User Manual

op5 Monitor 3.0

Table of Contents

Introduction

op5 Monitor is a highly flexible monitoring system for monitoring of IT infrastructure. op5 Monitor is based on the widely known open source surveillance system Nagios.

This manual includes information on how to use and configure op5 Monitor and its components.

Who is this manual for

This manual is targeted for a technical audience. The manual covers how to use and configure op5 Monitor through its web interface. For configuration using direct console access or SSH, see the op5 System manual.

Using op5 Monitor

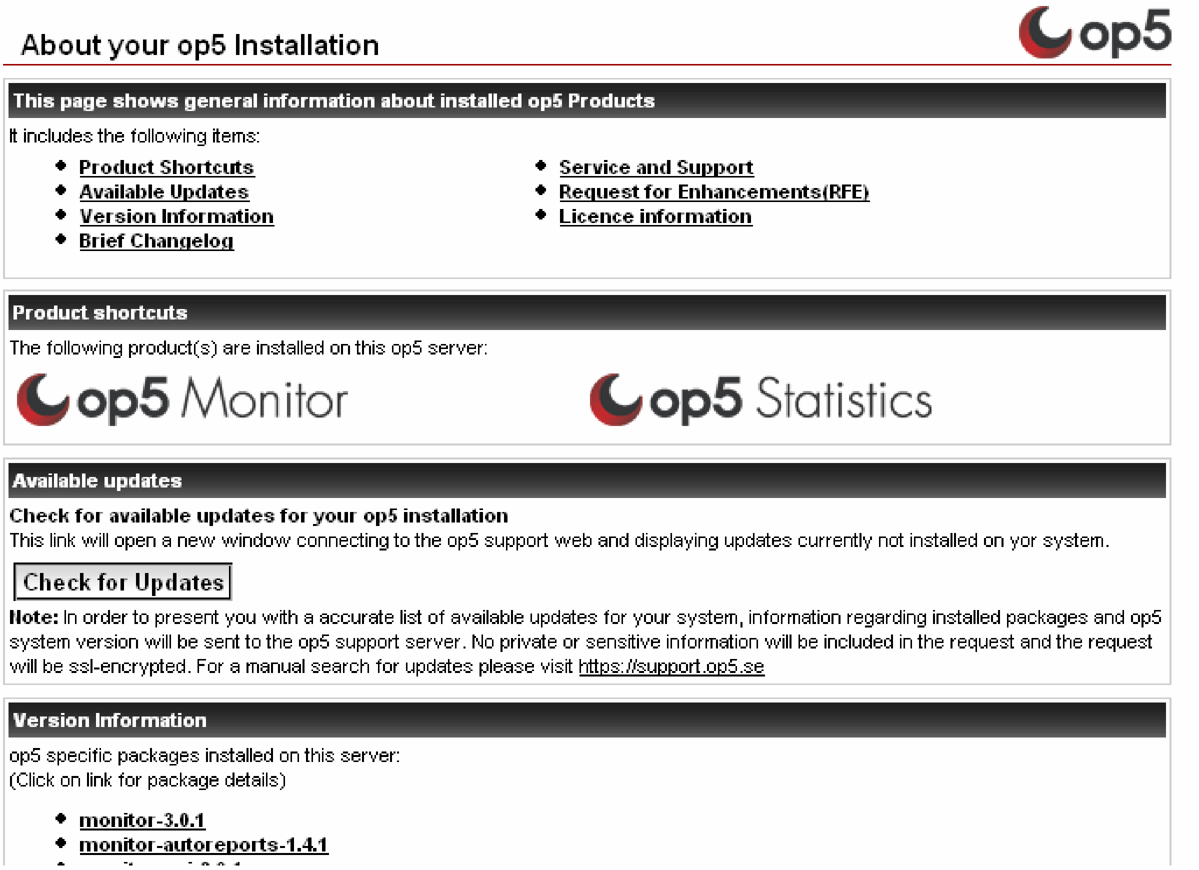
op5 Monitor is used and configured in a web interface using any standard browser. The most common browsers Explorer and Mozilla have been tested.

The interface is protected by using both authentication, you need to specify a username and password to get access, and by SSL “Secure Socket Layer” which enables a secure manner for accessing the web interface using encryption.

Start page

The start page is the first page that you access accessed by typing https://a.b.c.d/ in your browser. Change a.b.c.d to the IP address of your op5 Monitor system.

This will show general information about the system, what version of monitor that is installed, shortcuts to monitor, support information and more. To access op5 Monitor simply click on Monitor" below the headline Product Shortcuts. This will direct you to https://a.b.c.d/monitor/ which is the direct link to op5 Monitor. You can bookmark this link to get directly to op5 Monitor without having to go through the start page.



About your op5 Installation

This page shows general information about installed op5 Products

It includes the following items:

- Product Shortcuts
- Available Updates
- Version Information
- Brief Changelog
- Service and Support
- Request for Enhancements(RFE)
- Licence information

Product shortcuts

The following product(s) are installed on this op5 server:

Available updates

Check for available updates for your op5 installation

This link will open a new window connecting to the op5 support web and displaying updates currently not installed on yor system.

Note: In order to present you with a accurate list of available updates for your system, information regarding installed packages and op5 system version will be sent to the op5 support server. No private or sensitive information will be included in the request and the request will be ssl-encrypted. For a manual search for updates please visit https://support.op5.se

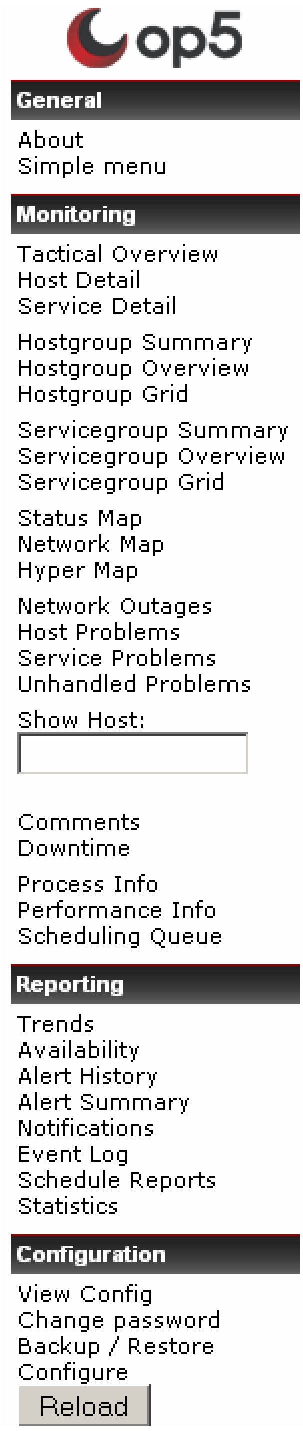
Version Information

op5 specific packages installed on this server:
(Click on link for package details)

- monitor-3.0.1
- monitor-autoreports-1.4.1

Working with the Web GUI

op5 Monitors web interface is divided in two parts, the navigation menu to the right and the main window to the left. The navigation menu has four headlines, General, Monitoring, Reporting and Configuration.



General

About

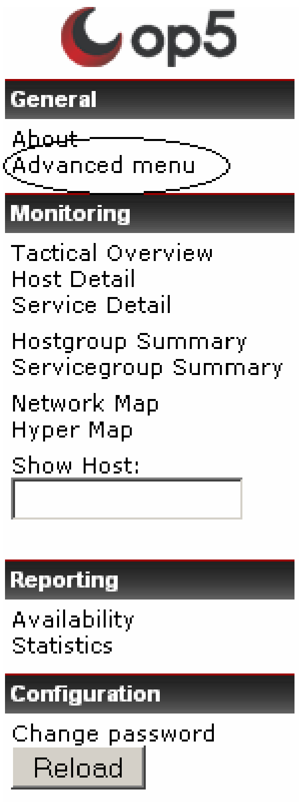
The about link gets you right back to the op5 System start page. The start page gives you information about the installed products, how to get support and most important of all an easy way to check for updates.

Simply click on the "Check for Updates" button. This will send version information to op5 Support web and generate a unique list of available updates for your system.

Simple/Advanced

There are two modes for the navigation menu, an advanced mode with the full set of selections in the menu and a simple mode with a limited set of selections.

When you log on to op5 Monitor for the first time the side menu will be displayed in simple mode. Just click on the "Advanced menu" link to change mode to advanced mode. The menu will show a full set of selections and the "Advanced menu" item will change name to "Simple menu". To return to simple mode just click on the "Simple menu" link.

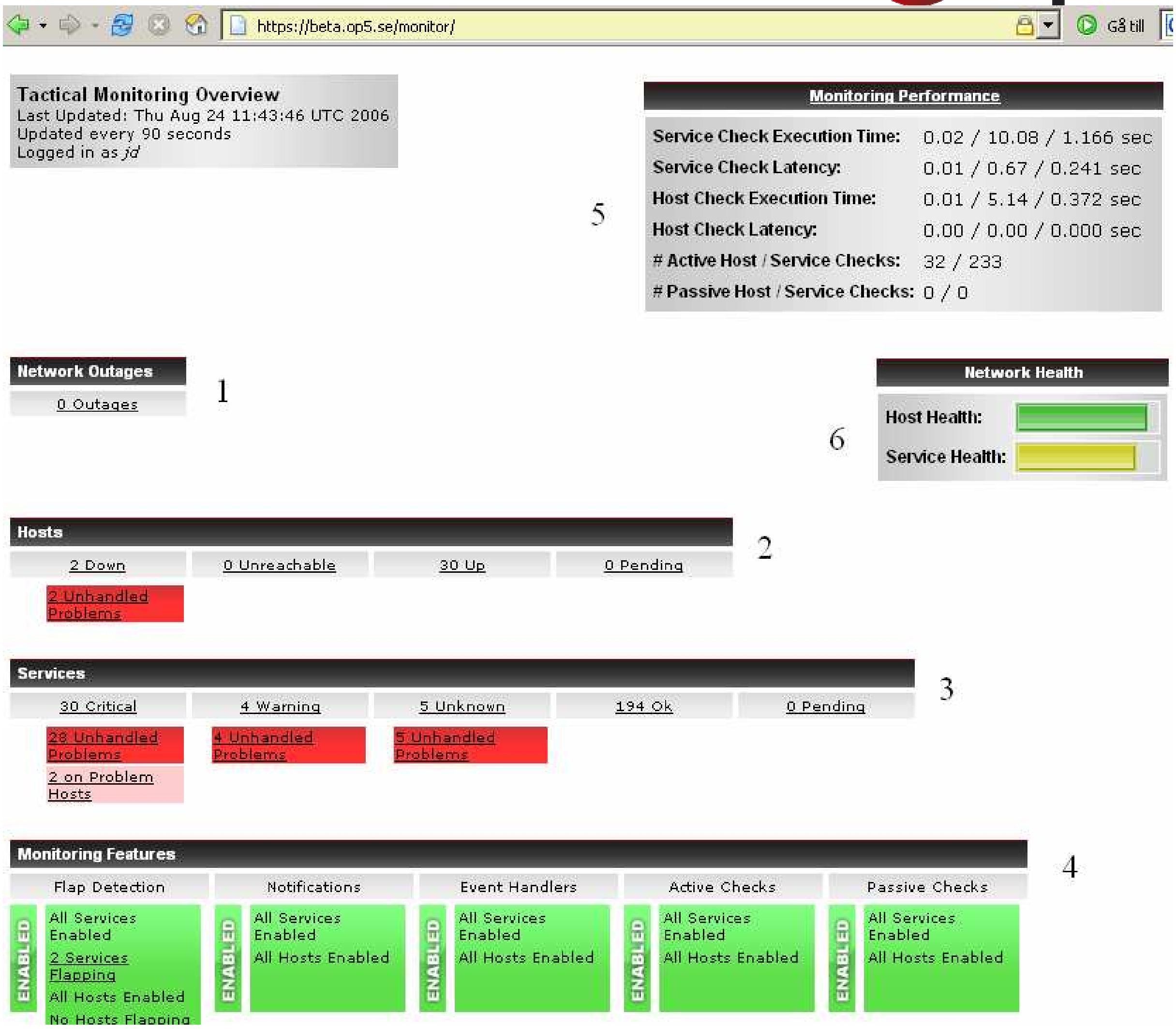


Monitoring

The monitoring headline is related to problem management and status of your network.

Tactical Overview

The Tactical Overview window enables the user to get a summarized picture of the overall network health. It also displays status of the system and gives you the possibility to enable and disable some functions on a system wide basis.



Tactical Monitoring Overview
Last Updated: Thu Aug 24 11:43:46 UTC 2006
Updated every 90 seconds
Logged in as *jd*

Monitoring Performance	
Service Check Execution Time:	0.02 / 10.08 / 1.166 sec
Service Check Latency:	0.01 / 0.67 / 0.241 sec
Host Check Execution Time:	0.01 / 5.14 / 0.372 sec
Host Check Latency:	0.00 / 0.00 / 0.000 sec
# Active Host / Service Checks:	32 / 233
# Passive Host / Service Checks:	0 / 0

Network Outages
0 Outages

Network Health	
Host Health:	🟩
Service Health:	🟨

Hosts			
2 Down	0 Unreachable	30 Up	0 Pending
2 Unhandled Problems			

Services				
30 Critical	4 Warning	5 Unknown	194 Ok	0 Pending
28 Unhandled Problems 2 on Problem Hosts	4 Unhandled Problems	5 Unhandled Problems		

Monitoring Features				
Flap Detection	Notifications	Event Handlers	Active Checks	Passive Checks
ENABLED All Services Enabled 2 Services Flapping All Hosts Enabled No Hosts 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 All Hosts Enabled

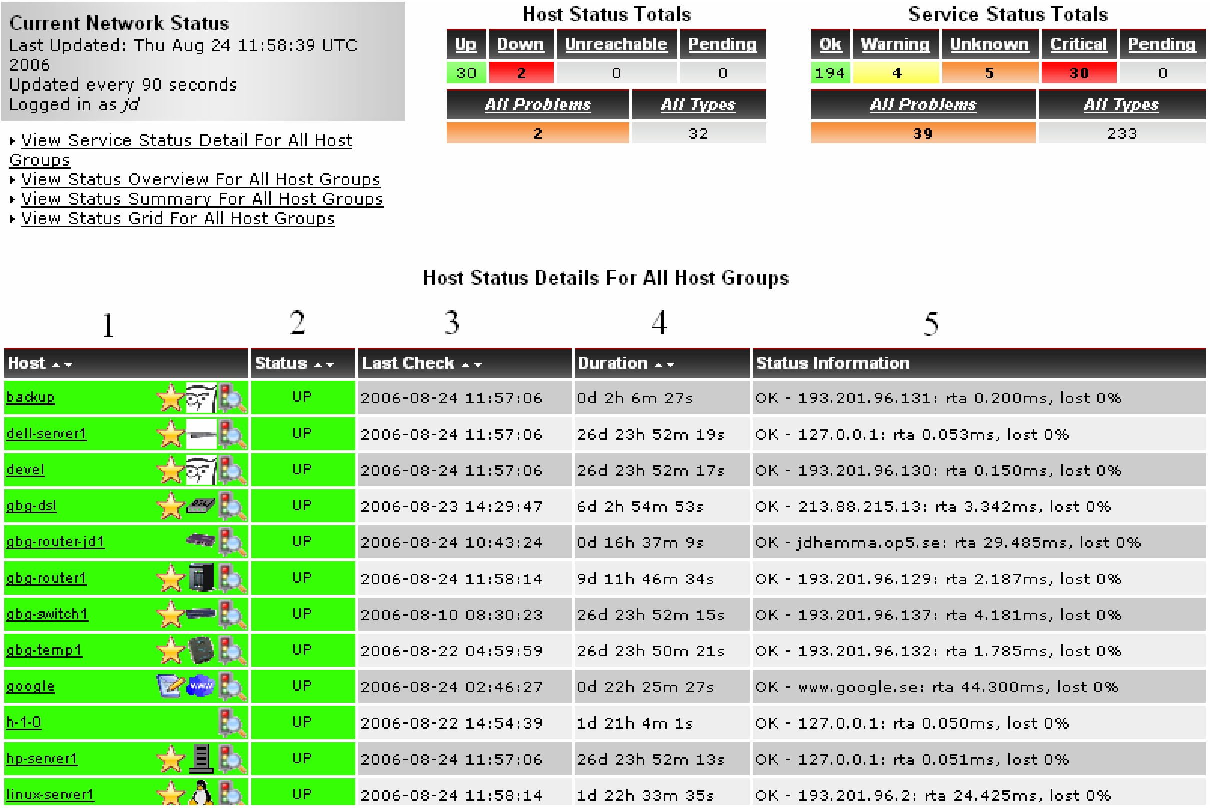
1. Network Outages, if a host, for example a switch, goes down it causes hosts located below to become unreachable from the op5 Monitor system. This will then be listed as a Network Outage. You can se what host is causing the outage and also how many hosts that are affected if you follow the link.
2. Hosts, Gives you a summarized view of the host and their status. There are four different states:
    a. Down, the host is not responding.
    b. Unreachable. The host is unreachable for the system due to a network outage (see network outage)
    c. Up, the host is working fine.
    d. Pending, the host has not yet been checked, the check of the host is in a queue about to be executed.
3. Services, gives you a summarized view of the service status. There are five different states:
    a. Critical, the service check responds with a value that is within the configured critical level.
    b. Warning, the service check responds with a value that is within the configured warning level.
    c. Unknown, the service of a host does not respond correctly to a service check, or the service check is misconfigured.

   d. Ok, the service is working fine.
   e. Pending, the service has not been checked yet. The check is queued, about to be executed or is configured to never be executed.
4. Main configuration Commands. You have the possibility to enable and disable some functionality on global basis. Just by clicking on the enabled icon you can change the configuration.
   a. Flap Detection. If a host or a service is changing 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.
   b. Notifications. All status changes, from an ok to a non ok and vice versa is a status change. All status changes can create notification to the configured contacts via email or sms. In this menu the notifications can enabled or disabled for the whole system.
   c. 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.
   d. 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.
   e. Passive Check. Monitor has the ability to receive check 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 or disables the processing of these check results.
5. Monitoring Performance. This information box gives you information about the op5 Monitor performance. For more information se, Performance Info.
6. Network Health. This information box displays an overall system status for hosts and services. It changes color between green and red depending on how good or bad the status is.

Host Detail and Service Detail

Host and Service detail gives you a detailed status list of all hosts. The list is sorted based on the hostname column by default but you can change that by clicking on the arrow icons next to the header of each column. You can also apply filters on what you want to be displayed on the page.

Host Detail



Current Network Status
Last Updated: Thu Aug 24 11:58:39 UTC 2006
Updated every 90 seconds
Logged in as *jd*

- 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
30	2	0	0

All Problems	*All Types*
2	32

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
194	4	5	30	0

All Problems	*All Types*
39	233

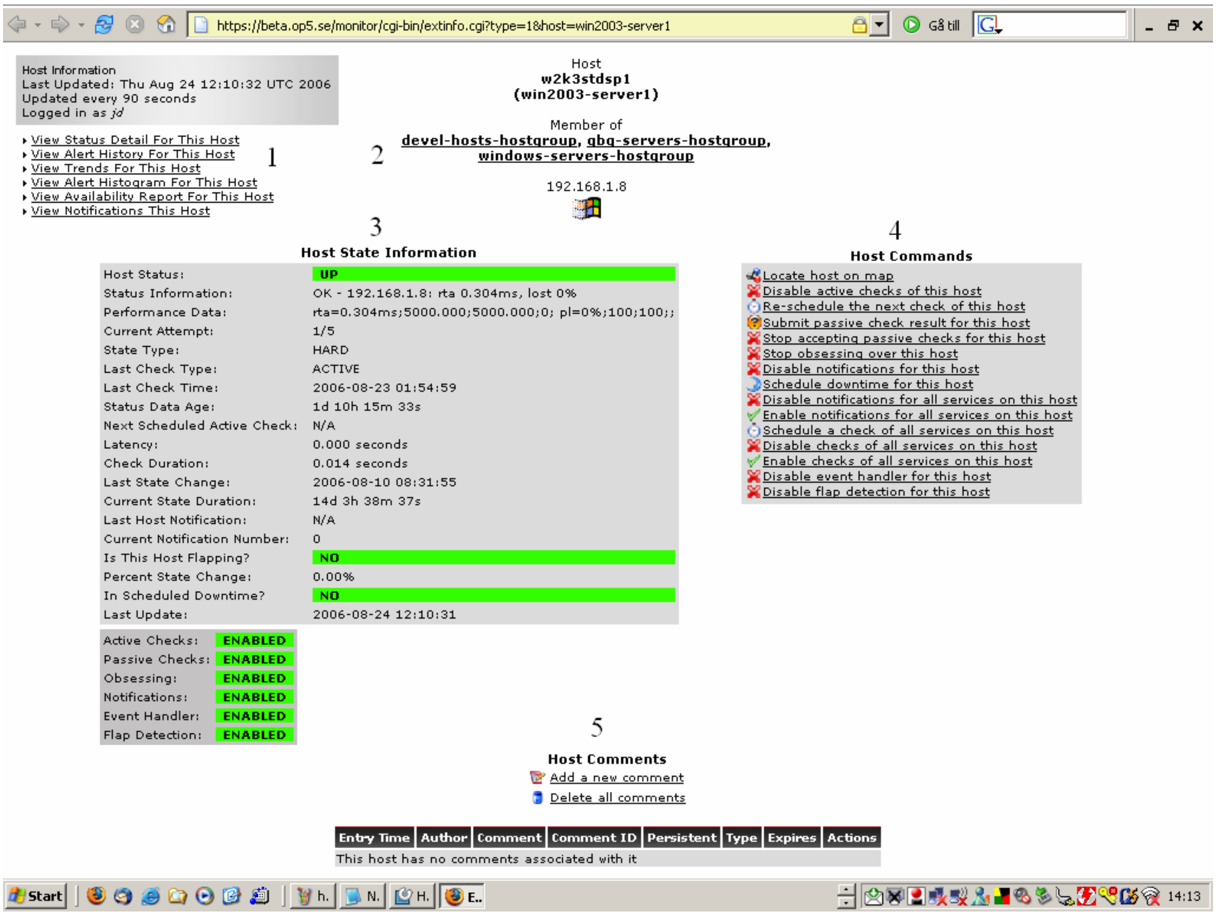
Host Status Details For All Host Groups

Host ▲▼	Status ▲▼	Last Check ▲▼	Duration ▲▼	Status Information
backup	UP	2006-08-24 11:57:06	0d 2h 6m 27s	OK - 193.201.96.131: rta 0.200ms, lost 0%
dell-server1	UP	2006-08-24 11:57:06	26d 23h 52m 19s	OK - 127.0.0.1: rta 0.053ms, lost 0%
devel	UP	2006-08-24 11:57:06	26d 23h 52m 17s	OK - 193.201.96.130: rta 0.150ms, lost 0%
gbg-dsl	UP	2006-08-23 14:29:47	6d 2h 54m 53s	OK - 213.88.215.13: rta 3.342ms, lost 0%
gbg-router-jd1	UP	2006-08-24 10:43:24	0d 16h 37m 9s	OK - jdhemma.op5.se: rta 29.485ms, lost 0%
gbg-router1	UP	2006-08-24 11:58:14	9d 11h 46m 34s	OK - 193.201.96.129: rta 2.187ms, lost 0%
gbg-switch1	UP	2006-08-10 08:30:23	26d 23h 52m 15s	OK - 193.201.96.137: rta 4.181ms, lost 0%
gbg-temp1	UP	2006-08-22 04:59:59	26d 23h 50m 21s	OK - 193.201.96.132: rta 1.785ms, lost 0%
google	UP	2006-08-24 02:46:27	0d 22h 25m 27s	OK - www.google.se: rta 44.300ms, lost 0%
h-1-0	UP	2006-08-22 14:54:39	1d 21h 4m 1s	OK - 127.0.0.1: rta 0.050ms, lost 0%
hp-server1	UP	2006-08-24 11:57:06	26d 23h 52m 13s	OK - 127.0.0.1: rta 0.051ms, lost 0%
linux-server1	UP	2006-08-24 11:58:14	1d 22h 33m 35s	OK - 193.201.96.2: rta 24.425ms, lost 0%

1. Host. Shows you the configured name of the host.
2. Status. Shows the current status of the host.
3. Last Check. Lists the date and time when the last check was executed. Note: Hosts is only checked when there is a problem with a service, therefore this value can be very old.
4. Duration. Shows you the amount of time the host has been in the current state.
5. Status Information. Shows you the output of the host check.

