host choose the host you want to change, click go. A new window appear. In top of the window you can easily choose another host to configure. You also have the possibility to configure the services for this host by clicking 'Service configuration: <host name>'. You can also scan the host for new services by choosing 'Scan <host name> for new services. On the right side of the window there are three links: scan, expand, delete. Scan scans for new services, Expand gives you a window with all the options that can be configured on the host. Delete, deletes the host.



Host configuration

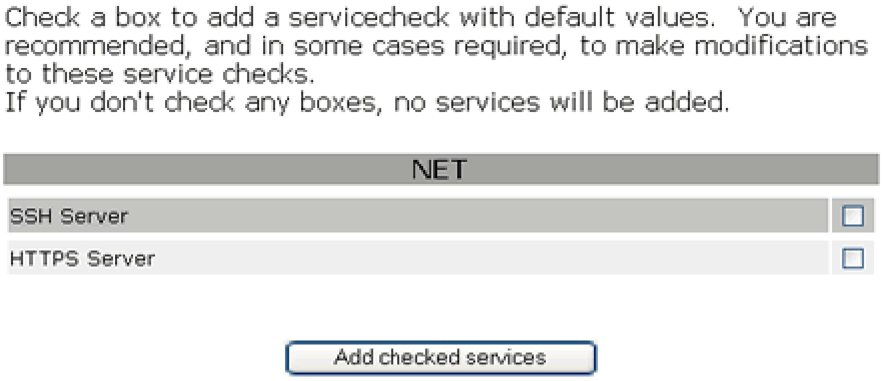
Host: backup Go

Service configuration: backup
Scan backup for new services

backup	scan	expand	delete

use	default-host-template
host_name	backup
alias	OP5 Backup Server
address	82.182.116.45
parents	backup devel gbg-router1 gbg-temp1
FILE	etc/hosts.cfg

Scan Window:

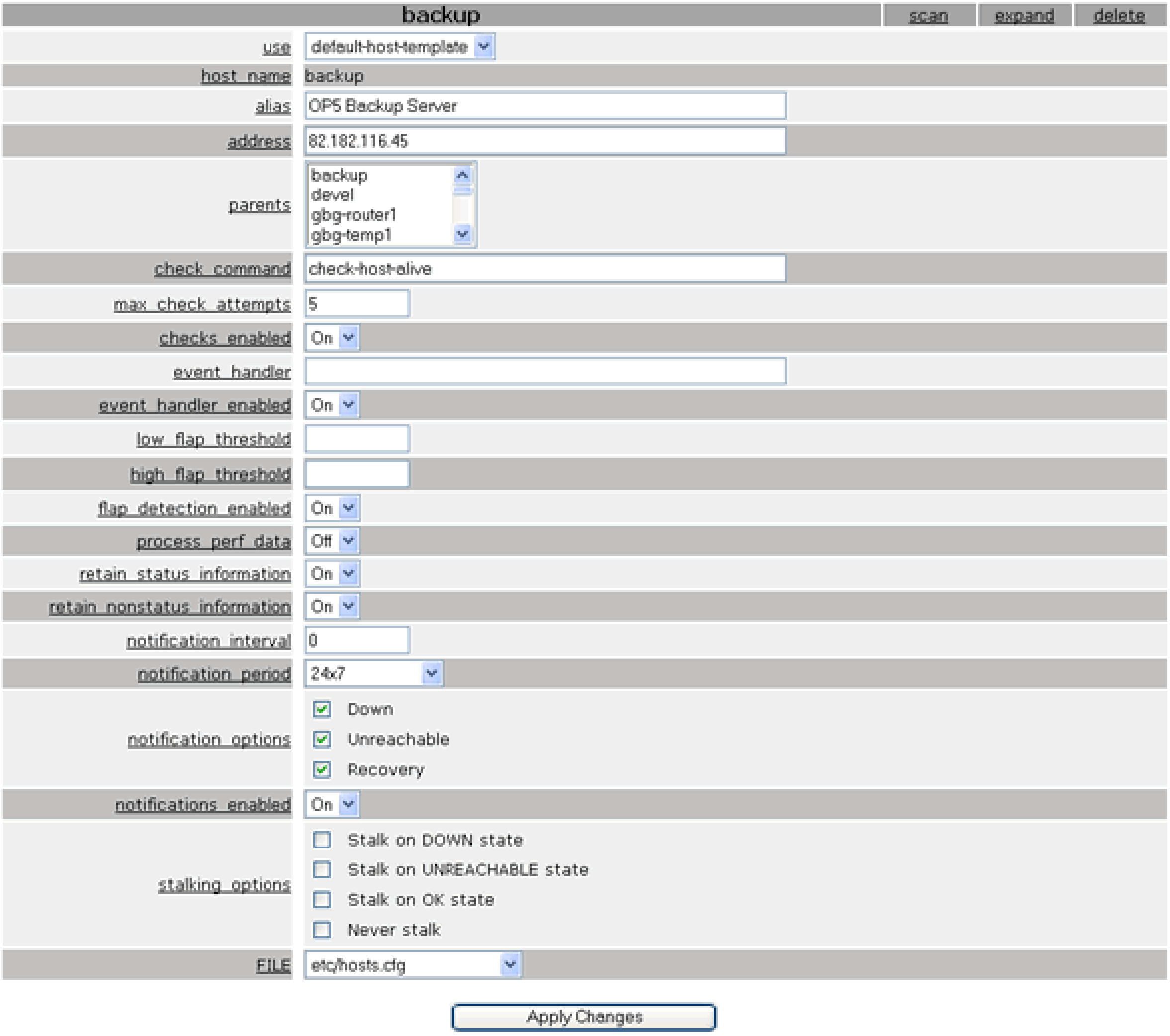


Check a box to add a servicecheck with default values. You are recommended, and in some cases required, to make modifications to these service checks.
If you don't check any boxes, no services will be added.

NET	
SSH Server	□
HTTPS Server	□

To activate changes click 'Apply changes'. Don't forget to save your configuration to get the changes to take effect.

Expanded window:



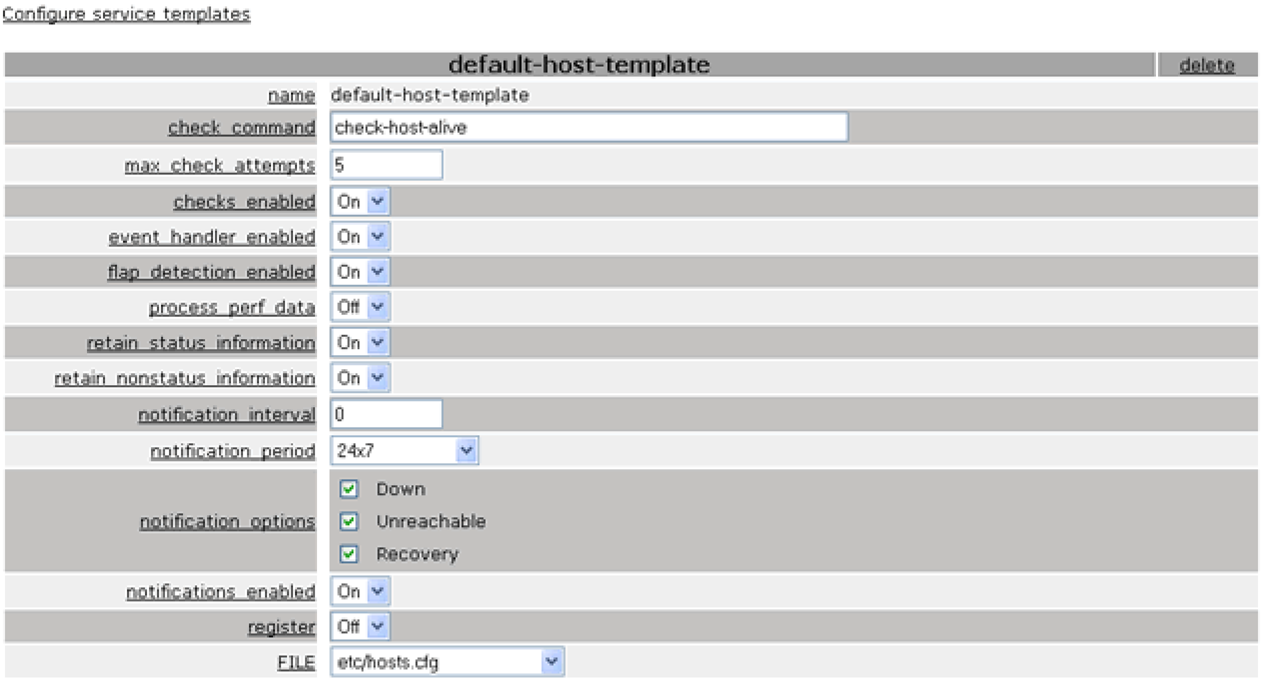
backup

use	default-host-template
host_name	backup
alias	OP5 Backup Server
address	82.182.116.45
parents	backup devel gbg-router1 gbg-temp1
check_command	check-host-alive
max_check_attempts	5
checks_enabled	On
event_handler	
event_handler_enabled	On
low_flap_threshold	
high_flap_threshold	
flap_detection_enabled	On
process_perf_data	Off
retain_status_information	On
retain_nonstatus_information	On
notification_interval	0
notification_period	24x7
notification_options	☑ Down ☑ Unreachable ☑ Recovery
notifications_enabled	On
stalking_options	□ Stalk on DOWN state □ Stalk on UNREACHABLE state □ Stalk on OK state □ Never stalk
FILE	etc/hosts.cfg

For details on the options click on the field name to the left or see the section: View Configuration for Hosts.

Add, Change or Delete Host Templates

Since there are a lot of values that can be set for hosts and a lot of them are similar between hosts templates are used. To change or add a template click on Host template link on the start page. A new window appear:



Configure service templates

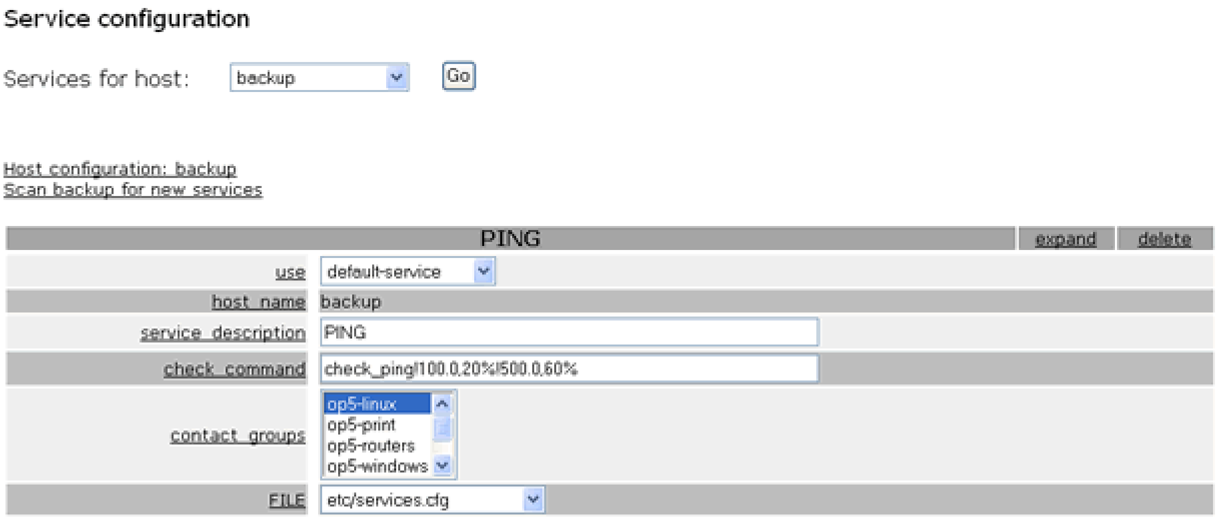
	default-host-template	delete
name	default-host-template	
check command	check-host-alive	
max check attempts	5	
checks enabled	On	
event handler enabled	On	
flap detection enabled	On	
process perf data	Off	
retain status information	On	
retain nonstatus information	On	
notification interval	0	
notification period	24x7	
notification options	☑ Down ☑ Unreachable ☑ Recovery	
notifications enabled	On	
register	Off	
FILE	etc/hosts.cfg	

ON the top left hand side you'll have the option to change or add service templates. On the right hand side you have the option to delete the template. In the bottom there is an ádd template' section. Mostly these values are not touched. If you still need to do changes in the template here are explanations to the fields:

- Name (The name of the template)
- Check Command (The name of the macro to execute as a default check)
- Max Check Attempts (The number of attempts before the host goes from a soft to hard state)
- Checks Enabled (On or Off, enabling of checks)
- Event Handler Enabled (Event handling, i.e possibility to run commands when state changes occures. Event handling is turned on or off)
- Flap Detection Enabled (On or Off, detection and suppression of alarms of hosts that are changing states very often)
- Process Performance Data (Turns extensive performance data performance data, On or Off. Normally this option shall be turned off)
- Retain Status Information (If monitor is restarted the status of a host using this template is assumed to be in the same state as it was before restarting, On or Off)
- Retain Non-Status Information (On or Off, savings of other information than states for the hosts thats using this template, ex. CPU load)
- Notification Interval (The interval in minutes between notifications are sent)
- Notification Period (The time period where notifications are sent)
- Notification Options (State changes where a notification will be sent)
- Notifications Enabled (Turn on or off notifications)
- Register (Off means that it is a template)
- File (File in which the template is stored)

Add, Change or Delete Services

To add change or delete services choose the Services form the start page and the host for which services you want to change, click go. A new window appear:



Service configuration

Services for host: backup

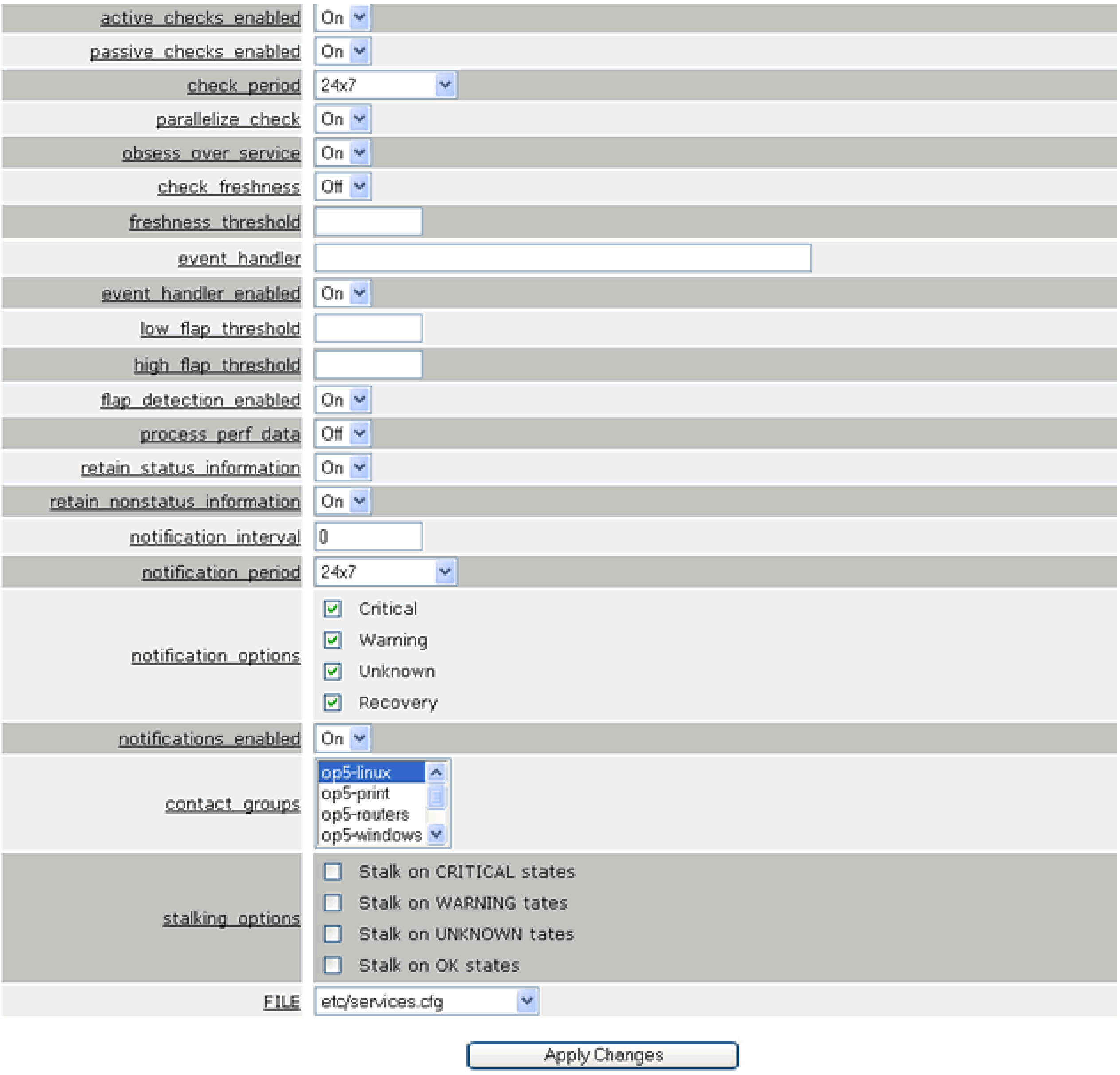
Host configuration: backup
Scan backup for new services

PING	expand	delete
use	default-service	
host_name	backup	
service_description	PING	
check_command	check_ping!100.0,20%!500.0,60%	
contact_groups	op5-linux op5-print op5-routers op5-windows	
FILE	etc/services.cfg	

In top of the window you can choose a quick link to another service to change. On left hand side there is possibility to change the host configuration by clicking 'Host Configuration <Host name>. You can also scan the host for new services by clicking 'Scan <Host name> for new services. On the right hand side you can expand the window, this option shows all configuration that can be made for services on this host. The delete link deletes this service. All services that this host is configured for are listed. In the bottom of the list you have a section to add a new services, even though the best way is to scan a host for new services. Click Apply changes when done configuring. Don't forget to Save Configuration for the changes to take effect.

