Users Manual

OP5 Monitor 2.4
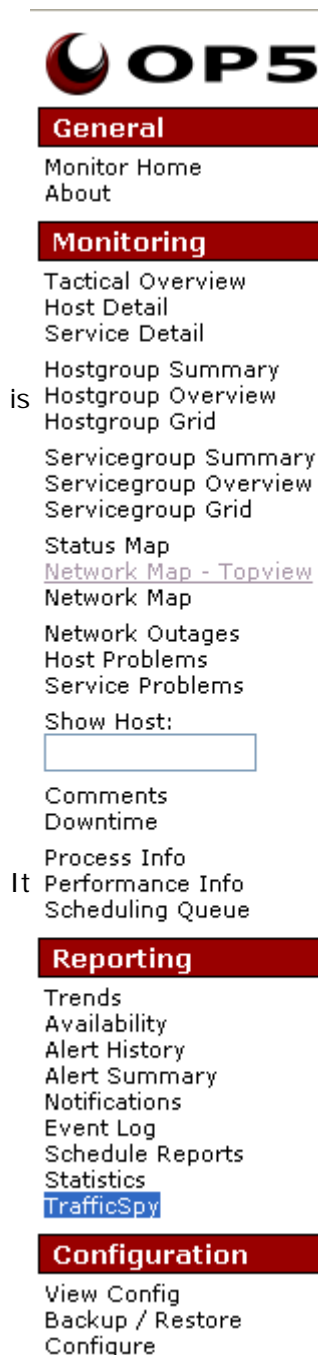
Table of Contents

Who is this manual for?

This manual is targeted for a technical audience. The manual covers the users side of OP5 Monitor. For reference using the SSH interface, see the OP5 System manual.

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 four sections, 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 related to configuration of the system. The web user interface enables you to handle the whole OP5 Monitor system from a single point.
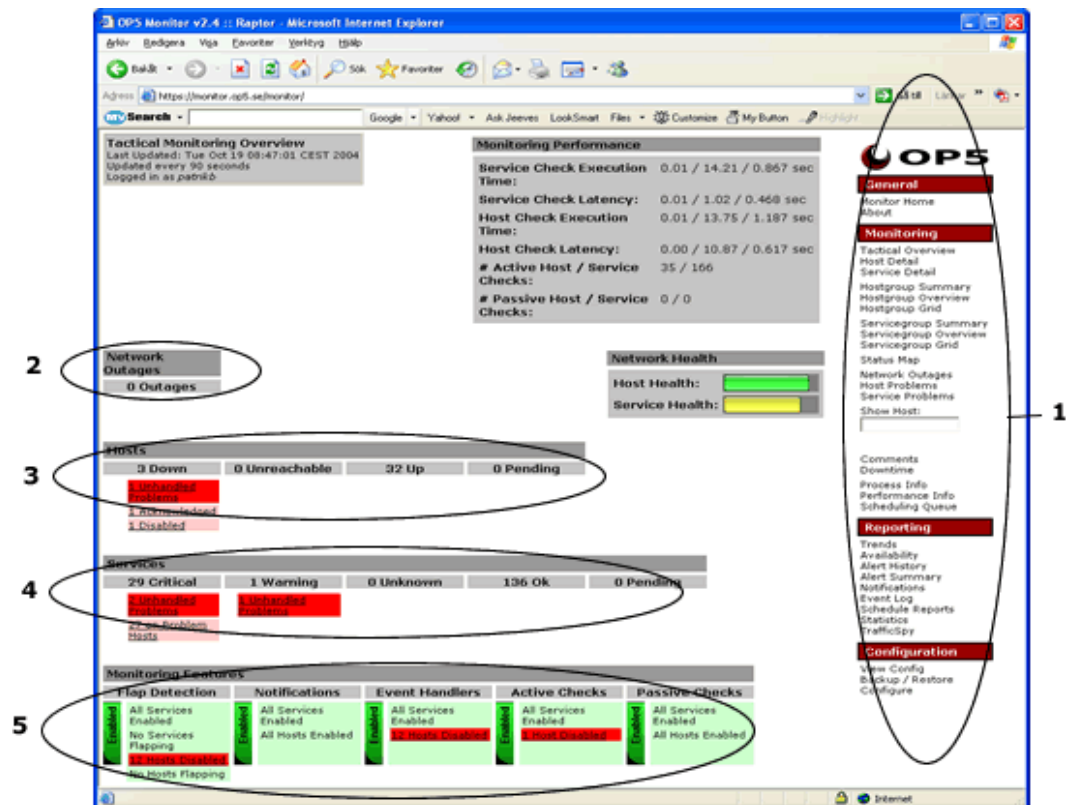
Lets go through the main menu choices.

Show Host

is now possible to search for host by typing the initial letters of the host name in the field that says "show host" in the main menu. A new window showing host and it's services detail will be shown.

Tactical Overview

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

1. Main Menu, The main menu is accessible at all times no matter what window your in. This enables you make choices faster.
2. Outages, shows if a central host is faulty and causing 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.
3. 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.
4. 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 mis configured.
   4. Ok, the service is working fine.
   5. Pending, the service has not been checked yet. The check is queued about to be executed.
5. 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 high frequency, 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 abillity to receive results from the outside where the check initially was not performed by Monitor. An example is SNMP traps which are sent from a host. This menu choice enables to enable or disable the reception of these checks.

Overall Health, gives you an overall health view. The bars represent a percentage view of the status in the network.

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.
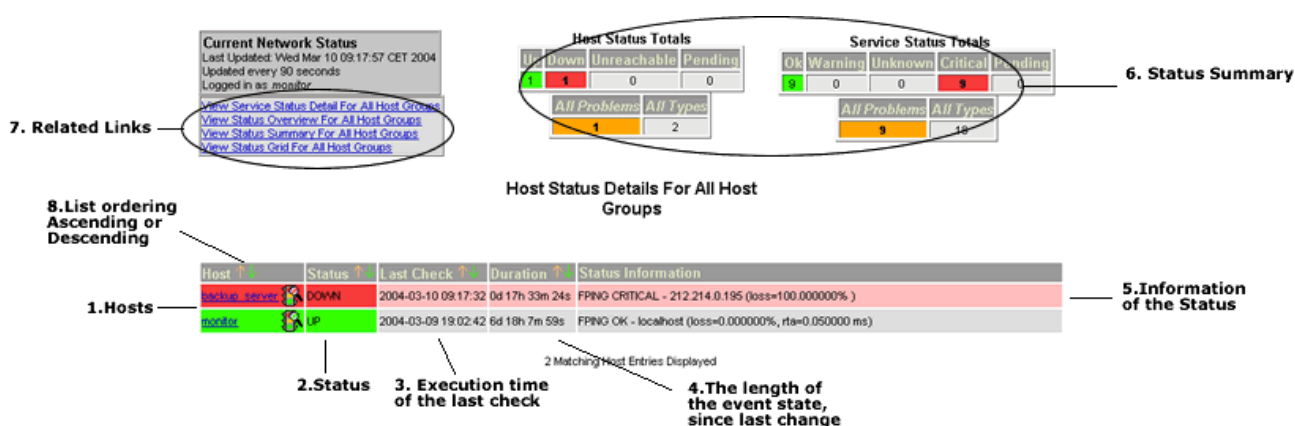
1. Hosts. Shows you the name of the host. This is the name configured for a certain host or service.