Extended host information

To get more detailed information about a specific host simply click on the hostname.



https://beta.op5.se/monitor/cgi-bin/extinfo.cgi?type=1&host=win2003-server1

Host Information
Last Updated: Thu Aug 24 12:10:32 UTC 2006
Updated every 90 seconds
Logged in as *jd*

1
- View Status Detail For This Host
- View Alert History For This Host
- View Trends For This Host
- View Alert Histogram For This Host
- View Availability Report For This Host
- View Notifications This Host

2
Host
w2k3stdsp1
(win2003-server1)

Member of
devel-hosts-hostgroup, gbg-servers-hostgroup, windows-servers-hostgroup

192.168.1.8

3
Host State Information

Host Status:	UP
Status Information:	OK - 192.168.1.8: rta 0.304ms, lost 0%
Performance Data:	rta=0.304ms;5000.000;5000.000;0; pl=0%;100;100;;
Current Attempt:	1/5
State Type:	HARD
Last Check Type:	ACTIVE
Last Check Time:	2006-08-23 01:54:59
Status Data Age:	1d 10h 15m 33s
Next Scheduled Active Check:	N/A
Latency:	0.000 seconds
Check Duration:	0.014 seconds
Last State Change:	2006-08-10 08:31:55
Current State Duration:	14d 3h 38m 37s
Last Host Notification:	N/A
Current Notification Number:	0
Is This Host Flapping?	NO
Percent State Change:	0.00%
In Scheduled Downtime?	NO
Last Update:	2006-08-24 12:10:31

Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	ENABLED
Flap Detection:	ENABLED

4
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

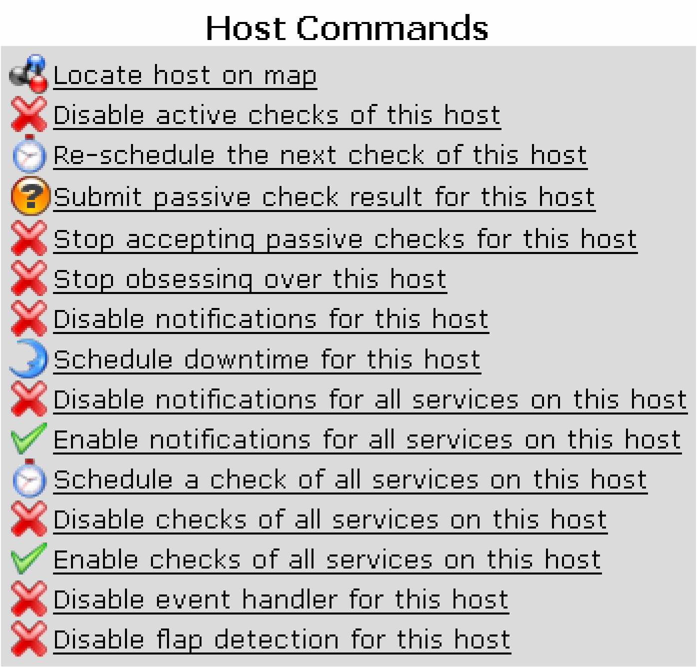
5
Host Comments

- Add a new comment
- Delete all comments

Entry Time	Author	Comment	Comment ID	Persistent	Type	Expires	Actions
This host has no comments associated with it							

1. Useful links to status pages and reports for the selected host.
2. Base information about the host. Hostname, description, ipaddress and so on.
3. Host State Information gives you more detailed information about the host status
4. Host Commands lets you issue commands for that specific host. Read more: Host Commands
5. Host Comments lets you add a comment for that specific host, it also lists all comments if there are any.

Host Commands



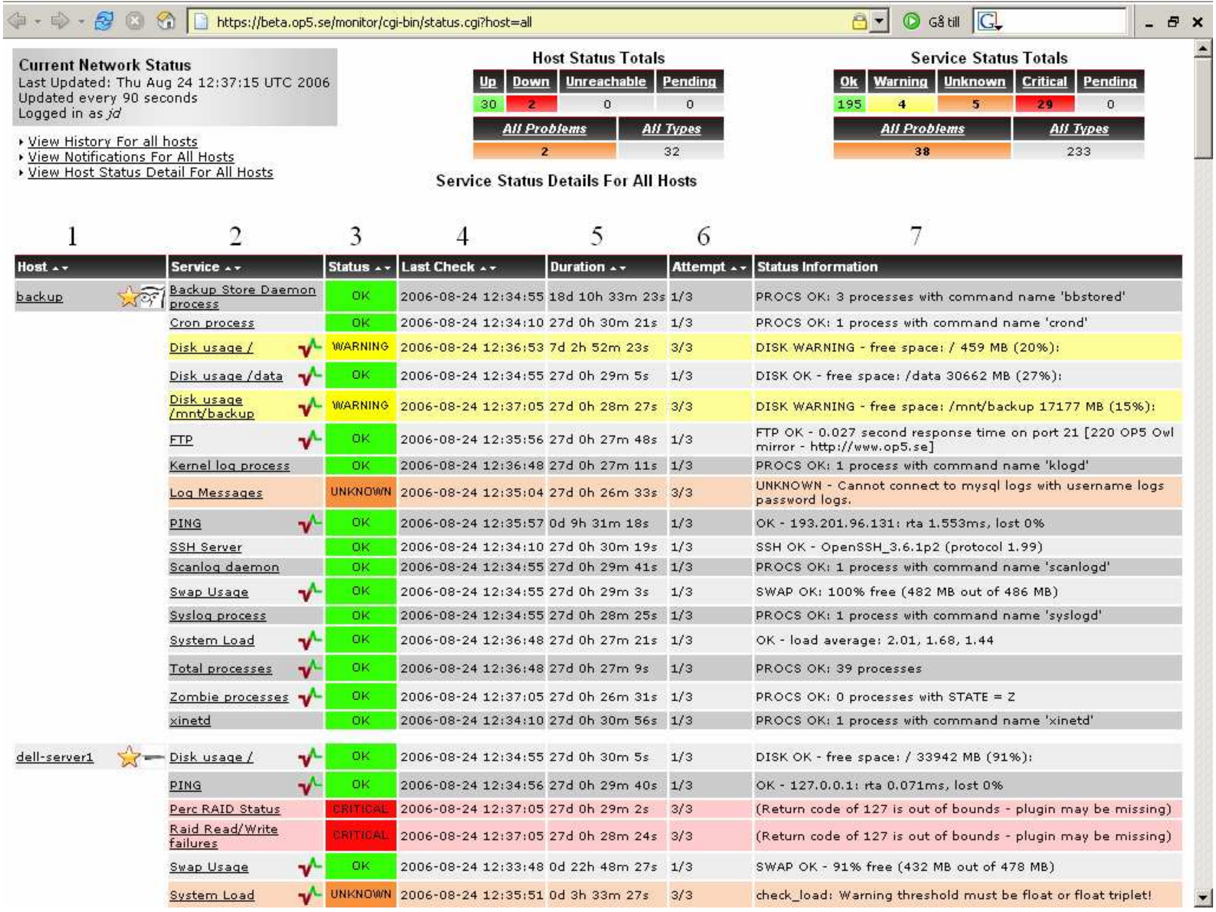
Host Commands

- 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 with focus on the host
- **Disable Active Checks Of This Host:** This can be used to temporary disable the host checks for that host.
- **Re-schedule Next Host Check:** This command is used to schedule the next check of the selected host. Monitor will re-schedule 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 the selected host. It can for example be used to clear the state on a passive host.
- **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 is only used when configuring certain redundant solutions and should normally not be used.
- **Acknowledge this host problem:** This alternative is only displayed if the host is in a non ok state. It lets you acknowledge the problem and type in a log message. This message is sent out as a notification and also displayed in the system for everybody to see. This functionality is highly recommended.
- **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 on the selected host.

- **Disable Notifications For All Services On This Host:** This command is used to prevent notifications from being sent out for all services on the selected 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 selected 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 Of All Services On This Host:** This command is used to schedule the next check of all services on the selected 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 on the selected host. When a service is disabled op5 Monitor will execute any service checks. 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 on the selected 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 op5 Monitor from running the host event handler on the selected host.
- **Disable Flap Detection For This Host:** This command is used to disable flap detection for the selected host.

Service Detail



https://beta.op5.se/monitor/cgi-bin/status.cgi?host=all

Current Network Status
Last Updated: Thu Aug 24 12:37:15 UTC 2006
Updated every 90 seconds
Logged in as *jd*

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

Host Status Totals

Up	Down	Unreachable	Pending
30	2	0	0

All Problems	All Types
2	32

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
195	4	5	29	0

All Problems	All Types
38	233

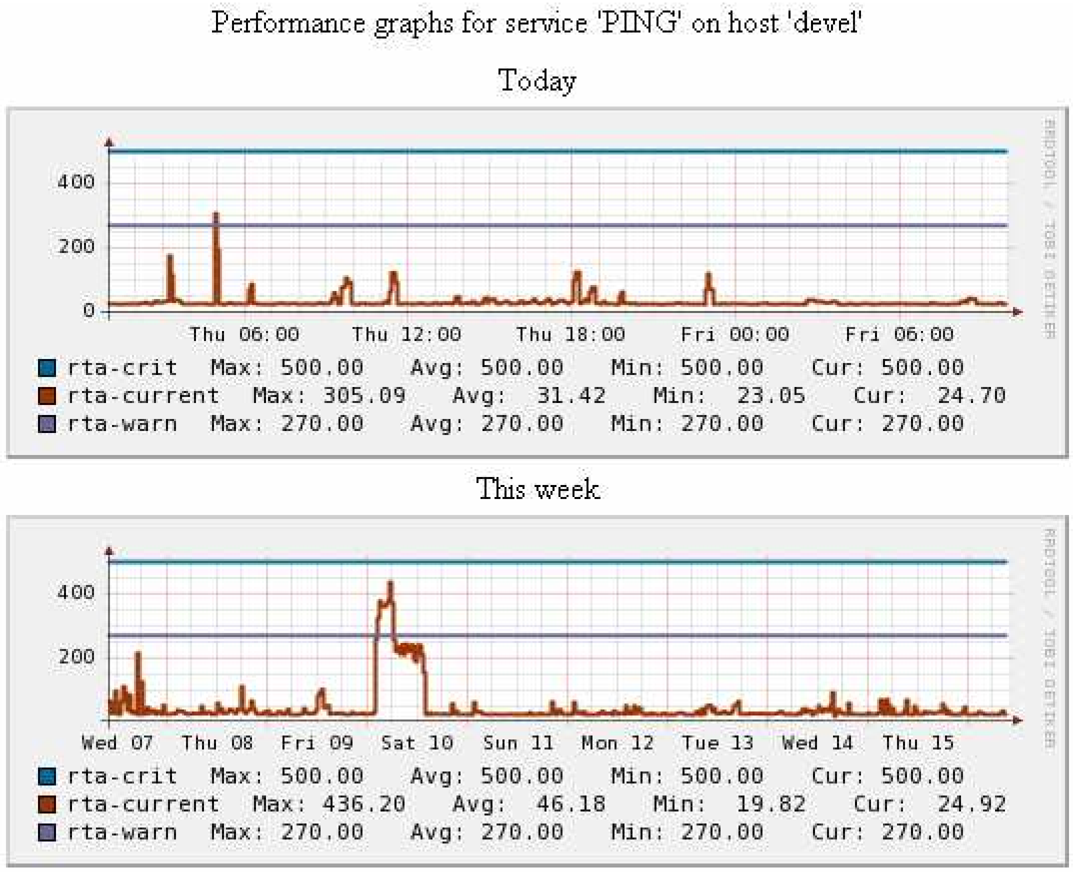
Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
backup	Backup Store Daemon process	OK	2006-08-24 12:34:55	18d 10h 33m 23s	1/3	PROCS OK: 3 processes with command name 'bbstored'
	Cron process	OK	2006-08-24 12:34:10	27d 0h 30m 21s	1/3	PROCS OK: 1 process with command name 'crond'
	Disk usage /	WARNING	2006-08-24 12:36:53	7d 2h 52m 23s	3/3	DISK WARNING - free space: / 459 MB (20%):
	Disk usage /data	OK	2006-08-24 12:34:55	27d 0h 29m 5s	1/3	DISK OK - free space: /data 30662 MB (27%):
	Disk usage /mnt/backup	WARNING	2006-08-24 12:37:05	27d 0h 28m 27s	3/3	DISK WARNING - free space: /mnt/backup 17177 MB (15%):
	FTP	OK	2006-08-24 12:35:56	27d 0h 27m 48s	1/3	FTP OK - 0.027 second response time on port 21 [220 OP5 Owl mirror - http://www.op5.se]
	Kernel log process	OK	2006-08-24 12:36:48	27d 0h 27m 11s	1/3	PROCS OK: 1 process with command name 'klogd'
	Log Messages	UNKNOWN	2006-08-24 12:35:04	27d 0h 26m 33s	3/3	UNKNOWN - Cannot connect to mysql logs with username logs password logs.
	PING	OK	2006-08-24 12:35:57	0d 9h 31m 18s	1/3	OK - 193.201.96.131: rta 1.553ms, lost 0%
	SSH Server	OK	2006-08-24 12:34:10	27d 0h 30m 19s	1/3	SSH OK - OpenSSH_3.6.1p2 (protocol 1.99)
	Scanlog daemon	OK	2006-08-24 12:34:55	27d 0h 29m 41s	1/3	PROCS OK: 1 process with command name 'scanlogd'
	Swap Usage	OK	2006-08-24 12:34:55	27d 0h 29m 3s	1/3	SWAP OK: 100% free (482 MB out of 486 MB)
	Syslog process	OK	2006-08-24 12:34:55	27d 0h 28m 25s	1/3	PROCS OK: 1 process with command name 'syslogd'
	System Load	OK	2006-08-24 12:36:48	27d 0h 27m 21s	1/3	OK - load average: 2.01, 1.68, 1.44
	Total processes	OK	2006-08-24 12:36:48	27d 0h 27m 9s	1/3	PROCS OK: 39 processes
	Zombie processes	OK	2006-08-24 12:37:05	27d 0h 26m 31s	1/3	PROCS OK: 0 processes with STATE = Z
	xinetd	OK	2006-08-24 12:34:10	27d 0h 30m 56s	1/3	PROCS OK: 1 process with command name 'xinetd'
dell-server1	Disk usage /	OK	2006-08-24 12:34:55	27d 0h 30m 5s	1/3	DISK OK - free space: / 33942 MB (91%):
	PING	OK	2006-08-24 12:34:56	27d 0h 29m 40s	1/3	OK - 127.0.0.1: rta 0.071ms, lost 0%
	Perc RAID Status	CRITICAL	2006-08-24 12:37:05	27d 0h 29m 2s	3/3	(Return code of 127 is out of bounds - plugin may be missing)
	Raid Read/Write failures	CRITICAL	2006-08-24 12:37:05	27d 0h 28m 24s	3/3	(Return code of 127 is out of bounds - plugin may be missing)
	Swap Usage	OK	2006-08-24 12:33:48	0d 22h 48m 27s	1/3	SWAP OK - 91% free (432 MB out of 478 MB)
	System Load	UNKNOWN	2006-08-24 12:35:51	0d 3h 33m 27s	3/3	check_load: Warning threshold must be float or float triplet!

1. **Host:** Shows you the configured name of the host.
2. **Service:** Shows you the name of the service.
3. **Status:** Shows the current status of the service.
4. **Last Check:** Lists the date and time when the last check was executed.
5. **Duration:** Shows you the amount of time the service has been in the current state.
6. **Attempt:** Shows you how many attempts the system has made to decide the current state of the service.
7. **Status Information:** Shows you the output of the service check.

op5 Monitor Simple Graphs

The output data from service checks can be parsed and displayed as graphs. Click on the ✓ icon that is displayed next to the service name to see the graphs.



Performance graphs for service 'PING' on host 'devel'

Today

```
■ rta-crit     Max: 500.00   Avg: 500.00   Min: 500.00   Cur: 500.00
■ rta-current  Max: 305.09   Avg:  31.42   Min:  23.05   Cur:  24.70
■ rta-warn     Max: 270.00   Avg: 270.00   Min: 270.00   Cur: 270.00
```

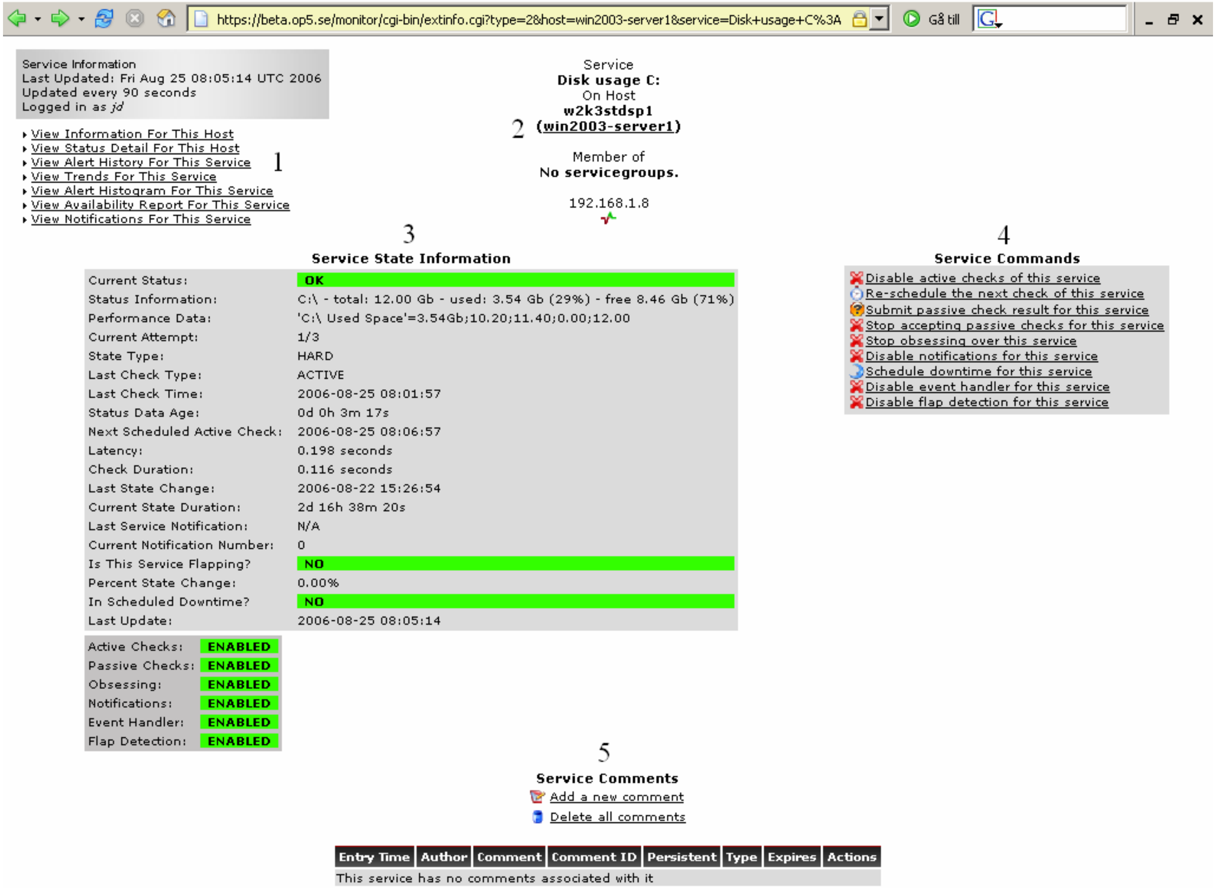
This week

```
■ rta-crit     Max: 500.00   Avg: 500.00   Min: 500.00   Cur: 500.00
■ rta-current  Max: 436.20   Avg:  46.18   Min:  19.82   Cur:  24.92
■ rta-warn     Max: 270.00   Avg: 270.00   Min: 270.00   Cur: 270.00
```

There are fore graphs displayed, daily, weekly, monthly and yearly.

Extended service Information

To get more detailed information about a specific service simply click on the service name.



https://beta.op5.se/monitor/cgi-bin/extinfo.cgi?type=2&host=win2003-server1&service=Disk+usage+C%3A
Gå till
1
2
3
4
5

Service Information
Last Updated: Fri Aug 25 08:05:14 UTC 2006
Updated every 90 seconds
Logged in as *jd*

- View Information For This Host
- View Status Detail For This Host
- View Alert History For This Service
- View Trends For This Service
- View Alert Histogram For This Service
- View Availability Report For This Service
- View Notifications For This Service

Service
Disk usage C:
On Host
w2k3stdsp1
(win2003-server1)

Member of
No servicegroups.

192.168.1.8

Service State Information

Current Status:	**OK**
Status Information:	C:\ - total: 12.00 Gb - used: 3.54 Gb (29%) - free 8.46 Gb (71%)
Performance Data:	'C:\ Used Space'=3.54Gb;10.20;11.40;0.00;12.00
Current Attempt:	1/3
State Type:	HARD
Last Check Type:	ACTIVE
Last Check Time:	2006-08-25 08:01:57
Status Data Age:	0d 0h 3m 17s
Next Scheduled Active Check:	2006-08-25 08:06:57
Latency:	0.198 seconds
Check Duration:	0.116 seconds
Last State Change:	2006-08-22 15:26:54
Current State Duration:	2d 16h 38m 20s
Last Service Notification:	N/A
Current Notification Number:	0
Is This Service Flapping?	**NO**
Percent State Change:	0.00%
In Scheduled Downtime?	**NO**
Last Update:	2006-08-25 08:05:14

Active Checks:	**ENABLED**
Passive Checks:	**ENABLED**
Obsessing:	**ENABLED**
Notifications:	**ENABLED**
Event Handler:	**ENABLED**
Flap Detection:	**ENABLED**

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

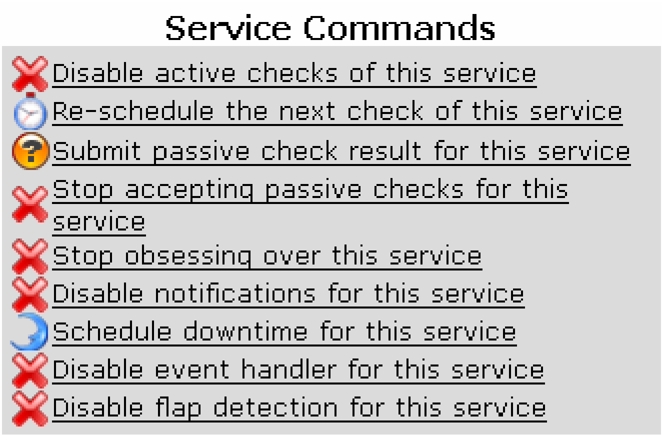
Service Comments

- Add a new comment
- Delete all comments

Entry Time	Author	Comment	Comment ID	Persistent	Type	Expires	Actions
This service has no comments associated with it							

1. Useful links to status pages and reports for the selected service.
2. Base information about the service. Service description, which host the service is located on and which service groups the service is member of.
3. Service State Information gives you more detailed information about the service status
4. Service Commands lets you issue commands for that specific service. Read more: Service commands
5. Service Comments lets you add a comment for that specific service, it also lists all comments if there are any.

Service commands

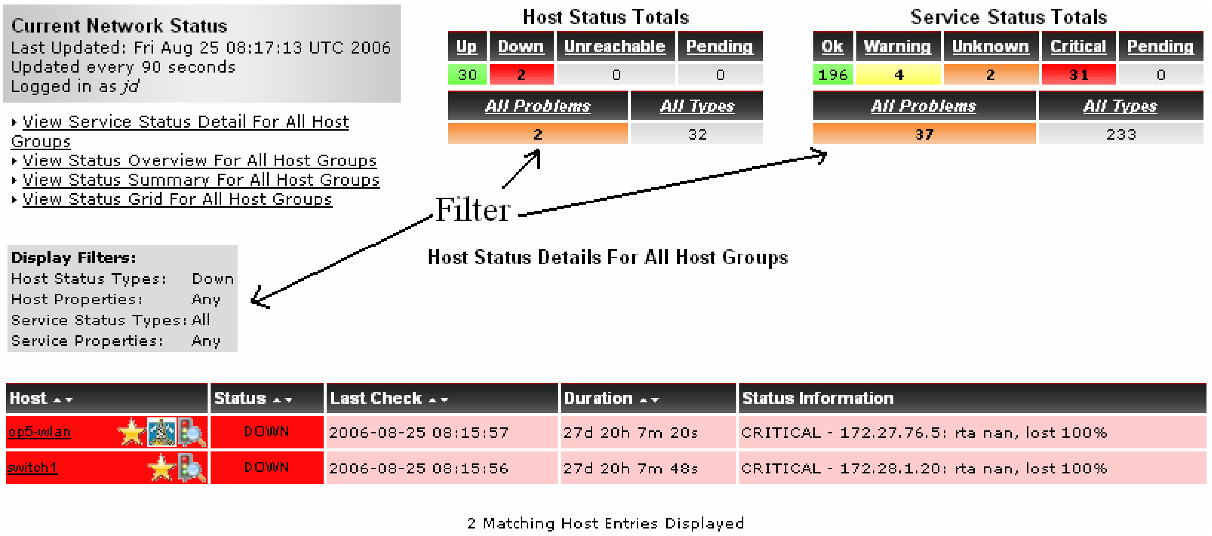


Service Commands

- 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

- **Disable Active Checks Of This Service:** This can be used to temporary disable the checks for that service.
- **Re-schedule Next Service Check:** This command is used to reschedule the next check of the selected service. op5 Monitor will re-schedule the service to be checked at the time you specify. If you select the force check option, op5 Monitor will force a check of the service regardless of both what time the scheduled check occurs and whether or not checks are enabled.
- **Submit Passive Check Result For This Service:** This command is used to submit a passive check result for the selected service. It can for example be used to clear the state on a passive service.
- **Stop Accepting Passive Checks For This Service:** This command is used to stop op5 Monitor from accepting passive check results for the selected service. All passive check results that are found for service will be ignored.
- **Stop Obsessing Over This Service:** This is only used when configuring certain redundant solutions and should normally not be used.
- **Acknowledge This Service Problem:** This alternative is only displayed if the host is in a non ok state. It lets you acknowledge the problem and type in a log message. This message is sent out as a notification and also displayed in the system for everybody to see. This functionality is highly recommended.
- **Disable Notifications For This Service:** This command is used to prevent notifications from being sent out for the selected service. You will have to re-enable notifications for this service 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.
- **Delay Next Service Notification:** This command lets you delay the time until next notification is sent out. Normally op5 Monitor is configured to only send out one notification when a problem occurs but if you have configured reoccurring notifications you can use this command.
- **Schedule Downtime For This Service:** This command is used to schedule downtime on the selected service.
- **Disable Event Handler For This Service:** This command is used to temporarily prevent op5 Monitor from running the host event handler on the selected service.
- **Disable Flap Detection For This Service:** This command is used to disable flap detection for the selected host.