Expanded window:

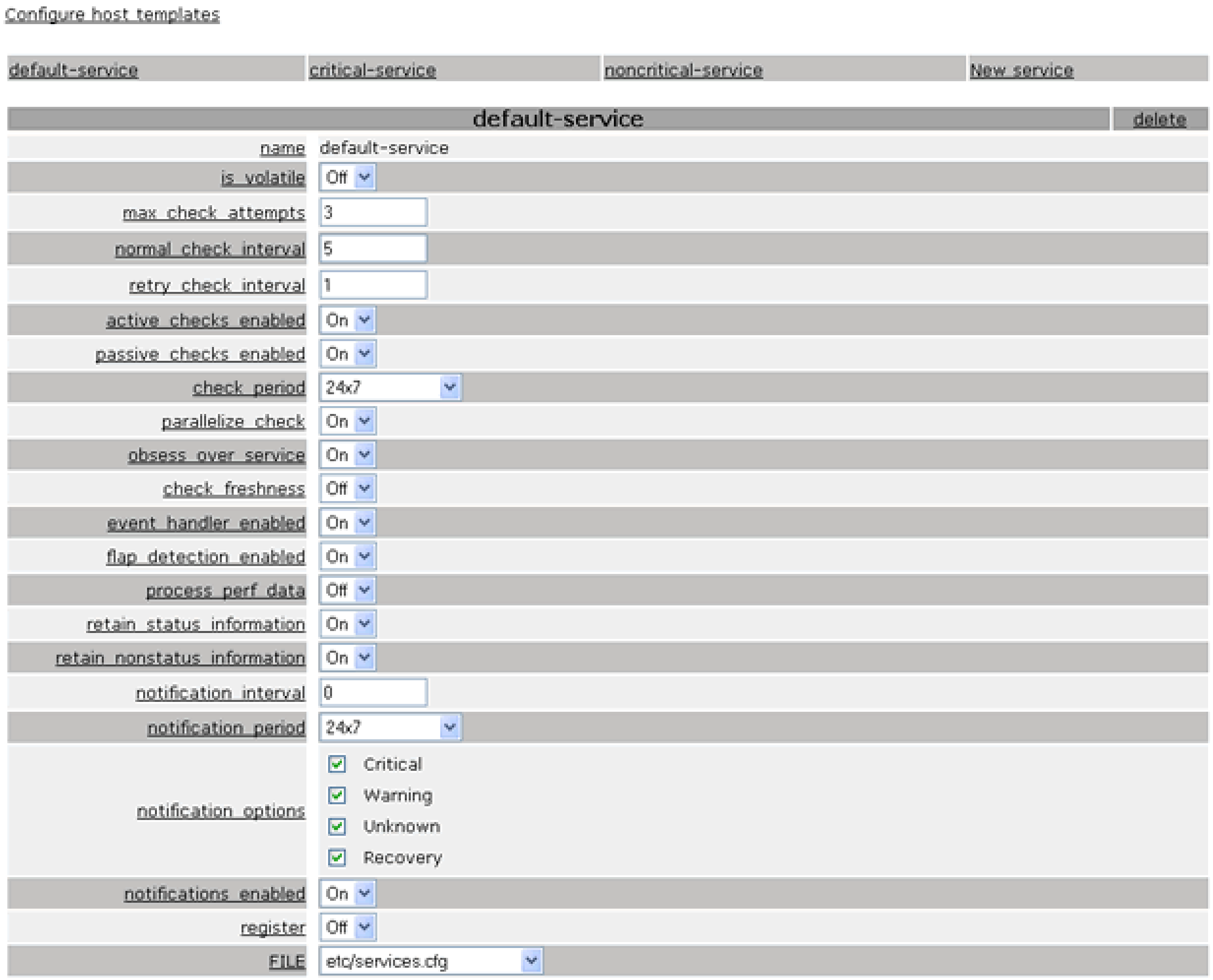
For explanations of the fields, see section: View Configuration – Services or click the field name in configuration window.



active_checks_enabled	On
passive_checks_enabled	On
check_period	24x7
parallelize_check	On
obsess_over_service	On
check_freshness	Off
freshness_threshold	
event_handler	
event_handler_enabled	On
low_flap_threshold	
high_flap_threshold	
flap_detection_enabled	On
process_perf_data	Off
retain_status_information	On
retain_nonstatus_information	On
notification_interval	0
notification_period	24x7
notification_options	☑ Critical ☑ Warning ☑ Unknown ☑ Recovery
notifications_enabled	On
contact_groups	op5-linux op5-print op5-routers op5-windows
stalking_options	☐ Stalk on CRITICAL states ☐ Stalk on WARNING tates ☐ Stalk on UNKNOWN tates ☐ Stalk on OK states
FILE	etc/services.cfg

Add, Change or Delete Service Templates

To change the templates for services choose Service Templates from the start page. The following window Appear:



Configure host templates

default-service	critical-service	noncritical-service	New service

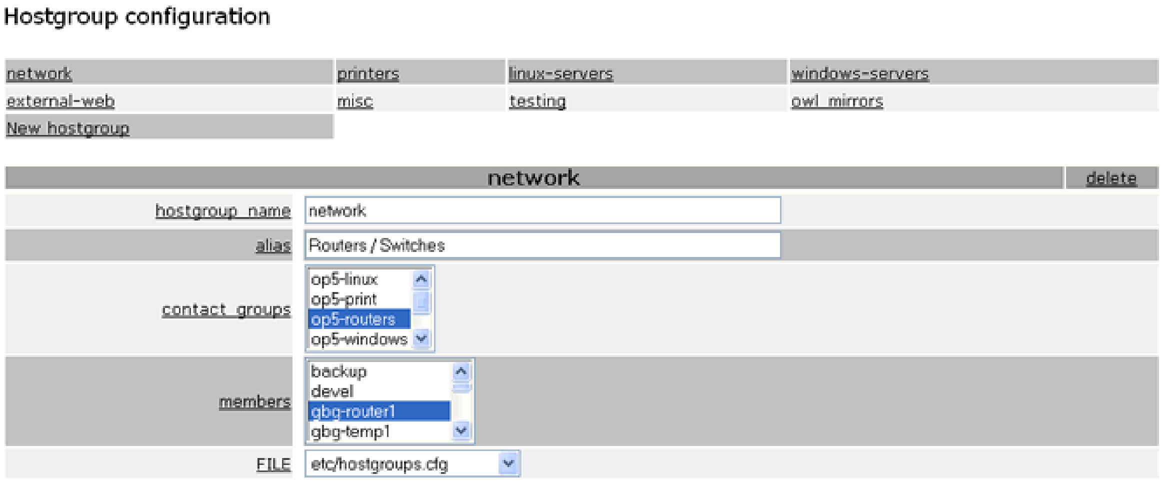
default-service | delete

name	default-service
is_volatile	Off
max_check_attempts	3
normal_check_interval	5
retry_check_interval	1
active_checks_enabled	On
passive_checks_enabled	On
check_period	24x7
parallelize_check	On
obsess_over_service	On
check_freshness	Off
event_handler_enabled	On
flap_detection_enabled	On
process_perf_data	Off
retain_status_information	On
retain_nonstatus_information	On
notification_interval	0
notification_period	24x7
notification_options	☑ Critical ☑ Warning ☑ Unknown ☑ Recovery
notifications_enabled	On
register	Off
FILE	etc/services.cfg

To configure host Template choose the quick link on top left hand side. All templates are listed after each other to jump to a specific template choose the template in the top. To delete a template choose delete for respective template on the right hand side. When done configuring, click 'Apply changes'. For the changes to take effect click the 'Save configuration' link. For explanation of the fields see section: View Configuration – Hosts, Services, Configure – Host Templates. You can also click the field names in the configuration window and et an on line help.

Add, Change or Delete Host Groups

To add, change or delete a host group choose the host group link from the start page. A new window will appear:



Hostgroup configuration

network	printers	linux-servers	windows-servers
external-web	misc	testing	owl_mirrors
New hostgroup			

network	delete
hostgroup_name	network
alias	Routers / Switches
contact_groups	op5-linux op5-print op5-routers op5-windows
members	backup devel gbg-router1 gbg-temp1
FILE	etc/hostgroups.cfg

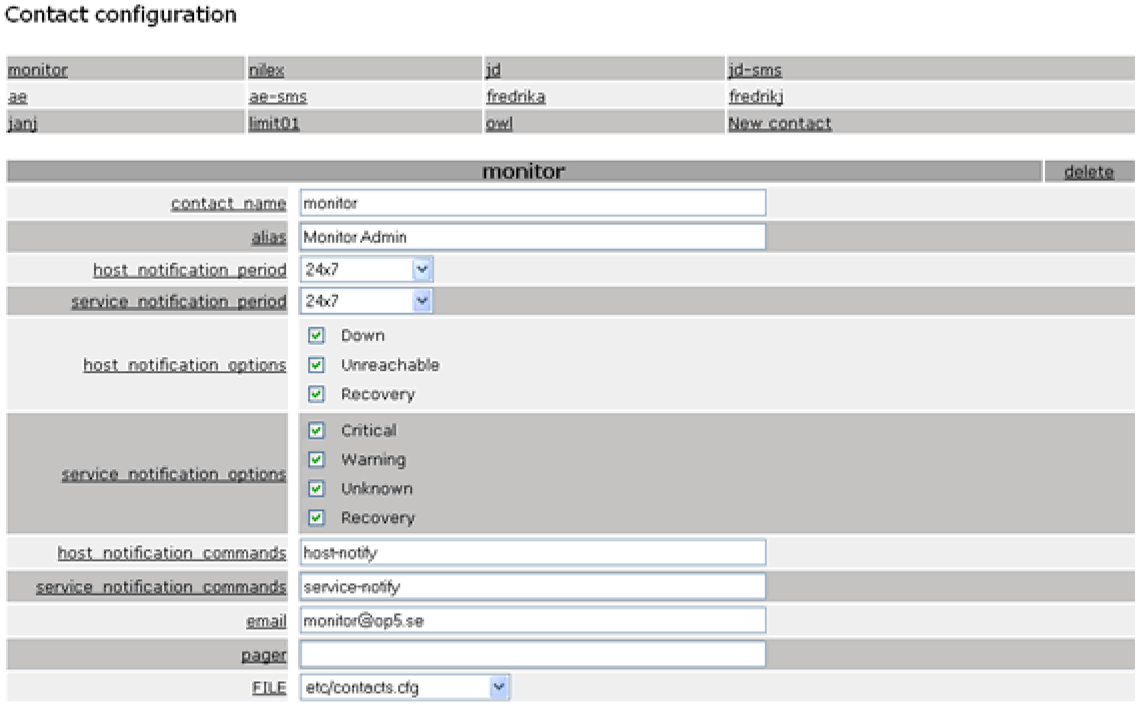
All host groups are listed after each other represented with a quick link in top of the window. In bottom of the list you have the possibility to add a new host group. On the right hand side of the host group configuration window you can click delete to delete chosen host group.

- Host group Name (Name of Host group)
- Alias (Description of Host group)
- Contact Groups (Contact groups that the host group is a member of)
- Members (Hosts that are members of this host group)
- File (The file in which this configuration is stored, default: hostgroups.cfg)

Click 'Apply changes' in the bottom of the window. Click 'Save Configuration' for the changes to take effect.

Add, Change or Delete Contacts

To add, change or delete a contact choose the contacts link from the start page. A new window will appear:



Contact configuration

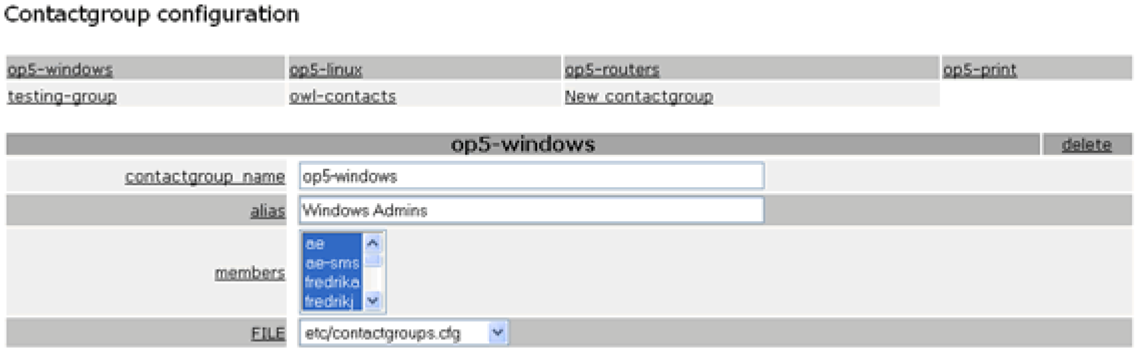
monitor	nilex	jd	jd-sms
ae	ae-sms	fredrika	fredrikj
janj	limit01	owl	New contact

monitor	delete
contact_name	monitor
alias	Monitor Admin
host_notification_period	24x7
service_notification_period	24x7
host_notification_options	☑ Down ☑ Unreachable ☑ Recovery
service_notification_options	☑ Critical ☑ Warning ☑ Unknown ☑ Recovery
host_notification_commands	host-notify
service_notification_commands	service-notify
email	monitor@op5.se
pager	
FILE	etc/contacts.cfg

All the contacts are listed in a list beneath each other, to quickly move to a certain contact use the quick links in top of the window. The last quick link is the new contact. Use this one to add a new contact. On the right hand side of each contact section you have the possibility to delete chosen contact. Click 'Apply changes' in the bottom of the window when done configuring. For the changes to take effect, choose 'Save Configuration' from the star page. For detailed information about the fields see section: View Configuration – Contacts or click the field name in the configuration window.

Add, Change or Delete Contact Groups

To add, change or delete a contact group please select the contact group link from the star page. A new window will appear:



Contactgroup configuration

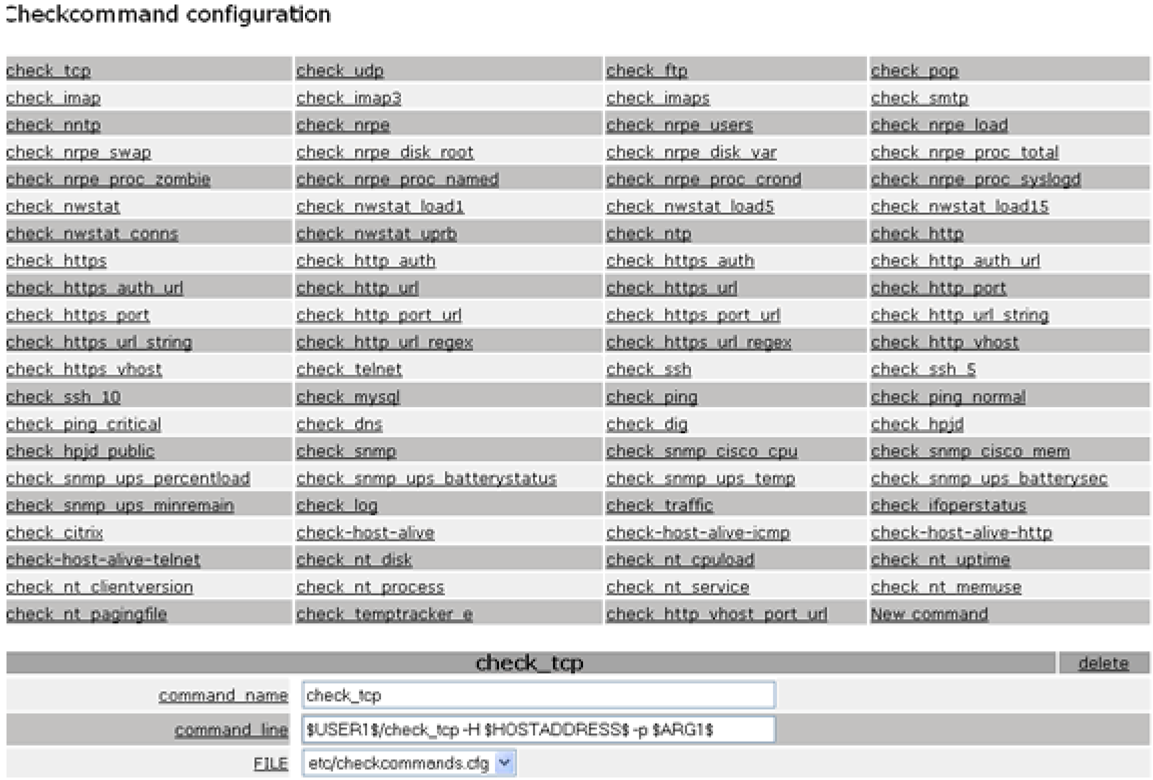
op5-windows	op5-linux	op5-routers	op5-print
testing-group	owl-contacts	New contactgroup	

op5-windows — delete

contactgroup_name	op5-windows
alias	Windows Admins
members	ae ae-sms fredrika fredrikj
FILE	etc/contactgroups.cfg

The contact group is basically a grouping of all contacts to optimize the notification process. All contact groups are listed beneath each other. To jump to certain contact group use the quick link in the top of the window. To add a new contact group choose the last quick link 'new contact group'.On the right hand side in each contact group section you have the possibility to delete chosen contact group. When done configuring click 'Apply changes'. For the changes to take effect choose the 'Save Configuration' from the star page.