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.

The meaning of the icons in the detail lists:

Management links, used to manage the host. SSH, Telnet, HTTP etc. Configured in the web configuration tool.

Comment. The host or service has comments attached to it.

Acknowledged. The host or service problem has been acknowledged. The host or service alarms will not be notified.

If you click this icon you'll get to the notes/documentation for the selected host. This need to be configured in the web configuration tool for hosts.

Status icon. When clicked you see the host and service status of the selected host.
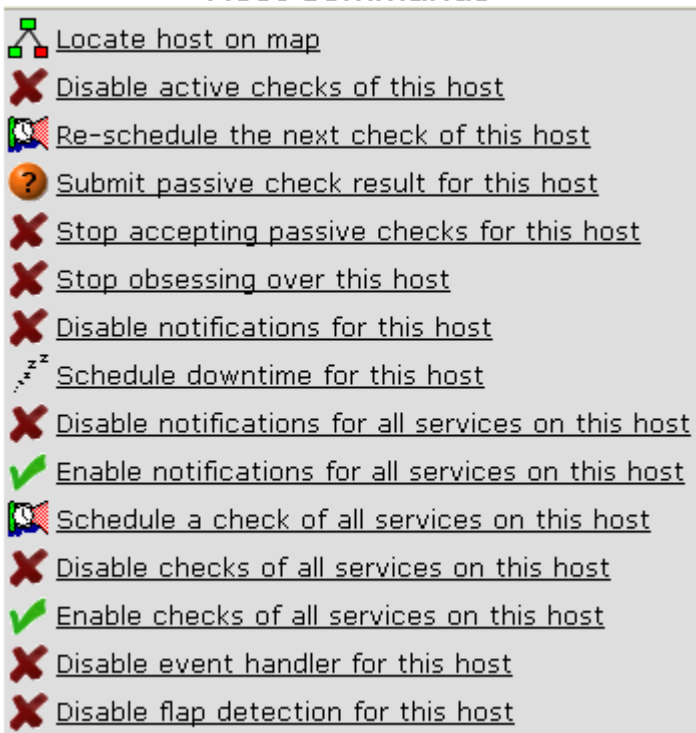
Status map icon. When clicked, it shows you the host on the status map.

Host Commands

When clicking a host in the service or host detail window you'll have the opportunity to run host commands.

Host Commands

- Locate host on map
- Disable active checks of this host
- Re-schedule the next check of this host
- Submit passive check result for this host
- Stop accepting passive checks for this host
- Stop obsessing over this host
- Disable notifications for this host
- Schedule downtime for this host
- Disable notifications for all services on this host
- Enable notifications for all services on this host
- Schedule a check of all services on this host
- Disable checks of all services on this host
- Enable checks of all services on this host
- Disable event handler for this host
- Disable flap detection for this host

Locate host on map: Link to status map.

Disable active checks for this host: This command is used to temporarily prevent Monitor from actively checking the status of a particular host. If Monitor needs to check the status of

this host, it will assume that it is in the same state that it was in before checks were disabled.

Re-schedule the next check for this host: This command is used to schedule the next check of a particular host. Monitor will re-queue the host to be checked at the time you specify. If you select the force check option, Monitor will force a check of the host regardless of both what time the scheduled check occurs and whether or not checks are enabled for the host.

Submit passive check result for this host: This command is used to submit a passive check result for a particular host. It can for example be used to clear the state on a passive service.

Stop accepting passive checks for this host: This command is used to stop Monitor from accepting passive host check results that it finds in the external command file for a particular host. All passive check results that are found for this host will be ignored.

Stop obsessing over this host: This command is used to stop Monitor from obsessing over a particular host.

Disable notifications for this host: This command is used to prevent notifications from being sent out for the specified host. You will have to re-enable notifications for this host before any alerts can be sent out in the future. Note that this command does not disable notifications for services associated with this host.

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

Disable notifications for all services on this host: This command is used to prevent notifications from being sent out for all services on the specified host. You will have to re-enable notifications for all services associated with this host before any alerts can be sent out in the future. This does not prevent notifications from being sent out about the host unless you check the 'Disable for host too' option.

Enable notifications for all services on this host: This command is used to enable notifications for all services on the specified host. Notifications will only be sent out for the service state types you defined in your service definition. This does not enable notifications for the host unless you check the 'Enable for host too' option.

Schedule a check for all service on this host: This command is used to scheduled the next check of all services on the specified host. If you select the force check option, Monitor will force a check of all services on the host regardless of both what time the scheduled checks occur and whether or not checks are enabled for those services.

Disable checks of all services on this host: This command is used to disable active checks of all services associated with the specified host. When a service is disabled Monitor will not monitor the service. Doing this will prevent any notifications being sent out for the specified service while it is disabled. In order to have Monitor check the service in the future you will have to re-enable the service. Note that disabling service checks may not necessarily prevent notifications from being sent out about the host which those services are associated with. This does not disable checks of the host unless you check the 'Disable for host too' option.

Enable checks of all services on this host: This command is used to enable active checks of all services associated with the specified host. This does not enable checks of the host unless you check the 'Enable for host too' option.
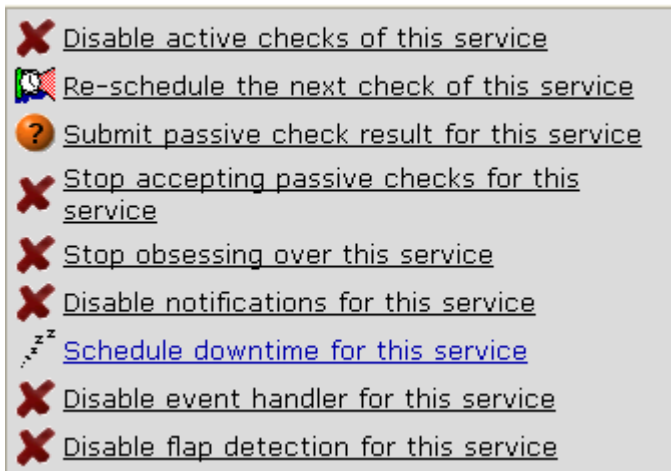
Disable event handler for this host: This command is used to temporarily prevent Monitor from running the host event handler for a particular host.

Disable flap detection for this host: This command is used to disable flap detection for a

specific host.

When choosing a service in the service detail or service problem window, you have the ability to run service commands:

Service Commands

- ❌ Disable active checks of this service
- 📅 Re-schedule the next check of this service
- ❓ Submit passive check result for this service
- ❌ Stop accepting passive checks for this service
- ❌ Stop obsessing over this service
- ❌ Disable notifications for this service
- 💤 Schedule downtime for this service
- ❌ Disable event handler for this service
- ❌ Disable flap detection for this service

See the host commands description to understand the choices.