Filtering



Current Network Status
Last Updated: Fri Aug 25 08:17:13 UTC 2006
Updated every 90 seconds
Logged in as *jd*

- 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

Display Filters:

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

Host Status Totals

Up	Down	Unreachable	Pending
30	2	0	0

All Problems	All Types
2	32

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
196	4	2	31	0

All Problems	All Types
37	233

Host Status Details For All Host Groups

Host	Status	Last Check	Duration	Status Information
op5-wlan	DOWN	2006-08-25 08:15:57	27d 20h 7m 20s	CRITICAL - 172.27.76.5: rta nan, lost 100%
switch1	DOWN	2006-08-25 08:15:56	27d 20h 7m 48s	CRITICAL - 172.28.1.20: rta nan, lost 100%

2 Matching Host Entries Displayed

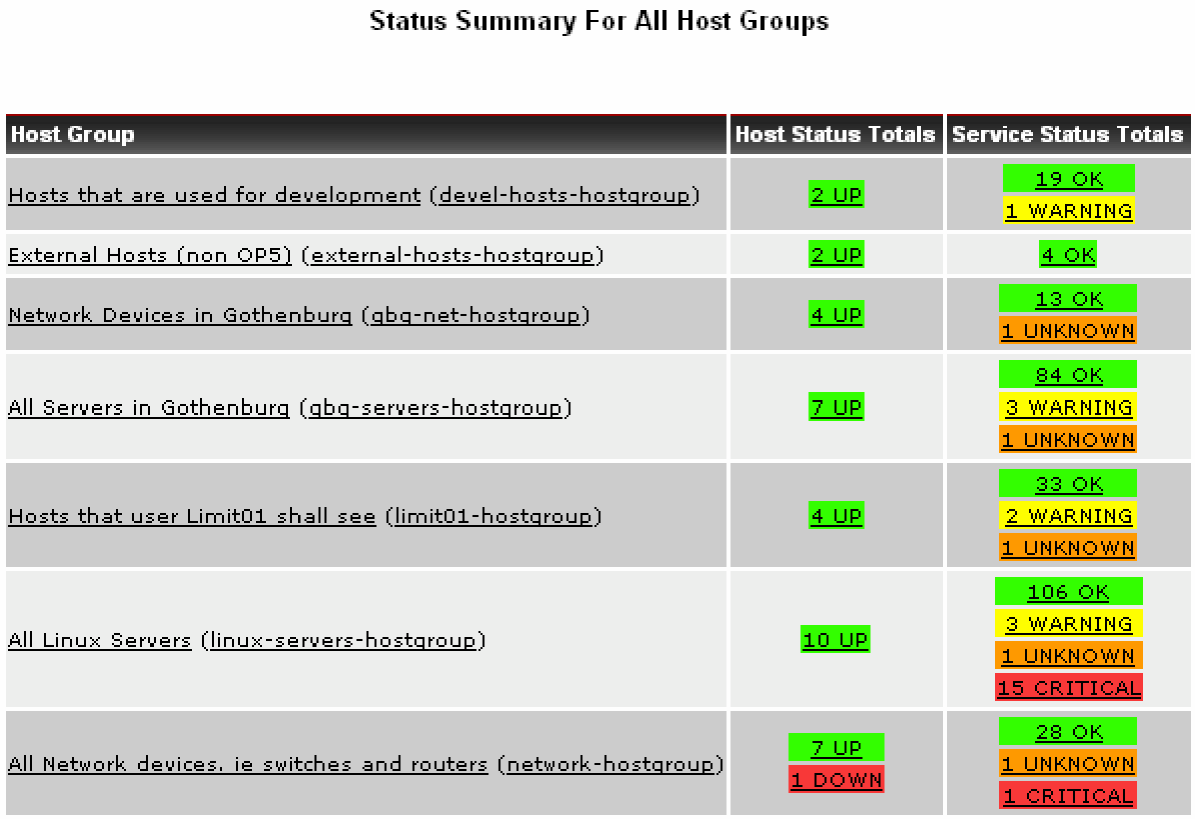
Many views below Monitoring provide you with the ability to filter what the page shall display. If you click on any of the links below “Host Status Totals” and “Service Status Totals” a textbox named “Display Filters” shows. This box tells you the filter that has been defined. Default mode is no filter applied. Filters are used at many places in op5 Monitor, for example when you click on some of the links in Tactical Overview.

Host group Summary, Overview and Grid

A host group is used to group one or more hosts together for display purposes. You can for example create host groups to reflect the geographical locations of your hosts or type of host. A host can be a member of several host groups.

The available views for host groups are:

Host group Summary

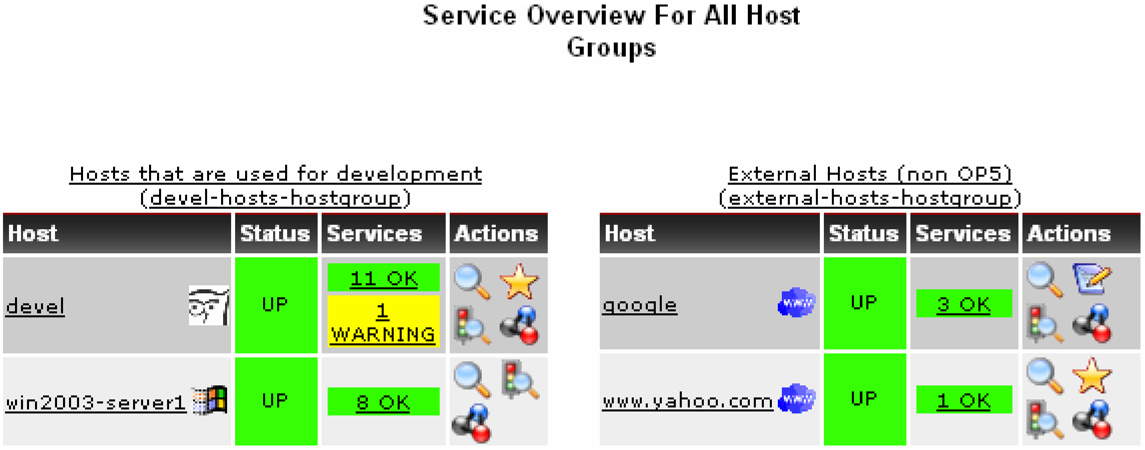


Status Summary For All Host Groups

Host Group	Host Status Totals	Service Status Totals
Hosts that are used for development (devel-hosts-hostgroup)	2 UP	19 OK 1 WARNING
External Hosts (non OP5) (external-hosts-hostgroup)	2 UP	4 OK
Network Devices in Gothenburg (gbg-net-hostgroup)	4 UP	13 OK 1 UNKNOWN
All Servers in Gothenburg (gbg-servers-hostgroup)	7 UP	84 OK 3 WARNING 1 UNKNOWN
Hosts that user Limit01 shall see (limit01-hostgroup)	4 UP	33 OK 2 WARNING 1 UNKNOWN
All Linux Servers (linux-servers-hostgroup)	10 UP	106 OK 3 WARNING 1 UNKNOWN 15 CRITICAL
All Network devices, ie switches and routers (network-hostgroup)	7 UP 1 DOWN	28 OK 1 UNKNOWN 1 CRITICAL

Hostgroup Summary shows you a table with a row for each host group and three columns, Host Group, Host Status Totals and Service Status totals. This is a god view if you quickly want to get a summary of all your host groups.

Host group Overview



Service Overview For All Host Groups

Hosts that are used for development (devel-hosts-hostgroup)

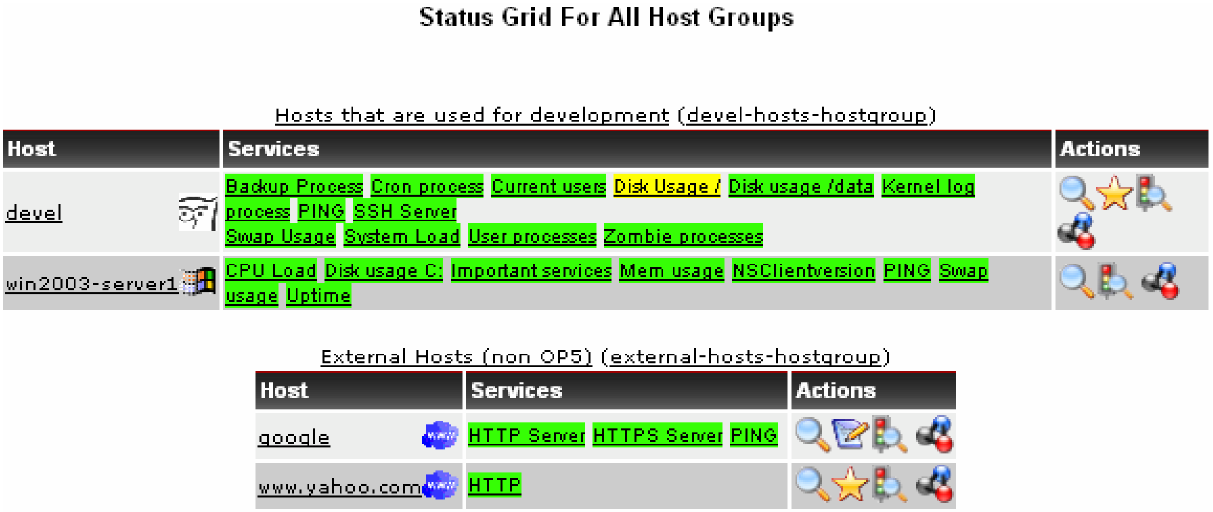
Host	Status	Services	Actions
devel	UP	11 OK 1 WARNING	
win2003-server1	UP	8 OK	

External Hosts (non OP5) (external-hosts-hostgroup)

Host	Status	Services	Actions
google	UP	3 OK	
www.yahoo.com	UP	1 OK	

Hostgroup Overview draws one table per host group listing each host and a summary of service status totals.

Host group Grid



Status Grid For All Host Groups

Hosts that are used for development (devel-hosts-hostgroup)

Host	Services	Actions
devel	Backup Process Cron process Current users Disk Usage / Disk usage /data Kernel log process PING SSH Server Swap Usage System Load User processes Zombie processes	
win2003-server1	CPU Load Disk usage C: Important services Mem usage NSClientversion PING Swap usage Uptime	

External Hosts (non OP5) (external-hosts-hostgroup)

Host	Services	Actions
google	HTTP Server HTTPS Server PING	
www.yahoo.com	HTTP	

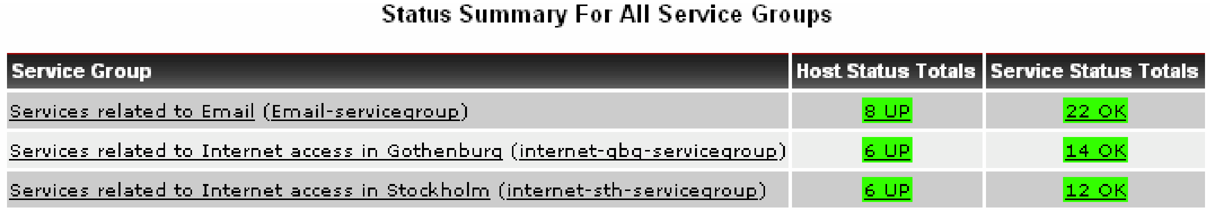
Hostgroup Grid is the most detailed view it shows one table per host group listing each host and service with colors representing status.

Service group Summary, Overview and Grid

A servicegroup definition is used to group one or more services together for display purposes. You can for example create a group and include all services related to a specific service you provide, process, disk usage, cpu usage, internet connectivity and so on. You can also create groups based on service type. A service can be a member of more than one service group. The service groups can also be used when creating Availability reports.

The available views for service groups are:

Service group Summary

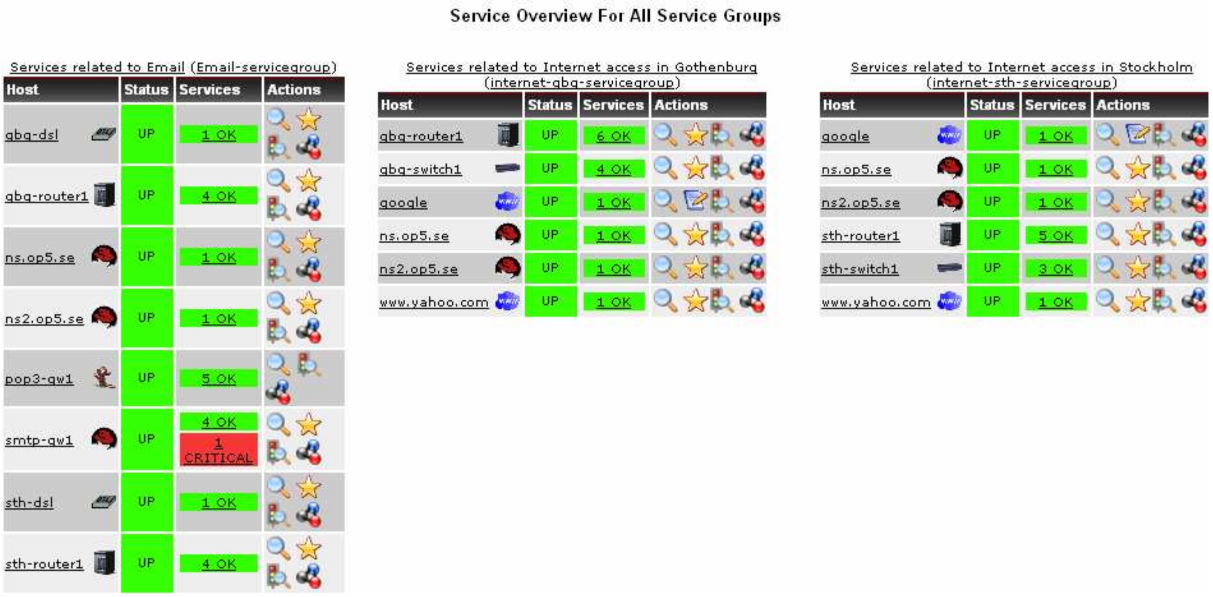


Status Summary For All Service Groups

Service Group	Host Status Totals	Service Status Totals
Services related to Email (Email-servicegroup)	8 UP	22 OK
Services related to Internet access in Gothenburg (internet-gbg-servicegroup)	6 UP	14 OK
Services related to Internet access in Stockholm (internet-sth-servicegroup)	6 UP	12 OK

Servicegroup Summary shows you a table with a row for each service group and three fields, Service Group, Host Status Totals and Service Status Totals. This is a god view if you quickly want to get a summary of all your service groups.

Service group Overview



Service Overview For All Service Groups

Services related to Email (Email-servicegroup)

Host	Status	Services	Actions
gbg-dsl	UP	1 OK	
gbg-router1	UP	4 OK	
ns.op5.se	UP	1 OK	
ns2.op5.se	UP	1 OK	
pop3-gw1	UP	5 OK	
smtp-gw1	UP	4 OK 1 CRITICAL	
sth-dsl	UP	1 OK	
sth-router1	UP	4 OK	

Services related to Internet access in Gothenburg (internet-gbg-servicegroup)

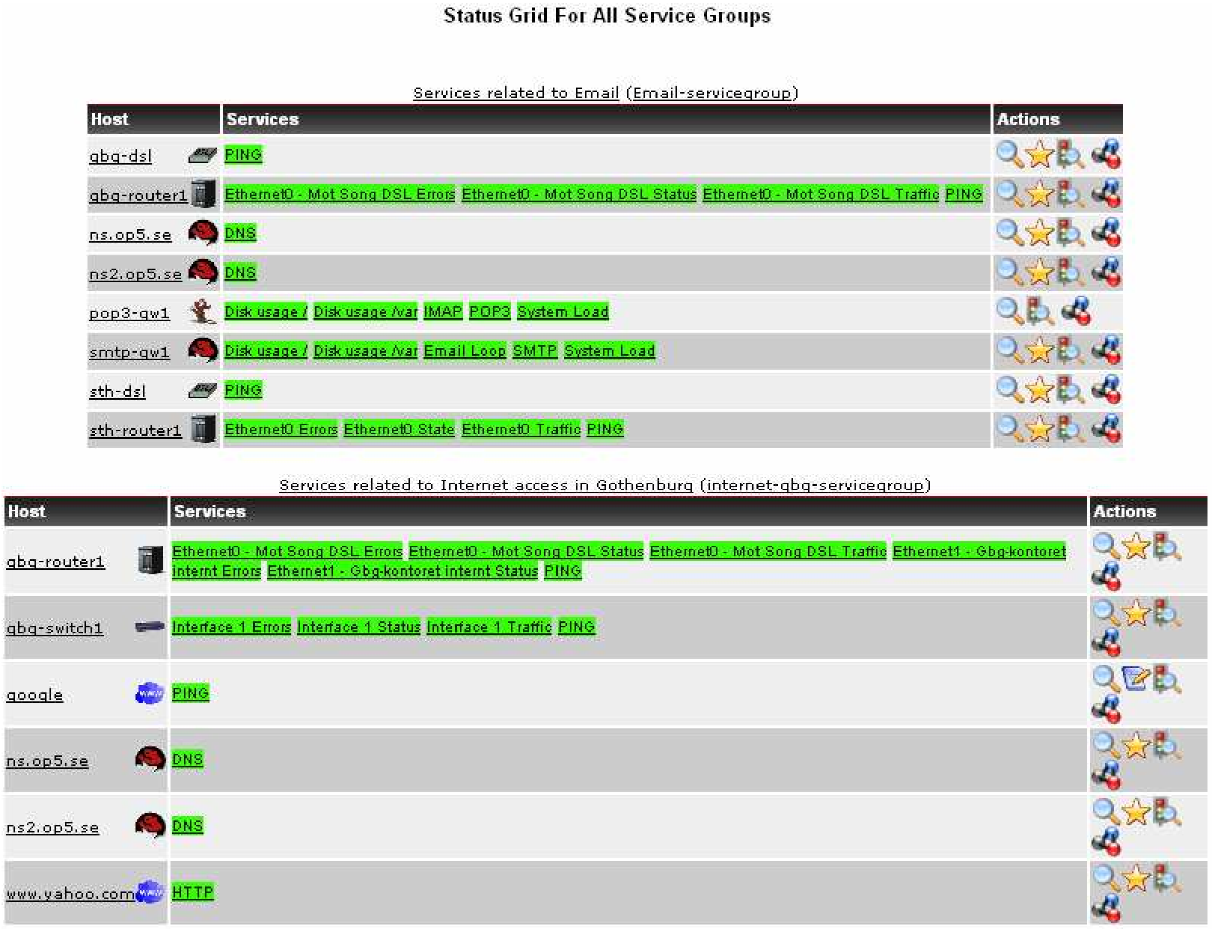
Host	Status	Services	Actions
gbg-router1	UP	6 OK	
gbg-switch1	UP	4 OK	
google	UP	1 OK	
ns.op5.se	UP	1 OK	
ns2.op5.se	UP	1 OK	
www.yahoo.com	UP	1 OK	

Services related to Internet access in Stockholm (internet-sth-servicegroup)

Host	Status	Services	Actions
google	UP	1 OK	
ns.op5.se	UP	1 OK	
ns2.op5.se	UP	1 OK	
sth-router1	UP	5 OK	
sth-switch1	UP	3 OK	
www.yahoo.com	UP	1 OK	

Servicegroup Overview draws one table per service group listing each host and a summary of service status totals.

Service group Grid



Status Grid For All Service Groups

Services related to Email (Email-servicegroup)

Host	Services	Actions
gbg-dsl	PING	
gbg-router1	Ethernet0 - Mot Song DSL Errors Ethernet0 - Mot Song DSL Status Ethernet0 - Mot Song DSL Traffic PING	
ns.op5.se	DNS	
ns2.op5.se	DNS	
pop3-gw1	Disk usage / Disk usage /var IMAP POP3 System Load	
smtp-gw1	Disk usage / Disk usage /var Email Loop SMTP System Load	
sth-dsl	PING	
sth-router1	Ethernet0 Errors Ethernet0 State Ethernet0 Traffic PING	

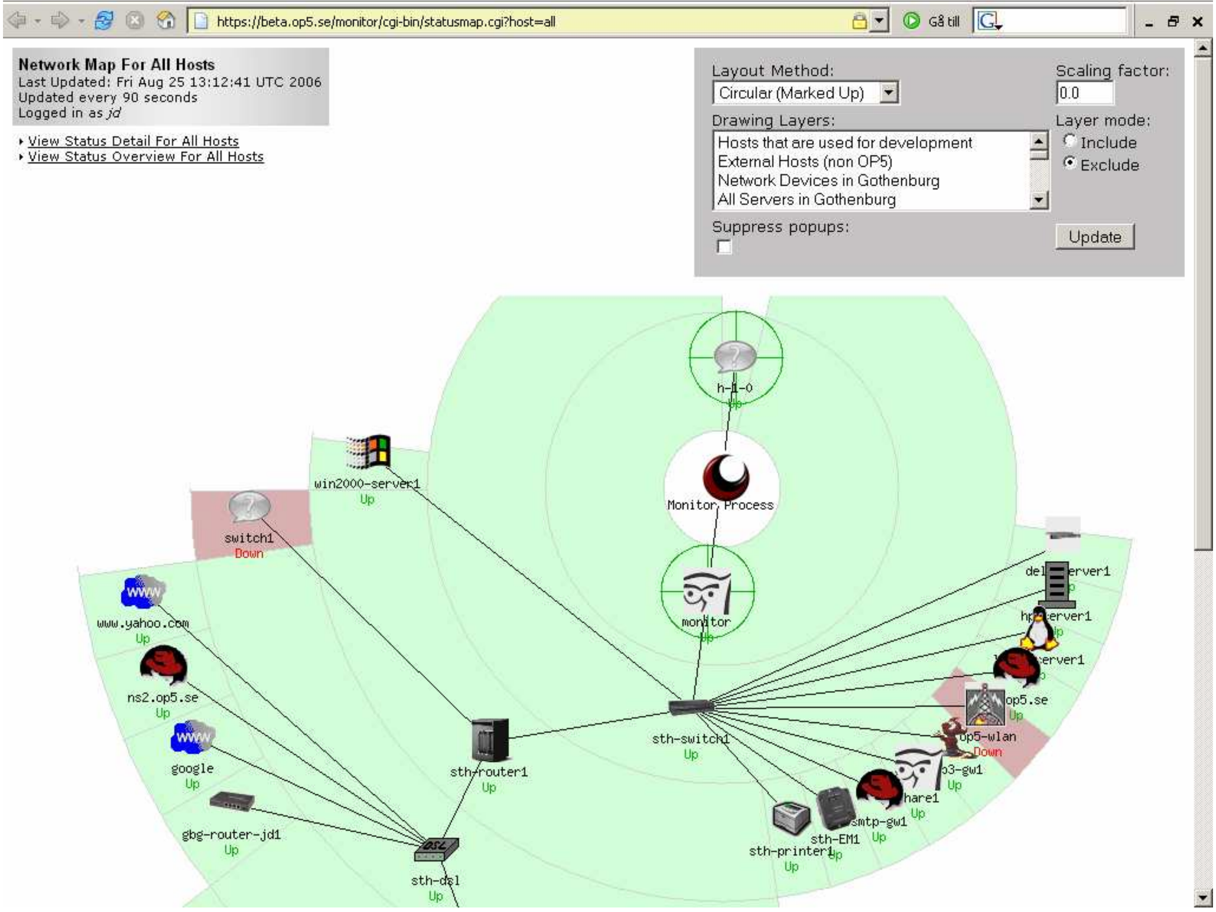
Services related to Internet access in Gothenburg (internet-gbg-servicegroup)

Host	Services	Actions
gbg-router1	Ethernet0 - Mot Song DSL Errors Ethernet0 - Mot Song DSL Status Ethernet0 - Mot Song DSL Traffic Ethernet1 - Gbg-kontoret internt Errors Ethernet1 - Gbg-kontoret internt Status PING	
gbg-switch1	Interface 1 Errors Interface 1 Status Interface 1 Traffic PING	
google	PING	
ns.op5.se	DNS	
ns2.op5.se	DNS	
www.yahoo.com	HTTP	

Servicegroup Grid is the most detailed view it shows one table per service group listing each host and service with colors representing status.