Add, Change or Delete Check Commands (Plug ins)



Checkcommand configuration

check_tcp	check_udp	check_ftp	check_pop
check_imap	check_imap3	check_imaps	check_smtp
check_nntp	check_nrpe	check_nrpe_users	check_nrpe_load
check_nrpe_swap	check_nrpe_disk_root	check_nrpe_disk_var	check_nrpe_proc_total
check_nrpe_proc_zombie	check_nrpe_proc_named	check_nrpe_proc_crond	check_nrpe_proc_syslogd
check_nwstat	check_nwstat_load1	check_nwstat_load5	check_nwstat_load15
check_nwstat_conns	check_nwstat_uprb	check_ntp	check_http
check_https	check_http_auth	check_https_auth	check_http_auth_url
check_https_auth_url	check_http_url	check_https_url	check_http_port
check_https_port	check_http_port_url	check_https_port_url	check_http_url_string
check_https_url_string	check_http_url_regex	check_https_url_regex	check_http_vhost
check_https_vhost	check_telnet	check_ssh	check_ssh_5
check_ssh_10	check_mysql	check_ping	check_ping_normal
check_ping_critical	check_dns	check_dig	check_hpjd
check_hpjd_public	check_snmp	check_snmp_cisco_cpu	check_snmp_cisco_mem
check_snmp_ups_percentload	check_snmp_ups_batterystatus	check_snmp_ups_temp	check_snmp_ups_batterysec
check_snmp_ups_minremain	check_log	check_traffic	check_ifoperstatus
check_citrix	check-host-alive	check-host-alive-icmp	check-host-alive-http
check-host-alive-telnet	check_nt_disk	check_nt_cpuload	check_nt_uptime
check_nt_clientversion	check_nt_process	check_nt_service	check_nt_memuse
check_nt_pagingfile	check_temptracker_e	check_http_vhost_port_url	New command

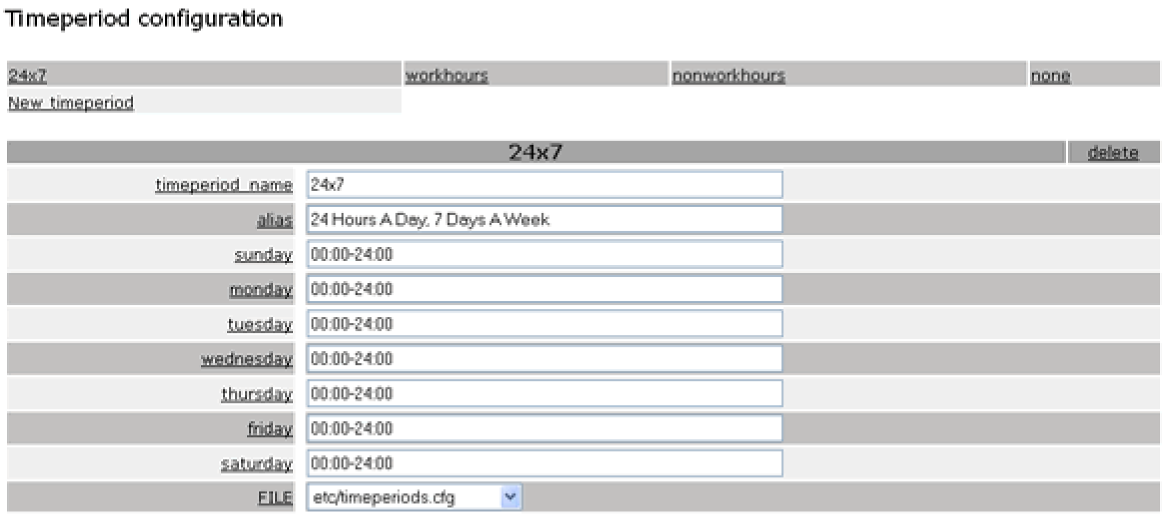
check_tcp — delete

command_name	check_tcp
command_line	$USER1$/check_tcp -H $HOSTADDRESS$ -p $ARG1$
FILE	etc/checkcommands.cfg

To add, change or delete a plug in (check command) choose commands from the star page. All commands are listed in section beneath each other in one window. To jump to a section use the quick link in top of the window. To add a new command choose the last quick link that says 'New command'. In each section you have the possibility to delete a chosen command by clicking delete on the right hand side. Click 'Apply changes' to save the configuration. Choose 'Save Configuration' from the start page for the changes to take effect. All commands uses arguments. For a detailed list of plug ins and arguments see Appendix B – Plug ins.

Add, Change or Delete Time Periods

To add, change or delete a Time period choose Time periods from the star page. All time periods are listed in section beneath each other in one window. To jump to a section use the quick link in top of the window. To add a new time period choose the last quick link that says 'New time period'. In each section you have the possibility to delete a chosen time period by clicking delete on the right hand side. Click 'Apply changes' to save the configuration. Choose 'Save Configuration' from the start page for the changes to take effect.

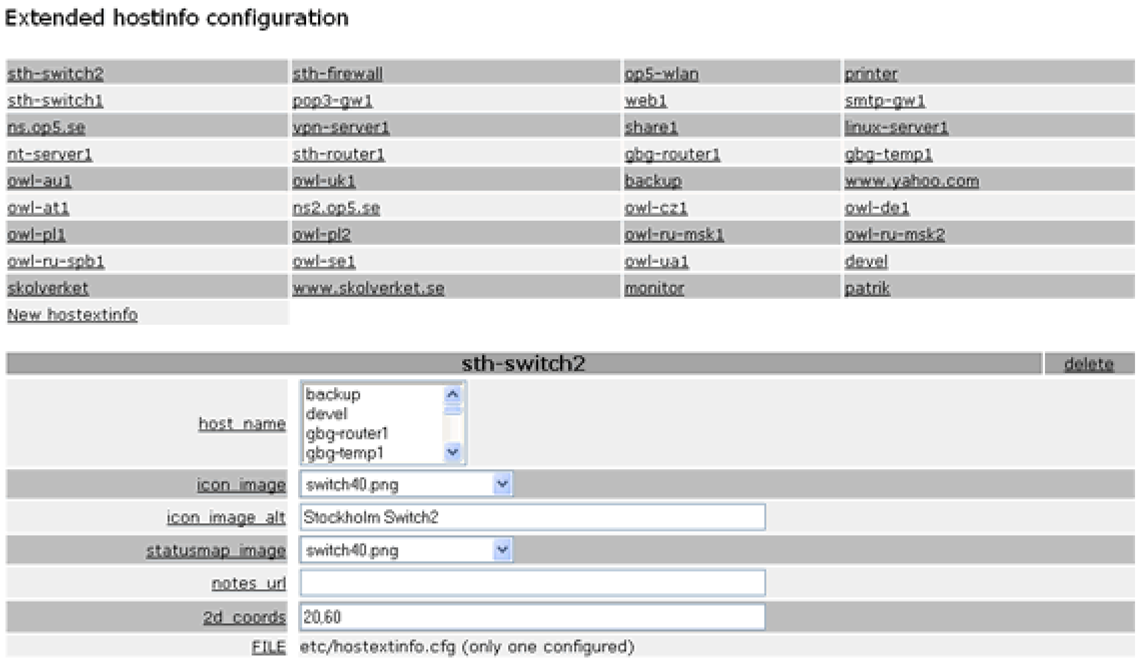


Timeperiod configuration

24x7	workhours	nonworkhours	none
New timeperiod			

24x7	delete
timeperiod_name	24x7
alias	24 Hours A Day, 7 Days A Week
sunday	00:00-24:00
monday	00:00-24:00
tuesday	00:00-24:00
wednesday	00:00-24:00
thursday	00:00-24:00
friday	00:00-24:00
saturday	00:00-24:00
FILE	etc/timeperiods.cfg

Add, change or Delete Extended Host Information



Extended hostinfo configuration

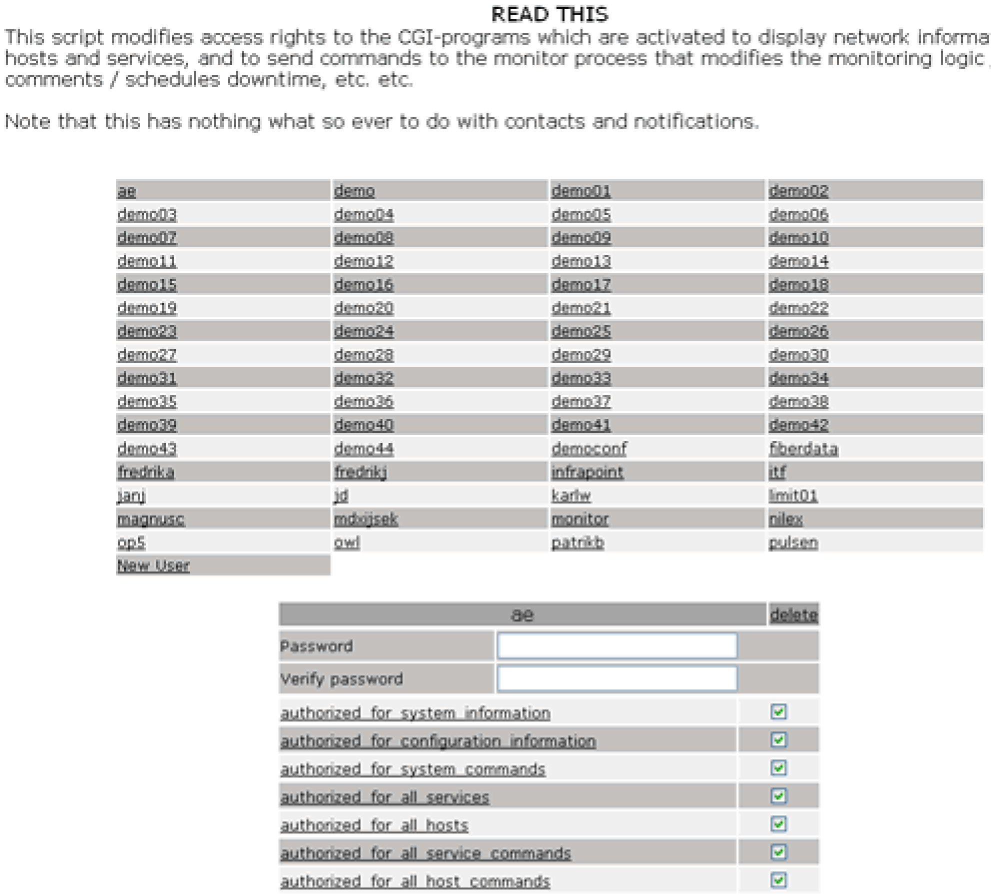
sth-switch2	sth-firewall	op5-wlan	printer
sth-switch1	pop3-gw1	web1	smtp-gw1
ns.op5.se	vpn-server1	share1	linux-server1
nt-server1	sth-router1	gbg-router1	gbg-temp1
owl-au1	owl-uk1	backup	www.yahoo.com
owl-at1	ns2.op5.se	owl-cz1	owl-de1
owl-pl1	owl-pl2	owl-ru-msk1	owl-ru-msk2
owl-ru-spb1	owl-se1	owl-ua1	devel
skolverket	www.skolverket.se	monitor	patrik
New hostextinfo			

sth-switch2	delete
host_name	backup devel gbg-router1 gbg-temp1
icon_image	switch40.png
icon_image_alt	Stockholm Switch2
statusmap_image	switch40.png
notes_url	
2d_coords	20,60
FILE	etc/hostextinfo.cfg (only one configured)

To add, change or delete extended host information choose extended host information from the star page. All extended information are listed in sections beneath each other in one window. To jump to a section use the quick link in top of the window. To add a new extended information choose the last quick link that says 'New hostextinfo'. In each section you have the possibility to delete a chosen extended information by clicking delete on the right hand side. Click 'Apply changes' to save the configuration. Choose 'Save Configuration' from the start page for the changes to take effect.

Add, Change or Delete User Access

To add, change or delete users that has access to the OP5 Monitor Web interface choose 'Users Access' from the start page. All users are listed in sections beneath each other in one window. To jump to a section use the quick link in top of the window. To add a new user choose the last quick link that says 'New User'. In each section you have the possibility to delete a chosen user by clicking delete on the right hand side. Click 'Apply changes' to save the configuration. Choose 'Save Configuration' from the start page for the changes to take effect.



READ THIS

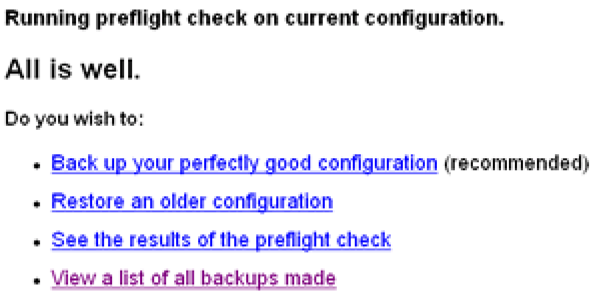
This script modifies access rights to the CGI-programs which are activated to display network information about hosts and services, and to send commands to the monitor process that modifies the monitoring logic / adds comments / schedules downtime, etc. etc.

Note that this has nothing what so ever to do with contacts and notifications.

ae	demo	demo01	demo02
demo03	demo04	demo05	demo06
demo07	demo08	demo09	demo10
demo11	demo12	demo13	demo14
demo15	demo16	demo17	demo18
demo19	demo20	demo21	demo22
demo23	demo24	demo25	demo26
demo27	demo28	demo29	demo30
demo31	demo32	demo33	demo34
demo35	demo36	demo37	demo38
demo39	demo40	demo41	demo42
demo43	demo44	democonf	fiberdata
fredrika	fredrikj	infrapoint	itf
janj	jd	karlw	limit01
magnusc	mdxijsek	monitor	nilex
op5	owl	patrikb	pulsen
New User			

ae		delete
Password		
Verify password		
authorized_for_system_information		☑
authorized_for_configuration_information		☑
authorized_for_system_commands		☑
authorized_for_all_services		☑
authorized_for_all_hosts		☑
authorized_for_all_service_commands		☑
authorized_for_all_host_commands		☑

Backup and Restore Configuration



Running preflight check on current configuration.

All is well.

Do you wish to:

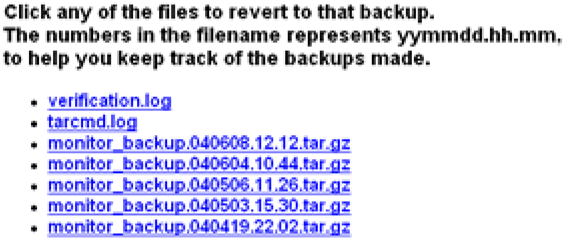
- Back up your perfectly good configuration (recommended)
- Restore an older configuration
- See the results of the preflight check
- View a list of all backups made

When choosing Backup and Restore configuration from the main menu you'll see the window shown in the picture above. Basically is shows a list of options you have:

Backup Configuration

When clicking this link a tar ball will be created and stored on the server. The name will consists of the text: monitor_backup + date + time.tar.gz. You also have the option to view the output of the tar ball process.

Restore Configuration



Click any of the files to revert to that backup.
The numbers in the filename represents yymmdd.hh.mm,
to help you keep track of the backups made.

- verification.log
- tarcmd.log
- monitor_backup.040608.12.12.tar.gz
- monitor_backup.040604.10.44.tar.gz
- monitor_backup.040506.11.26.tar.gz
- monitor_backup.040503.15.30.tar.gz
- monitor_backup.040419.22.02.tar.gz

When choosing restore a configuration the windows shown in the picture above will appear. Choose the file you want to restore and the configuration will be restored and activated. Activation means, that the configuration will be verified and the monitor process restarted with the old , chosen, configuration.

See results from a preflight check.

Lets you see the result of configuration verification. If everything is ok, the output will look like this:

```
Nagios 1.2
Copyright (c) 1999-2004 Ethan Galstad (nagios@nagios.org)
Last Modified: 02-02-2004
License: GPL

Reading configuration data...

Running pre-flight check on configuration data...

Checking services...
        Checked 149 services.
Checking hosts...
        Checked 35 hosts.
Checking host groups...
        Checked 8 host groups.
Checking contacts...
        Checked 11 contacts.
Checking contact groups...
        Checked 6 contact groups.
Checking service escalations...
        Checked 0 service escalations.
Checking host group escalations...
        Checked 1 host group escalations.
Checking service dependencies...
        Checked 0 service dependencies.
Checking host escalations...
        Checked 0 host escalations.
Checking host dependencies...
        Checked 0 host dependencies.
Checking commands...
        Checked 85 commands.
Checking time periods...
        Checked 4 time periods.
```

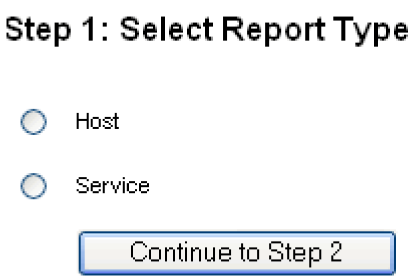
```
Checking for circular paths between hosts...
Checking for circular service execution dependencies...
Checking global event handlers...
Checking obsessive compulsive service processor command...
Checking misc settings...

Total Warnings: 0
Total Errors:   0

Things look okay - No serious problems were detected during the pre-flight check
```

View a list of all backups made - Shows all stored backups.

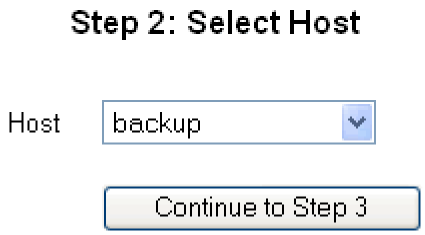
Reporting

Trends

By choosing trends from the reporting section in main menu you have the possibility to look at how well a host or a service has work in the past. The following window will appear:

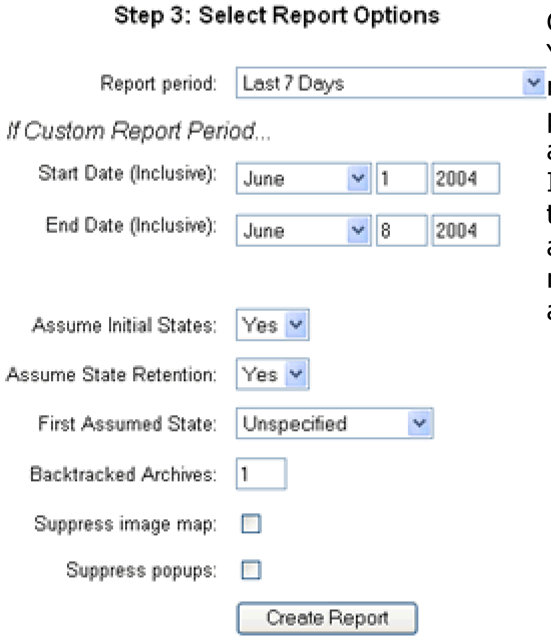


Choose the of report you want, host or service. Click on the 'Continue to Step 2' button.



Host: backup

Select the Host or (Service) you want the report to based on. Click 'Continue to step 3' when done.



Report period: Last 7 Days

Start Date (Inclusive): June 1 2004

End Date (Inclusive): June 8 2004

Assume Initial States: Yes

Assume State Retention: Yes

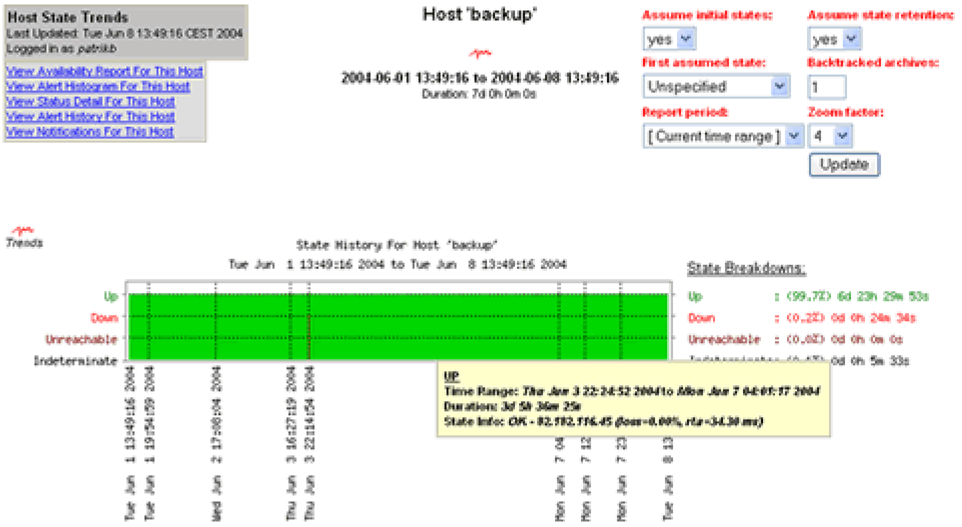
First Assumed State: Unspecified

Backtracked Archives: 1

Suppress image map: □

Suppress popups: □

Choose report period (Days, week, months or year. You also have the possibility to create a custom report period. If thats the case choose the staring period, start and end date. The other options are advanced and nothing you have to touch in general. Initial states and state retention has to do with how to handle states when restarting the server. You can assume these states as they are saved when rebooting the server. Or you can make the assumption yourself.