Host group Detail, Grid, 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).
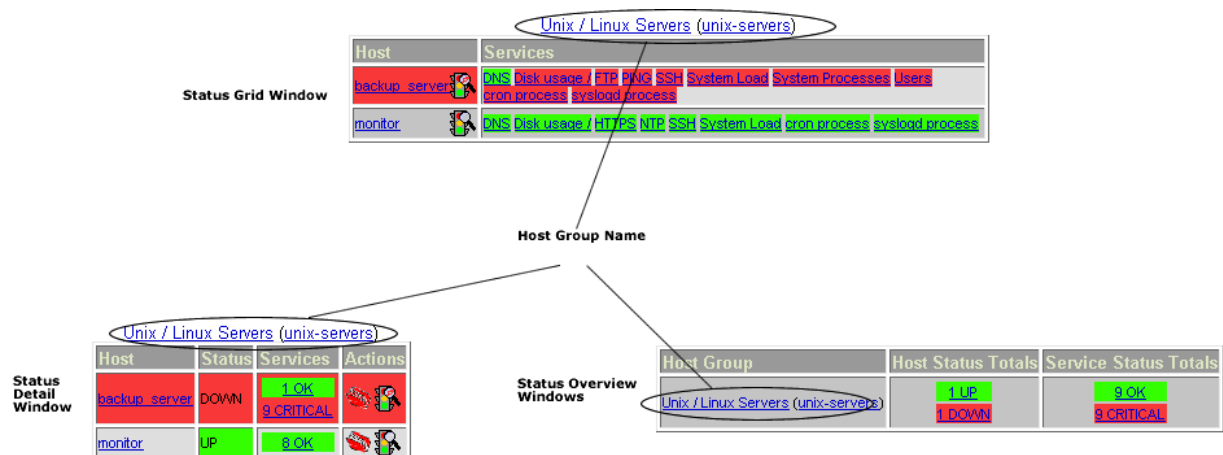
Grid Window

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.

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.

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.

Service group Detail, Grid, Summary

These three windows gives you a Status view of the network where the hosts and services are grouped into service groups. Service groups is a way of grouping services 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 functional instances, like e-shop, administration. The administrators for these functions can then utilize the Status windows and only see their portion of the network (hosts and services and their status). Furthermore they are able to extract availability reports on the groups.

Grid Window

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

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.

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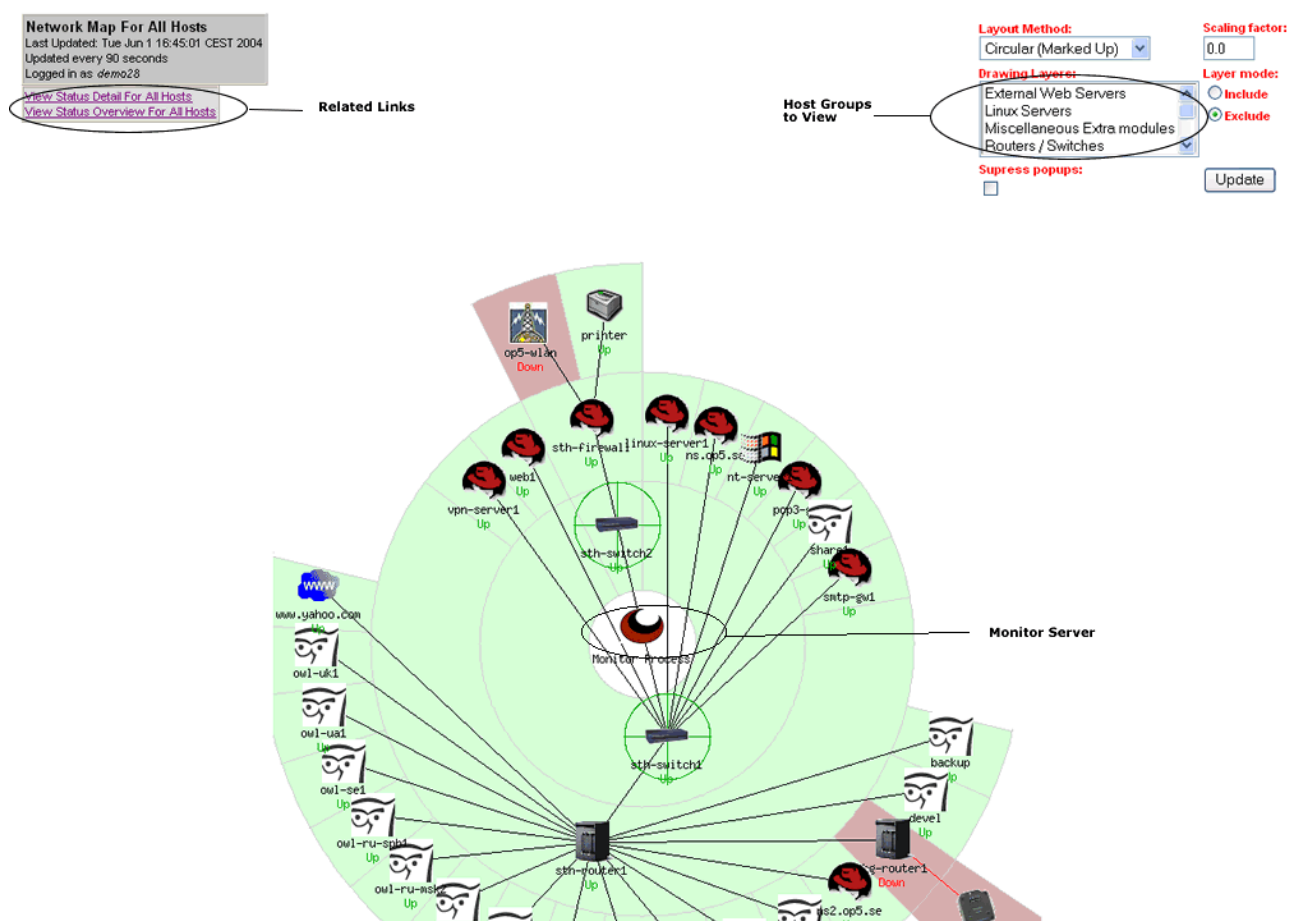
Furthermore the Status Map can be configured with a background to show a map as an example. All the icons enables you to find your hosts quickly further pinpoint the location of the problem. The icons can be replaced by your choice.

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.