Status Map

The Status Map gives you a graphical view of the network including the relations between the hosts. The Map also shows what parts of the network that is functional, non-functional and if there are any network outages.



https://beta.op5.se/monitor/cgi-bin/statusmap.cgi?host=all

Network Map For All Hosts
Last Updated: Fri Aug 25 13:12:41 UTC 2006
Updated every 90 seconds
Logged in as *jd*

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

Layout Method: Circular (Marked Up)

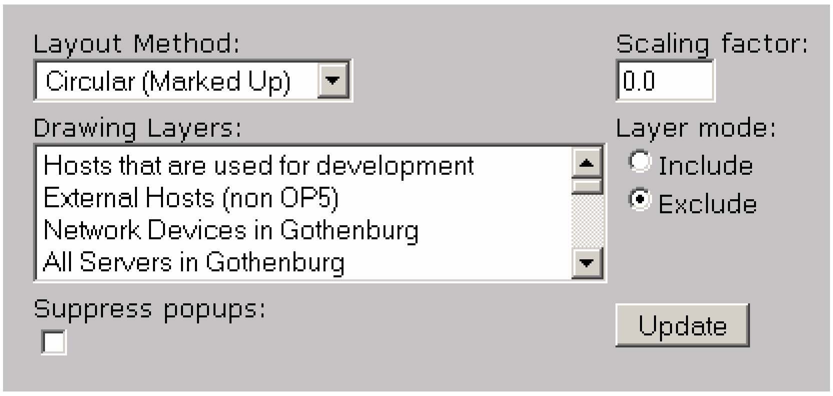
Scaling factor: 0.0

Drawing Layers:
Hosts that are used for development
External Hosts (non OP5)
Network Devices in Gothenburg
All Servers in Gothenburg

Layer mode: ○ Include ● Exclude

Suppress popups: □

In the upper right corner you can change a couple of settings that controls the layout and behavior for the status map.



Layout Method: Circular (Marked Up)

Scaling factor: 0.0

Drawing Layers:
Hosts that are used for development
External Hosts (non OP5)
Network Devices in Gothenburg
All Servers in Gothenburg

Layer mode: ○ Include ● Exclude

Suppress popups: □

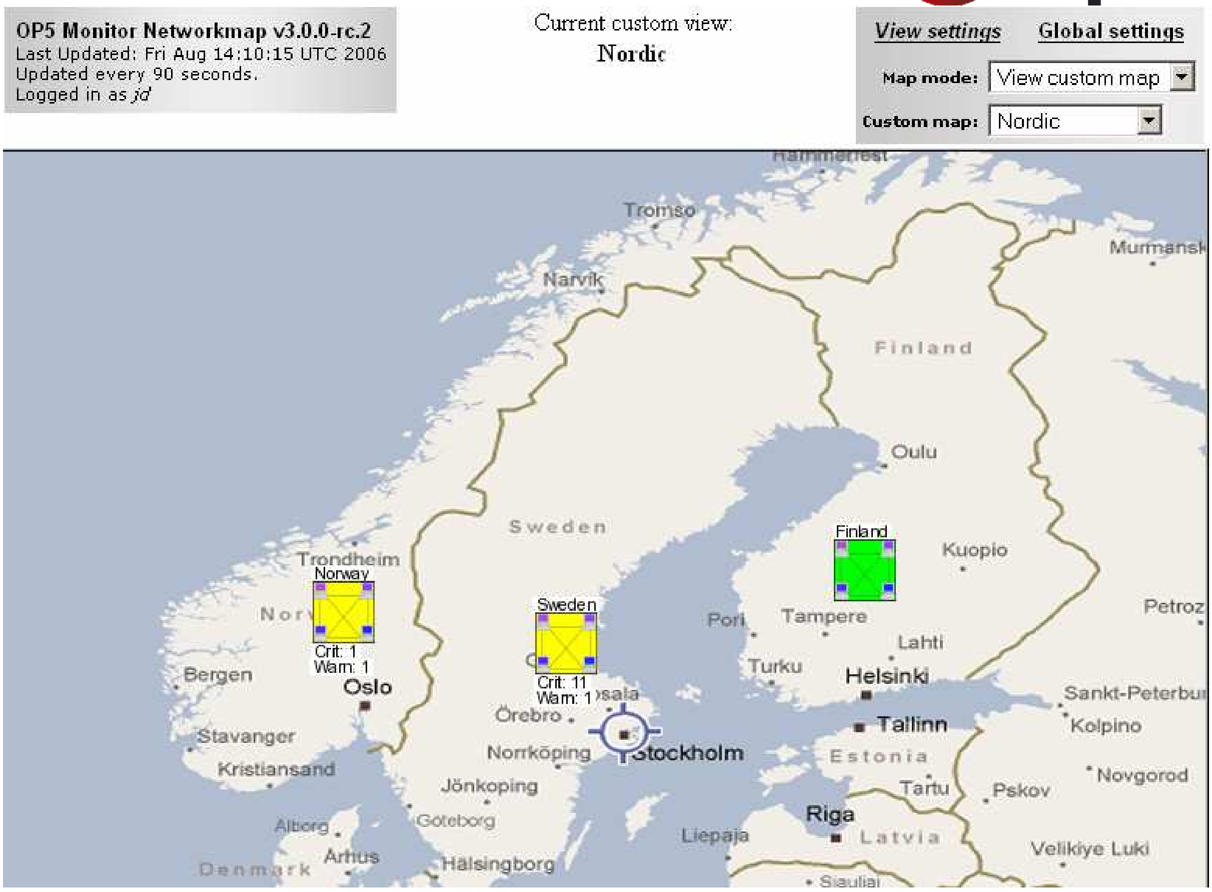
- Layout Method, there are a couple of layout methods available
  - User-supplied coords, you can configure x and y coords for your hosts (see host Extras for more information)

    - Depth layers, shows only one level of the network at a time. Click on a host to display the host and the underlying layer.
    - Collapsed tree, shows the network in a tree layout with everything centered towards the middle
    - Balanced tree, shows the network in a tree layout but with the underlying levels centered below each parent host.
    - Circular, shows a circular layout.
    - Circular (Marked Up), this is the default selection. It shows a circular layout with a background that shows the different levels of the network and also changes color depending of the status of the hosts.
    - Circular (Balloon), shows a circular layout with each host represented as a balloon with the size determined of how many services that are monitored for the host. More services gives you larger balloons.
- Drawing Layers, together with Layer mode you can select to include or exclude hosts based on hostgroup from the status map. Default is to show all hosts.
- Scaling factor, simply changes the size of the status map image. 0.0 is default, if you want to display half the size enter 0.5, double the size 2.0 and so on.

Note: If your network is large or designed in a flat way, for example a layer 2 ethernet network, the status map isn’t really usable. Take a look at Network Map or Hyper Map instead.

Network Map

The network map is an enhanced version of the status map with possibility to create highly customized views of a network by just click and place hosts, host groups and views on a map.



OP5 Monitor Networkmap v3.0.0-rc.2
Last Updated: Fri Aug 14:10:15 UTC 2006
Updated every 90 seconds.
Logged in as *jd*

Current custom view:
Nordic

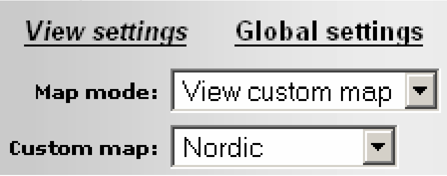
View settings Global settings

Map mode: View custom map

Custom map: Nordic

The image above shows you the default layout of the network map, a background image of the Nordic countries including 3 custom maps.

Configuration of the network map is done from the configuration box in the upper right corner



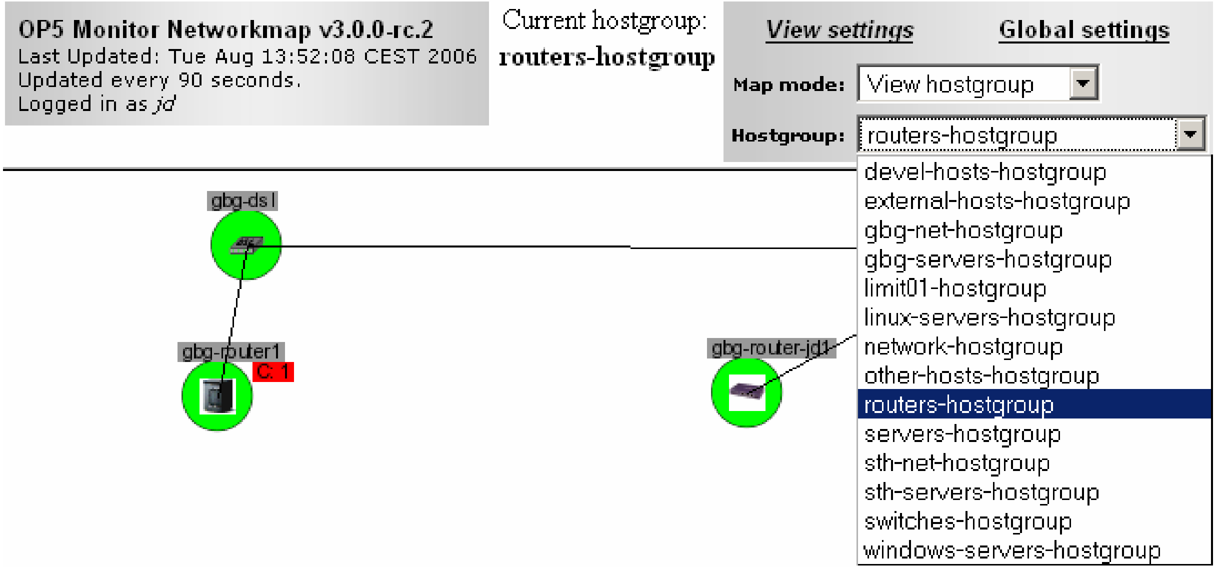
View settings Global settings

Map mode: View custom map

Custom map: Nordic

- View settings, is displayed by default and let you change Map mode. What's displayed below Map mode is determined off what you select. There are 4 available map modes, View hostgroup, View custom map (default), Edit hostgroup and Edit custom map. Each of the modes is displayed further down.
- Global Settings, lets you change refresh rate of the page and Map scale. With map scale you can change the size of your network map.

View host group



OP5 Monitor Networkmap v3.0.0-rc.2
Last Updated: Tue Aug 13:52:08 CEST 2006
Updated every 90 seconds.
Logged in as *jd*

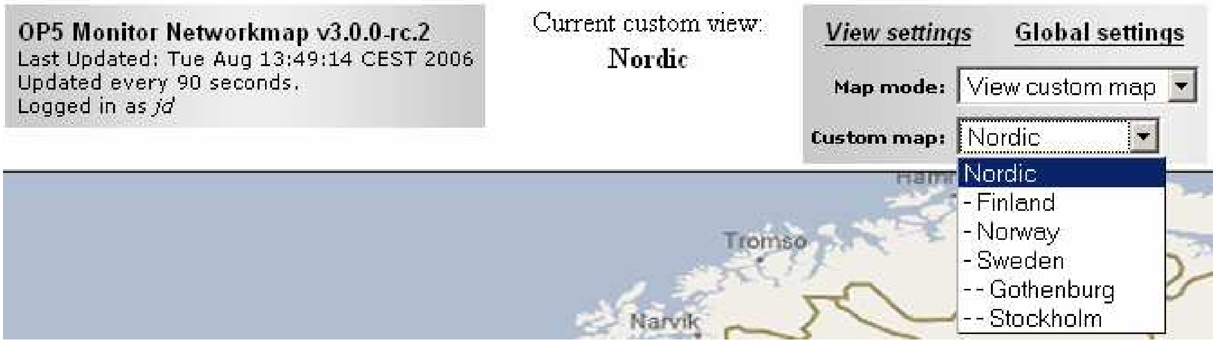
Current hostgroup:
routers-hostgroup

Map mode: View hostgroup

Hostgroup: routers-hostgroup

With View hostgroup you can view a map of each hostgroup. You get a drop down menu with all hostgroups listed.

View custom map (default)



OP5 Monitor Networkmap v3.0.0-rc.2
Last Updated: Tue Aug 13:49:14 CEST 2006
Updated every 90 seconds.
Logged in as *jd*

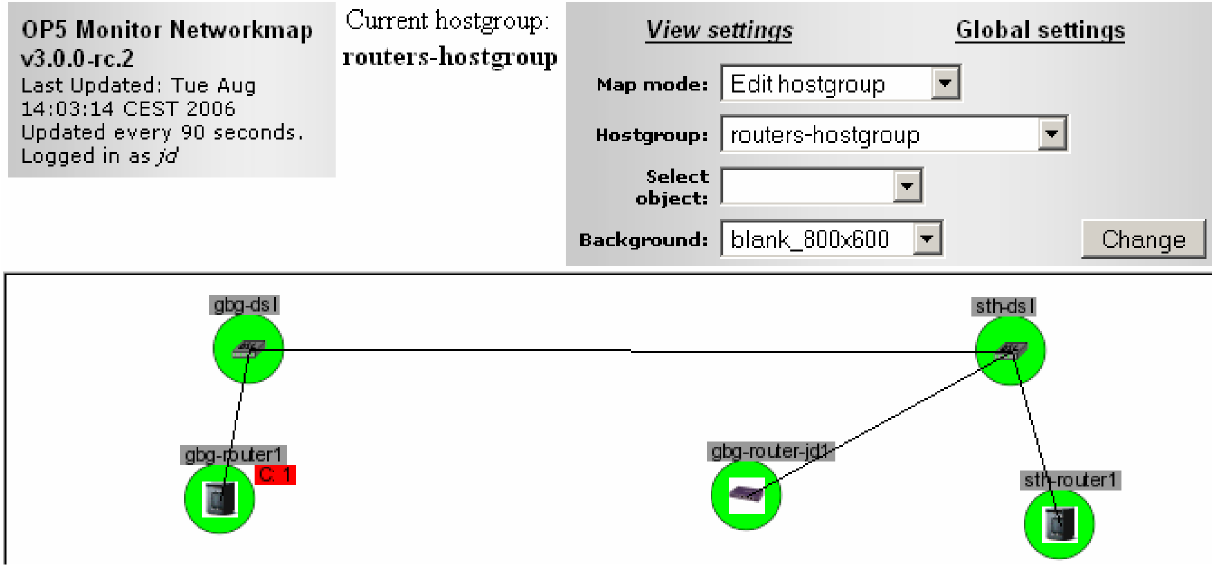
Current custom view:
Nordic

Map mode: View custom map

Custom map: Nordic

View custom map let you select from all custom maps that are defined. Custom maps are configured with Edit custom map.

Edit host group



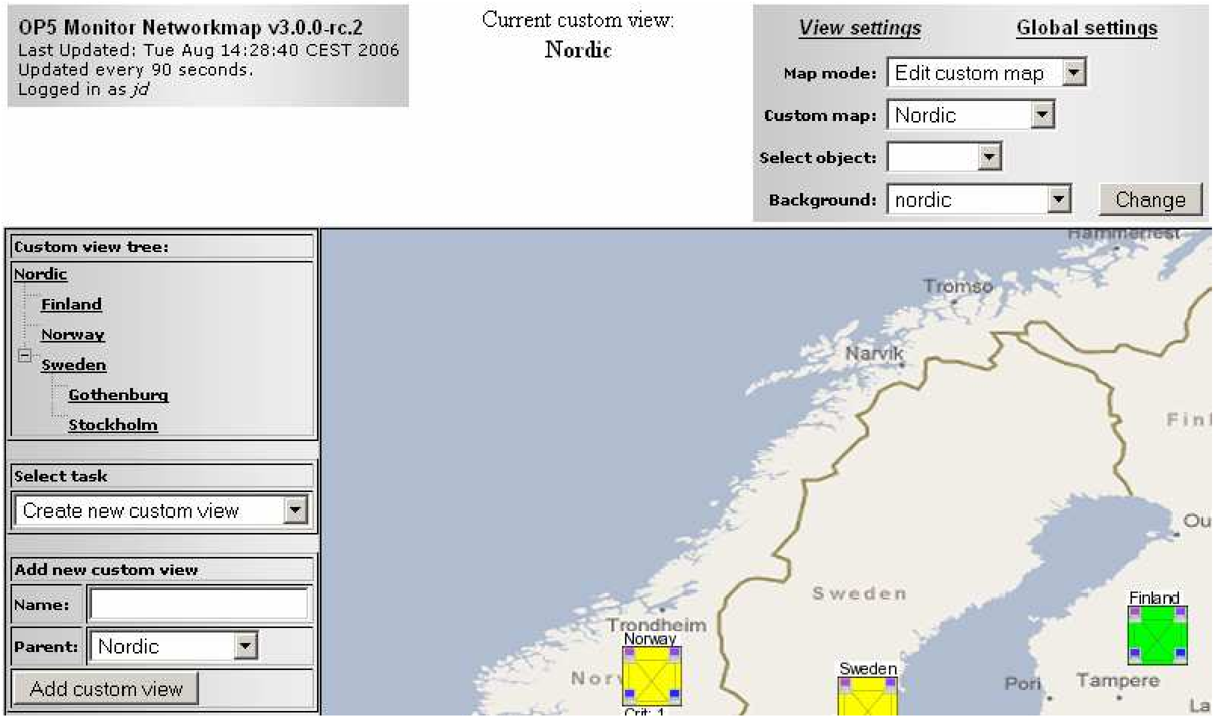
OP5 Monitor Networkmap v3.0.0-rc.2
Last Updated: Tue Aug 14:03:14 CEST 2006
Updated every 90 seconds.
Logged in as *jd*

Current hostgroup:
routers-hostgroup

Map mode: Edit hostgroup
Hostgroup: routers-hostgroup
Select object:
Background: blank_800x600

Here you can configure the layout of the hosts. You can place the hosts where you want either clicking on the host you want to move or select it from the “Select object:” drop down menu and then click on the new location for the host.

Edit custom map



OP5 Monitor Networkmap v3.0.0-rc.2
Last Updated: Tue Aug 14:28:40 CEST 2006
Updated every 90 seconds.
Logged in as *jd*

Current custom view:
Nordic

Map mode: Edit custom map
Custom map: Nordic
Select object:
Background: nordic

Custom view tree:
Nordic
Finland
Norway
Sweden
Gothenburg
Stockholm

Select task: Create new custom view

Add new custom view
Name:
Parent: Nordic

Custom maps are configured in a tree hierarchy. This makes it possible to have several network layers.

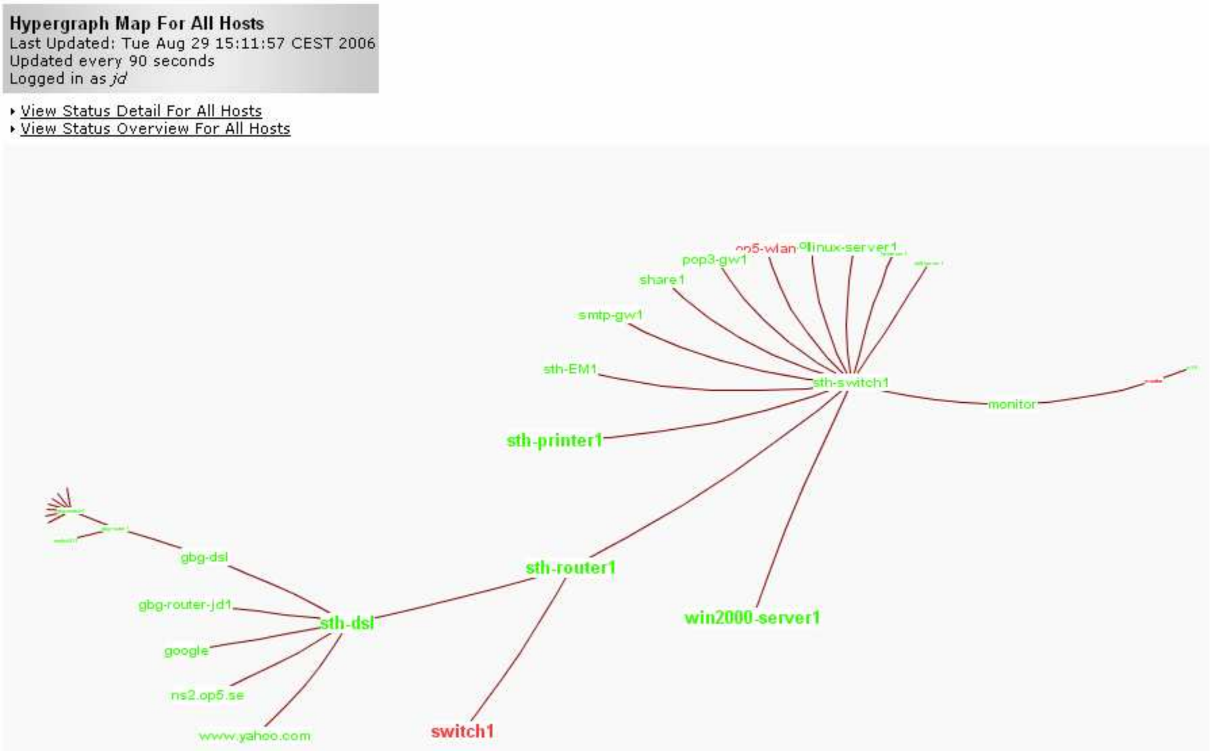
In the top you have “Custom view tree:” where you can navigate through the tree. Below you have “Select task”.

Available tasks are:

- **Create new custom view:** Allows you to create new views

- **Rename this view:** Allows you to rename the selected view
- **Add items to this view:** Allows you to add items (host groups and hosts) to the selected view
- **Remove items from this view:** Allows you to remove items (host groups and hosts) from the selected view
- **Handle background images:** Allows you to upload new background images (must be .png format), Set default background and delete existing background images.

Hyper Map



Hypergraph Map For All Hosts
Last Updated: Tue Aug 29 15:11:57 CEST 2006
Updated every 90 seconds
Logged in as *jd*

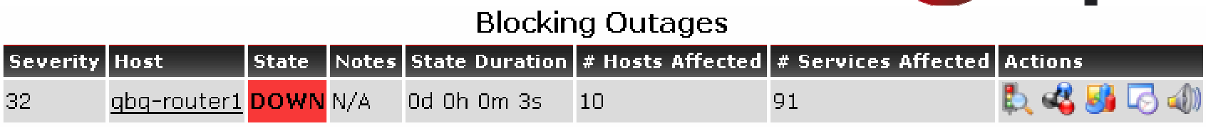
- View Status Detail For All Hosts
- View Status Overview For All Hosts

Hyper Map is a new map introduced in op5 Monitor 3.0. It is a java applet that draws all hosts and connections and then let you, by using the mouse. Drag the map or click in it to change its layout.

If you click on a spot on the map it will center itself to that spot. If you hold the mouse pointer over a host you will se a status summary for the host. If you click on a host you will get to the service detail page for that host.

Network Outages

By using event correlation op5 Monitor will suppress all host alarms that comes from hosts behind a faulty host. Monitor is preconfigured with knowledge of the physical 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 is any number of things which might actually be the cause of the problem.

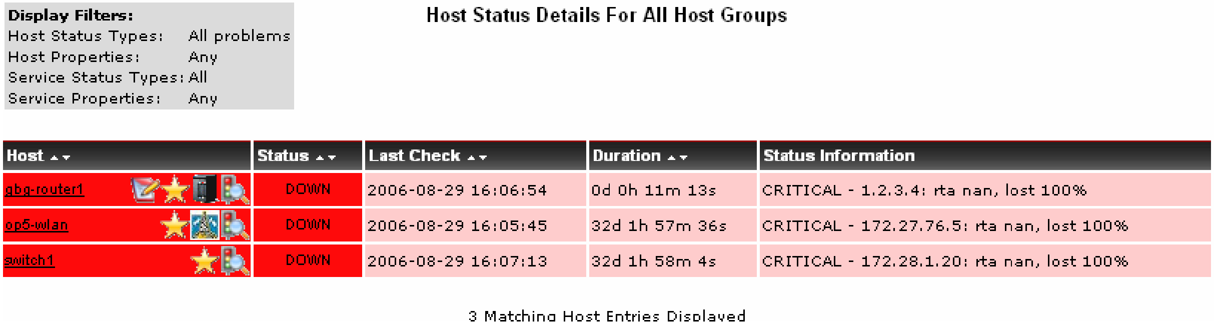


Blocking Outages

Severity	Host	State	Notes	State Duration	# Hosts Affected	# Services Affected	Actions
32	gbg-router1	DOWN	N/A	0d 0h 0m 3s	10	91	

- **Severity:** 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:** Name of the host causing the network outage
- **State:** State of the host
- **Notes:** Link to comments for the host, if there are no comments N/A is displayed
- **State Duration:** For how long has the outage been going on
- **Hosts Affected:** Number of hosts affected by the outage
- **Services Affected:** Number of services affected by the outage
- **Actions:** A couple of icons that links you to different status pages. For a full list of icons and images se **Fel! Hittar inte referenskälla.**.