Host State Trends
Last Updated: Tue Jun 8 13:49:16 CEST 2004
Logged in as *patrikb*

View Availability Report For This Host
View Alert Histogram For This Host
View Status Detail For This Host
View Alert History For This Host
View Notifications For This Host

Host 'backup'

2004-06-01 13:49:16 to 2004-06-08 13:49:16
Duration: 7d 0h 0m 0s

Assume initial states: yes
Assume state retention: yes
First assumed state: Unspecified
Backtracked archives: 1
Report period: [Current time range]
Zoom factor: 4

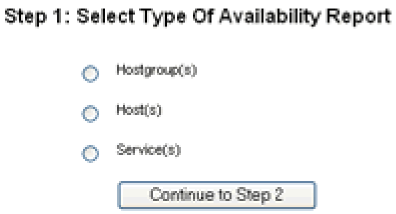
State History For Host 'backup'
Tue Jun 1 13:49:16 2004 to Tue Jun 8 13:49:16 2004

State Breakdowns:
Up : (99.7%) 6d 23h 29m 53s
Down : (0.2%) 0d 0h 24m 34s
Unreachable : (0.0%) 0d 0h 0m 0s
Indeterminate : (0.1%) 0d 0h 5m 33s

UP
Time Range: Thu Jun 3 22:24:52 2004 to Mon Jun 7 04:01:17 2004
Duration: 3d 5h 36m 25s
State Info: OK - 92.192.116.45 (loss=0.00%, rta=34.30 ms)

This is basically what the outcome is. Trends shows you the status of a host or service under an interval in the past. The status is shown in colors with averages in totals and percentage to the right side of the picture. You can also click the picture to zoom the statistics. In the top of the window you have the possibility to reconfigure the output without going back.

Availability

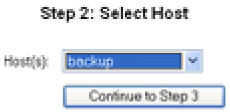


Step 1: Select Type Of Availability Report

○ Hostgroup(s)
○ Host(s)
○ Service(s)

From the main menu under section reporting choose Availability. A new window will appear:

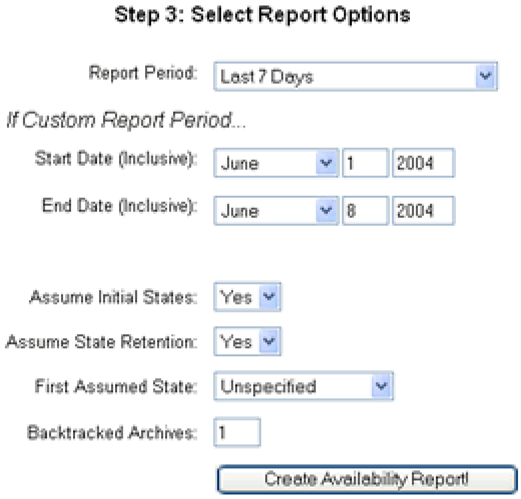
Select type of report to create; Host groups, hosts or services. Click 'Continue to Step2'.



Step 2: Select Host

Host(s): backup

Select the Host, (host group or service) you want to report on. Click 'Continue to step 3'.



Step 3: Select Report Options

Report Period: Last 7 Days

If Custom Report Period...

Start Date (Inclusive): June 1 2004

End Date (Inclusive): June 8 2004

Assume Initial States: Yes

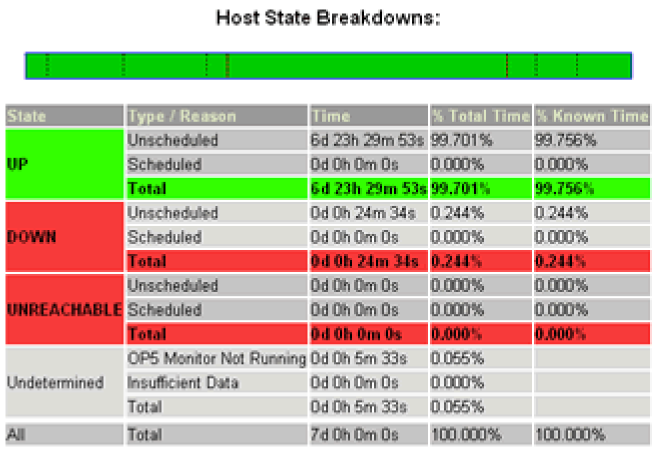
Assume State Retention: Yes

First Assumed State: Unspecified

Backtracked Archives: 1

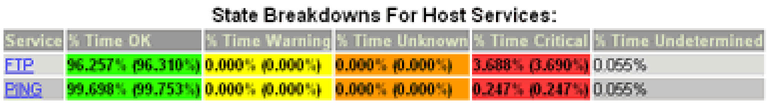
Select report periods, see section trends fro details. Click 'Create Availability Report'

And this is basically the outcome:



Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	6d 23h 29m 53s	99.701%	99.756%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	**6d 23h 29m 53s**	**99.701%**	**99.756%**
DOWN	Unscheduled	0d 0h 24m 34s	0.244%	0.244%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	**0d 0h 24m 34s**	**0.244%**	**0.244%**
UNREACHABLE	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	**0d 0h 0m 0s**	**0.000%**	**0.000%**
Undetermined	OP5 Monitor Not Running	0d 0h 5m 33s	0.055%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 5m 33s	0.055%	
All	Total	7d 0h 0m 0s	100.000%	100.000%

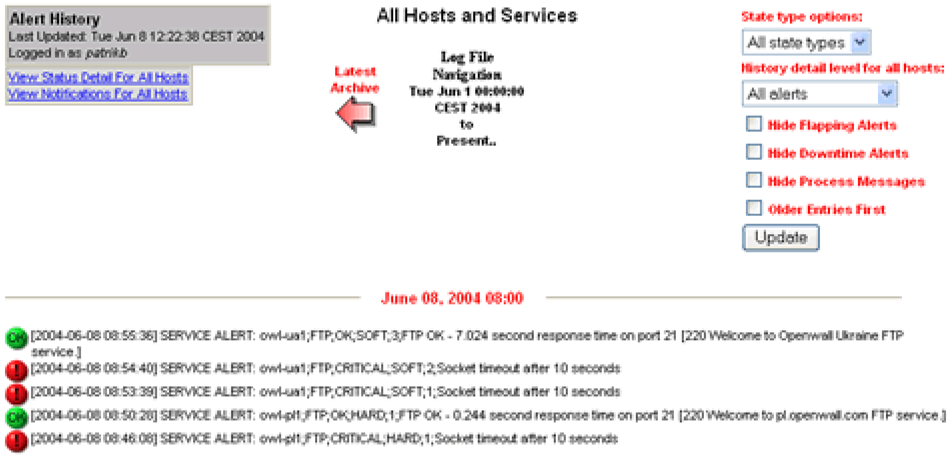


State Breakdowns For Host Services:

Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
FTP	96.257% (96.310%)	0.000% (0.000%)	0.000% (0.000%)	3.688% (3.690%)	0.055%
PING	99.698% (99.753%)	0.000% (0.000%)	0.000% (0.000%)	0.247% (0.247%)	0.055%

The states are showed in totals and percentages, divided in scheduled and unscheduled, which means if the host has been scheduled for downtime or not. So If the figures for Up are unscheduled, this means that the host has NOT been scheduled for downtime. If there are figures for Scheduled, the host has been scheduled for downtime. The report also shows state breakdowns divided in time, state shown in percentages.

Alert History



Alert History
Last Updated: Tue Jun 8 12:22:38 CEST 2004
Logged in as *patrikb*

View Status Detail For All Hosts
View Notifications For All Hosts

All Hosts and Services

Log File Navigation
Tue Jun 1 00:00:00 CEST 2004 to Present..

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

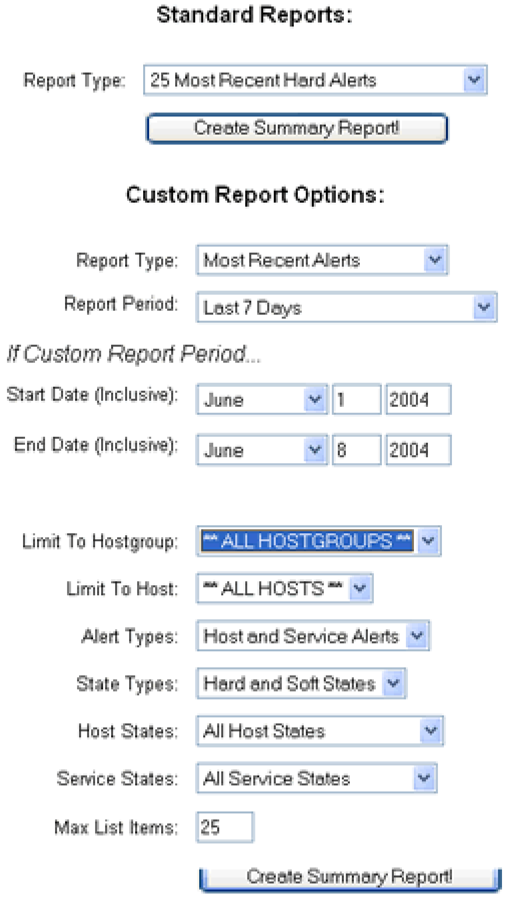
June 08, 2004 08:00

```
[2004-06-08 08:55:36] SERVICE ALERT: owl-ua1;FTP;OK;SOFT;3;FTP OK - 7.024 second response time on port 21 [220 Welcome to Openwall Ukraine FTP service.]
[2004-06-08 08:54:40] SERVICE ALERT: owl-ua1;FTP;CRITICAL;SOFT;2;Socket timeout after 10 seconds
[2004-06-08 08:53:39] SERVICE ALERT: owl-ua1;FTP;CRITICAL;SOFT;1;Socket timeout after 10 seconds
[2004-06-08 08:50:20] SERVICE ALERT: owl-pl1;FTP;OK;HARD;1;FTP OK - 0.244 second response time on port 21 [220 Welcome to pl.openwall.com FTP service.]
[2004-06-08 08:46:08] SERVICE ALERT: owl-pl1;FTP;CRITICAL;HARD;1;Socket timeout after 10 seconds
```

Alert History shows you all events filtered by date and time. By clicking Alert History in the main menu under Reporting the window shown in the picture above appears. The list can be filtered using the History Detail level list shown in top right hand side of the window. The list can be filtered according to the event state and depending on whether it's a host or a service, further more the list can be filtered according to soft and hard states (types). On the top left hand side of the windows are the related links; Status Detail for Hosts and Notifications for Hosts.

Alert Summary

Alert Summary shows you a summarized picture of all problems, like the top alert producers, or the most recent alert producers and so on. When selecting Alert Summary from the main menu a new window will appear, see next page. You'll have the possibility to choose a standard report or make a customized report. The standard reports are:



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): June 1 2004

End Date (Inclusive): June 8 2004

Limit To Hostgroup: ** ALL HOSTGROUPS **

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: 25

25 most recent hard alerts

25 most recent hard host alerts

25 most recent hard service alerts

Top 25 hard host producers

Top 25 hard service producers

The customized reports requires you to set a number of criteria for the report;

Report type: Most Recent Alerts, Alert Totals, Alert totals by Host group, Alert totals by Hosts, Alert totals by Service.

Report Period: The interval of the report, choosing the past in days, weeks, months or years. The period can also be customized further(See custom Report period)

Custom Report Period: Choose the start and end date if you chosen custom report period above.

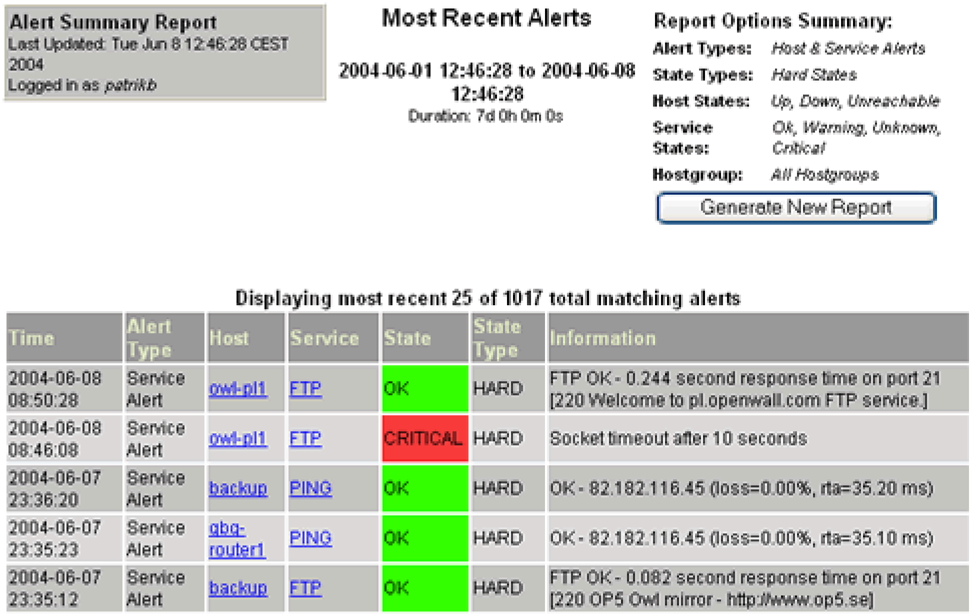
Filter by choosing: Limit to host group, limit to host, alert types, state types, host states, service states.

Choose the size of the report by enter the Max list item value.

Click the 'Create Summary Report'

Remember either you choose the standard reports or you use the customized one

And this what the outcome is for a standard report 'Most Recent Alerts'.



Alert Summary Report
Last Updated: Tue Jun 8 12:46:28 CEST 2004
Logged in as *patrikb*

Most Recent Alerts

2004-06-01 12:46:28 to 2004-06-08 12:46:28
Duration: 7d 0h 0m 0s

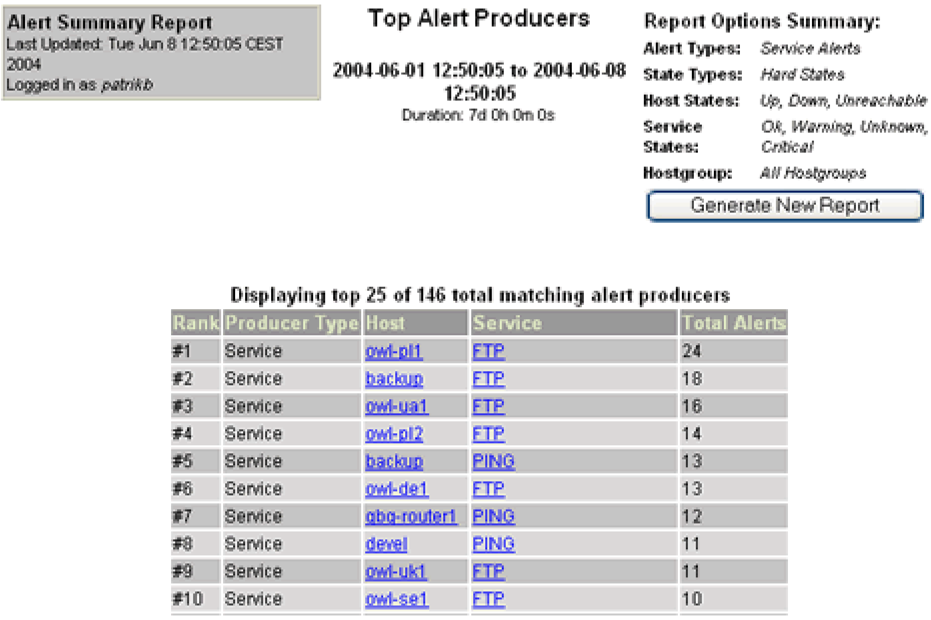
Report Options Summary:

Alert Types: *Host & Service Alerts*
State Types: *Hard States*
Host States: *Up, Down, Unreachable*
Service States: *Ok, Warning, Unknown, Critical*
Hostgroup: *All Hostgroups*

Displaying most recent 25 of 1017 total matching alerts

Time	Alert Type	Host	Service	State	State Type	Information
2004-06-08 08:50:28	Service Alert	owl-pl1	FTP	OK	HARD	FTP OK - 0.244 second response time on port 21 [220 Welcome to pl.openwall.com FTP service.]
2004-06-08 08:46:08	Service Alert	owl-pl1	FTP	CRITICAL	HARD	Socket timeout after 10 seconds
2004-06-07 23:36:20	Service Alert	backup	PING	OK	HARD	OK - 82.182.116.45 (loss=0.00%, rta=35.20 ms)
2004-06-07 23:35:23	Service Alert	gbg-router1	PING	OK	HARD	OK - 82.182.116.45 (loss=0.00%, rta=35.10 ms)
2004-06-07 23:35:12	Service Alert	backup	FTP	OK	HARD	FTP OK - 0.082 second response time on port 21 [220 OP5 Owl mirror - http://www.op5.se]

This is what the outcome is for Top 25 Hard Service Alerts:



Alert Summary Report
Last Updated: Tue Jun 8 12:50:05 CEST 2004
Logged in as *patrikb*

Top Alert Producers

2004-06-01 12:50:05 to 2004-06-08 12:50:05
Duration: 7d 0h 0m 0s

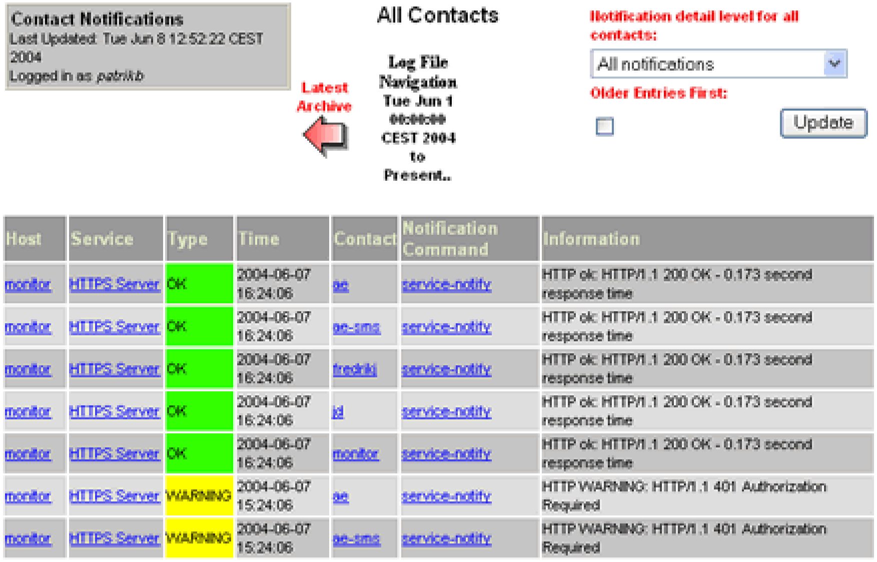
Report Options Summary:

Alert Types:	*Service Alerts*
State Types:	*Hard States*
Host States:	*Up, Down, Unreachable*
Service States:	*Ok, Warning, Unknown, Critical*
Hostgroup:	*All Hostgroups*

Displaying top 25 of 146 total matching alert producers

Rank	Producer Type	Host	Service	Total Alerts
#1	Service	owl-pl1	FTP	24
#2	Service	backup	FTP	18
#3	Service	owl-ua1	FTP	16
#4	Service	owl-pl2	FTP	14
#5	Service	backup	PING	13
#6	Service	owl-de1	FTP	13
#7	Service	gbg-router1	PING	12
#8	Service	devel	PING	11
#9	Service	owl-uk1	FTP	11
#10	Service	owl-se1	FTP	10

Notifications



Contact Notifications
Last Updated: Tue Jun 8 12:52:22 CEST 2004
Logged in as *patrikb*

All Contacts

Log File Navigation
Tue Jun 1 00:00:00 CEST 2004 to Present..