Network Map

The network map is an enhanced version of the status map. From version 2.4 it is possible to move around and configure the layout of the network map.
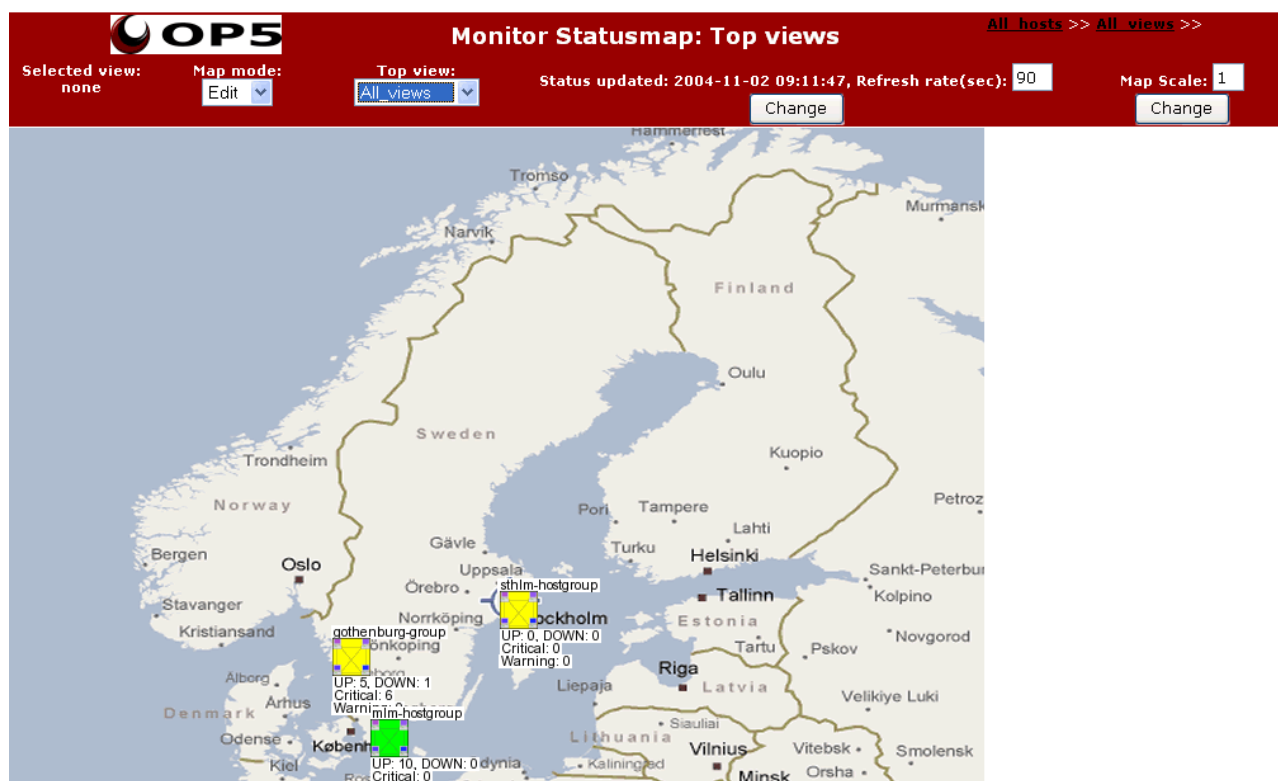
The picture above shows you the layout of the network map including three host groups. The host groups shows you a mirror of the status of the hosts and the services contained in the host groups. The network map can be in two states, edit and view. The view state is basically a view and move around state, whilst the edit state lets you change backgrounds and move the group and host icons. It is possible to have different views containing a unique layout for each view. To get to the top view or move around in the hierarchy of the views click on the top right hand of the window, marked with black text that says "all hosts >> all views". You can also select the top view by choosing the view in the selection tab "Top View". By default the window is updated every 90 seconds. Click "Change" to change the value to a different one. To change the size of the map, choose the scaling factor in the "Map scale" bar. 1 is a 100% 0.5 is 50% size etc.

When entering "edit" mode" the bottom of the window extracts to show a the configurations that can be made. From here you can upload new background. The network map can only

show png files. The uploaded files are listed in on the right hand side of the configuration window that says "Change background". To change the background, choose your uploaded file The field and click "change". Top Views in Top view lets you choose which View you want to be visible in the top view. To select host groups to be viewed in your view, select the hostgroups in the field "Host groups in top view". To add a new view choose a name for the view in the bottom of the window that says "Add new top window". The view will appear in the filed "Top views in top view" for further configuration.
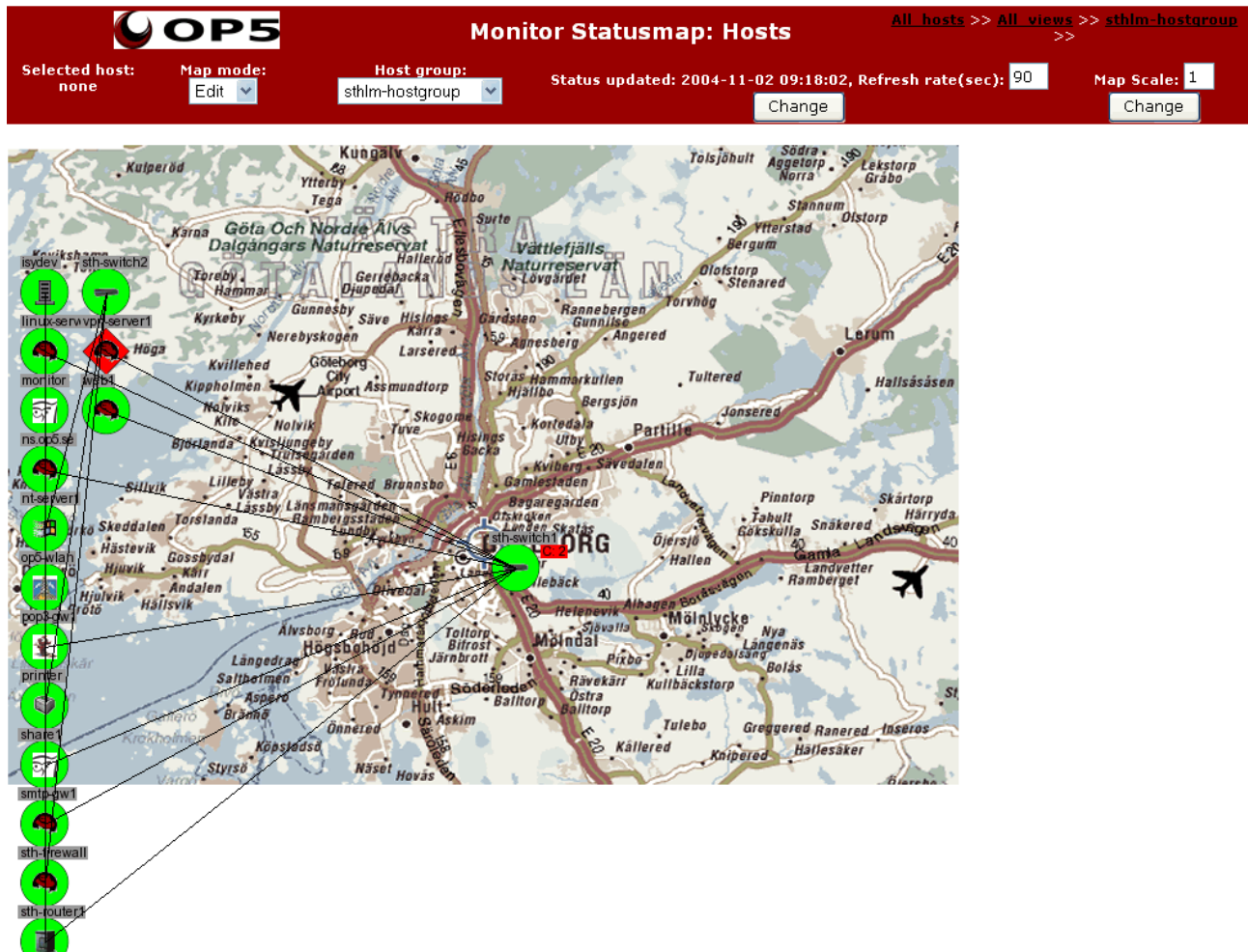
When clicking a host group in "view" mode, a new window will appear containing all hosts in that host group. The icons are already configured in the web configuration for the specific hosts. If the host is in an ok state the icon will be surrounded with a green circle. If the host is in another state, the icon is surrounded by a red triangle. To move around the icons you have to be in edit mode.