Host Problems



Display Filters:
Host Status Types: All problems
Host Properties: Any
Service Status Types: All
Service Properties: Any

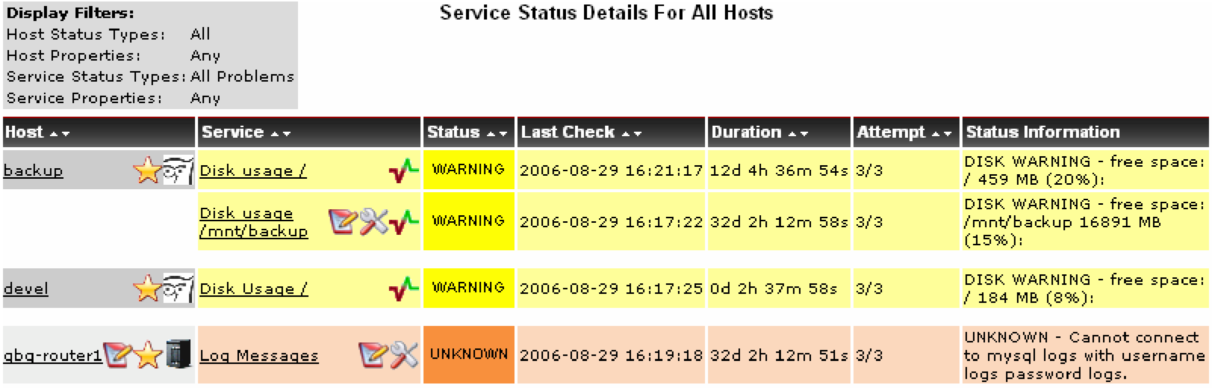
Host Status Details For All Host Groups

Host	Status	Last Check	Duration	Status Information
gbg-router1	DOWN	2006-08-29 16:06:54	0d 0h 11m 13s	CRITICAL - 1.2.3.4: rta nan, lost 100%
op5-wlan	DOWN	2006-08-29 16:05:45	32d 1h 57m 36s	CRITICAL - 172.27.76.5: rta nan, lost 100%
switch1	DOWN	2006-08-29 16:07:13	32d 1h 58m 4s	CRITICAL - 172.28.1.20: rta nan, lost 100%

3 Matching Host Entries Displayed

The host problems view is similar to the Host Detail view. The difference is the display of status, The host problems view only shows hosts in a non ok state.

Service Problems



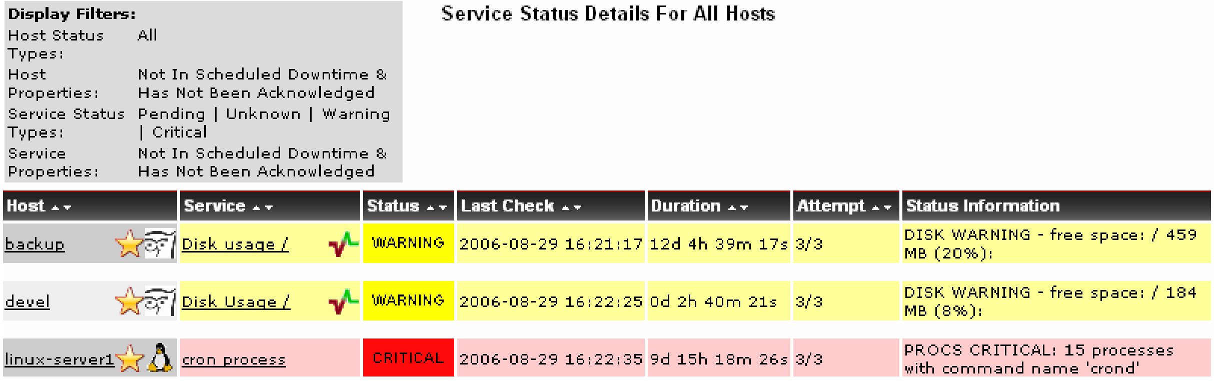
Display Filters:
Host Status Types: All
Host Properties: Any
Service Status Types: All Problems
Service Properties: Any

Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
backup	Disk usage /	WARNING	2006-08-29 16:21:17	12d 4h 36m 54s	3/3	DISK WARNING - free space: / 459 MB (20%):
	Disk usage /mnt/backup	WARNING	2006-08-29 16:17:22	32d 2h 12m 58s	3/3	DISK WARNING - free space: /mnt/backup 16891 MB (15%):
devel	Disk Usage /	WARNING	2006-08-29 16:17:25	0d 2h 37m 58s	3/3	DISK WARNING - free space: / 184 MB (8%):
gbg-router1	Log Messages	UNKNOWN	2006-08-29 16:19:18	32d 2h 12m 51s	3/3	UNKNOWN - Cannot connect to mysql logs with username logs password logs.

The service problems view is similar to the Service Detail view. The difference is the display of status, service problems only shows services in a non ok state.

Unhandled Problems



Display Filters:

Host Status Types:	All
Host Properties:	Not In Scheduled Downtime & Has Not Been Acknowledged
Service Status Types:	Pending | Unknown | Warning | Critical
Service Properties:	Not In Scheduled Downtime & Has Not Been Acknowledged

Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
backup	Disk usage /	WARNING	2006-08-29 16:21:17	12d 4h 39m 17s	3/3	DISK WARNING - free space: / 459 MB (20%):
devel	Disk Usage /	WARNING	2006-08-29 16:22:25	0d 2h 40m 21s	3/3	DISK WARNING - free space: / 184 MB (8%):
linux-server1	cron process	CRITICAL	2006-08-29 16:22:35	9d 15h 18m 26s	3/3	PROCS CRITICAL: 15 processes with command name 'crond'

Unhandled problems show all problems that is not in scheduled downtime, or has not been acknowledged as stated in the Display Filter info box.

The idea of this view is that is should give the user a good view of new problems that hasn't been taken care of. Unhandled Problems is a good status view for helpdesk staff.

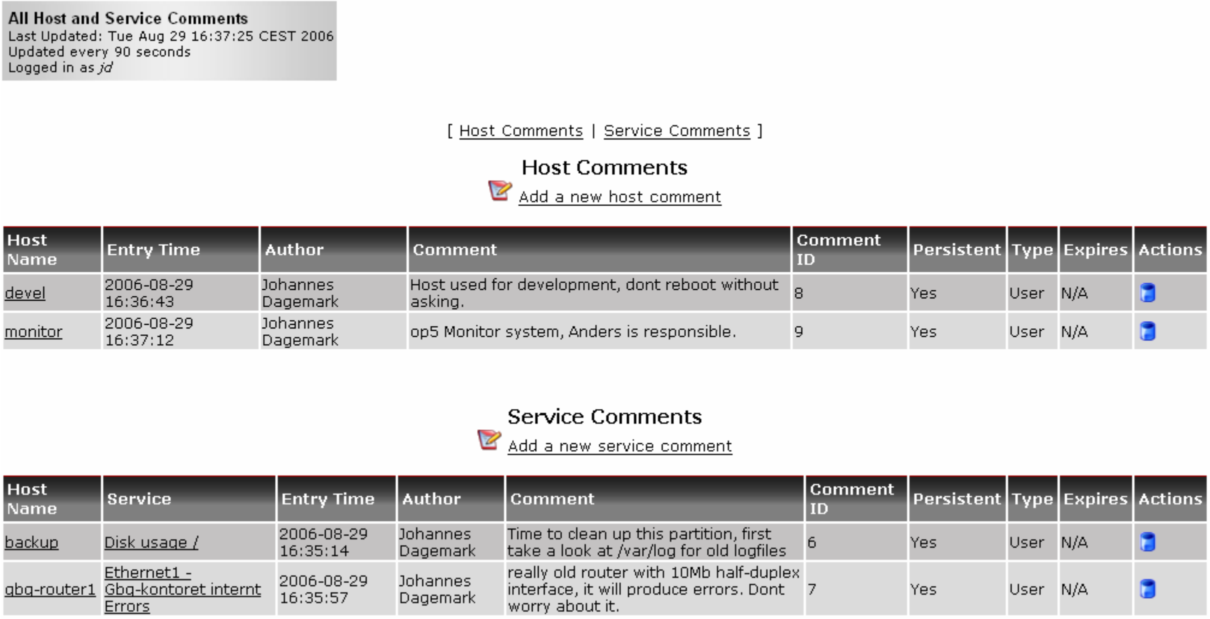
Show Host

Simple search box that let you search for a host by typing the initial letters of the host name in the field that says "show host" in the main menu. Press enter and the host and its services detail will be shown.

Note: This is really a simple search, it will only show the first match and the search is case sensitive.

Comments

All hosts and service can have one or more comments related to it. A comment is a free text note of your choice.



All Host and Service Comments
Last Updated: Tue Aug 29 16:37:25 CEST 2006
Updated every 90 seconds
Logged in as *jd*

[Host Comments | Service Comments]

Host Comments

Add a new host comment

Host Name	Entry Time	Author	Comment	Comment ID	Persistent	Type	Expires	Actions
devel	2006-08-29 16:36:43	Johannes Dagemark	Host used for development, dont reboot without asking.	8	Yes	User	N/A	🗑
monitor	2006-08-29 16:37:12	Johannes Dagemark	op5 Monitor system, Anders is responsible.	9	Yes	User	N/A	🗑

Service Comments

Add a new service comment

Host Name	Service	Entry Time	Author	Comment	Comment ID	Persistent	Type	Expires	Actions
backup	Disk usage /	2006-08-29 16:35:14	Johannes Dagemark	Time to clean up this partition, first take a look at /var/log for old logfiles	6	Yes	User	N/A	🗑
gbg-router1	Ethernet1 - Gbg-kontoret internt Errors	2006-08-29 16:35:57	Johannes Dagemark	really old router with 10Mb half-duplex interface, it will produce errors. Dont worry about it.	7	Yes	User	N/A	🗑

Host name: The host the comment is related to.
Service: The service the comment is related to.
Entry Time: Date and time when the comment was added.

Author: The author of the comment.
Comment: The comment itself.
Comment ID: A Unique ID number for the comment, it 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.
Type: What kind of comment, User, System or acknowledgement.
Expires: This is only used for comments automatically added by the system such as scheduled downtime or flapping comments.
Actions: Possibility to delete a comment.

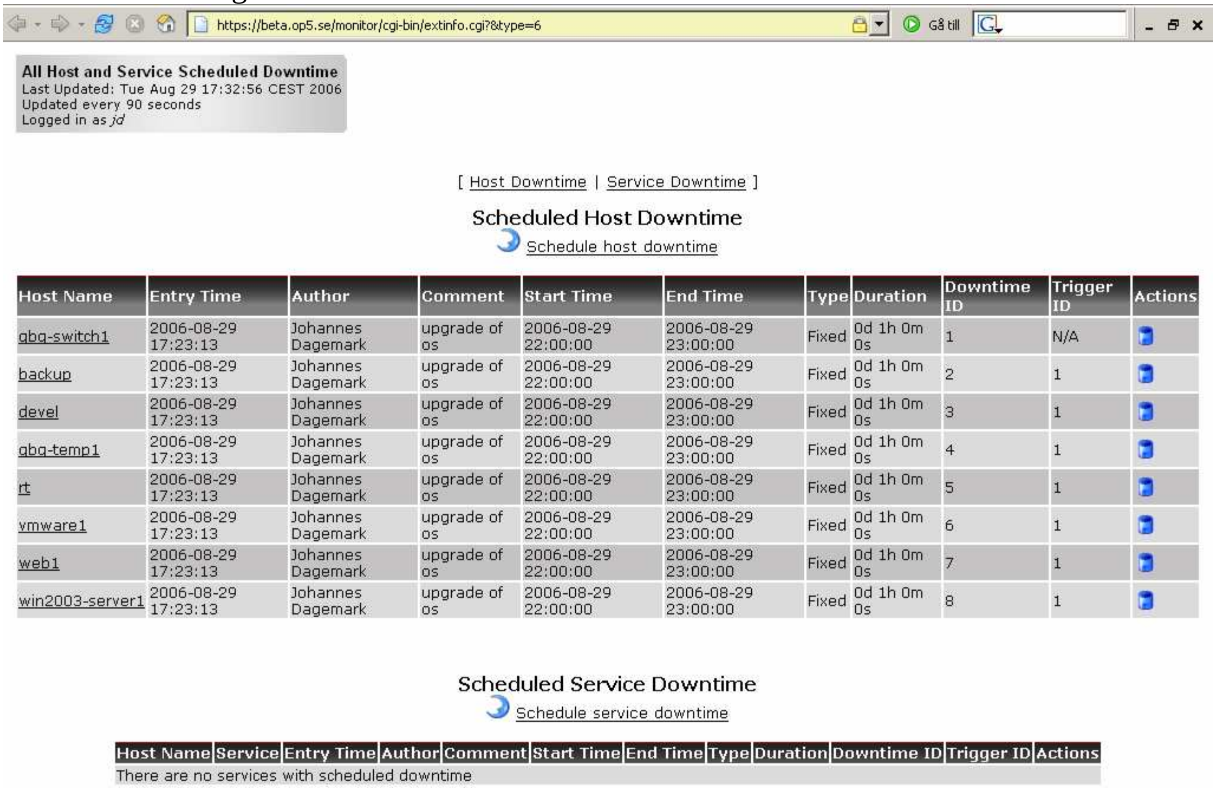
Downtime

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 op5 Monitor informs you about when a host or service is scheduled for downtime through the web interface. Information about the scheduled downtime is also stored in the logs so that planned system work does not affect availability reports (read more on Availability).

It is possible to schedule downtime for hosts, services, entire host groups and service groups. You can also configure triggered downtime for hosts located below a host currently during scheduled downtime.

Basically the window consists of shortcuts to the currently configured scheduled downtime for hosts and services. There is also a links to schedule downtime. Those links can be reached from each host and service view as well.

The rest is a listing of all scheduled downtime.



All Host and Service Scheduled Downtime
Last Updated: Tue Aug 29 17:32:56 CEST 2006
Updated every 90 seconds
Logged in as *jd*

[Host Downtime | Service Downtime]

Scheduled Host Downtime

Schedule host downtime

Host Name	Entry Time	Author	Comment	Start Time	End Time	Type	Duration	Downtime ID	Trigger ID	Actions
gbg-switch1	2006-08-29 17:23:13	Johannes Dagemark	upgrade of os	2006-08-29 22:00:00	2006-08-29 23:00:00	Fixed	0d 1h 0m 0s	1	N/A	🗑
backup	2006-08-29 17:23:13	Johannes Dagemark	upgrade of os	2006-08-29 22:00:00	2006-08-29 23:00:00	Fixed	0d 1h 0m 0s	2	1	🗑
devel	2006-08-29 17:23:13	Johannes Dagemark	upgrade of os	2006-08-29 22:00:00	2006-08-29 23:00:00	Fixed	0d 1h 0m 0s	3	1	🗑
gbg-temp1	2006-08-29 17:23:13	Johannes Dagemark	upgrade of os	2006-08-29 22:00:00	2006-08-29 23:00:00	Fixed	0d 1h 0m 0s	4	1	🗑
rt	2006-08-29 17:23:13	Johannes Dagemark	upgrade of os	2006-08-29 22:00:00	2006-08-29 23:00:00	Fixed	0d 1h 0m 0s	5	1	🗑
vmware1	2006-08-29 17:23:13	Johannes Dagemark	upgrade of os	2006-08-29 22:00:00	2006-08-29 23:00:00	Fixed	0d 1h 0m 0s	6	1	🗑
web1	2006-08-29 17:23:13	Johannes Dagemark	upgrade of os	2006-08-29 22:00:00	2006-08-29 23:00:00	Fixed	0d 1h 0m 0s	7	1	🗑
win2003-server1	2006-08-29 17:23:13	Johannes Dagemark	upgrade of os	2006-08-29 22:00:00	2006-08-29 23:00:00	Fixed	0d 1h 0m 0s	8	1	🗑

Scheduled Service Downtime

Schedule service downtime

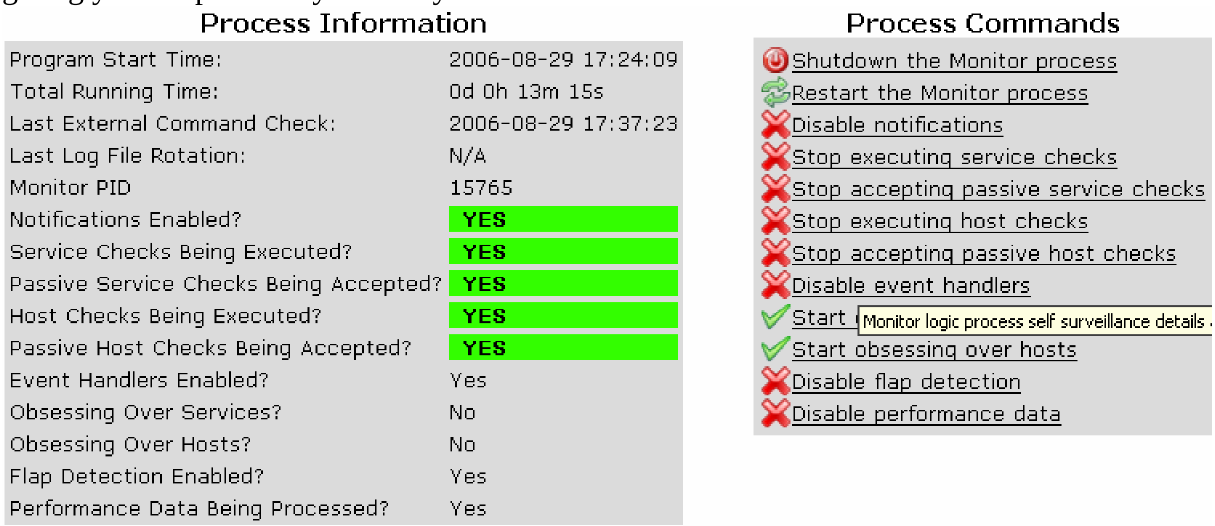
Host Name	Service	Entry Time	Author	Comment	Start Time	End Time	Type	Duration	Downtime ID	Trigger ID	Actions
There are no services with scheduled downtime											

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.
Type: 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 in-between the Start and End time and lasts as long as the configured duration (very useful if you don't really know when you will start your maintenance)
Duration: Is the duration of flexible scheduled downtime.
Downtime ID: Unique ID of the scheduled downtime.
Trigger ID: ID of the downtime that triggers start of this downtime.
Actions: Allows you to delete a configured scheduled downtime.

Process Info

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:	2006-08-29 17:24:09
Total Running Time:	0d 0h 13m 15s
Last External Command Check:	2006-08-29 17:37:23
Last Log File Rotation:	N/A
Monitor PID	15765
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?	Yes

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 Monitor logic process self surveillance details
- ✓ Start obsessing over hosts
- ✗ Disable flap detection
- ✗ Disable performance data

The process information

Program start time: The date and time when the monitor process was started or reloaded.
Total running time: The amount of time Monitor has been up and running.
Last external command check: The date and time when the last check for external commands was executed. Op5 Monitor's web gui is controlled using external commands so it needs to check for them often.
Last log file rotation: Date and time when the log files where rotated.
Monitor PID: op5 Monitor's Process ID.
Notifications enabled: (Yes or No)
Service Checks Being Executed: (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)

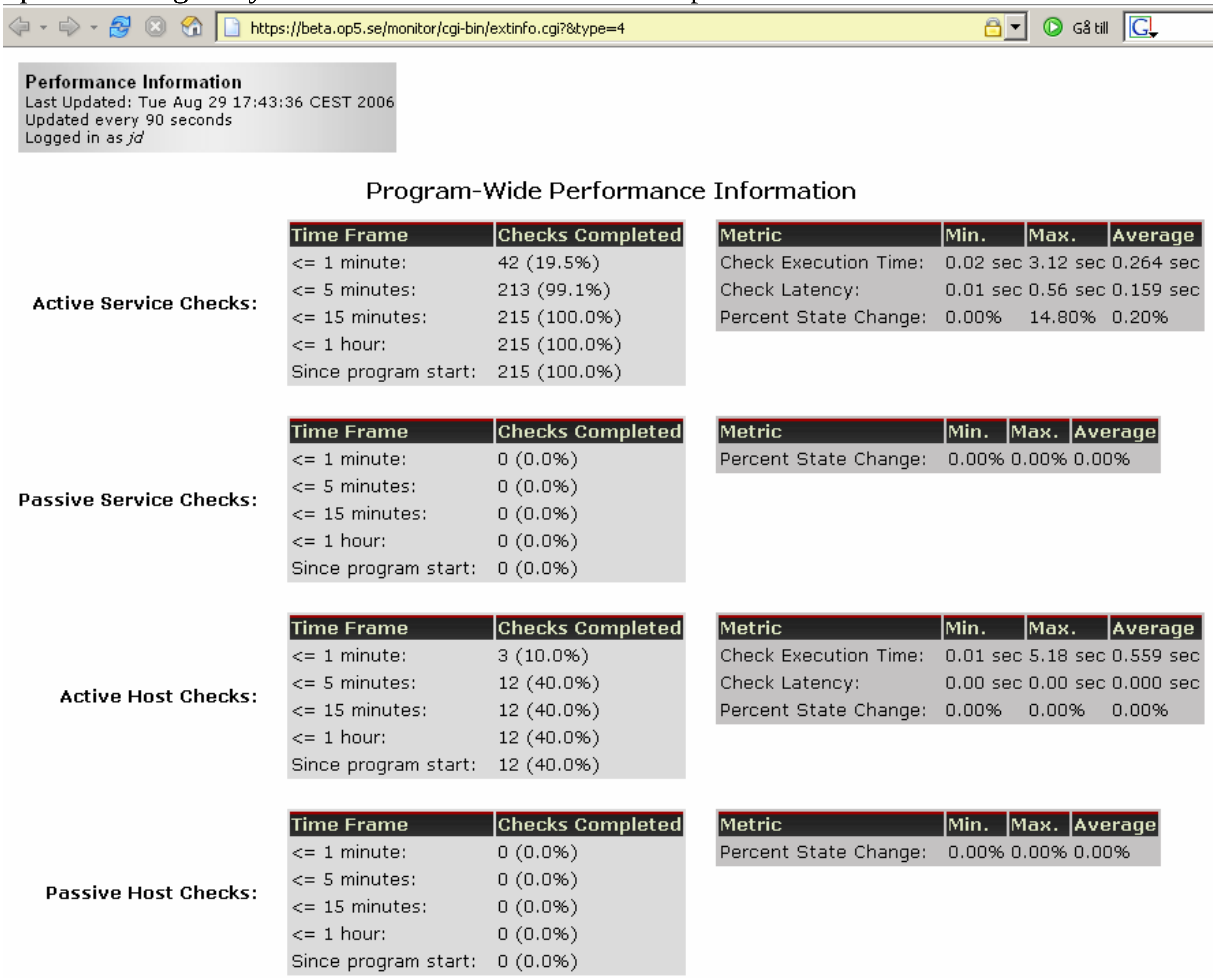
Flap Detection enabled: (Yes or No)
Performance data being processed: (Yes or No)

Process Commands

Shutdown the Monitor Process: Shutdown the Monitor program. Be aware that to start the process again you need to access the system by console or SSH, se the op5 System manual for more information.
Restart the Monitor Process: The op5 Monitor process stops and starts again.
Disable Notifications: All notifications are disabled.
Stop executing service checks: This will cause op5 Monitor to stop all execution of all service checks.
Stop accepting passive service checks: This will cause op5 Monitor to stop accepting all passive service checks.
Stop executing host checks: This will cause op5 Monitor to stop all execution of host checks.
Stop accepting passive host checks: This will cause op5 Monitor to stop receiving external host checks.
Disable event handlers: This will cause op5 Monitor to disable event handling (automatic reaction to events).
Start obsessing over services: Only used in certain redundant setups.
Start obsessing over hosts: Only used in certain redundant setups.
Disable flap detection: Disable the detection of hosts and services pending between different states.
Enable performance data: Storage of performance data for hosts and services.

Performance Info

op5 Monitor gives you detailed information about its performance.



Performance Information
Last Updated: Tue Aug 29 17:43:36 CEST 2006
Updated every 90 seconds
Logged in as *jd*

Program-Wide Performance Information

Active Service Checks:

Time Frame	Checks Completed
<= 1 minute:	42 (19.5%)
<= 5 minutes:	213 (99.1%)
<= 15 minutes:	215 (100.0%)
<= 1 hour:	215 (100.0%)
Since program start:	215 (100.0%)

Metric	Min.	Max.	Average
Check Execution Time:	0.02 sec	3.12 sec	0.264 sec
Check Latency:	0.01 sec	0.56 sec	0.159 sec
Percent State Change:	0.00%	14.80%	0.20%

Passive Service 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%

Active Host Checks:

Time Frame	Checks Completed
<= 1 minute:	3 (10.0%)
<= 5 minutes:	12 (40.0%)
<= 15 minutes:	12 (40.0%)
<= 1 hour:	12 (40.0%)
Since program start:	12 (40.0%)

Metric	Min.	Max.	Average
Check Execution Time:	0.01 sec	5.18 sec	0.559 sec
Check Latency:	0.00 sec	0.00 sec	0.000 sec
Percent State Change:	0.00%	0.00%	0.00%

Passive Host 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%

Active Service Checks

The textbox to the left shows you how many active service checks the system has done in a time frame of 1 minute, 5 minutes, 15 minutes, 1 hour and since program start. An active check is a check that op5 Monitor has scheduled and executed it self. Read more about Passive Service Checks below. The values can be used to get an idea of how op5 Monitor is performing. If you have configured a default check interval of five minutes you should have a value close to 100%.