Notification detail level for all contacts: All notifications

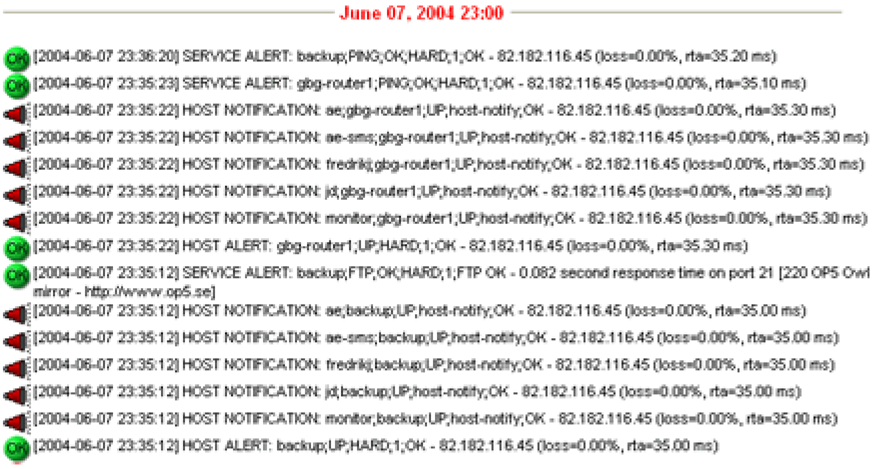
Older Entries First: □

Host	Service	Type	Time	Contact	Notification Command	Information
monitor	HTTPS Server	OK	2004-06-07 16:24:06	ae	service-notify	HTTP ok: HTTP/1.1 200 OK - 0.173 second response time
monitor	HTTPS Server	OK	2004-06-07 16:24:06	ae-sms	service-notify	HTTP ok: HTTP/1.1 200 OK - 0.173 second response time
monitor	HTTPS Server	OK	2004-06-07 16:24:06	fredrikj	service-notify	HTTP ok: HTTP/1.1 200 OK - 0.173 second response time
monitor	HTTPS Server	OK	2004-06-07 16:24:06	jd	service-notify	HTTP ok: HTTP/1.1 200 OK - 0.173 second response time
monitor	HTTPS Server	OK	2004-06-07 16:24:06	monitor	service-notify	HTTP ok: HTTP/1.1 200 OK - 0.173 second response time
monitor	HTTPS Server	WARNING	2004-06-07 15:24:06	ae	service-notify	HTTP WARNING: HTTP/1.1 401 Authorization Required
monitor	HTTPS Server	WARNING	2004-06-07 15:24:06	ae-sms	service-notify	HTTP WARNING: HTTP/1.1 401 Authorization Required

When choosing Notifications from the reporting section of the main menu, the windows shown in the picture above will appear. You'll get a log of all notifications sent out. The list includes: Host, Service, State, Time, Contact, Executed Macro, Information sent out. Further more the list can be sorted according to state type using the menu in the top of the windows right hand side.

Event Log

The Event Log shows all past event in the server listed by date. The Event Log can be viewed choosing 'Event Log' from the main menu under the reporting section.

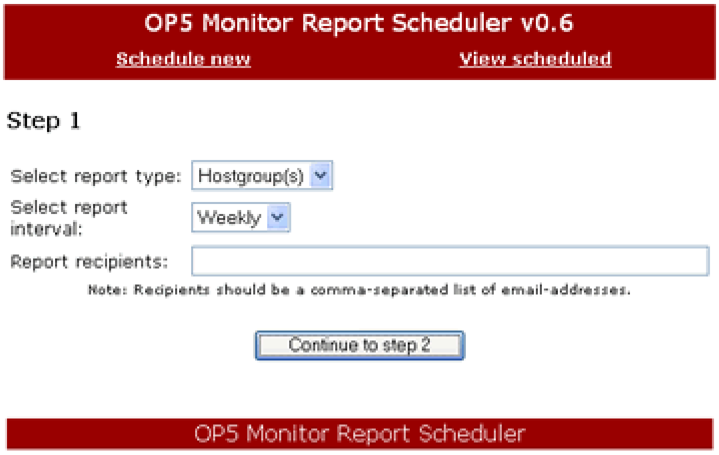


June 07, 2004 23:00

```
[2004-06-07 23:36:20] SERVICE ALERT: backup;PING;OK;HARD;1;OK - 82.182.116.45 (loss=0.00%, rta=35.20 ms)
[2004-06-07 23:35:23] SERVICE ALERT: gbg-router1;PING;OK;HARD;1;OK - 82.182.116.45 (loss=0.00%, rta=35.10 ms)
[2004-06-07 23:35:22] HOST NOTIFICATION: ae;gbg-router1;UP;host-notify;OK - 82.182.116.45 (loss=0.00%, rta=35.30 ms)
[2004-06-07 23:35:22] HOST NOTIFICATION: ae-sms;gbg-router1;UP;host-notify;OK - 82.182.116.45 (loss=0.00%, rta=35.30 ms)
[2004-06-07 23:35:22] HOST NOTIFICATION: fredrik;gbg-router1;UP;host-notify;OK - 82.182.116.45 (loss=0.00%, rta=35.30 ms)
[2004-06-07 23:35:22] HOST NOTIFICATION: jd;gbg-router1;UP;host-notify;OK - 82.182.116.45 (loss=0.00%, rta=35.30 ms)
[2004-06-07 23:35:22] HOST NOTIFICATION: monitor;gbg-router1;UP;host-notify;OK - 82.182.116.45 (loss=0.00%, rta=35.30 ms)
[2004-06-07 23:35:22] HOST ALERT: gbg-router1;UP;HARD;1;OK - 82.182.116.45 (loss=0.00%, rta=35.30 ms)
[2004-06-07 23:35:12] SERVICE ALERT: backup;FTP;OK;HARD;1;FTP OK - 0.082 second response time on port 21 [220 OP5 Owl
mirror - http://www.op5.se]
[2004-06-07 23:35:12] HOST NOTIFICATION: ae;backup;UP;host-notify;OK - 82.182.116.45 (loss=0.00%, rta=35.00 ms)
[2004-06-07 23:35:12] HOST NOTIFICATION: ae-sms;backup;UP;host-notify;OK - 82.182.116.45 (loss=0.00%, rta=35.00 ms)
[2004-06-07 23:35:12] HOST NOTIFICATION: fredrik;backup;UP;host-notify;OK - 82.182.116.45 (loss=0.00%, rta=35.00 ms)
[2004-06-07 23:35:12] HOST NOTIFICATION: jd;backup;UP;host-notify;OK - 82.182.116.45 (loss=0.00%, rta=35.00 ms)
[2004-06-07 23:35:12] HOST NOTIFICATION: monitor;backup;UP;host-notify;OK - 82.182.116.45 (loss=0.00%, rta=35.00 ms)
[2004-06-07 23:35:12] HOST ALERT: backup;UP;HARD;1;OK - 82.182.116.45 (loss=0.00%, rta=35.00 ms)
```

Report Scheduler

By choosing Schedule Reports from the main menu under section reporting you'll have the possibility to create automated availability reports. The following window will appear:



OP5 Monitor Report Scheduler v0.6

Step 1

Select report type: Hostgroup(s)

Select report interval: Weekly

Report recipients:

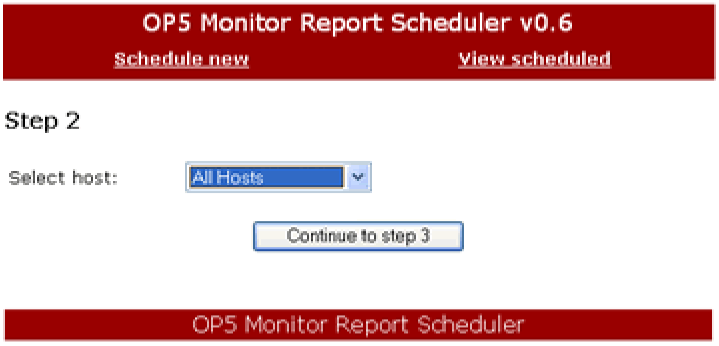
Note: Recipients should be a comma-separated list of email-addresses.

Choose report type: Host groups, hosts or services.

Choose Report Interval: Weekly or Monthly.

Enter the email address of whom should receive the report.

Click 'Continue to Step 2'

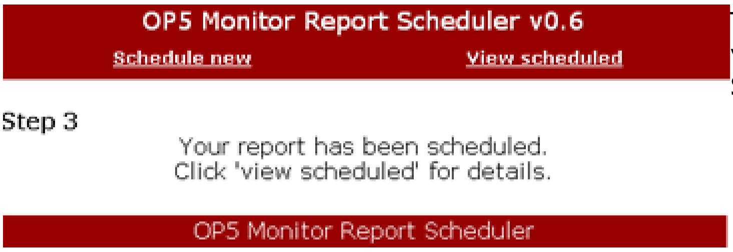


OP5 Monitor Report Scheduler v0.6

Step 2

Select host: All Hosts

Choose the host, service or host group you want to report on and click 'Continue to step 3'

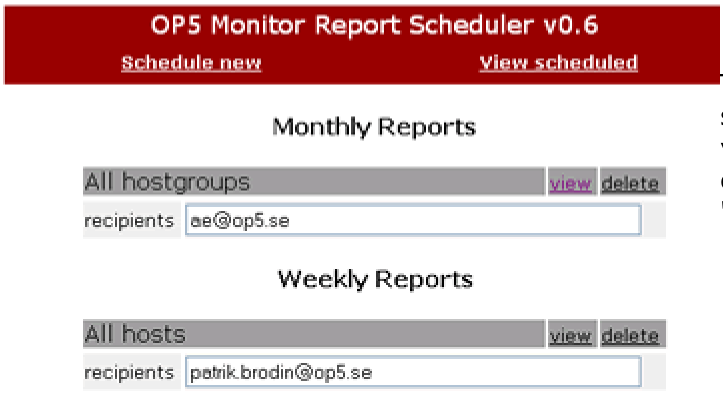

OP5 Monitor Report Scheduler v0.6
Schedule new
View scheduled

Step 3

Your report has been scheduled.
Click 'view scheduled' for details.

OP5 Monitor Report Scheduler

The report has now been scheduled. To view scheduled reports click 'View Scheduled'



Monthly Reports

All hostgroups	view	delete
recipients	ae@op5.se	

Weekly Reports

All hosts	view	delete
recipients	patrik.brodin@op5.se	

The View Scheduled reports shows all scheduled reports in a list. From here you can delete the report and view the contents of the report by clicking the 'Delete' or 'View' on the report.

Appendix A – Field names

Here is a list of all field names used in the Configuration windows in Monitor.

FILE	Tells the web configuration interface where to store the object. For security reasons, file creation through the web-interface is not supported.
active_checks_enabled	Boolean value. Tells Monitor whether or not active checks (probing) should be performed for this host. Some hosts (typically firewalls and hosts behind them) can't be probed properly.
address	IP-address or DNS-resolvable network host name. Tells Monitor at what address it can find the host in question. It is strongly recommended to use IP-addresses, but network host names is ok too (but only if it can be resolved). Windows 'computer names' will NOT work.
alias	A longer description of the object. F.e. 'External web-server' for a host, or 'No time is a good time' for time periods.
authorized_for_all_host_commands	This grants a user access to acknowledge host problems, disable / enable host checking and notifications, as well as some other minor things. If combined with 'authorized_for_all_hosts', this belongs to admins only.
authorized_for_all_hosts	This grants a user access to view the status of all services on the network. The default behavior is to let users view only those hosts and services for which he / she is a configured contact.

authorized_for_all_service_commands	This grants a user access to acknowledge service problems, disable / enable service checking and notifications, as well as some other minor things. If combined with 'authorized_for_all_services', this belongs to admins only.
authorized_for_all_services	This grants a user access to view the status of all services on the network. The default behavior is to let users view only those hosts and services for which he / she is a configured contact.
authorized_for_configuration_information	Grants a user access to view **AND MODIFY** your configuration. You should be VERY restrictive with this.
authorized_for_system_commands	This grants a user access to start and stop Monitor and disable and / or enable notifications / logging / flap detection and lots of other things. Needless to say, this option belongs with administrators only.
authorized_for_system_information	Users which have this configured are allowed to view basic information about the system (i.e. tactical overview).
check_command	Reference pointer to command_name. This tells Monitor which command should be run, and what arguments to pass to it.
check_freshness	Boolean value. Tells Monitor whether or not it should accept 'old' retained status information for the remainder of the 'check_period', instead of being skeptical and scheduling a check as soon as possible.
command_line	The command that the above command_name refers to.
command_name	Tells monitor how to identify this particular command.
contact_groups	Comma separated list of references to contactgroup_name. Tells monitor which contacts should receive notifications when the service / host in question changes state.
contact_name	The identifying name of this particular contact (this is what goes into the 'members' field under contactgroups).
contactgroup_name	Identifies or refers to a particular contact group within Monitor. Must be unique.
email	The contacts e-mail address.

event_handler_enabled	Boolean value. Tells Monitor if event handlers (if configured) should be enabled. This is useful f.e. if you want to automatically reboot a server when one of its processes fails, but the host is still up. Keep in mind that it is dangerous to rely solemnly on automation, and you should enable the 'recovery' option for all contacts that receive notifications on services that have this type of auto fixing enabled.
flap_detection_enabled	Boolean value. If a service goes up and down quite a lot (this often happens with web-servers whose hardware configuration can't handle what's requested of it), the service enters 'flapping' state, and a notification is sent out. Enabling this requires some extra memory, but not so much that it is worth disabling.
friday	Self-explanatory.
host_group	Tells Monitor which host group a host belongs to. A host can be a member of several host groups, or none at all. This has to do with notifications, access rights and (of course) host grouping in the status grid.
host_name	Identifies a host in Monitor. This has nothing to do with domain-names or fqdn's. Many hosts can share the same IP, but no two hosts can have the same host_name
host_notification_commands	Reference pointer to command_name. The command that should be executed when the host changes state. Macros will be expanded.
host_notification_options	A comma separated list of single character options. Can be either any combination of the letters d (down), u (unreachable) and r (recovery), or the single character n (never).
host_notification_period	Reference to timeperiod_name. A time period during which notifications will be sent out when the host goes down.
hostgroup_name	Identifies a host group in Monitor. This, like ALL variables ending in '_name', must be a unique name.
is_volatile	Boolean value. A 'volatile' service can't be 'recovered' with anything less than resetting its status through the web interface. Do NOT configure Monitor to resend notifications when 'is_volatile' is set to 1 (ON).

max_check_attempts	Integer value. Tells Monitor how many times it should retry a service / host before it should be considered to have changed HARD state. It is only when a service / host changes its HARD state that a notification is sent out. The service / host will, however, be displayed in accordance to it's SOFT state in the web interface immediately when the SOFT state changes.
members	A comma-separated list of object identifiers (i.e. host_name for host groups). In the web configuration interface this is displayed as a multiple selection for easy 'pick and click'. Press the control key to mark more than one object.
Monday	Self-explanatory.
name	The name to use when the object is being called as a template. Any object can have templates, and any object can BE a template. Variables set within the object in question always overrides those set in the used template(s).
normal_check_interval	Integer value. Tells Monitor how often (in minutes) it should check the services of this host. If you set this too low for a large number of services, everything will fall behind. For best performance, you should set this to a high value (120 or so) for disks and other items that don't rapidly change state.
notification_interval	Integer value. This tells Monitor how often it should resend checks if a service is down. Do NOT use this on services / hosts that are anything but extremely critical, as sending and resending many mails _may_ bog down the internal mail-server, and ultimately result in a system wide denial of service state. It can also be very annoying, and if the problem is ignored the first time, it's probably so for a good reason.
notification_options	Can be either any combination of the four letters c (critical), w (warning), r (recovery) and u (unknown), or the single letter n (never). This is checked before the notification_options set for the contact to which the notification should be sent. If both match, then the notification is sent out.
notification_period	Reference to timeperiod_name. Tells monitor during which times notifications should be sent. The date and time of the state change must be within BOTH this period AND the contacts configured period.

notifications_enabled	Boolean value. Tells monitor if notifications should be sent out when this host or service changes state. If this is set to 0 (OFF), NO notifications will be sent out.
obsess_over_service	Boolean value. I'm not sure what this means, but it's the funniest variable name in an otherwise pretty unfunny configuration syntax.
pager	The contacts cellphone or pager number. Must begin with country code WITHOUT leading '+'-sign (46733709032 for example).
parallelize_check	Boolean value. Tells monitor whether or not it should try and run ALL checks for this host at once, instead of one at the time. If you have extremely limited hardware resources, set this to 0 (OFF).
parents	Comma separated list of references to host_name. This tells Monitor every host of which at least one must be up and running for it to be able to check the host in question. If a 'parent' server is down, it is considered to be a network blocking outage.
passive_checks_enabled	Boolean value. A 'passive' check is ASSUMED to be up and running until Monitor gets notified that it is not. A typical 'passive' check is the snmp trap service, which works exactly like this.
process_perf_data	Boolean value. Tells monitor whether or not it should log processing performance data (this MUST be enabled for reporting to work properly).
register	Boolean value. If this is set to 1 (ON), the object is considered to be part of the configuration. Otherwise it is used only for expanding other objects.
retain_nonstatus_information	Boolean value. Tells Monitor whether or not it should auto-save extra information about the host / service every hour. This is useful for continuance in services checking CPU Load, interface traffic and other checks where a longer-term average can be used to define what's critical and such.
retain_status_information	Boolean value. This tells monitor whether or not it should auto-save the service's / host's STATUS information (OK, CRITICAL and so on) every hour. When you reload Monitor (after changing the configuration, f.e.), the program will then assume that everything is as it was the last time the information was saved. It's generally considered to be a good thing.

retry_check_interval	Integer value. Tells Monitor how many minutes it should wait before retrying a check before it is considered to have changed its HARD state (i.e. before notifications are sent out). The SOFT state changes immediately, and is visible (and audible, if configured) within the web configuration interface.
saturday	Self-explanatory.
service_description	String value. A long description (75 chars, spaces allowed) of the service in question. This (together with 'host_name') also identifies the service, so a host can't have two services with identical descriptions.
service_notification_commands	Reference pointer to command_name. The command that should be executed when the services changes state. Macros will be expanded.
service_notification_options	A comma separated list of options. Can be either any combination of c (critical), w (warning), u (unknown) and r (recovery), or the single letter n (never).
service_notification_period	Reference to timeperiod_name. A time period during which notifications will be sent out for failing services.
sunday	Self-explanatory.
thursday	Self-explanatory.
timeperiod_name	String value, no spaces allowed. Identifier for a time period object, as referenced by various objects.
tuesday	Self-explanatory.
use	Tells Monitor which template to use for this object. All objects can have templates, but templates can not be cross-used (i.e. a host can't inherit the variables of a service template)
wednesday	Self-explanatory.