1. Click the icon you want to move.

2. The window reload.

3. The icon now shows a bold cross.

4. Point in the location where you want to place your icon.

5. Save the changes by selecting the view mode again.

When selecting edit mode, a new part of the window will be shown in the bottom of the network map window. From this configuration window you can upload and change the background.

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.

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

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.

Scheduled Host Downtime
.ᶻ 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
.ᶻ 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.

Process information

The process information window gives you information about the monitor system as well as giving you the possibility to run system wide commands.

Process Information

Program Start Time:	2004-10-29 16:14:17
Total Running Time:	3d 19h 42m 18s
Last External Command Check:	2004-11-02 10:56:31
Last Log File Rotation:	2004-11-01 00:00:00
Monitor PID	21870
Notifications Enabled?	**YES**
Service Checks Being Executed?	**YES**
Passive Service Checks Being Accepted?	**YES**
Host Checks Being Executed?	**YES**
Passive Host Checks Being Accepted?	**YES**
Event Handlers Enabled?	Yes
Obsessing Over Services?	No
Obsessing Over Hosts?	No
Flap Detection Enabled?	Yes
Performance Data Being Processed?	No

Process Commands

Shutdown the Monitor process
Restart the Monitor process
Disable notifications
Stop executing service checks
Stop accepting passive service checks
Stop executing host checks
Stop accepting passive host checks
Disable event handlers
Start obsessing over services
Start obsessing over hosts
Disable flap detection
Enable performance data

The process information:

Program start time. The date and time when starring the monitor process.

Total running time: The amount of time Monitor has been up and running.

Last external command check: The date and time when the last plugin was executed.

Last log file rotation: Date and time when the log files where rotated.

Monitor PID: Unix Process ID used in the system.

Notifications enabled: (Yes or No)

Passive service checks being accepted: (Yes or No)

Host check being executed: (Yes or No)

Passive host checks being accepted: (Yes or No)

Event handler enabled: (Yes or No)

Obsessing over services: (Yes or No)

Obsessing over hosts: (Yes or No)

Flap Detection enabled: (Yes or No)

Performance data being processed (Yes or No)

Process Commands

Shutdown the Monitor Process: Shutdown the Monitor program in the Linux environment. deletion of the Process ID used. Be aware that to start the process again you need to access the system directly or use SSH, se the OP5 System manual for more information.
Restart the Monitor Process: The Linux Monitor process stops and starts again using a new PID.
Disable Notifications: All notifications send out to contacts are disabled.
Stop executing service checks: Stop all execution of plugins (checks) towards services.
Stop accepting passive service checks: Stop the receiving of all external checks (traps) for the system with regards to services.

Stop executing host checks: Stop all execution of plugins (checks) towards hosts.
Stop accepting passive host checks: Stop the receiving of all external checks (traps) for the system with regards to hosts.

Disable event handlers: Disable event handling (automatic reaction to events) for the system.

Start obsessing over services: Usage of extra plugins (checks) executed after the regular plugins. Used for services.

Start obsessing over hosts: Usage of extra plugins (checks) executed after the regular plugins. Used for hosts.

Disable flap detection: Disable the detection of hosts pending between ok and non ok states.

Enable performance data: Storage of performance data for hosts and services.

Performance Information

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

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.

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%

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.

This can be a way to see that the OP5 System is able to keep up with the work load. If Monitor uses a lot of time to execute checks or if the check latency is high you might need to upgrade to a larger system.

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.

Object Type:

Hosts

- Hosts
- Host Dependencies
- Host Escalations
- Host Groups
- Host Group Escalations
- Services
- Service Dependencies
- Service Escalations
- Contacts
- Contact Groups
- Timeperiods
- Commands
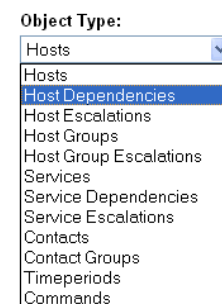
Hosts

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.

Host	Description	Max. Check Attempts	Normal Check Interval	Retry Check Interval	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 (Allows Monitor to run a command before and after every service check, this can be used to implement distributed monitoring for large networks but is normally not used

in Monitor).

- 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	

Configure

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

OP5 Monitor Configuration v2.4.0

Configure   Save Configuration   Undo Changes   Configuration Help

New Hosts

Host: [backup ▾] [Go]

Templates
Host Groups
Service Groups
Contacts
Contact Groups
Check Commands
Time Periods
Access Rights

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

Configure

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 (If you haven't clicked 'Save Configuration' the 'Undo Changes' link takes you 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' you'll have the possibility to add more than one host at the same time. By choosing 'Auto detect network nodes' you can scan the network for new nodes by choosing the IP interval to detect in.

Add New Hosts

Autodetect network nodes (pingsweep)

Number of hosts to add: [1 ▼] [Go]

New Host 1	
Add this host?	[Yes ▼]
template	[default-host-template ▼]
host_name	[_____]
alias	[_____]
address	[_____]
contact_groups	limit01-contactgroup / op5-linux / op5-print / op5-routers
hostgroups	external-web / gothenburg-group / limit01-hostgroup / linux-servers
parents	backup / beta / devel / gbg-router1
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	[ssh ▼]
Host logo	[_____ ▼]
FILE	[etc/hosts.cfg ▼]

[Scan hosts for services]

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)

- Contact groups (The contact groups the host will be associated with)

- 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)

- Service Checks (Add the items that Monitor will scan for in the host. By default auto detect network services are checked. This option scans the host for common used ports and also looks for the presence of a client. You can also force checks associated with a specific client to be included. This can be useful if you haven't installed the client yet for an example.

- 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 and network map)

- File (the configuration file that this data will be stored in, default is hosts.cfg)

Click the 'Scan hosts for services' to continue to add a new host.

Network Probe: Service Scan

Note: All new services will inherit the Initial Service Settings.