The textbox to the right shows:

- Check Execution Time: This is the time it takes for op5 Monitor to execute its checks. The average value should be fairly low, close to one second in most cases.
- Check Latency: This value tells you how far behind the system is when scheduling its checks. The average value should be fairly close to zero.
- Percent State Change: This is a quite interesting number. It tells you the stability of the monitored infrastructure. If the average value is high it tells you that a lot of things in your infrastructure are changing state. If the value is low it can mean that everything is constantly up or down.

Passive Service Checks

The textbox to the right shows you how many passive service checks the system has done in a time frame of 1 minute, 5 minutes, 15 minutes, 1 hour and since program start. A passive service check is a check where the check result has been delivered to op5 Monitor from an external source, for example a script. Normally most checks are Active Service Checks so the values can be quite low or equal to zero.

Active Host Checks

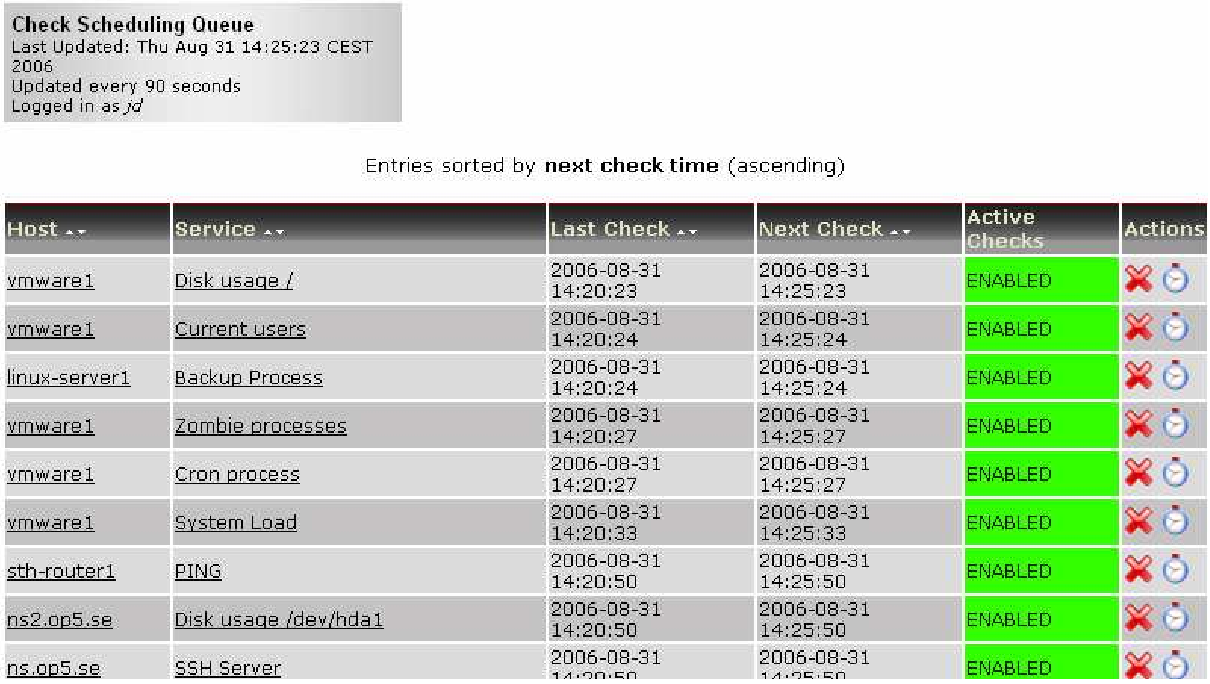
The textbox to the left shows you how many active host checks the system has done in a time frame of 1 minute, 5 minutes, 15 minutes, 1 hour and since program start. An active host check is a check that op5 Monitor has scheduled and executed it self. Read more about Passive Host Checks below. Host checks are normally not scheduled to be checked at a certain interval, default behavior is that op5 Monitor only executes host checks if there is a problem with one of the hosts services. The values in this box can therefore not be used as a performance measurement.
Note that if you have a lot of active hosts checks executed then you probably have an unstable network and a large “percent state change” value.

Passive Host Checks

The textbox to the right shows you how many passive host checks the system has done in a time frame of 1 minute, 5 minutes, 15 minutes, 1 hour and since program start. A passive host check is a check where the check result has been delivered to op5 Monitor from an external source, for example a script. Normally most host checks are Active Service Checks.

Scheduling Queue

This is op5 Monitors working schedule. The list includes all services that are scheduled and information about when last check was executed and when next check will be. 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.



Check Scheduling Queue
Last Updated: Thu Aug 31 14:25:23 CEST 2006
Updated every 90 seconds
Logged in as *jd*

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

Host	Service	Last Check	Next Check	Active Checks	Actions
vmware1	Disk usage /	2006-08-31 14:20:23	2006-08-31 14:25:23	ENABLED	✖ ⏲
vmware1	Current users	2006-08-31 14:20:24	2006-08-31 14:25:24	ENABLED	✖ ⏲
linux-server1	Backup Process	2006-08-31 14:20:24	2006-08-31 14:25:24	ENABLED	✖ ⏲
vmware1	Zombie processes	2006-08-31 14:20:27	2006-08-31 14:25:27	ENABLED	✖ ⏲
vmware1	Cron process	2006-08-31 14:20:27	2006-08-31 14:25:27	ENABLED	✖ ⏲
vmware1	System Load	2006-08-31 14:20:33	2006-08-31 14:25:33	ENABLED	✖ ⏲
sth-router1	PING	2006-08-31 14:20:50	2006-08-31 14:25:50	ENABLED	✖ ⏲
ns2.op5.se	Disk usage /dev/hda1	2006-08-31 14:20:50	2006-08-31 14:25:50	ENABLED	✖ ⏲
ns.op5.se	SSH Server	2006-08-31 14:20:50	2006-08-31 14:25:50	ENABLED	✖ ⏲

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

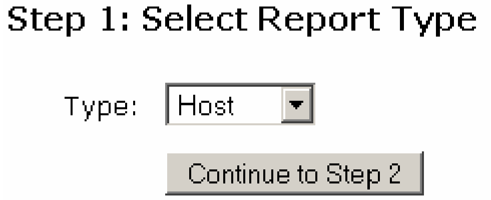
Service: The Service name for which the check is to be executed.
Last Check: When the check was last performed.
Next Check: When the next check will be performed.
Active Checks: If active checks is enabled or disabled.
Actions: The clock links you to specify a new time for check execution. The X let you disable an active check for that service and host.

Reporting

The Monitoring headline basically covers everything in op5 Monitor that is happening in real time. It shows you the status on your hosts and services right now. The Reporting headline is about letting the user create historical reports from the information that op5 Monitor has collected.

Trends

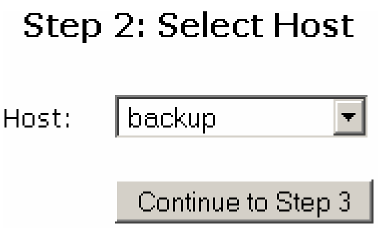
Trends display a graphic view of status on a host or a service during a selected report period. This graphical view can also be reached from Availability reports.



Step 1: Select Report Type

Type: Host

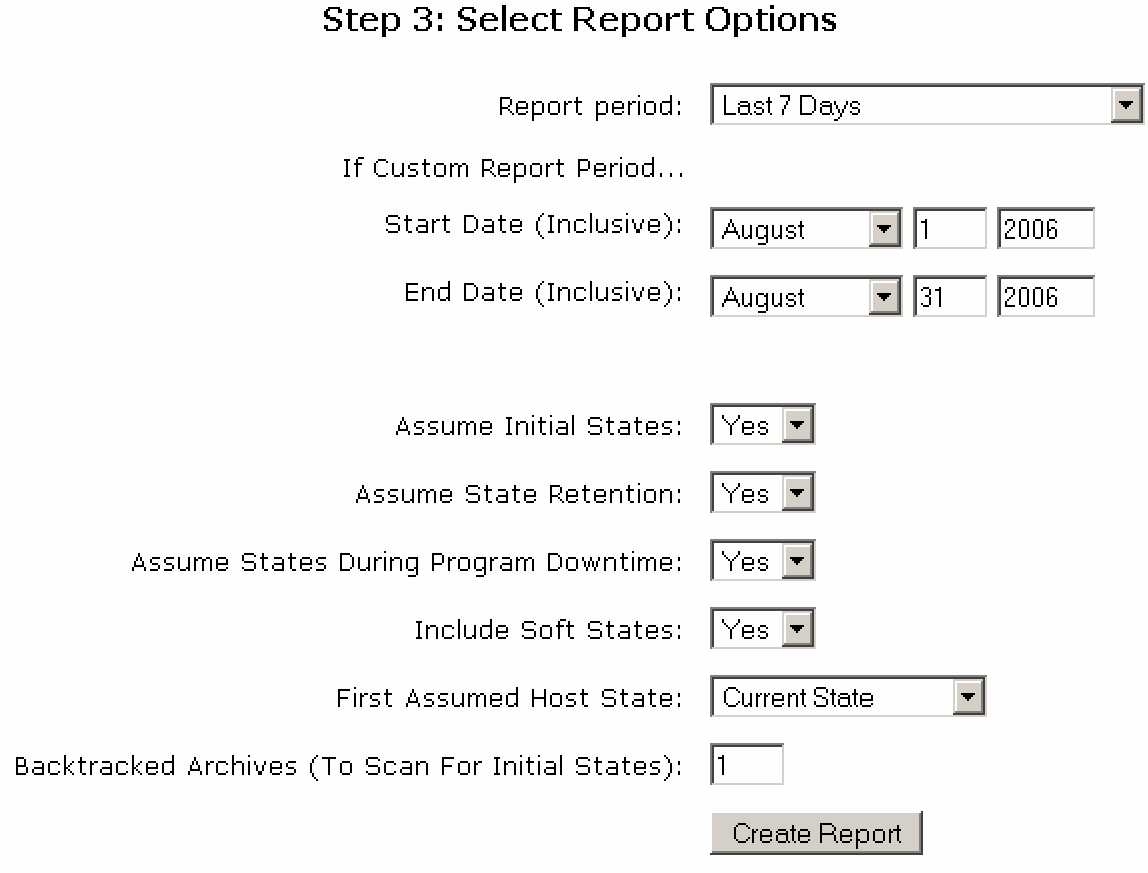
Select the preferred report type, Host or Service.



Step 2: Select Host

Host: backup

Select host or service you want the report based on.



Step 3: Select Report Options

Report period: Last 7 Days

If Custom Report Period...

Start Date (Inclusive): August 1 2006

End Date (Inclusive): August 31 2006

Assume Initial States: Yes

Assume State Retention: Yes

Assume States During Program Downtime: Yes

Include Soft States: Yes

First Assumed Host State: Current State

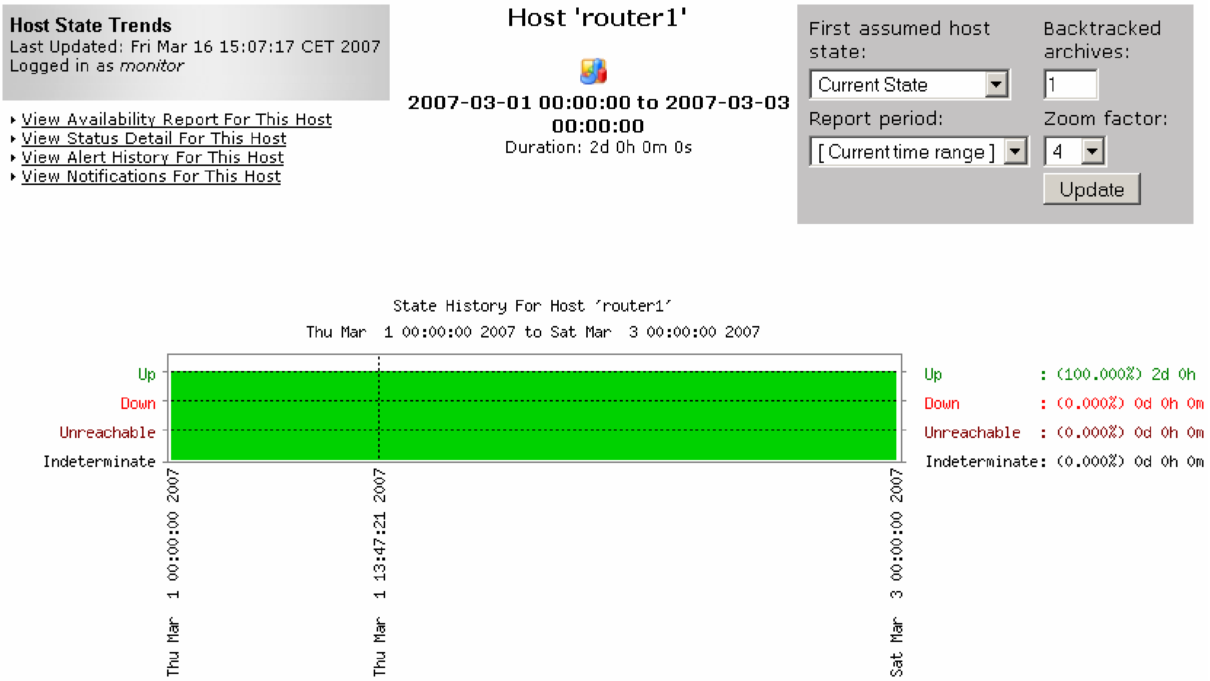
Backtracked Archives (To Scan For Initial States): 1

Now you have the ability to select report options to customize your report

Report period: Choose by a set of predefined report periods or choose “CUSTOM REPORT PERIOD”, and specify Start and End date.
Start Date (Inclusive): Specify Start Date if “CUSTOM REPORT PERIOD” was selected above
End Date (Inclusive): Specify End Date if “CUSTOM REPORT PERIOD” was selected above
Assume Initial States: Whether to assume logging of initial states or not. Default values are YES. For advanced users the value can be modified by editing the nagios.cfg config file located in the /opt/monitor/etc directory.
Assume State Retention: Whether to assume state retention or not. State retention determines if op5 Monitor should retain the states of hosts and services between program restarts. Default is YES. For advanced users the value can be modified by editing the nagios.cfg config file located in the /opt/monitor/etc directory.
Assume States During Program Downtime: If op5 Monitor is not running for some time during a report period we can by this option decide to assume states for hosts and services during the downtime. Default value is YES.
Include Soft States: A problem is classified as a SOFT problem until the number of checks has reached the configured max_check_attempts value. When max_check_attempts is reached the problem is reclassified as HARD and normally op5 Monitor will send out a notification about the problem. SOFT problem’s does not result in a notification. If you select YES, SOFT states will be included in the report, if NO only HARD states will be included.
First Assumed Host State: If there is no information about the host or service in the current log file, op5 Monitor can assume status of the host/service. Default value is “Current State”.

First Assumed Service State: If there is no information about the host or service in the current log file, op5 Monitor can assume status of the host/service. Default value is "Current State".
Backtracked Archives (To Scan For Initial States): How many log archives to look through when searching for initial states. op5 Monitor is configured to rotate the log monthly.

Click on "Create Report" to proceed and create the report.



Host State Trends
Last Updated: Fri Mar 16 15:07:17 CET 2007
Logged in as *monitor*

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

Host 'router1'

2007-03-01 00:00:00 to 2007-03-03 00:00:00
Duration: 2d 0h 0m 0s

First assumed host state: Current State
Backtracked archives: 1
Report period: [Current time range]
Zoom factor: 4
Update

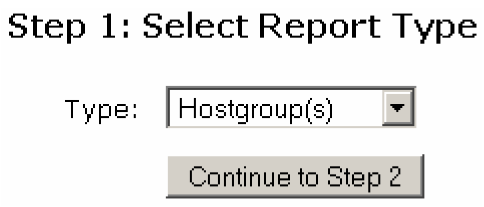
State History For Host 'router1'
Thu Mar 1 00:00:00 2007 to Sat Mar 3 00:00:00 2007

```
Up            : (100.000%) 2d 0h
Down          : (0.000%) 0d 0h 0m
Unreachable   : (0.000%) 0d 0h 0m
Indeterminate: (0.000%) 0d 0h 0m
```

The graph that is created shows what state the host has been in over the selected report interval. You can zoom into the graph by clicking on it.

Availability

The availability report shows availability of hostgroups, servicegroups, hosts or services during a selected report period.

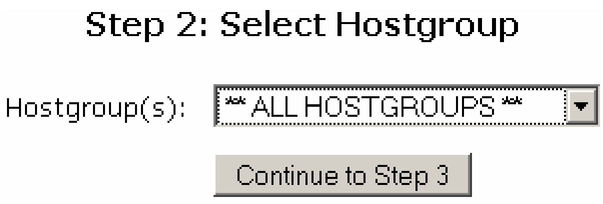


Step 1: Select Report Type

Type: Hostgroup(s)

Continue to Step 2

Select the preferred report type, Hostgroup, Host, Servicegroup or Service.

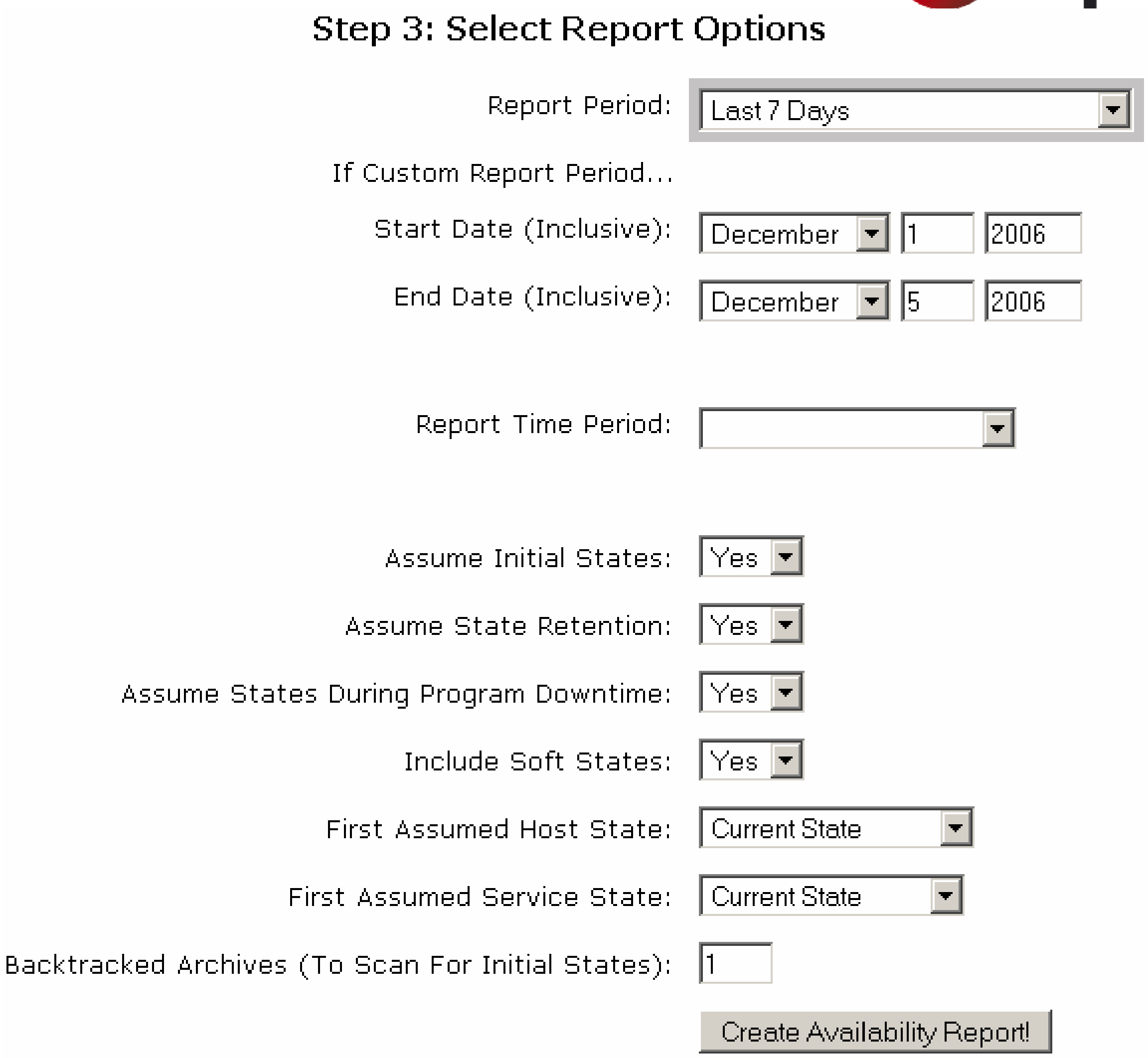


Step 2: Select Hostgroup

Hostgroup(s): ** ALL HOSTGROUPS **

Continue to Step 3

Select the object for your report. Note that you can now select to create a report for all objects in the list or for one specific object.



Step 3: Select Report Options

Report Period: Last 7 Days

If Custom Report Period...

Start Date (Inclusive): December 1 2006

End Date (Inclusive): December 5 2006

Report Time Period:

Assume Initial States: Yes

Assume State Retention: Yes

Assume States During Program Downtime: Yes

Include Soft States: Yes

First Assumed Host State: Current State

First Assumed Service State: Current State

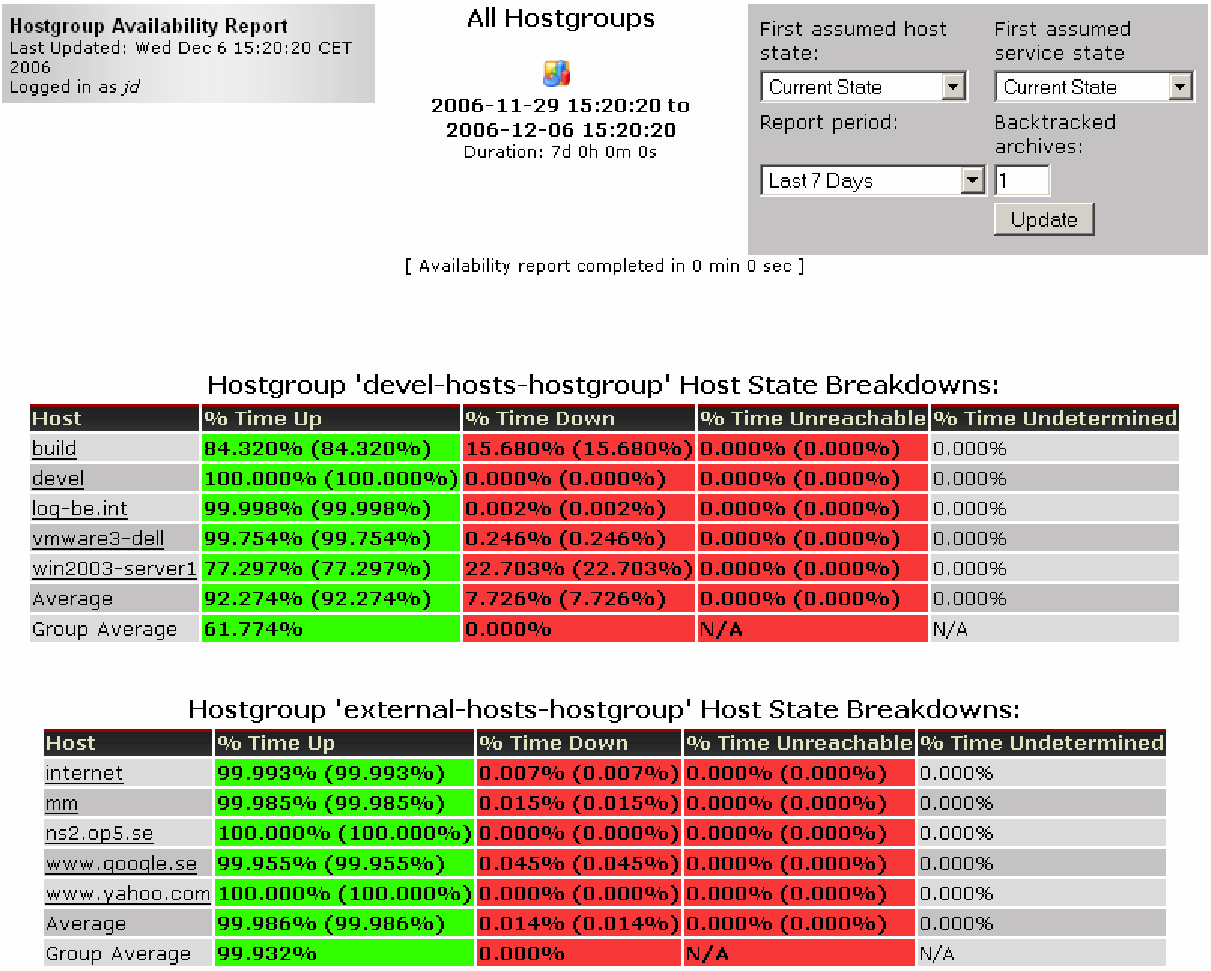
Backtracked Archives (To Scan For Initial States): 1

Now you have the ability to select report options to customize your report

Report Period: Choose by a set of predefined report periods or choose "CUSTOM REPORT PERIOD", and specify Start and End date.
Start Date (Inclusive): Specify Start Date if "CUSTOM REPORT PERIOD" was selected above
End Date (Inclusive): Specify End Date if "CUSTOM REPORT PERIOD" was selected above
Report Time Period: What time should the report be created for. Tip: This can be used for SLA reporting.
Assume Initial States: Whether to assume logging of initial states or not. Default values are YES. For advanced users the value can be modified by editing the nagios.cfg config file located in the /opt/monitor/etc directory.
Assume State Retention: Whether to assume state retention or not. State retention determines if op5 Monitor should retain the states of hosts and services between program restarts. Default is YES. For advanced users the value can be modified by editing the nagios.cfg config file located in the /opt/monitor/etc directory.
Assume States During Program Downtime: If op5 Monitor is not running for some time during a report period we can by this option decide to assume states for hosts and services during the downtime. Default value is YES.