Appendix B – Plug ins

Dummy, Non-Real State Check [check_dummy]

Usage: ./check_dummy <integer state>

This plug in will simply return the state corresponding to the numeric value of the <state> argument.

SSH, Secure Shell Check [check_SSH]

This plug in will execute a command on a remote host using SSH

Usage:
check_by_ssh [-f46] [-t timeout] [-i identity] [-l user] -H <host> -C <command> [-n name] [-s service list] [-O output file] [-p port]
check_by_ssh -V prints version info
check_by_ssh -h prints more detailed help

Options:
-H, --host name=HOST | *name or IP address of remote host*
-C, --command='COMMAND STRING' | *command to execute on the remote machine*
-f | *tells ssh to fork rather than create a tty*
-t, --timeout=INTEGER | *specify timeout (default: 10 seconds) [optional]*
-p, --port=PORT | *port to connect to on remote system [optional]*
-l, --logname=USERNAME | *SSH user name on remote host [optional]*
-i, --identity=KEYFILE| *identity of an authorized key [optional]*
-O, --output=FILE | *external command file for nagios [optional]*
-s, --services=LIST | *list of nagios service names, separated by ':' [optional]*
-n, --name=NAME | *short name of host in nagios configuration [optional]*
-4, --use-ipv4| *tell ssh to use IPv4*
-6, --use-ipv6 | *tell ssh to use IPv6*

The most common mode of use is to refer to a local identity file with the '-i' option. In this mode, the identity pair should have a null passphrase and the public key should be listed in the authorized_keys file of the remote host. Usually the key will be restricted to running only one command on the remote server. If the remote SSH server tracks invocation arguments, the one remote program may be an agent that can execute additional commands as proxy

To use passive mode, provide multiple '-C' options, and provide all of -O, -s, and -n options (service list order must match '-C' options)

DNS, Name Server Check using dig [check_dig]

Test the DNS service on the specified host using dig

Usage: check_dig -H host -l lookup [-t timeout] [-v]
check_dig --help
check_dig --version

Options:
-H, --host name=STRING or IPADDRESS | *Check server on the indicated host*
-l, --lookup=STRING | *machine name to lookup*
-t, --timeout=INTEGER | *Seconds before connection attempt times out (default: 10)*
-v, --verbose | *Print extra information (command-line use only)*
-h, --help | *Print detailed help screen*
-V, --version | *Print version information*

DISK Usage Check, LINUX[check_disk]

This plug in will check the percent of used disk space on a mounted UNIX file system and generate an alert if percentage is above one of the threshold values.

Usage: check_disk -w limit -c limit [-p path | -x device] [-t timeout] [-m] [-e] [--verbose]
check_disk (-h|--help)
check_disk (-V|--version)

Options:
-w, --warning=INTEGER| *Exit with WARNING status if less than INTEGER kilobytes of disk are free*
-w, --warning=PERCENT% | *Exit with WARNING status if less than PERCENT of disk space is free*
-c, --critical=INTEGER | *Exit with CRITICAL status if less than INTEGER kilobytes of disk are free*
-c, --critical=PERCENT% | *Exit with CRITCAL status if less than PERCENT of disk space is free*
-p, --path=PATH, --partition=PARTTION | *Path or partition (checks all mounted partitions if unspecified)*

-m, --mountpoint | *Display the mount point instead of the partition*
-x, --exclude_device=PATH | *Ignore device (only works if -p unspecified)*
-e, --errors-only | *Display only devices/mount points with errors*
-v, --verbose | *Show details for command-line debugging (do not use with nagios server)*
-h, --help | *Print detailed help screen*
-V, --version | *Print version information*

DISK Usage Check, WINDOWS [check_disk_smb]

Perl Check SMB Disk plug in for Monitor

Usage: check_disk_smb -H <host> -s <share> -u <user> -p <password> -w <warn> -c <crit> [-W <work group>]

Options:

-H, --host name=HOST| *NetBIOS name of the server*
-s, --share=STRING| *Share name to be tested*
-W, --workgroup=STRING | Work group *or Domain used (Defaults to "WORKGROUP")*
-u, --user=STRING| User name *to log in to server. (Defaults to "guest")*
-p, --password=STRING | *Password to log in to server. (Defaults to "guest")*
-w, --warning=INTEGER or INTEGER[kMG] | *Percent of used space at which a warning will be generated (Default: 85%)*

-c, --critical=INTEGER or INTEGER[kMG] | *Percent of used space at which a critical will be generated (Defaults: 95%)*

If thresholds are followed by either a k, M, or G then check to see if that much disk space is available (kilobytes, Megabytes, Gigabytes)

Warning percentage should be less than critical
Warning (remaining) disk space should be greater than critical.

DNS, Name Server Check [check_dns]
Usage: check_dns -H host [-s server] [-a expected-address] [-t timeout]
check_dns --help
check_dns --version

Options:
-H, --host name=HOST | *The name or address you want to query*
-s, --server=HOST| *Optional DNS server you want to use for the lookup*
-a, --expected-address=IP-ADDRESS | *Optional IP address you expect the DNS server to return*
-t, --timeout=INTEGER | *Seconds before connection times out (default: 10)*
-h, --help | *Print detailed help*
-V, --version | *Print version numbers and license information*

This plug in uses the nslookup program to obtain the IP address for the given host/domain query. A optional DNS server to use may be specified. If no DNS server is specified, the default server(s) specified in /etc/resolv.conf will be used.

Flexlm [Flex License Manager check]

Check available flexlm license managers

Usage:
check_flexlm -F <filename> [-v] [-t] [-V] [-h]
check_flexlm --help
check_flexlm --version

-F, --filename=FILE | *Name of license file (usually "license.dat")*
-v, --verbose | *Print some extra debugging information (not advised for normal operation)*
-t, --timeout | *plug in time out in seconds (default = 15)*
-V, --version | *Show version and license information*

-h, --help | *Show this help screen*

Flexlm license managers usually run as a single server or three servers and a quorum is needed. The plug in return OK if 1 (single) or 3 (triple) servers are running, CRITICAL if 1 (single) or 3 (triple) servers are down, and WARNING if 1 or 2 of 3 servers are running

FTP host check [check_ftp]

This plug in tests FTP connections with the specified host.

Usage: check_ftp -H host -p port [-w warn_time] [-c crit_time] [-s send_string] [-e expect_string] [-q quit_string] [-m maxbytes] [-d delay] [-t to_sec] [-v]

Options:
-H, --host name=ADDRESS | *Host name argument for servers using host headers (use numeric address if possible to bypass DNS lookup).*
-p, --port=INTEGER | *Port number*
-s, --send=STRING | *String to send to the server*
-e, --expect=STRING | *String to expect in server response*
-q, --quit=STRING | *String to send server to initiate a clean close of the connection*
-m, --maxbytes=INTEGER | *Close connection once more than this number of bytes are received*
-d, --delay=INTEGER | *Seconds to wait between sending string and polling for response*
-w, --warning=DOUBLE | *Response time to result in warning status (seconds)*
-c, --critical=DOUBLE | *Response time to result in critical status (seconds)*
-t, --timeout=INTEGER | *Seconds before connection times out (default: 10)*
-v, --verbose | *Show details for command-line debugging (do not use with nagios server)*
-h, --help | *Print detailed help screen*
-V, --version | *Print version information*

HP JetDirect Printer Check [check_hpjd]

This plug in tests the STATUS of an HP printer with a JetDirect card. Net-snmp must be installed on the computer running the plug in.

Usage: check_hpjd -H host [-C community]
check_hpjd --help
check_hpjd --version

Options:
-H, --host name=STRING or IPADDRESS| *Check server on the indicated host*
-C, --community=STRING | *The SNMP community name (default=public)*
-h, --help | *Print detailed help screen*
-V, --version | *Print version information*

HTTP, HTTPS Checks [check_http]

This plug in tests the HTTP service on the specified host. It can test normal (http) and secure (https) servers, follow redirects, search for strings and regular expressions, check connection times, and report on certificate expiration times.

Usage:
check_http (-H <vhost> | -I <IP-address>) [-u <uri>] [-p <port>] [-w <warn time>] [-c <critical time>] [-t <timeout>] [-L] [-a auth] [-f <ok | warn | critical | follow>] [-e <expect>] [-s string] [-l] [-r <regex> | -R <case-insensitive regex>] [-P string]
check_http (-h | --help) for detailed help
check_http (-V | --version) for version information
NOTE: One or both of -H and -I must be specified

Options:
-H, --host name=ADDRESS| *Host name argument for servers using host headers (virtual host)*
-I, --IP-address=ADDRESS | *IP address or name (use numeric address if possible to bypass DNS lookup).*
-e, --expect=STRING | *String to expect in first (status) line of server response (default: HTTP/1.) If specified skips all other status line logic (ex: 3xx, 4xx, 5xx processing)*

-s, --string=STRING | *String to expect in the content*
-u, --url=PATH | *URL to GET or POST (default: /)*
-p, --port=INTEGER | *Port number (default: 80)*
-P, --post=STRING | *URL encoded http POST data*
-w, --warning=INTEGER | *Response time to result in warning status (seconds)*
-c, --critical=INTEGER | *Response time to result in critical status (seconds)*
-t, --timeout=INTEGER | *Seconds before connection times out (default: 10)*
-a, --authorization=AUTH_PAIR | User name*:password on sites with basic authentication*
-L, --link=URL | *Wrap output in HTML link (obsoleted by urlize)*
-f, --onredirect=<ok|warning|critical|follow> | *How to handle redirected pages*
-S, --ssl | *Connect via SSL*
-C, --certificate=INTEGER | *Minimum number of days a certificate has to be valid. (when this option is used the url is not checked.)*
-l, --linespan | *Allow regex to span newlines (must precede -r or -R)*
-r, --regex, --ereg=STRING | *Search page for regex STRING*
-R, --eregi=STRING | *Search page for case-insensitive regex STRING*
-v, --verbose | *Show details for command-line debugging (do not use with nagios server)*
-h, --help | *Print detailed help screen*
-V, --version | *Print version information*

This plug in can also check whether an SSL enabled web server is able to serve content (optionally within a specified time) or whether the X509 certificate is still valid for the specified number of days.

CHECK CONTENT: check_http -w 5 -c 10 --ssl www.verisign.com

When the 'www.verisign.com' server returns its content within 5 seconds, a STATE_OK will be returned. When the server returns its content but exceeds the 5-second threshold, a STATE_WARNING will be returned. When an error occurs, a STATE_CRITICAL will be returned.

CHECK CERTIFICATE: check_http www.verisign.com -C 14

When the certificate of 'www.verisign.com' is valid for more than 14 days, a STATE_OK is returned. When the certificate is still valid, but for less than 14 days, a STATE_WARNING is returned. A STATE_CRITICAL will be returned when the certificate is expired.

Network Interface Status Check [check_ifoperstatus]

check_ifoperstatus plug in for Monitor monitors operational status of a particular network interface on the target host

Usage: check_ifoperstatus [-H host] [-C community] [-v 1|2] [-k index] [-d description] [-p port] [-I ifmib] [-n name] [-w i|w|c] [-V] [-h]

Options:
-H ,--host name=HOST | *host name to query - (required)*
-C , --community=COMMUNITY | *SNMP read community (defaults to public, used with SNMP v1 and v2c*
-v, --snmp_version=NR | *1 for SNMP v1 (default) 2 for SNMP v2c*. *SNMP v2c will use get_bulk for less overhead if monitoring with -d*
-k, --key=INDEX | *SNMP IfIndex value*
-d, --descr=DESCRIPTION | *SNMP ifDescr value*
-p , --port=PORT | *SNMP port (default 161)*
-I, --ifmib=IFMIB| *Agent supports IFMIB ifXTable. Do not use if you don't know what this is.*
-n, --name=NAME | *the value should match the returned ifName (Implies the use of -I)*
-w, --warn =i|w|c | *ignore|warn|crit if the interface is dormant (default critical)*
-V, --version | *plug in version*
-h, --help | *usage help*

-k or -d must be specified

Note: either -k or -d must be specified and -d is much more network intensive. Use it sparingly or not at all. -n is used to match against a much more descriptive ifName value in the IfXTable to verify that the snmpkey has not changed to some other network interface after a reboot.

Interface Status Check (check_ifstatus)

check_ifstatus plug in for Monitor monitors operational status of each network interface (except PPP interfaces) on the target host.

Usage: check_ifstatus [-H host] [-C community] [-v 1|2] [-p port] [-I ifmib] [-V] [-h]

Options:

-H, --host name=HOST | *host name to query - (required)*
-C, --community=COMMUNITY | *SNMP read community (defaults to public, used with SNMP v1 and v2c*
-v, --snmp_version=VER | *1 for SNMP v1 (default) 2 for SNMP v2c. SNMP v2c will use get_bulk for less overhead*
-p, --port=PORT | *SNMP port (default 161)*
-I , --ifmib=MIB | *Agent supports IFMIB ifXTable. Do not use if you don't know what this is.*
-V, --version | *plug in version*
-h, --help | *Usage help*

IMAP Mail check [check_imap]

This plug in tests IMAP connections with the specified host.

Usage: check_imap -H host -p port [-w warn_time] [-c crit_time] [-s send_string] [-e expect_string] [-q quit_string] [-m maxbytes] [-d delay] [-t to_sec] [-v]

Options:
-H, --host name=ADDRESS | *Host name argument for servers using host headers (use numeric address if possible to bypass DNS lookup).*
-p, --port=INTEGER | *Port number*
-s, --send=STRING | *String to send to the server*
-e, --expect=STRING | *String to expect in server response*
-q, --quit=STRING | *String to send server to initiate a clean close of the connection*
-m, --maxbytes=INTEGER | *Close connection once more than this number of bytes are received*
-d, --delay=INTEGER | *Seconds to wait between sending string and polling for response*
-w, --warning=DOUBLE | *Response time to result in warning status (seconds)*
-c, --critical=DOUBLE | *Response time to result in critical status (seconds)*
-t, --timeout=INTEGER | *Seconds before connection times out (default: 10)*
-v, --verbose | *Show details for command-line debugging (do not use with Monitor server)*
-h, --help | *Print detailed help screen*
-V, --version | *Print version information*

IRC Check [check_ircd]

Perl Check IRCD plug in for Monitor

Usage: check_ircd -H <host> [-w <warn>] [-c <crit>] [-p <port>]

Options:

-H, --host name=HOST | *Name or IP address of host to check*
-w, --warning=INTEGER | *Number of connected users which generates a warning state (Default: 50)*
-c, --critical=INTEGER | *Number of connected users which generates a critical state (Default: 100)*
-p, --port=INTEGER | *Port that the ircd daemon is running on <host> (Default: 6667)*
-v, --verbose | *Print extra debugging information*

LDAP Directory Check [check_ldap]

Checks the condition of a LDAP database.

Usage: check_ldap -H <host> -b <base_dn> [-p <port>] [-a <attr>] [-D <binddn>] [-P <password>] [-w <warn_time>] [-c <crit_time>] [-t timeout]
(Note: all times are in seconds.)

Options:
-H , --host=HOST | *host name where the LDAP database sits.*
-a , --attr=ATTR | *LDAP attribute to search (default: "(objectclass=*)"*)
-b , --base=BASE_DN | *LDAP base (eg. ou=my unit, o=my org, c=at)*
-D, --bind=BINDDN | *LDAP bind DN (if required)*
-P, --pass=PASSWORD | *LDAP password (if required)*
-p, --port=PORT | *LDAP port (default: 389)*
-w ,--warn=WARN_TIME | *Time in secs. - if the exceeds <warn> the STATE_WARNING will be returned*
-c , --crit=CRIT_TIME | *Time in secs. - if the exceeds <crit> the STATE_CRITICAL will be returned*

SYSTEM LOAD Check, LINUX [check_load]

This plug in tests the current system load average.

Usage: check_load [-w WLOAD1,WLOAD5,WLOAD15] [-c CLOAD1,CLOAD5,CLOAD15]
check_load --version
check_load --help

Options:
-w, --warning=WLOAD1,WLOAD5,WLOAD15 | *Exit with WARNING status if load average exceeds WLOADn*
-c, --critical=CLOAD1,CLOAD5,CLOAD15 | *Exit with CRITICAL status if load average exceed CLOADn*
-h, --help | *Print detailed help screen*
-V, --version | *Print version information*

the load average format is the same used by "uptime" and "w"

SYSTEM LOG Check, LINUX [check_log]

Log file pattern detector plug in for Nagios

Usage: check_log [-F logfile] [-O oldlog] [-q query]
Usage: check_log --help
Usage: check_log --version

Mail queue check, LINUX [check_mailq]

Checks the number of messages in the mail queue

Usage: check_mailq [-w <warn>] [-c <crit>] [-t <timeout>] [-v verbose]

Options:

-w ,--warning=WARN | *Min. number of messages in queue to generate warning*
-c , --critical=CRIT | *Min. number of messages in queu to generate critical alert (w < c)*
-t ,--timeout =TIMEOUT | *plug in timeout in seconds (default = 15)*
-h , --help | *Print detailed help screen*
-V , --version | *Print version information*
-v , --verbose | *Debugging output*

Statistics Module LOG Check [check_mrtg]

This plug in will check either the average or maximum value of one of the two variables recorded in an Statistics file.