Initial Service Settings	
template	default-service
FILE	etc/services.cfg

Check a box to add a servicecheck with default values. Some services require you to alter a few parameters (notably those requiring authentication of some form). If you don't check any boxes, no services will be added.

test @ 10.10.10.1 (test)	
NET	
PING	☑

[Continue to step 3]

The second step window appears and presents som options. In the top of the window all "non standard" settings that you use in the system is shown. If you don't want to use any of those settings just leave them as they are. 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'.

That's it. Now you added a new host to Monitor. You 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.

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 for host: <host name>'. You can also configure Host Templates, Check Commands, Contact Groups and Time Periods from this window. On the right side of the window there are three links: dependencies, escalations, extras, expand and delete. Dependencies lets you configure the relations this host has with other hosts in the network. Escalations lets you configure contacts, contact groups and time periods. Extras lets you configure cosmetic things as which logo you want to associate with the host. Expand gives you a window with all the extra options that can be configured on the host. Delete, deletes the host.

Host configuration

Host: [backup ▼] [Go]

Scan host **backup** for new services

Related items:
Services for host **backup**
Host Templates
Check Commands
Contact Groups
Time Periods

backup	dependencies escalations extras expand delete
template	[default-host-template ▼]
host_name	backup
alias	OP5 Backup Server
address	193.201.96.131
hostgroups	external-web / gothenburg-group / limit01-hostgroup / linux-servers
parents	beta / devel / gbg-router1 / gbg-temp1
FILE	[etc/hosts.cfg ▼]

[**Apply Changes**]

- Template (The template to use for this host. The template consists of standard settings also used by other hosts that uses the same template)

- host_name (The name of the host as presented by the DNS(Domain Name Server))

- alias (The description of the host)

- address (The Ip adress of the host)

- hostgroups (The groups that host will be associated with. Used to escalate events to the correct contacts and contact groups)

- parents (The closest relation to Monitor the host has in the network)

- FILE (The filename in which this information will be stored)

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

Dependencies window:

Host Dependency Configuration

Host: [backup ▼] [Go]

Related items:
Host configuration: **backup**

New hostdependency	
dependent_host_name	[backup ▼]
notification_failure_criteria	☐ Down ☐ Unreachable ☐ OK
inherits_parent	[Yes ▼]
FILE	[etc/checkcommands.cfg ▼]

[Apply Changes]

- dependent_host_name (The name of the parent host in the network)

- notification_failure_criteria (Which criteria the dependent host will be notified on)

- inherits_parent (Yes or no)

-

Escalations window:

Host Escalation Configuration

Host: [backup ▼] [Go]

Related items:
Host configuration: **backup**
Contact Groups
Time Periods

New hostescalation	
contact_groups	limit01-contactgroup op5-linux op5-print op5-routers
first_notification	[ ]
last_notification	[ ]
notification_interval	[ ]
escalation_period	[24x7 ▼]
escalation_options	☑ Down ☐ Unreachable ☐ OK
FILE	[etc/checkcommands.cfg ▼]

[Apply Changes]

- contact_groups (the associated contact groups for this host)

- first_notification (Which notification that shall be sent first)

- last_notification (Which notification that shall be sent last)

- notification_interval (The interval between the notifications, each interval is multiplied with 60 seconds by default)

- escalation_period (The time period used for which escalations will be made)

- escalation_options (The type of event that will be escalated)

- FILE (The filename used to save this configuration)

Extended Hostinfo Configuration

Host: [backup ▾] [Go]

Related items:
Host configuration: **backup**

HostExtInfo for backup		delete
icon_image	[▾]	
icon_image_alt	Backup Server	
statusmap_image	[▾]	
action_url	ssh://$HOSTADDRESS$	
notes_url	[ ]	
2d_coords	260,180	
FILE	etc/hostextinfo.cfg ▾	

[**Apply Changes**]

Extras Window:

- icon_image (The graphic file used to represent the host in the status or network map.)
- icon_image_alt (The alternativ Alias for the host, shown in the status map)
- statusmap_image (The image used as a background in the status map.)
- action_url (The url used to manage the host. i.e ftp, ssh, http, https..)
- notes_url (The documentation url for this host)
- 2d_coords (The coordinates where the icon should be placed in the status map when using user supplied coords.)
- FILE (The filename where this configuration will be stored)

Expand Window (Bottom of window):

check_command	check-host-alive
check_command_args	
contact_groups	limit01-contactgroup op5-linux op5-print op5-routers op5-windows owl-contacts testing-group
max_check_attempts	5
checks_enabled	Yes
event_handler	
event_handler_enabled	Yes
low_flap_threshold	
high_flap_threshold	
flap_detection_enabled	Yes
process_perf_data	No
retain_status_information	Yes
retain_nonstatus_information	Yes
notification_interval	0
notification_period	24x7
notification_options	☑ Down ☑ Unreachable ☑ Recovery
notifications_enabled	Yes
stalking_options	☐ Down ☐ Unreachable ☐ OK
FILE	etc/hosts.cfg

Apply Changes

- check_command: (The check command used to see if this host is alive.)

- check_command_args (The arguments, if any, used with the check command)

- contact_groups (The associated contact groups for this host)

- max_check_attempts (The maximum checks attempted on this host before notification occurs.)

- Check_enabled (Yes or No)

- event_handler (Action performed upon an event change, running a script as an example)

- event_handler_enabled (Yes or No)

- low_flap_treshold, high_flap_treshold (The intervall for a flap to occur. When outside the interval the flap disappears)

- flap_detection_enabled (Yes or No)

- retain_status_information (When Monitor is restarted the host retains the status it had before the restart)

- retain_nonstatus_information (The same as above, but it retains pending and unknown status as well)
- notification_interval (If the notification is to be sent more than once, the interval is put here)
- notification_period (The the time period used for the notifications to be seen by the contact)
- notification_options (The type of notifications that shall be seen by the contact)
- notifications_enabled (Yes or No)

To delete a host simply press the delete link in the host window.

Add, Change or Delete Host, service and contact Templates

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

Choose a template type to configure.

Host Templates
Service Templates
Contact Templates

Host Templates:

default-host-template		delete
name	default-host-template	
check_command	check-host-alive	
check_command_args		
contact_groups	limit01-contactgroup op5-linux op5-print op5-routers	
max_check_attempts	5	
checks_enabled	Yes	
event_handler		
event_handler_enabled	Yes	
low_flap_threshold		
high_flap_threshold		
flap_detection_enabled	Yes	
process_perf_data	No	
retain_status_information	Yes	
retain_nonstatus_information	Yes	
notification_interval	0	
notification_period	24x7	
notification_options	☑ Down ☑ Unreachable ☑ Recovery	
notifications_enabled	Yes	
stalking_options	☐ Down ☐ Unreachable ☐ OK	
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)

Service Templates:

To configure service 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 to get on line help.

critical-service		delete
name	critical-service	
is_volatile	No	
check_command	check-host-alive	
check_command_args		
max_check_attempts	2	
normal_check_interval	1	
retry_check_interval	1	
active_checks_enabled	Yes	
passive_checks_enabled	Yes	
check_period	24x7	
parallelize_check	Yes	
obsess_over_service	Yes	
check_freshness	No	
freshness_threshold		
event_handler		
event_handler_enabled	Yes	
low_flap_threshold		
high_flap_threshold		
flap_detection_enabled	Yes	
process_perf_data	No	
retain_status_information	Yes	
retain_nonstatus_information	Yes	
notification_interval	0	
notification_period	24x7	
	☑ Critical	
	☑ Warning	

Contact Template:

The contact template can be populated with information later associated with each contact. See contacts for more information.