Include Soft States: A problem is classified as a SOFT problem until the number of checks has reached the configured max_check_attempts value. When max_check_attempts is reached the problem is reclassified as HARD and normally op5 Monitor will send out a notification about the problem. SOFT problem's does not result in a notification. If you select YES, SOFT states will be included in the report, if NO only HARD states will be included.
First Assumed Host State: If there is no information about the host or service in the current log file, op5 Monitor can assume status of the host/service. Default value is "Current State".
First Assumed Service State: If there is no information about the host or service in the current log file, op5 Monitor can assume status of the host/service. Default value is "Current State".
Backtracked Archives (To Scan For Initial States): How many log archives to look through when searching for initial states. op5 Monitor is configured to rotate the log monthly.

Click on "Create Report" to create the availability report



Hostgroup Availability Report
Last Updated: Wed Dec 6 15:20:20 CET 2006
Logged in as *jd*

All Hostgroups

2006-11-29 15:20:20 to 2006-12-06 15:20:20
Duration: 7d 0h 0m 0s

First assumed host state: Current State
First assumed service state: Current State
Report period: Last 7 Days
Backtracked archives: 1

[Availability report completed in 0 min 0 sec]

Hostgroup 'devel-hosts-hostgroup' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
build	84.320% (84.320%)	15.680% (15.680%)	0.000% (0.000%)	0.000%
devel	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
log-be.int	99.998% (99.998%)	0.002% (0.002%)	0.000% (0.000%)	0.000%
vmware3-dell	99.754% (99.754%)	0.246% (0.246%)	0.000% (0.000%)	0.000%
win2003-server1	77.297% (77.297%)	22.703% (22.703%)	0.000% (0.000%)	0.000%
Average	92.274% (92.274%)	7.726% (7.726%)	0.000% (0.000%)	0.000%
Group Average	61.774%	0.000%	N/A	N/A

Hostgroup 'external-hosts-hostgroup' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
internet	99.993% (99.993%)	0.007% (0.007%)	0.000% (0.000%)	0.000%
mm	99.985% (99.985%)	0.015% (0.015%)	0.000% (0.000%)	0.000%
ns2.op5.se	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
www.google.se	99.955% (99.955%)	0.045% (0.045%)	0.000% (0.000%)	0.000%
www.yahoo.com	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average	99.986% (99.986%)	0.014% (0.014%)	0.000% (0.000%)	0.000%
Group Average	99.932%	0.000%	N/A	N/A

The report displays a couple of values related to availability, in this example hostgroup availability.

Host: The name of a specific host in the group.
% Time Up: The amount of time the host has been in the state UP during the report period.
% Time Down: The amount of time the host has been in the state DOWN during the report period.

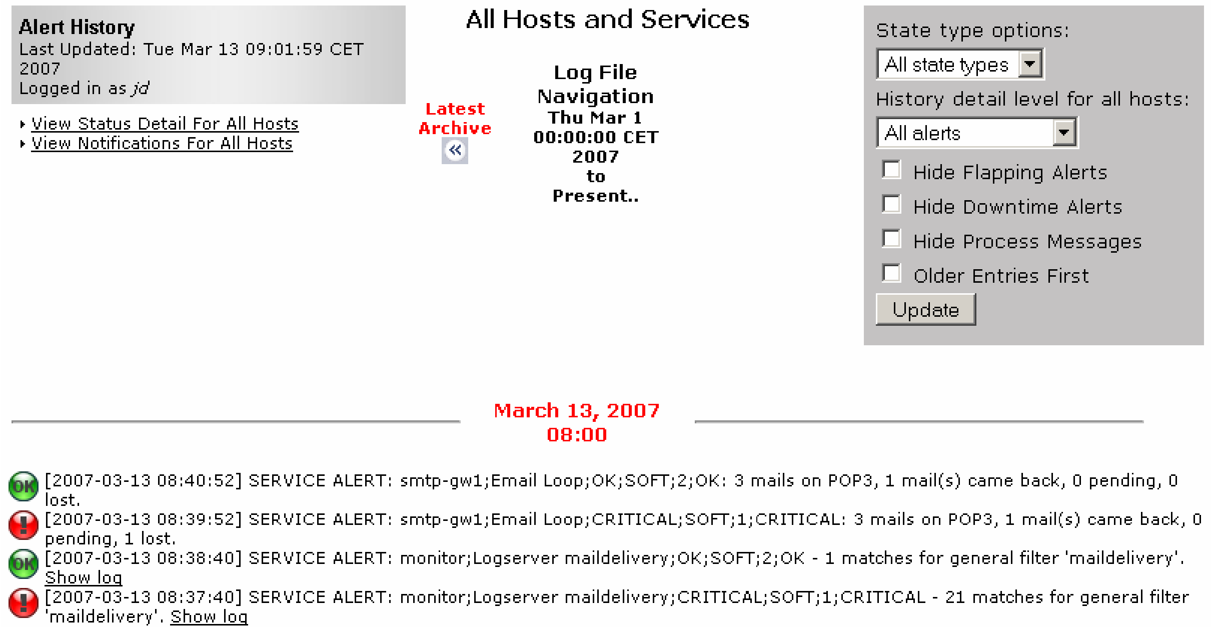
% Time Unreachable: The amount of time the host has been in the state UNREACHABLE during the report period
% Time Undetermined: The amount of time the host has been in UNDETERMINED state. This describes the time where op5 Monitor for some reason does not have any data in the report period. For example if a report includes a host which has not been existing in op5 Monitor’s configuration during the whole report period.

There are two values displayed for each time above except for the %Time Undetermined value.
There are also two summary values for each hostgroup report

Average: This is the average value for the group. It is calculated by adding the % Time for each host and then divide the total value with the amount of hosts in the group. This can also be done on servicegroup reports.
Group Average: This value is only calculated for UP and DOWN states. It displays the amount of time where all hosts in the group has been UP or DOWN at the same time.

Alert History

Alert history displays a raw log of state changes. This can be useful to debug problems in you IT infrastructure that normally would go undetected. An even more detailed log can be displayed on Event Log.



Alert History
Last Updated: Tue Mar 13 09:01:59 CET 2007
Logged in as *jd*

- View Status Detail For All Hosts
- View Notifications For All Hosts

All Hosts and Services

Latest Archive

Log File Navigation
Thu Mar 1 00:00:00 CET 2007
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
Update

March 13, 2007 08:00

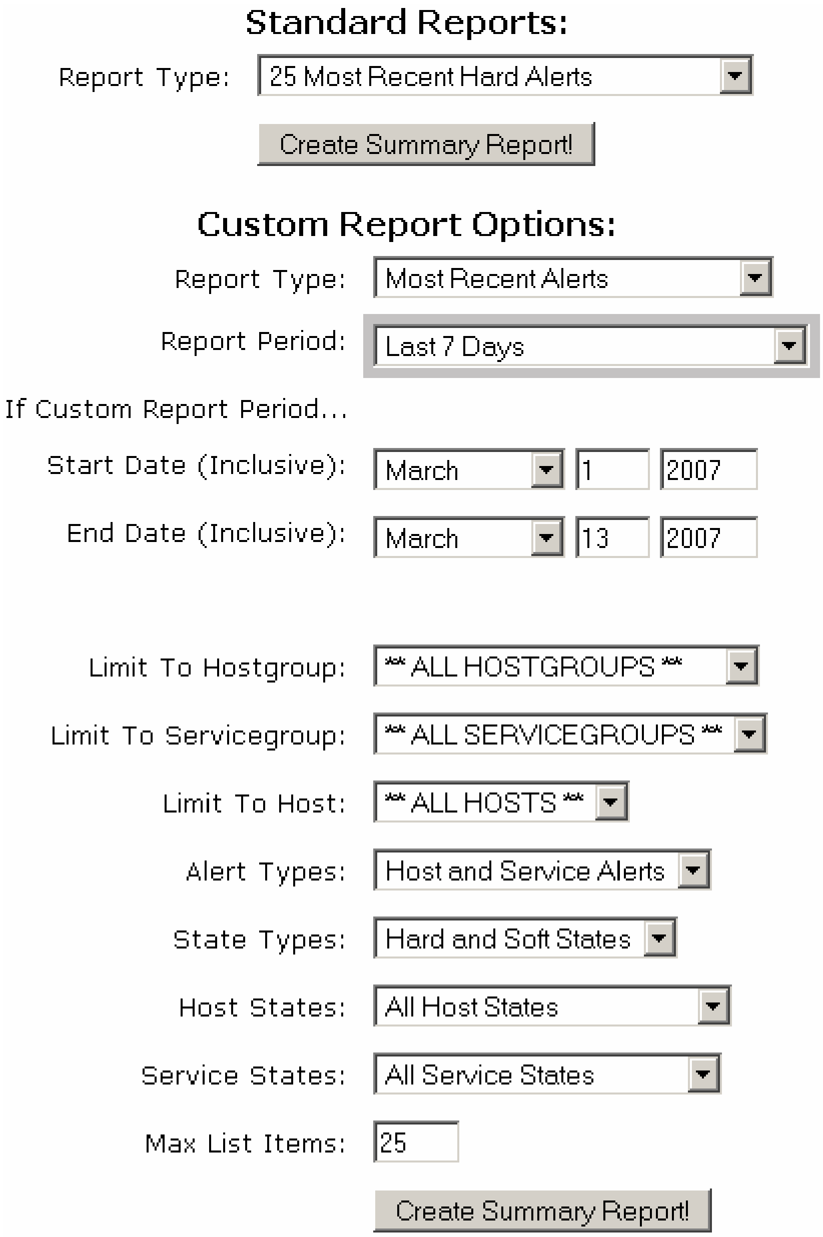
```
[2007-03-13 08:40:52] SERVICE ALERT: smtp-gw1;Email Loop;OK;SOFT;2;OK: 3 mails on POP3, 1 mail(s) came back, 0 pending, 0 lost.
[2007-03-13 08:39:52] SERVICE ALERT: smtp-gw1;Email Loop;CRITICAL;SOFT;1;CRITICAL: 3 mails on POP3, 1 mail(s) came back, 0 pending, 1 lost.
[2007-03-13 08:38:40] SERVICE ALERT: monitor;Logserver maildelivery;OK;SOFT;2;OK - 1 matches for general filter 'maildelivery'. Show log
[2007-03-13 08:37:40] SERVICE ALERT: monitor;Logserver maildelivery;CRITICAL;SOFT;1;CRITICAL - 21 matches for general filter 'maildelivery'. Show log
```

In the top right option box you can affect what should be displayed in the log.

The information in the log is divided in segments consisting in log entries with one hour of log data for each segment.

Alert Summary

The alert summary report gives you a subset of possibilities to create different reports based on the data op5 Monitor has collected.



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): March 1 2007

End Date (Inclusive): March 13 2007

Limit To Hostgroup: ** ALL HOSTGROUPS **

Limit To Servicegroup: ** ALL SERVICEGROUPS **

Limit To Host: ** ALL HOSTS **

Alert Types: Host and Service Alerts

State Types: Hard and Soft States

Host States: All Host States

Service States: All Service States

Max List Items: 25

Create Summary Report!

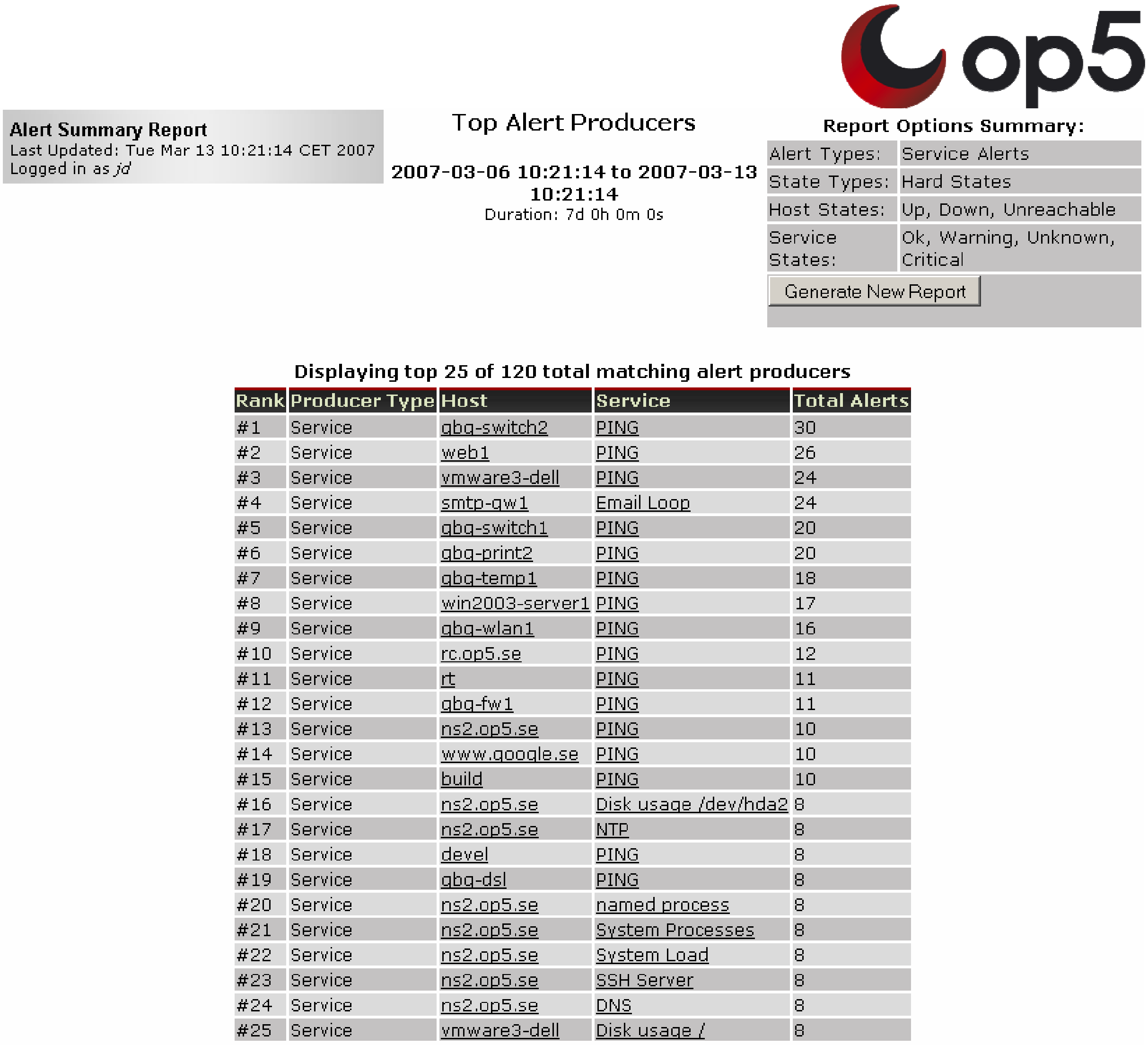
The page gives you the possibility to create a subset of standard reports and it is also possible to create customized reports.

With the custom reports you can create a various amount of report types. I will not go through all available report types but walk through a couple of useful example reports.

Top 25 Hard Service Alert Producers

Select the Top 25 Hard Service Alert Producers from the Standard Reports drop down menu and click "Create Summary Report"

This will create a report that can be use to prioritize your work since it will show you the things causing most problems in your environment.



Alert Summary Report
Last Updated: Tue Mar 13 10:21:14 CET 2007
Logged in as *jd*

Top Alert Producers

2007-03-06 10:21:14 to 2007-03-13 10:21:14
Duration: 7d 0h 0m 0s

Report Options Summary:

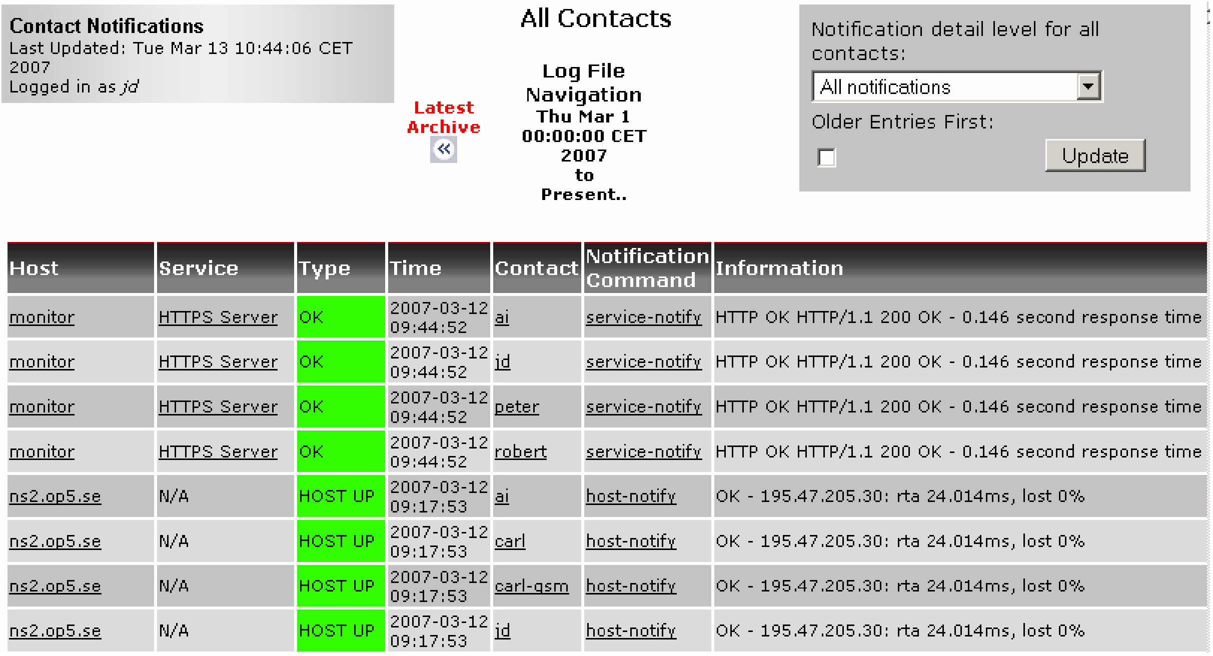
Alert Types:	Service Alerts
State Types:	Hard States
Host States:	Up, Down, Unreachable
Service States:	Ok, Warning, Unknown, Critical

Displaying top 25 of 120 total matching alert producers

Rank	Producer Type	Host	Service	Total Alerts
#1	Service	gbg-switch2	PING	30
#2	Service	web1	PING	26
#3	Service	vmware3-dell	PING	24
#4	Service	smtp-gw1	Email Loop	24
#5	Service	gbg-switch1	PING	20
#6	Service	gbg-print2	PING	20
#7	Service	gbg-temp1	PING	18
#8	Service	win2003-server1	PING	17
#9	Service	gbg-wlan1	PING	16
#10	Service	rc.op5.se	PING	12
#11	Service	rt	PING	11
#12	Service	gbg-fw1	PING	11
#13	Service	ns2.op5.se	PING	10
#14	Service	www.google.se	PING	10
#15	Service	build	PING	10
#16	Service	ns2.op5.se	Disk usage /dev/hda2	8
#17	Service	ns2.op5.se	NTP	8
#18	Service	devel	PING	8
#19	Service	gbg-dsl	PING	8
#20	Service	ns2.op5.se	named process	8
#21	Service	ns2.op5.se	System Processes	8
#22	Service	ns2.op5.se	System Load	8
#23	Service	ns2.op5.se	SSH Server	8
#24	Service	ns2.op5.se	DNS	8
#25	Service	vmware3-dell	Disk usage /	8

Notifications

This is a raw log of the notifications that op5 Monitor has sent. It can be used to verify that notifications has been sent out and also to see who should have got the notifications.



Contact Notifications
Last Updated: Tue Mar 13 10:44:06 CET 2007
Logged in as *jd*

All Contacts

Log File Navigation
Thu Mar 1 00:00:00 CET 2007
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	2007-03-12 09:44:52	ai	service-notify	HTTP OK HTTP/1.1 200 OK - 0.146 second response time
monitor	HTTPS Server	OK	2007-03-12 09:44:52	jd	service-notify	HTTP OK HTTP/1.1 200 OK - 0.146 second response time
monitor	HTTPS Server	OK	2007-03-12 09:44:52	peter	service-notify	HTTP OK HTTP/1.1 200 OK - 0.146 second response time
monitor	HTTPS Server	OK	2007-03-12 09:44:52	robert	service-notify	HTTP OK HTTP/1.1 200 OK - 0.146 second response time
ns2.op5.se	N/A	HOST UP	2007-03-12 09:17:53	ai	host-notify	OK - 195.47.205.30: rta 24.014ms, lost 0%
ns2.op5.se	N/A	HOST UP	2007-03-12 09:17:53	carl	host-notify	OK - 195.47.205.30: rta 24.014ms, lost 0%
ns2.op5.se	N/A	HOST UP	2007-03-12 09:17:53	carl-gsm	host-notify	OK - 195.47.205.30: rta 24.014ms, lost 0%
ns2.op5.se	N/A	HOST UP	2007-03-12 09:17:53	jd	host-notify	OK - 195.47.205.30: rta 24.014ms, lost 0%

Host: The name of the host, you can click on the hostname to get more information about the host.
Service: The name of the service the notification is about, if it is a host notification this is displayed with N/A. You can click on the service name to get more information about the service.
Type: What kind of notification that was sent.
Time: Timestamp that shows when the notification was sent.
Contact: The contact that the notification was sent to, you can click on the contact name to se full contact details.
Notification Command: The command used to send the notification, se more on Check Commands.
Information: The status output that resulted in the notification. This is not necessary the information sent in the notification it just indicates the reason for the notification.

Event Log

The event log is a raw log of events in the system. This can be interesting if you want to do troubleshooting on the op5 Monitor system or your IT infrastructure.

This log is also available for advanced users in text format directly on your op5 Monitor system in /opt/monitor/var/nagios.log

The log file is rotated once every month and moved to /opt/monitor/var/archive/. The rotation interval can be changed by advanced users by editing the variable 'log_rotation_method' in /opt/monitor/etc/nagios.cfg.

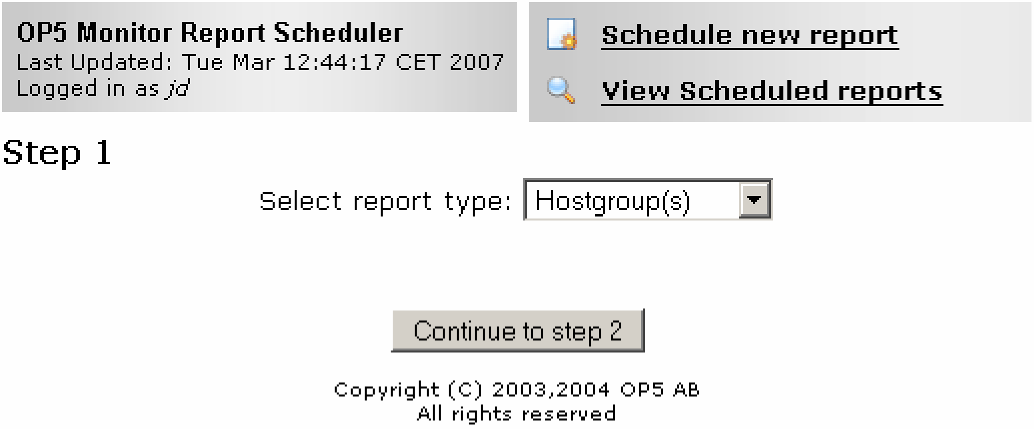
Warning: this log can be really large if you are at the end of the month just before rotation or if you monitor a large amount of hosts and services. The size of the log can even crash some browsers or make your system slow and unresponsive. A good alternative to the Event Log is the Alert History which contains a more filtered list of events.

Schedule Reports

Schedule reports provides the exact same function as Availability reports with the addition that the report is sent out as an html email to one or several recipients. The reports can be sent out on a monthly or weekly basis.

To configure a scheduled report do following

Select the preferred report type, Hostgroup, Host, Servicegroup or Service.