Usage:

check_mrtg [-F log_file] [-a AVG | MAX] [-v variable] [-w warning] [-c critical] [-l label] [-u units] [-e expire_minutes] [-t timeout] [-v]

Options:
-F, --logfile=FILE | *The Statistics log file containing the data you want to monitor*
-e, --expires=MINUTES | *Minutes before MRTG data is considered to be too old*
-a, --aggregation=AVG|MAX | *Should we check average or maximum values?*
-v, --variable=INTEGER | *Which variable set should we inspect? 1 or 2?*
-w, --warning=INTEGER | *Threshold value for data to result in WARNING status*
-c, --critical=INTEGER | *Threshold value for data to result in CRITICAL status*
-l, --label=STRING | *Type label for data (Examples: Conns, "Processor Load", In, Out)*
-u, --units=STRING | *Option units label for data (Example: Packets/Sec, Errors/Sec, "Bytes Per Second", "% Utilization")*
-h, --help | *Print detailed help screen*
-V, --version | *Print version information*

If the value exceeds the <vwl> threshold, a WARNING status is returned. If the value exceeds the <vcl> threshold, a CRITICAL status is returned. If the data in the log file is older than <expire_minutes> old, a WARNING status is returned and a warning message is printed.

This plug in is useful for monitoring Statistics data that does not correspond to bandwidth usage. (Use the check_mrtgtraf plug in for monitoring bandwidth). It can be used to monitor any kind of data that Statistics is monitoring - errors, packets/sec, etc. I use Statistics in conjunction with the Novell NLM that allows me to track processor utilization, user connections, drive space, etc and this plug in works well for monitoring that kind of data as well.

Notes:
- This plug in only monitors one of the two variables stored in the Statistics log file. If you want to monitor both values you will have to define two
commands with different values for the <variable> argument.

UPS Service Check [check_mrtgtraf]

This plug in tests the UPS service on the specified host.

Usage: check_mrtgtraf -F <log_file> -a <AVG | MAX> -v <variable> -w <warning_pair> -c <critical_pair> [-e expire_minutes] [-t timeout] [-v]

Options:
-F, --filename=STRING | *File to read log from*
-e, --expires=INTEGER | *Minutes after which log expires*
-a, --aggregation=(AVG|MAX) | *Test average or maximum -w, --warning. Warning threshold pair "<incoming>,<outgoing>"*
-c, --critical | *Critical threshold pair "<incoming>,<outgoing>"*
-h, --help | *Print detailed help screen*
-V, --version | *Print version information*

MySQL Database Check[check_mysql]

This plug in is for testing a mysql server.

Usage: check_mysql [-d database] [-H host] [-P port] [-u user] [-p password]

There are no required arguments. By default, the local database with a server listening on MySQL standard port 3306 will be checked.

Options:
-d, --database=STRING | *Check database with indicated name*
-H, --host name=STRING or IPADDRESS | *Check server on the indicated host*
-P, --port=INTEGER | *Make connection on the indicated port*
-u, --username=STRING | *Connect using the indicated user name*
-p, --password=STRING | *Use the indicated password to authenticate the connection ==> IMPORTANT: THIS FORM OF AUTHENTICATION IS NOT SECURE!!! <== Your clear-text password will be visible as a process table entry*

-h, --help | *Print detailed help screen*
-V, --version | *Print version information*

Monitor Process Check [check_nagios]

This plug in attempts to check the status of the Nagios process on the local machine. The plug in will check to make sure the Nagios status log is no older than the number of minutes specified by the <expire_minutes> option. It also uses the /bin/ps command to check for a process matching whatever you specify
by the <process_string> argument.

Usage: check_nagios -F <status log file> -e <expire_minutes> -C <process_string>

Options:
-F, --filename=FILE | *Name of the log file to check*
-e, --expires=INTEGER | *Seconds aging after which log file is considered stale*
-C, --command=STRING | *Command to search for in process table*
-h, --help | *Print this help screen*
-V, --version | *Print version information*

Example:
./check_nagios -F /opt/monitor/var/status.log -e 5 -C /opt/monitor/bin/monitor

NNTP [check_nntp]

This plug in tests NNTP connections with the specified host.

Usage: check_nntp -H host -p port [-w warn_time] [-c crit_time] [-s send_string] [-e expect_string] [-q quit_string] [-m maxbytes] [-d delay] [-t to_sec] [-v]

Options:
-H, --host name=ADDRESS | *Host name argument for servers using host headers (use numeric address if possible to bypass DNS lookup)*.
-p, --port=INTEGER | *Port number*
-s, --send=STRING | *String to send to the server*
-e, --expect=STRING | *String to expect in server response*
-q, --quit=STRING | *String to send server to initiate a clean close of the connection*
-m, --maxbytes=INTEGER | *Close connection once more than this number of bytes are received*
-d, --delay=INTEGER | *Seconds to wait between sending string and polling for response*
-w, --warning=DOUBLE | *Response time to result in warning status (seconds)*
-c, --critical=DOUBLE | *Response time to result in critical status (seconds)*
-t, --timeout=INTEGER | *Seconds before connection times out (default: 10)*
-v, --verbose| *Show details for command-line debugging (do not use with Monitors server)*
-h, --help | *Print detailed help screen*
-V, --version | *Print version information*

Linux Remote Monitoring [check_nrpe]

Usage: check_nrpe -H <host> [-p <port>] [-t <timeout>] [-c <command>] [-a <arglist...>]

Options:
-H=HOST | *The address of the host running the NRPE daemon*
-p=PORT | *The port on which the daemon is running (default=5666)*
-t=TIMEOUT | *Number of seconds before connection times out (default=10)*
-c=COMMAND | *The name of the command that the remote daemon should run*
-a=ARGLIST | *Optional arguments that should be passed to the command. Multiple arguments should be separated by a space. If provided, this must be the last option supplied on the command line.*

Note:
This plug in requires that you have the NRPE daemon running on the remote host. You must also have configured the daemon to associate a specific plug in command with the [command]

option you are specifying here. Upon receipt of the [command] argument, the NRPE daemon will run the appropriate plug in command and send the plug in output and return code back to *this* plug in. This allows you to execute plug ins on remote hosts and 'fake' the results to make Monitor think the plug in is being run locally.

Windows Remote Monitoring [check_nt]

This plug in attempts to contact the NSClient service running on a Windows NT/2000/XP server to gather the requested system information.

Usage: check_nt -H host -v variable [-p port] [-w warning] [-c critical] [-l params] [-d SHOWALL] [-t timeout]

Options:
-H, --host name=HOST | *Name of the host to check*
-p, --port=INTEGER | *Optional port number (default: 1248)*
-s <password> | *Password needed for the request*
-v, --variable=STRING | *Variable to check. Valid variables are:*

CLIENTVERSION = Get the NSClient version
CPULOAD = Average CPU load on last x minutes. Request a -l parameter with the following syntax: -l <minutes range>,<warning threshold>,<critical threshold>. <minute range> should be less than 24*60. Thresholds are percentage and up to 10 requests can be done in one shot. ie: -l 60,90,95,120,90,95
UPTIME = Get the uptime of the machine. No specific parameters. No warning or critical threshold
USEDDISKSPACE = Size and percentage of disk use. Request a -l parameter containing the drive letter only. Warning and critical thresholds can be specified with -w and -c.
MEMUSE = Memory use. Warning and critical thresholds can be specified with -w and -c.
SERVICESTATE = Check the state of one or several services. Request a -l parameters with the following syntax: -l <service1>,<service2>,<service3>,... You can specify -d SHOWALL in case you want to see working services in the returned string.
PROCSTATE = Check if one or several process are running. Same syntax as SERVICESTATE.
COUNTER = Check any performance counter of Windows NT/2000. Request a -l parameters with the following syntax: -l "\\<performance object>\\counter","<description>" The <description> parameter is optional and is given to a printf output command which require a float parameters. Some examples: "Paging file usage is %.2f %%" or "%.f %% paging file used."
-w, --warning=INTEGER | *Threshold which will result in a warning status*
-c, --critical=INTEGER | *Threshold which will result in a critical status*
-t, --timeout=INTEGER | *Seconds before connection attempt times out (default: 10)*
-h, --help | *Print this help screen*
-V, --version | *Print version information*

Notes:
- The NSClient service should be running on the server to get any information.
- Critical thresholds should be lower than warning thresholds

Network Time Service Checks (check_ntp)

Checks the local time stamp offset versus <host> with ntpdate. Checks the jitter/dispersion of clock signal between <host> and its sys.peer with ntpq.

Usage: check_ntp -H <host> [-w <warn>] [-c <crit>] [-j <warn>] [-k <crit>] [-v verbose]

Options:

-w (--warning) | *Clock offset in seconds at which a warning message will be generated. Defaults to 60.*
-c (--critical) | *Clock offset in seconds at which a critical message will be generated. Defaults to 120.*
-j (--jwarn) | *Clock jitter in milliseconds at which a warning message will be generated. Defaults to 5000.*
-k (--jcrit) | *Clock jitter in milliseconds at which a warning message will be generated. Defaults*

to 10000.

If jitter/dispersion is specified with -j or -k and ntpq times out, then a warning is returned.

Novell Netware Remote Monitoring

This plug in attempts to contact the MRTGEXT NLM running on a Novell server to gather the requested system information.

Usage:
check_nwstat -H host [-v variable] [-w warning] [-c critical] [-p port] [-t timeout]

Options:
-H, --host name=HOST | *Name of the host to check*
-v, --variable=STRING | *Variable to check. Valid variables include:*
LOAD1 = 1 minute average CPU load
LOAD5 = 5 minute average CPU load
LOAD15 = 15 minute average CPU load
CONNS = number of currently licensed connections
VPF<vol> = percent free space on volume <vol>
VKF<vol> = KB of free space on volume <vol>
LTCH = percent long term cache hits
CBUFF = current number of cache buffers
CDBUFF = current number of dirty cache buffers
LRUM = LRU sitting time in minutes
DSDB = check to see if DS Database is open
LOGINS = check to see if logins are enabled
UPRB = used packet receive buffers
PUPRB = percent (of max) used packet receive buffers
SAPENTRIES = number of entries in the SAP table
SAPENTRIES<n> = number of entries in the SAP table for SAP type <n>
OFILES = number of open files
VPP<vol> = percent purgeable space on volume <vol>
VKP<vol> = KB of purgeable space on volume <vol>
VPNP<vol> = percent not yet purgeable space on volume <vol>
VKNP<vol> = KB of not yet purgeable space on volume <vol>
ABENDS = number of abended threads (NW 5.x only)
CSPROCS = number of current service processes (NW 5.x only)
-w, --warning=INTEGER | *Threshold which will result in a warning status*
-c, --critical=INTEGER | *Threshold which will result in a critical status*
-p, --port=INTEGER | *Optional port number (default: 9999)*
-t, --timeout=INTEGER | *Seconds before connection attempt times out (default: 10)*
-o, --osversion | *Include server version string in results*
-h, --help | *Print this help screen*
-V, --version | *Print version information*

Notes:
- This plug in requires that the MRTGEXT.NLM file from James Drews' MRTG extension for NetWare be loaded on the Novell servers you wish to check.

- Values for critical thresholds should be lower than warning thresholds when the following variables are checked: VPF, VKF, LTCH, CBUFF, and LRUM.

Oracle Database Check [check_oracle]

Check remote or local TNS status and check local Database status

Usage:
check_oracle --tns <Oracle Sid or host name/IP address>
check_oracle --db <ORACLE_SID>
check_oracle --login <ORACLE_SID>

check_oracle --cache <USER> <PASS> <INST> <CRITICAL> <WARNING>
check_oracle --tablespace <USER> <PASS> <INST> <TABLESPACE> <CRITICAL> <WARNING>
check_oracle --oranames <host name>
check_oracle --help
check_oracle --version

--tns=SID/IP Address | *Check remote TNS server*
--db=SID | *Check local database (search /bin/ps for PMON process and check file system for sgadefORACLE_SID.dbf*
--login=SID | *Attempt a dummy login and alert if not ORA-01017: invalid user name/password*
--cache | *Check local database for library and buffer cache hit ratios ---> Requires Oracle user/password and SID specified. ---> Requires select on v_ and v_*
--tablespace | *Check local database for tablespace capacity in ORACLE_SID ---> Requires Oracle user/password specified. ---> Requires select on dba_data_files and dba_free_space*
--oranames=host name | *Check remote Oracle Names server*
--help | *Print this help screen*
--version | *Print version and license information*

If the plug in doesn't work, check that the ORACLE_HOME environment variable is set, that ORACLE_HOME/bin is in your PATH, and the tnsnames.ora file is locatable and is properly configured.

When checking Local Database status your ORACLE_SID is case sensitive.

If you want to use a default Oracle home, add in your oratab file:
*:/opt/app/oracle/product/7.3.4:N

Over-CR System Information Collector, Unix [check_overcr]

This plug in attempts to contact the Over-CR collector daemon running on the remote UNIX server in order to gather the requested system information. This
plug in requires that Eric Molitors' Over-CR collector daemon be running on the remote server.
Over-CR can be downloaded from ttp://www.molitor.org/overcr
(This plug in was tested with version 0.99.53 of the Over-CR collector)

Usage: check_overcr -H host [-p port] [-v variable] [-w warning] [-c critical] [-t timeout]

Options:
-H, --host name=HOST | *Name of the host to check*
-p, --port=INTEGER | *Optional port number (default: 2000)*
-v, --variable=STRING | *Variable to check. Valid variables include:*
LOAD1 = 1 minute average CPU load
LOAD5 = 5 minute average CPU load
LOAD15 = 15 minute average CPU load
DPU<filesys> = percent used disk space on filesystem <filesys>
PROC<process> = number of running processes with name <process>
NET<port> = number of active connections on TCP port <port>
UPTIME = system uptime in seconds
-w, --warning=INTEGER | *Threshold which will result in a warning status*
-c, --critical=INTEGER | *Threshold which will result in a critical status*
-t, --timeout=INTEGER | *Seconds before connection attempt times out (default: 10)*
-h, --help | *Print this help screen*
-V, --version | *Print version information*

Notes:
- For the available options, the critical threshold value should always be higher than the warning threshold value, EXCEPT with the uptime variable (i.e. lower uptime is worse).

PostGres SQL Database Check [check_pgsql]

Tests to see if a PostgreSQL DBMS is accepting connections.

Usage:

```
check_pgsql [-c critical_time] [-w warning_time] [-t timeout] [-H host] [-P port] [-d database]
[-l logname] [-p password]
```

Options:
-c, --critical=INTEGER
Exit STATE_CRITICAL if connection time exceeds threshold (default: 2)
-w, --warning=INTEGER
Exit STATE_WARNING if connection time exceeds threshold (default: 8)
-t, --timeout=INTEGER
Terminate test if timeout limit is exceeded (default: 30)
-H, --host name=STRING
Name or numeric IP address of machine running back end
-P, --port=INTEGER
Port running back end (default: 5432)
-d, --database=STRING
Database to check (default: template1)
-l, --logname = STRING
Login name of user
-p, --password = STRING
Password (BIG SECURITY ISSUE)

All parameters are optional.

This plug in tests a PostgreSQL DBMS to determine whether it is active and accepting queries. In its current operation, it simply connects to the specified database, and then disconnects. If no database is specified, it connects to the template1 database, which is present in every functioning PostgreSQL DBMS.

The plug in will connect to a local postmaster if no host is specified. To connect to a remote host, be sure that the remote postmaster accepts TCP/IP connections (start the postmaster with the -i option).

Typically, the nagios user (unless the --logname option is used) should be able to connect to the database without a password. The plug in can also send a password, but no effort is made to obscure or encrypt the password.

Ping, Connection Statistics Checks [check_ping]

Use ping to check connection statistics for a remote host.

Usage:

```
check_ping -H <host_address> -w <wrta>,<wpl>%% -c <crta>,<cpl>%% [-p packets] [-t
timeout] [-L]
```

Options:
-H, --host name=HOST
host to ping
-w, --warning=THRESHOLD
warning threshold pair
-c, --critical=THRESHOLD
critical threshold pair
-p, --packets=INTEGER
number of ICMP ECHO packets to send (Default: 5)
-t, --timeout=INTEGER
optional specified timeout in second (Default: 10)
-L, --link
show HTML in the plug in output (obsoleted by urlize)
THRESHOLD is <rta>,<pl>% where <rta> is the round trip average travel time (ms) which triggers a WARNING or CRITICAL state, and <pl> is the percentage of packet loss to trigger an

alarm state.

This plug in uses the ping command to probe the specified host for packet loss (percentage) and round trip average (milliseconds).

POP Email Service Check [check_pop]

This plug in tests POP connections with the specified host.

Usage: check_pop -H host -p port [-w warn_time] [-c crit_time] [-s send_string] [-e expect_string] [-q quit_string] [-m maxbytes] [-d delay] [-t to_sec] [-v]

Options:
-H, --host name=ADDRESS
Host name argument for servers using host headers (use numeric
address if possible to bypass DNS lookup).
-p, --port=INTEGER
Port number
-s, --send=STRING
String to send to the server
-e, --expect=STRING
String to expect in server response
-q, --quit=STRING
String to send server to initiate a clean close of the connection
-m, --maxbytes=INTEGER
Close connection once more than this number of bytes are received
-d, --delay=INTEGER
Seconds to wait between sending string and polling for response
-w, --warning=DOUBLE
Response time to result in warning status (seconds)
-c, --critical=DOUBLE
Response time to result in critical status (seconds)
-t, --timeout=INTEGER
Seconds before connection times out (default: 10)
-v, --verbose Show details for command-line debugging (do not use with nagios server)
-h, --help
Print detailed help screen
-V, --version
Print version information

Process Amount Checks, Linux [check_procs]

Check the number of currently running processes and generates WARNING or CRITICAL states if the process count is outside the specified threshold ranges. The process count can be filtered by process owner, parent process PID, current state (e.g., 'Z'), or may be the total number of running processes

Usage:
check_procs -w <range> -c <range> [-s state] [-p ppid] [-u user] [-a argument-array] [-C command]

Required Arguments:
-w, --warning=RANGE
generate warning state if process count is outside this range
-c, --critical=RANGE
generate critical state if process count is outside this range

Optional Filters:
-s, --state=STATUSFLAGS
Only scan for processes that have, in the output of `ps`, one or

more of the status flags you specify (for example R, Z, S, RS,
RSZDT, plus others based on the output of your 'ps' command).
-p, --ppid=PPID
Only scan for children of the parent process ID indicated.
-u, --user=USER
Only scan for processes with user name or ID indicated.
-a, --argument-array=STRING
Only scan for processes with args that contain STRING.
-C, --command=COMMAND
Only scan for exact matches to the named COMMAND.