New contact template	
name	
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_notification_commands_args	
service_notification_commands	
service_notification_commands_args	
email	
pager	
address1	
address2	
address3	
address4	
address5	
address6	
FILE	etc/contacts.cfg

Apply Changes

Add, Change or Delete Services

To add change or delete services choose the specific host from the start page, click go. A new window appear:

Service configuration

Services for host: [backup ▾] [Go]

Scan host **backup** for new services

Related items:
Host configuration: **backup**
Service Templates
Check Commands
Contact Groups
Time Periods
Service Groups

FTP	PING	New service

FTP		dependencies escalations extras expand delete
template	default-service ▾	
service_description	FTP	
check_command	check_ftp ▾	
contact_groups	limit01-contactgroup / op5-linux / op5-print / op5-routers	
FILE	etc/services.cfg ▾	

In top of the window you can choose a quick link to another host for which services you want 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 <Host name> for new services. Furthermore there are quick links to service templates, check commands, contact groups, time periods and service groups.. 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. On the right hand side you can choose to configure: dependencies, (Failure criteria), escalations (contacts), extras (actions and notes urls), expand (all configuration options) or delete the service.

Dependencies window:

Service Dependency Configuration

Host: [backup;FTP ▾] [Go]

Related items:
Services for host **backup**

New servicedependency	
dependent_service	backup;FTP ▾
execution_failure_criteria	☑ Critical / ☑ Warning / ☐ Unknown / ☐ OK
notification_failure_criteria	☑ Critical / ☑ Warning / ☐ Unknown / ☐ OK
inherits_parent	No ▾
FILE	▾

[Apply Changes]

• dependent_service (The parent service to this service)

- execution_failure_criteria (sets the event when failed to service failed)
- notification_failure_criteria (The notification type used when the service failed)
- Inherits_parent (Yes or No)
- FILE (The file name used to store this configuration)

Escalations window:

Host Escalation Configuration

Host: [gbg-router1 ▾] [Go]

Related items:
Services for host
Contact Groups
Time Periods

New hostescalation	
contact_groups	limit01-contactgroup / op5-linux / op5-print / op5-routers
first_notification	[ ]
last_notification	[ ]
notification_interval	[ ]
escalation_period	[24x7 ▾]
escalation_options	☑ Down ☐ Unreachable ☐ OK
FILE	[etc/checkcommands.cfg ▾]

[Apply Changes]

See the host escalation window under host, adds and changes.

Extras window:

Extended Serviceinfo Configuration

Service: [backup;FTP ▾] [Go]

Related items:
Services for host **backup**

New serviceextinfo	
notes	[ ]
notes_url	[ ]
action_url	[ ]
icon_image	[▾]
icon_image_alt	[ ]
FILE	[etc/serviceextinfo.cfg ▾]

[Apply Changes]

- notes (Notes about the service)
- notes_url (the url used to see documentation about the service)
- action_url (the url used to manage the service)
- icon_image (The icon used to represent the service in the status map)

- icon_image_alt (the alternativ text shown in the status map for this service)
- FILE (The filename used to store this configuration information)

To delet a service click the delete link in the right section of the service configuration window.

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

external-web	gothenburg-group	limit01-hostgroup
linux-servers	misc	mlm-hostgroup
network	owl_mirrors	printers
sthlm-hostgroup	testing	windows-servers
New hostgroup		

external-web		delete
hostgroup_name	external-web	
alias	External Web Servers	
members	backup beta devel gbg-router1	
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)
- 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 Service Groups

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

Servicegroup configuration

email-services	office-services	New servicegroup

email-services		delete
servicegroup_name	email-services	
alias	Email service	
members	backup;FTP backup;PING beta;Cron process beta;Current users	
FILE	etc/contacts.cfg	

All service 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 service group. On the right hand side of the host group configuration window you can click delete to delete chosen host group.

- Service group Name (Name of the service group)

- Alias (Description of Host group)

- Members (Services that are members of this service group)

- File (The file in which this configuration is stored, default: servicegroups.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:

Related items:
Access-rights
Contact Groups
Timeperiods
Contact Templates

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

ae	delete
contact_name	ae
alias	Andreas Ericsson
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
contactgroups	limit01-contactgroup op5-linux op5-print op5-routers
email	ae@op5.se
pager	
FILE	etc/contacts.cfg

You can quickly configure related items as: access-rights, contact groups, time periods and contact templates from 'Related Items' menu. 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

Related items:
Contacts

limit01-contactgroup	op5-linux	op5-print
op5-routers	op5-windows	owl-contacts
testing-group	New contactgroup	

limit01-contactgroup		delete
contactgroup_name	limit01-contactgroup	
alias	Limit01 Contactgroup	
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

To add, change or delete a plug in (check command) choose commands from the start 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.

check-host-alive		delete
command_name	check-host-alive	
command_line	$USER2$/check_fping -H $HOSTADDRESS$ -w 1000,100% -c 100	
FILE	etc/checkcommands.cfg	

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 | friendly-nonworkhours | none |
| nonworkhours | workhours | 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 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.

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		☑

- authorized_for_system_information (The user has the right to see information about the system.
- authorized_for_configuration_information (The user has the rights to see the configuration of the system)
- Authorized_for_system_commands (The user has the right to configure the system)

- authorized_for_all_services (The user has the right to see status of all services)

- authorized_for_all_hosts (The user has the right to see status of all hosts)

- authorized_for_all_service_commands (The user has the right to issue commands on all services)

- authorized_for_all_host_commands (Te user has the right to issue commands on all hosts)

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.

- monitor_backup.041101.13.21.tar.gz
- monitor_backup.040924.22.23.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:

```
OP5 Monitor 2.4.2
Last Modified: 2004-11-18
License: GPL

Reading configuration data...

Running pre-flight check on configuration data...

Checking services...
        Checked 154 services.
Checking hosts...
        Checked 36 hosts.
Checking host groups...
        Checked 12 host groups.
Checking service groups...
        Checked 2 service groups.
Checking contacts...
        Checked 11 contacts.
Checking contact groups...
        Checked 7 contact groups.
Checking service escalations...
        Checked 0 service 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 87 commands.
Checking time periods...
        Checked 5 time periods.
Checking extended host info definitions...
        Checked 34 extended host info definitions.
Checking extended service info definitions...
        Checked 0 extended service info definitions.
Checking for circular paths between hosts...
Checking for circular host and service dependencies...
Checking global event handlers...
Checking obsessive compulsive processor commands...
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

The reporting functionality in OP5 Monitor can present you with data on how your It infrastructure has performed in a historical perspective. This can be a good tool to match the systems uptime with your company SLA (Service Level Agreement)

Trends

Step 1: Select Report Type

Type: [Host ▾]

[Continue to Step 2]

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.

Step 2: Select Host

Host: [afrodite ▾]

[Continue to Step 3]

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

Step 3: Select Report Options

Report period:	[Last 7 Days ▾]
If Custom Report Period...	
Start Date (Inclusive):	[November ▾] [1] [2004]
End Date (Inclusive):	[November ▾] [23] [2004]
Assume Initial States:	[Yes ▾]
Assume State Retention:	[Yes ▾]
Assume States During Program Downtime:	[Yes ▾]
First Assumed Host State:	[Unspecified ▾]
Backtracked Archives (To Scan For Initial States):	[1]
Suppress image map:	☐
Suppress popups:	☐
	[Create Report]

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.

- Start /End date (The date interval for which the report will be presented)

- Assume initial states (Uses the states of the device that was used before a restart of OP5 Monitor)

- Assume State Retention (Yes or No)

- Assume states during program downtime (Uses last known state during the time OP5 Monitor was down)

- First assumed host state (The state OP5 Monitor shall assume for host till it received a state)

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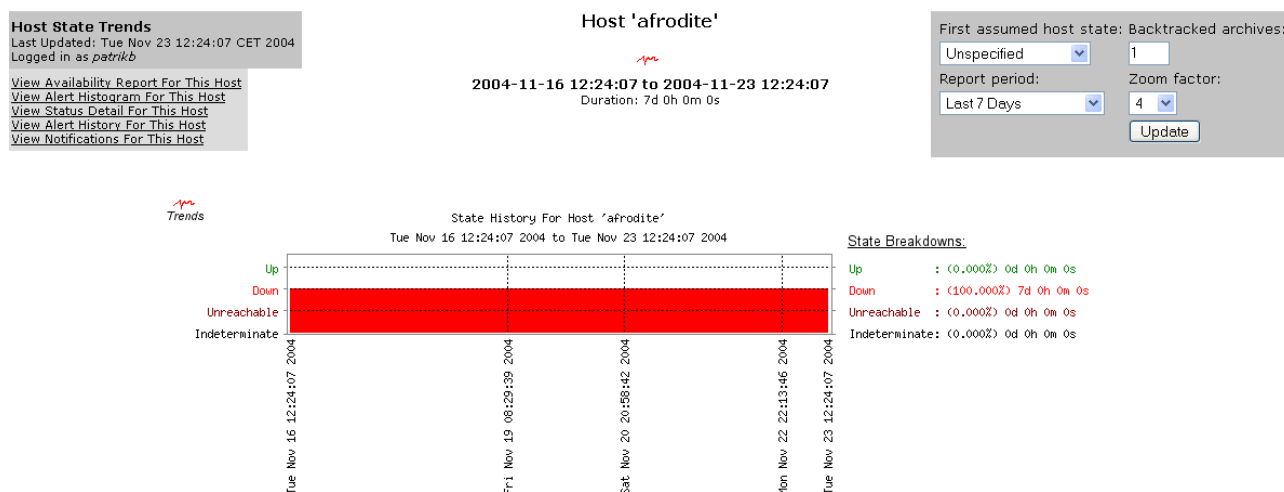
This is basically what the outcome is. Trends shows you the status of a host or service under an interval in the past. The status is shown in colors with averages in totals and percentage to the right side of the picture. You can also click the picture to zoom the statistics. In the top of the window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

Availability

From the main menu under section reporting choose Availability.

Step 1: Select Report Type

Type: [Hostgroup(s) ▼]
Hostgroup(s)
Host(s)
Servicegroup(s)
Service(s)

A new window will appear:

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

Step 2: Select Servicegroup

Servicegroup(s): [** ALL SERVICEGROUPS ** ▼]
** ALL SERVICEGROUPS **
email-services
office-services

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

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

Report Period: [Last 7 Days ▼]

If Custom Report Period...

Start Date (Inclusive): [November ▼] [1] [2004]

End Date (Inclusive): [November ▼] [2] [2004]

Report time Period: [None ▼]

[Create Availability Report!]

The report time period is configured under the web configuration 'Time Periods'. Choosed time is included in the report.
And this is basically the outcome:

Servicegroup 'email-services'

2004-11-16 12:37:14 to 2004-11-23 12:37:14
Duration: 7d 0h 0m 0s

First assumed host state: First assumed service state

| Unspecified | Unspecified |

Report period: Backtracked archives:

| Last 7 Days | 1 |

[Update]

[Availability report completed in 0 min 0 sec]

Servicegroup 'email-services' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
gbg-router1	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
pop3-gw1	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
smtp-gw1	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
sth-router1	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
sth-switch1	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%

Servicegroup 'email-services' Service State Breakdowns:

Host	Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
gbg-router1	Ethernet0 Errors	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Ethernet0 State	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Ethernet0 Traffic	99.851% (99.851%)	0.099% (0.099%)	0.000% (0.000%)	0.050% (0.050%)	0.000%
pop3-gw1	Disk usage /var	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	IMAP	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	POP3	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	System Load	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
smtp-gw1	Disk usage /var	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	SMTP	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	System Load	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	System Processes	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
sth-router1	CPU Load	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Ethernet0 Errors	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
sth-switch1	FastEthernet0/9 State	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000% (100.000%)	0.000%
	FastEthernet0/9 Traffic	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average		93.323% (93.323%)	0.007% (0.007%)	0.000% (0.000%)	6.670% (6.670%)	0.000%

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

All Hosts and Services

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

Latest
Archive

State type options:

| All state types |

History detail level for all hosts:

| All alerts |

☐ Hide Flapping Alerts
☐ Hide Downtime Alerts
☐ Hide Process Messages
☐ Older Entries First

[Update]

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 08:50:28] 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 a log of all HARD state changes. This are all events that can be generate notifications if you configure them to do so. This view can be useful to see problems in your network that occurs during time that you normally doesn't care about.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

Create Summary Report!

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

Create Summary Report!

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*

Generate New Report

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	qbq-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*

Generate New Report

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	qbq-router1	PING	12
#8	Service	devel	PING	11
#9	Service	owl-uk1	FTP	11
#10	Service	owl-se1	FTP	10

Notifications

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. This can be useful to look for problems in the network that normally doesn't generate notifications.The Event Log can be viewed choosing 'Event Log' from the main menu under the reporting section.

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:

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'

Step 1

Select report type: Hostgroup(s) ▼

Select report interval: Weekly ▼

Report recipients: [   ]

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

[Continue to step 2]

Step 2

Select hostgroup: All Hostgroups ▼

[Continue to step 3]

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

Step 3

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

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

Weekly Reports

All hosts			view	delete
recipients	jd@op5.se			

Host nt-server1			view	delete
recipients	janj@op5.se			

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

[Apply changes]

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.