RANGEs are specified 'min:max' or 'min:' or ':max' (or 'max'). If specified 'max:min', a warning status will be generated if the count is inside the specified range

Radius, Remote Authentications Server Checks [check_radius]

Tests to see if a radius server is accepting connections.

Usage:
check_radius -H host -F config_file -u username -p password' [-P port] [-t timeout] [-r retries] [-e expect]

Options:
-H, --host name=HOST
Host name argument for servers using host headers (use numeric
address if possible to bypass DNS lookup).
-P, --port=INTEGER
Port number (default: 1645)
-u, --username=STRING
The user to authenticate
-p, --password=STRING
Password for autentication (SECURITY RISK)
-F, --filename=STRING
Configuration file
-e, --expect=STRING
Response string to expect from the server
-r, --retries=INTEGER
Number of times to retry a failed connection
-t, --timeout=INTEGER
Seconds before connection times out (default: 10)
-v, --verbose
Show details for command-line debugging (do not use with nagios server)
-h, --help
Print detailed help screen
-V, --version
Print version information

The server to test must be specified in the invocation, as well as a user name and password. A configuration file may also be present. The format of the configuration file is described in the radius client library sources.

The password option presents a substantial security issue because the password can be determined by careful watching of the command line in a process listing. This risk is exacerbated because Monitor will run the plug in at regular predictable intervals. Please be sure that the password used does not allow access to sensitive system resources, otherwise compromise could occur.

Real Service Check [check_real]

This plug in tests the REAL service on the specified host.

Usage: check_real -H host [-e expect] [-p port] [-w warn] [-c crit] [-t timeout] [-v]

Options:

-H, --host name=STRING or IPADDRESS
Check this server on the indicated host
-I, --IPaddress=STRING or IPADDRESS
Check server at this host address
-p, --port=INTEGER
Make connection on the indicated port (default: 554)
-u, --url=STRING
Connect to this url
-e, --expect=STRING
String to expect in first line of server response (default: RTSP/1.)
-w, --warning=INTEGER
Seconds necessary to result in a warning status
-c, --critical=INTEGER
Seconds necessary to result in a critical status
-t, --timeout=INTEGER
Seconds before connection attempt times out (default: 10)
-v, --verbose
Print extra information (command-line use only)
-h, --help
Print detailed help screen
-V, --version
Print version information

RPC, Remote Procedure Call Check [check_rpc]

Check if a rpc service is registered and running using rpcinfo -H host -C rpc_command

Usage:
check_rpc -H host -C rpc_command [-p port] [-c program_version] [-u|-t] [-v]

-H <host> The server providing the rpc service
-C <rpc_command> The program name (or number).
-c <program_version> The version you want to check for (one or more) Should prevent checks of unknown versions being syslogged e.g. 2,3,6 to check v2, v3, and v6
-u | -t Test UDP or TCP
-v Verbose - will print supported programs and numbers

Sensor Hardware Status Check [check_sensors]

This plug in checks hardware status using the lm_sensors package.

Usage: check_sensors

SIMAP Service Checks [check_simap]

This plug in tests SIMAP connections with the specified host.

Usage: check_simap -H host -p port [-w warn_time] [-c crit_time] [-s send_string] [-e expect_string] [-q quit_string] [-m maxbytes] [-d delay] [-t to_sec] [-v]

Options:
-H, --host name=ADDRESS
Host name argument for servers using host headers (use numeric
address if possible to bypass DNS lookup).
-p, --port=INTEGER
Port number
-s, --send=STRING
String to send to the server
-e, --expect=STRING
String to expect in server response

-q, --quit=STRING
String to send server to initiate a clean close of the connection
-m, --maxbytes=INTEGER
Close connection once more than this number of bytes are received
-d, --delay=INTEGER
Seconds to wait between sending string and polling for response
-w, --warning=DOUBLE
Response time to result in warning status (seconds)
-c, --critical=DOUBLE
Response time to result in critical status (seconds)
-t, --timeout=INTEGER
Seconds before connection times out (default: 10)
-v, --verbose Show details for command-line debugging (do not use with nagios server)
-h, --help
Print detailed help screen
-V, --version
Print version information

SMTP Mail Service Check [check_smtp]

This plug in test the SMTP service on the specified host.

Usage: check_smtp -H host [-e expect] [-p port] [-f from addr] [-w warn] [-c crit] [-t timeout] [-v]

Options:
-H, --host name=STRING or IPADDRESS
Check server on the indicated host
-p, --port=INTEGER
Make connection on the indicated port (default: 25)
-e, --expect=STRING
String to expect in first line of server response (default: 220)
-f, --from=STRING
from address to include in MAIL command (default NULL, Exchange2000 requires one)
-w, --warning=INTEGER
Seconds necessary to result in a warning status
-c, --critical=INTEGER
Seconds necessary to result in a critical status
-t, --timeout=INTEGER
Seconds before connection attempt times out (default: 10)
-v, --verbose
Print extra information (command-line use only)
-h, --help
Print detailed help screen
-V, --version
Print version information

SNMP, Remote Network Management Check [check_snmp]

Check status of remote machines using SNMP.

Usage:
check_snmp -H <ip_address> -o <OID> [-w warn_range] [-c crit_range]
[-C community] [-s string] [-r regex] [-R regexi] [-t timeout]
[-l label] [-u units] [-p port-number] [-d delimiter]
[-D output-delimiter] [-m miblist] [-P snmp version]
[-L seclevel] [-U secname] [-a authproto] [-A authpasswd]
[-X privpasswd]

```
check_snmp (-h | --help) for detailed help
check_snmp (-V | --version) for version information

Options:
-H, --host name=HOST
Name or IP address of the device you wish to query
-o, --oid=OID(s)
Object identifier(s) whose value you wish to query
-w, --warning=INTEGER_RANGE(s)
Range(s) which will not result in a WARNING status
-c, --critical=INTEGER_RANGE(s)
Range(s) which will not result in a CRITICAL status
-C, --community=STRING
Optional community string for SNMP communication
(default is "public")
-u, --units=STRING
Units label(s) for output data (e.g., 'sec.').
-p, --port=STRING
UDP port number target is listening on. Default is "161"
-P, --protocol=[1|3]
SNMP protocol version
-L, --seclevel=[noAuthNoPriv|authNoPriv|authPriv]
SNMPv3 security Level
-U, --secname=USERNAME
SNMPv3 username
-a, --authproto=[MD5|SHA]
SNMPv3 auth proto
-A, --authpassword=PASSWORD
SNMPv3 authentication password
-X, --privpasswd=PASSWORD
SNMPv3 crypt passwd (DES)
-d, --delimiter=STRING
Delimiter to use when parsing returned data. Default is "="
Any data on the right hand side of the delimiter is considered
to be the data that should be used in the evaluation.
-t, --timeout=INTEGER
Seconds to wait before plug in times out (see also nagios server timeout).
Default is 10 seconds
-D, --output-delimiter=STRING
Separates output on multiple OID requests
-s, --string=STRING
Return OK state (for that OID) if STRING is an exact match
-r, --ereg=REGEX
Return OK state (for that OID) if extended regular expression REGEX matches
-R, --eregi=REGEX
Return OK state (for that OID) if case-insensitive extended REGEX matches
-l, --label=STRING
Prefix label for output from plug in (default -s 'SNMP')
-v, --verbose
Debugging the output
-m, --miblist=STRING
List of MIBS to be loaded (default = ALL)

This plug in gets system information on a remote server via snmp.

- This plug in uses the 'snmpget' command included with the NET-SNMP package.
- Multiple OIDs may be indicated by a comma- or space-delimited list (lists with internal
spaces must be quoted) [max 8 OIDs]
- Ranges are inclusive and are indicated with colons. When specified as 'min:max' a STATE_OK
will be returned if the result is within the indicated
```

range or is equal to the upper or lower bound. A non-OK state will be returned if the result is outside the specified range.
- If specified in the order 'max:min' a non-OK state will be returned if the result is within the (inclusive) range.
- Upper or lower bounds may be omitted to skip checking the respective limit.
- Bare integers are interpreted as upper limits.
- When checking multiple OIDs, separate ranges by commas like '-w 1:10,1:,:20'
- Note that only one string and one regex may be checked at present
- All evaluation methods other than PR, STR, and SUBSTR expect that the value returned from the SNMP query is an unsigned integer.

SPOP Service Check [check_spop]

This plug in tests SPOP connections with the specified host.

Usage: check_spop -H host -p port [-w warn_time] [-c crit_time] [-s send_string] [-e expect_string] [-q quit_string] [-m maxbytes] [-d delay] [-t to_sec] [-v]

Options:
-H, --host name=ADDRESS
Host name argument for servers using host headers (use numeric
address if possible to bypass DNS lookup).
-p, --port=INTEGER
Port number
-s, --send=STRING
String to send to the server
-e, --expect=STRING
String to expect in server response
-q, --quit=STRING
String to send server to initiate a clean close of the connection
-m, --maxbytes=INTEGER
Close connection once more than this number of bytes are received
-d, --delay=INTEGER
Seconds to wait between sending string and polling for response
-w, --warning=DOUBLE
Response time to result in warning status (seconds)
-c, --critical=DOUBLE
Response time to result in critical status (seconds)
-t, --timeout=INTEGER
Seconds before connection times out (default: 10)
-v, --verbose Show details for command-line debugging (do not use with nagios server)
-h, --help
Print detailed help screen
-V, --version
Print version information

SSH, Secure Shell Check [check_ssh]

Checks the availability of SSH service on a host.

Usage:
check_ssh -t [timeout] -p [port] <host>
check_ssh -V prints version info
check_ssh -h prints more detailed help
by default, port is 22

Swap Space Check, Linux [check_swap]

Check swap space on local server.

Usage:

check_swap [-a] -w <used_percentage>% -c <used_percentage>%
check_swap [-a] -w <bytes_free> -c <bytes_free>
check_swap (-h | --help) for detailed help
check_swap (-V | --version) for version information

Options:
-w, --warning=INTEGER
Exit with WARNING status if less than INTEGER bytes of swap space are free
-w, --warning=PERCENT%
Exit with WARNING status if more than PERCENT of swap space has been used
-c, --critical=INTEGER
Exit with CRITICAL status if less than INTEGER bytes of swap space are free
-c, --critical=PERCENT%
Exit with CRITCAL status if more than PERCENT of swap space has been used
-a, --allswaps
Conduct comparisons for all swap partitions, one by one
-h, --help
Print detailed help screen
-V, --version
Print version information

TCP Connection Check [check_tcp]

This plug in tests TCP connections with the specified host.

Usage: check_tcp -H host -p port [-w warn_time] [-c crit_time] [-s send_string] [-e expect_string] [-q quit_string] [-m maxbytes] [-d delay] [-t to_sec] [-v]

Options:
-H, --host name=ADDRESS
Host name argument for servers using host headers (use numeric
address if possible to bypass DNS lookup).
-p, --port=INTEGER
Port number
-s, --send=STRING
String to send to the server
-e, --expect=STRING
String to expect in server response
-q, --quit=STRING
String to send server to initiate a clean close of the connection
-m, --maxbytes=INTEGER
Close connection once more than this number of bytes are received
-d, --delay=INTEGER
Seconds to wait between sending string and polling for response
-w, --warning=DOUBLE
Response time to result in warning status (seconds)
-c, --critical=DOUBLE
Response time to result in critical status (seconds)
-t, --timeout=INTEGER
Seconds before connection times out (default: 10)
-v, --verbose Show details for command-line debugging (do not use with nagios server)
-h, --help
Print detailed help screen
-V, --version
Print version information

Temperature Checks using Temptrax Model E [check_temptraxe]

Usage: ./check_temptraxe -H <host> -p <probe_num> -w <warn_temp> -c <crit_temp> [--invert] [--Celsius | --Fahrenheit]

Options:

-H <host> = IP address of TempTrax Model E
-p <probe_num> = Probe number to check (1-16)
-w <warn_temp> = Warning temperature threshold
-c <crit_temp> = Critical temperature threshold
--invert = Invert normal temp threshold checking, so that colder temperatures are more critical that warmer ones
--Celsius = Temp thresholds are specified in degrees Celsius
--Fahrenheit = Temp thresholds are specified in degrees Fahrenheit (default)

Notes:

This plug in is designed to check temperature readings of probes attached to TempTrax Model E devices (4-, 8-, or 16-port models). More information on TempTrax devices can be found at http://www.sensatronics.com

Time Check [check_time]

Check time on the specified host.

Usage:
check_time -H <host_address> [-p port] [-w variance] [-c variance]
[-W connect_time] [-C connect_time] [-t timeout]
check_time (-h | --help) for detailed help
check_time (-V | --version) for version information

Options:
-H, --host name=ADDRESS
Host name argument for servers using host headers (use numeric address if possible to bypass DNS lookup).
-w, --warning-variance=INTEGER
Time difference (sec.) necessary to result in a warning status
-c, --critical-variance=INTEGER
Time difference (sec.) necessary to result in a critical status
-W, --warning-connect=INTEGER
Response time (sec.) necessary to result in warning status
-C, --critical-connect=INTEGER
Response time (sec.) necessary to result in critical status
-t, --timeout=INTEGER
Seconds before connection times out (default: 10)
-p, --port=INTEGER
Port number (default: 37)
-h, --help
Print detailed help screen
-V, --version
Print version information

Bandwidth Usage Checks [check_traffic]

Usage: check_traffic -H host -i if_number -b if_max_speed [-r if_description] [-w warn] [-c crit]

Options:
-H --host STRING or IPADDRESS
Check interface on the indicated host.
-i --interface INTEGER
Interface number assigned by SNMP agent.
-b --bps INTEGER
Interface maximum speed in bytes per second.
-r --rrd STRING

Interface description used to store values in correct RRD file.
-w --warning INTEGER
% of bandwidth usage necessary to result in warning status
-c --critical INTEGER
% of bandwidth usage necessary to result in critical status

UDP Connection Check [check_udp]

This plug in tests an UDP connection with the specified host.

Usage: check_udp -H <host_address> [-p port] [-w warn_time] [-c crit_time] [-e expect] [-s send] [-t to_sec] [-v]

Options:
-H, --host name=ADDRESS
Host name argument for servers using host headers (use numeric address if possible to bypass DNS lookup).
-p, --port=INTEGER
Port number
-e, --expect=STRING <optional>
String to expect in first line of server response
-s, --send=STRING <optional>
String to send to the server when initiating the connection
-w, --warning=INTEGER <optional>
Response time to result in warning status (seconds)
-c, --critical=INTEGER <optional>
Response time to result in critical status (seconds)
-t, --timeout=INTEGER <optional>
Seconds before connection times out (default: 10)
-v, --verbose <optional>
Show details for command-line debugging (do not use with nagios server)
-h, --help
Print detailed help screen and exit
-V, --version
Print version information and exit

UPS Service Check [check_ups]

This plug in tests the UPS service on the specified host. Network UPS Tools for www.exploits.org must be running for this plug in to work.

Usage: check_ups -H host [-e expect] [-p port] [-w warn] [-c crit] [-t timeout] [-v]

Options:
-H, --host name=STRING or IPADDRESS
Check server on the indicated host
-p, --port=INTEGER
Make connection on the indicated port (default: 3493)
-u, --ups=STRING
Name of UPS
-w, --warning=INTEGER
Seconds necessary to result in a warning status
-c, --critical=INTEGER
Seconds necessary to result in a critical status
-t, --timeout=INTEGER
Seconds before connection attempt times out (default: 10)
-v, --verbose
Print extra information (command-line use only)
-h, --help
Print detailed help screen

-V, --version
Print version information

User Amount Logged In, Linux [check_users]

This plug in checks the number of users currently logged in on the local system and generates an error if the number exceeds the thresholds specified.

Usage: check_users -w <users> -c <users>

Options:
-w, --warning=INTEGER
Set WARNING status if more than INTEGER users are logged in
-c, --critical=INTEGER
Set CRITICAL status if more than INTEGER users are logged in
-h, --help
Print detailed help screen
-V, --version
Print version information

Image size Check, Linux [check_vsz]

This plug in checks the image size of a running program and returns an error if the number is above either of the thresholds given.

Usage: check_vsz -w <wsize> -c <csize> [-C command]

Options:
-h, --help
Print detailed help
-V, --version
Print version numbers and license information
-w, --warning=INTEGER
Program image size necessary to cause a WARNING state
-c, --critical=INTEGER
Program image size necessary to cause a CRITICAL state
-C, --command=STRING
Program to search for [optional]

Wave Check [check_wave]

Usage: check_wave -H <host> [-w <warn>] [-c <crit>]

<warn> = Signal strength at which a warning message will be generated.
<crit> = Signal strength at which a critical message will be generated.

plug in Status Negator [negate]

Negates the status of a plug in (returns OK for CRITICAL, and vice-versa).

Usage:
negate [-t timeout] <definition of wrapped plug in>
negate (-h | --help) for detailed help
negate (-V | --version) for version information

Options:
-t, --timeout=INTEGER
Terminate test if timeout limit is exceeded (default: 9)
[keep this less than the plug in timeout to retain CRITICAL status]

This plug in is a wrapper to take the output of another plug in and invert it. If the wrapped plug in returns STATE_OK, the wrapper will return STATE_CRITICAL. If the wrapped plug in returns STATE_CRITICAL, the wrapper will return STATE_OK. Otherwise, the output state of the wrapped plug in is unchanged.

plug in HTML Wrapper [urlize]

This plug in wraps the text output of another command (plug in) in HTML <A> tags, thus displaying the plug in output in as a clickable link in the Monitor status screen. The return status is the same as the invoked plug in.

Usage:
./urlize <url> <plug in> <arg1> ... <argN>

Pay close attention to quoting to ensure that the shell passes the expected data to the plug in. For example, in:

```
urlize http://example.com/ check_http -H example.com -r 'two words'
```

the shell will remove the single quotes and urlize will see:

```
urlize http://example.com/ check_http -H example.com -r two words
```

You probably want:

```
urlize http://example.com/ "check_http -H example.com -r 'two words'"
```