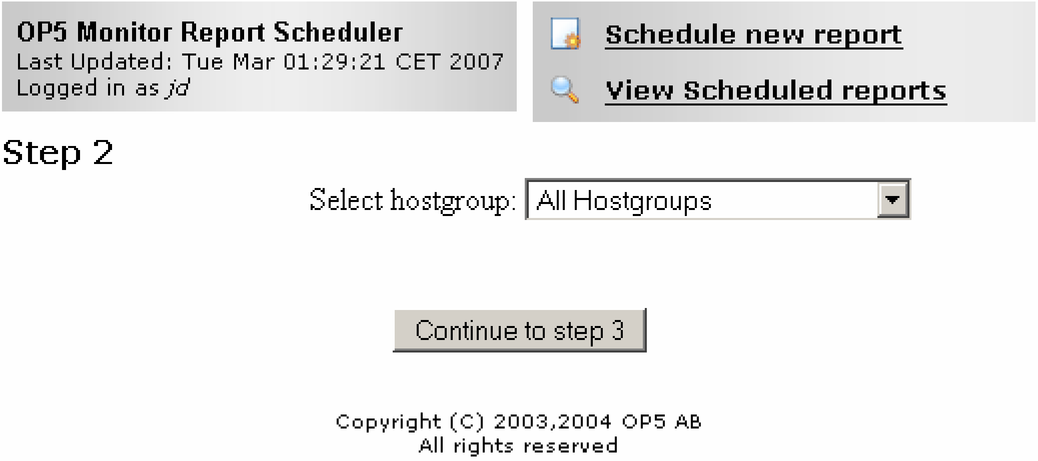
OP5 Monitor Report Scheduler
Last Updated: Tue Mar 12:44:17 CET 2007
Logged in as jd

Step 1

Select report type: Hostgroup(s)

Copyright (C) 2003,2004 OP5 AB
All rights reserved

Select the object for your report. Note that you can now select to create a report for all objects in the list or for one specific object.



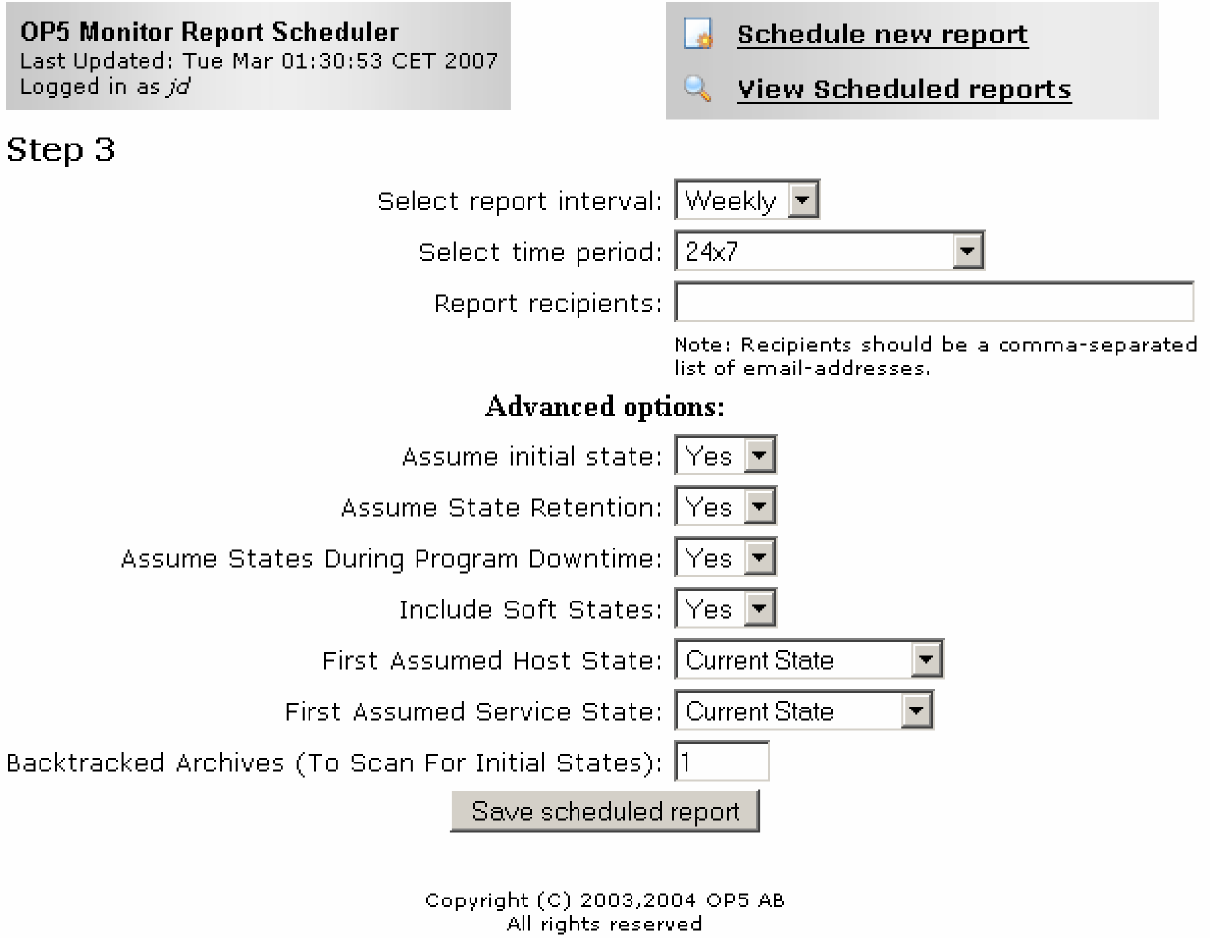
OP5 Monitor Report Scheduler
Last Updated: Tue Mar 01:29:21 CET 2007
Logged in as jd

Step 2

Select hostgroup: All Hostgroups

Copyright (C) 2003,2004 OP5 AB
All rights reserved

Now you have the possibility to customize the report. The options are the exact same as when creating Availability reports except for the Report recipients textbox.



OP5 Monitor Report Scheduler
Last Updated: Tue Mar 01:30:53 CET 2007
Logged in as *jd*

Step 3

Select report interval: Weekly

Select time period: 24x7

Report recipients:

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

Advanced options:

Assume initial state: Yes

Assume State Retention: Yes

Assume States During Program Downtime: Yes

Include Soft States: Yes

First Assumed Host State: Current State

First Assumed Service State: Current State

Backtracked Archives (To Scan For Initial States): 1

Copyright (C) 2003,2004 OP5 AB
All rights reserved

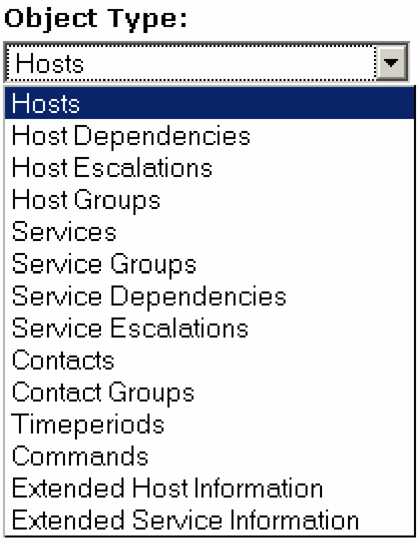
Enter the email address of the report recipient in the report recipient textbox. As stated in the note below it is possible to specify more than one address, to do that separate the email addresses with a comma sign.

Configuration

View Config

The View Configuration menu option enables you to view your entire configuration. This can be useful if you for example quickly want a list of all hosts with alias and ip address. This tool is referred to from many places in op5 Monitors web gui, for example when reviewing the Notifications log.

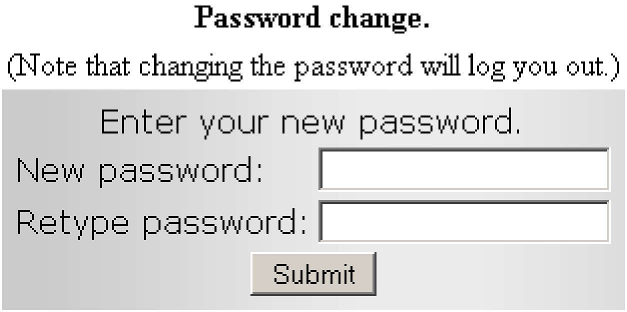
The configuration is divided in different objects. To view a list of a specific object type select that type from the Object Type drop down list.



The configuration will be more deeply covered on the Configure headline.

Change Password

User options are normally configured from the Configure tool, this option gives a user the option to change has own password without help from an administrator.



Password change.

(Note that changing the password will log you out.)

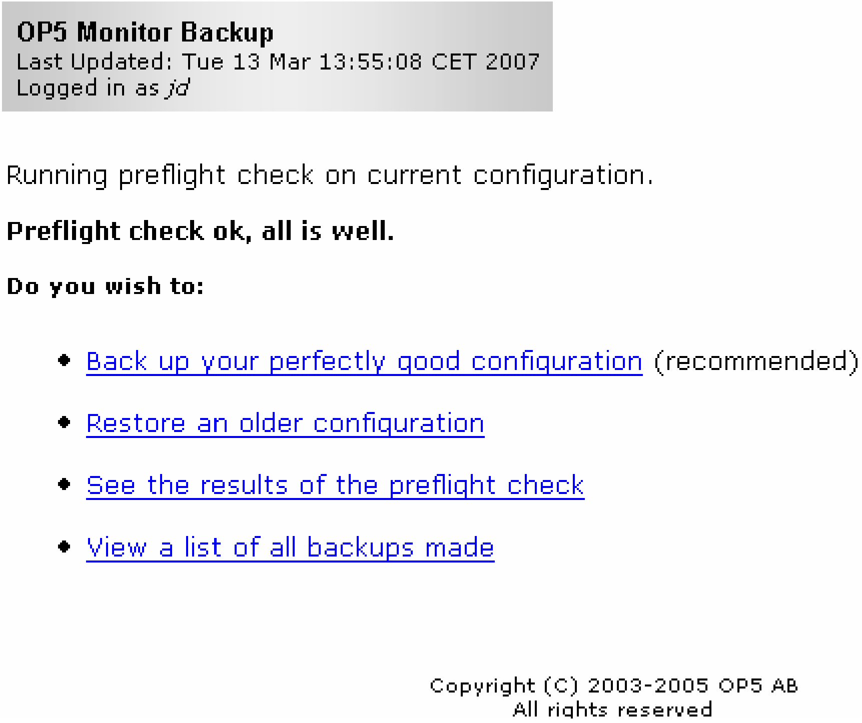
Enter your new password.

New password:

Retype password:

Backup / Restore

Backup and Restore is an easy way to create a backup of op5 Monitor’s configuration and log files. With help of this function you can easily restore an old configuration if the current one is messed up.



OP5 Monitor Backup
Last Updated: Tue 13 Mar 13:55:08 CET 2007
Logged in as *jd*

Running preflight check on current configuration.

Preflight check ok, all is well.

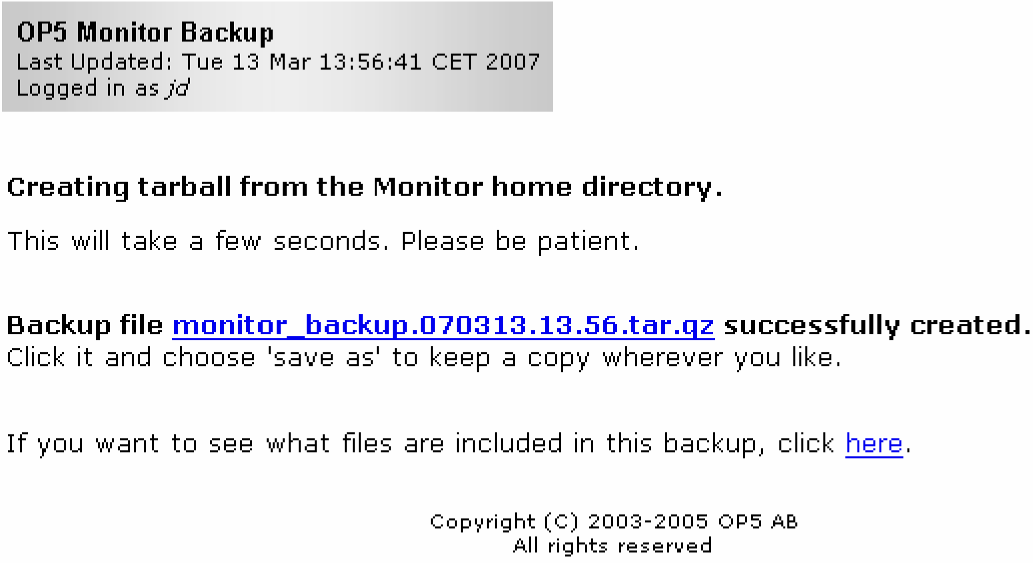
Do you wish to:

- 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

Copyright (C) 2003-2005 OP5 AB
All rights reserved

Create a backup

To create a backup simply click on the “Back up your perfectly good configuration” link. After a short time, depending on the size of your configuration and log files, a backup is created and the possibility to download it or examine its contents is shown.



OP5 Monitor Backup
Last Updated: Tue 13 Mar 13:56:41 CET 2007
Logged in as *jd*

Creating tarball from the Monitor home directory.

This will take a few seconds. Please be patient.

Backup file monitor_backup.070313.13.56.tar.gz successfully created.
Click it and choose 'save as' to keep a copy wherever you like.

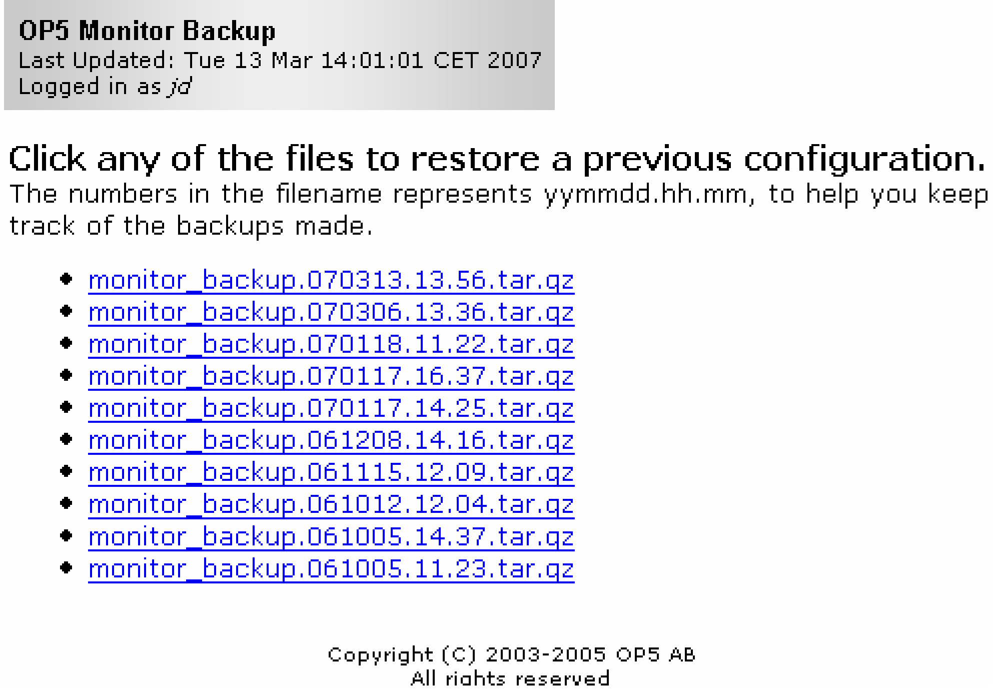
If you want to see what files are included in this backup, click here.

Copyright (C) 2003-2005 OP5 AB
All rights reserved

The backup is saved in tar.gz format which can be handled on most Linux systems.

Restore a backup

To restore a backup simply click on the “restore an older configuration” link and select one of the available backups.



OP5 Monitor Backup
Last Updated: Tue 13 Mar 14:01:01 CET 2007
Logged in as *jd*

Click any of the files to restore a previous configuration.
The numbers in the filename represents yymmdd.hh.mm, to help you keep track of the backups made.

- monitor_backup.070313.13.56.tar.gz
- monitor_backup.070306.13.36.tar.gz
- monitor_backup.070118.11.22.tar.gz
- monitor_backup.070117.16.37.tar.gz
- monitor_backup.070117.14.25.tar.gz
- monitor_backup.061208.14.16.tar.gz
- monitor_backup.061115.12.09.tar.gz
- monitor_backup.061012.12.04.tar.gz
- monitor_backup.061005.14.37.tar.gz
- monitor_backup.061005.11.23.tar.gz

Copyright (C) 2003-2005 OP5 AB
All rights reserved

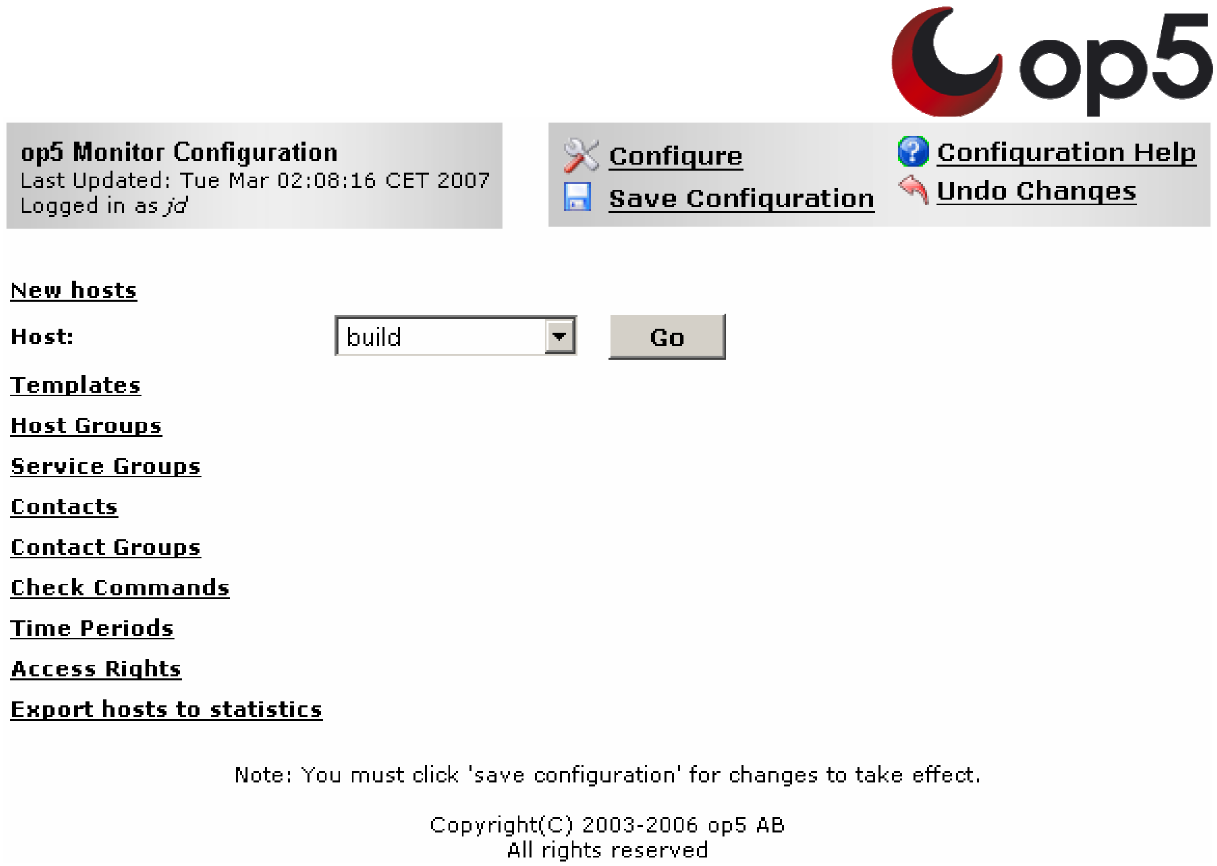
When restoring an old backup, not only the configuration is restored but also the log files, so be careful with restoring really old backups since you can loose a lot of history.

Note: it is still recommended to take a proper system backup using the included op5backup.sh script or a backup agent from your existing backup software provider. See the op5 System manual for information about backup options.

Configure

There is two ways to configure op5 Monitor. One is to edit text files which are located on the op5 Monitor server in the /opt/monitor/etc directory. The other is to use Configure which is a web based configuration GUI for op5 Monitor.

When you click on the Configure link in the navigation menu a copy of the configuration in the text files is imported to a database. You can force an import at any time by clicking on “Undo Changes”. The configuration can now be edited using the configure web gui. To save the configuration, click on “Save Configuration”. This will result in an export of the new configuration to the text files and op5 Monitor reloads to read the new configuration.



op5 Monitor Configuration
Last Updated: Tue Mar 02:08:16 CET 2007
Logged in as *jd*

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

Copyright(C) 2003-2006 op5 AB
All rights reserved

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

Configuration basics

The configuration is based on objects. There are several types of objects, each one defining different things in the monitoring process. Each object consists of a object name and a couple of variables that needs to be configured. For example on a host object you configure hostname, address and so on.

In the configure tool you can add new objects and modify existing objects. A lot of objects can be cross referenced in the configuration and the configure tool helps you with this to.

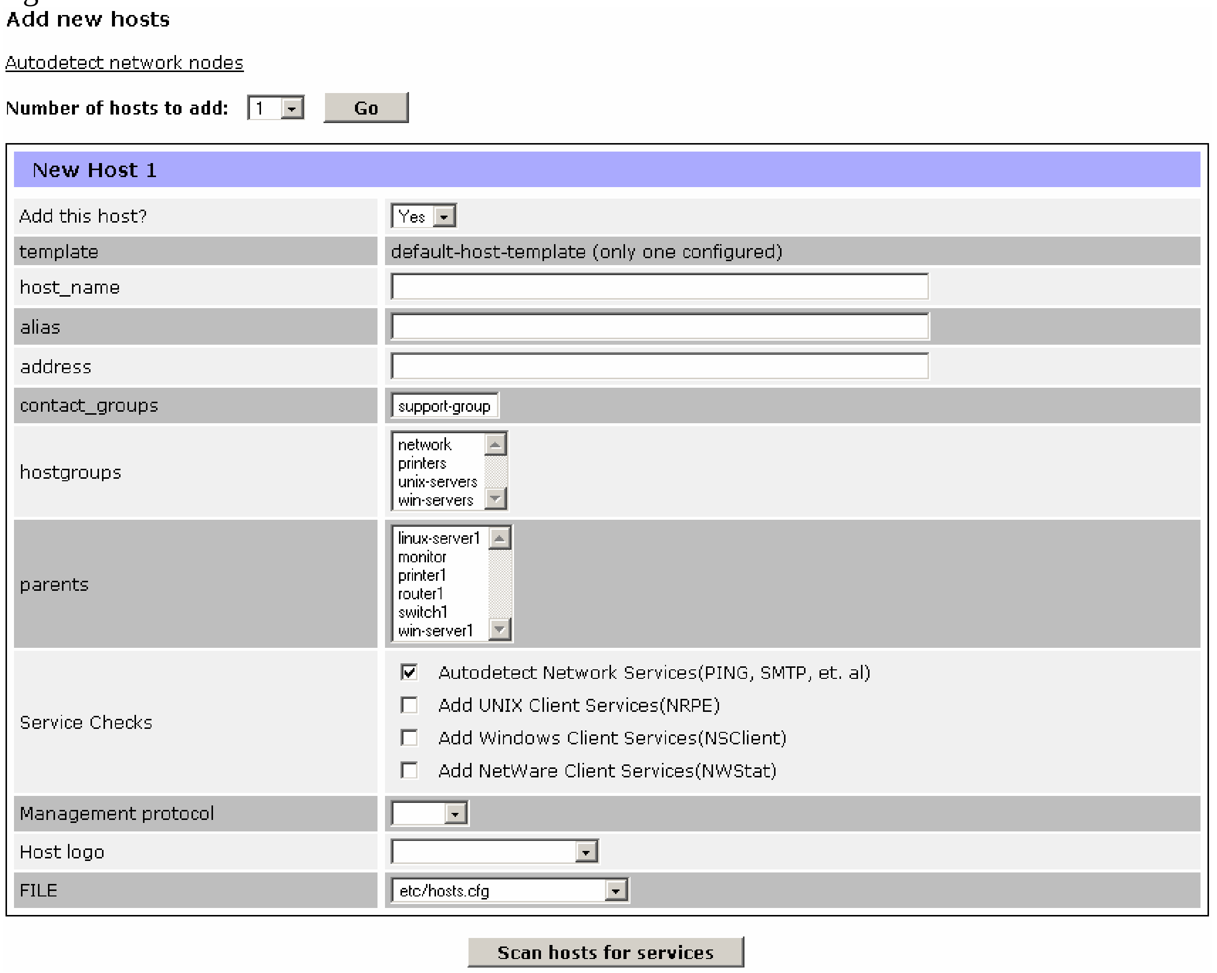
New Hosts

To add a host, click the 'New hosts' link. A new window appears that allows you to enter the data needed to add the host.

To add several hosts at a time you have two options.

1. Autodetect network nodes. This function scans one or several ip ranges to detect which IP addresses that responds to ping.
2. You can also change the number of hosts to add in the drop down menu in the top of the page.

To complete a new host a couple of variables need to be configured. Some of the variables are optional, the required variables are: host name, alias, address, contact_groups and hostgroups. If you fail to add information in these fields the configuration of the new host will fail. You can get a detailed description of all fields by clicking on “Configuration Help” in the upper right corner.



Add new hosts

Autodetect network nodes

Number of hosts to add: 1 Go

New Host 1

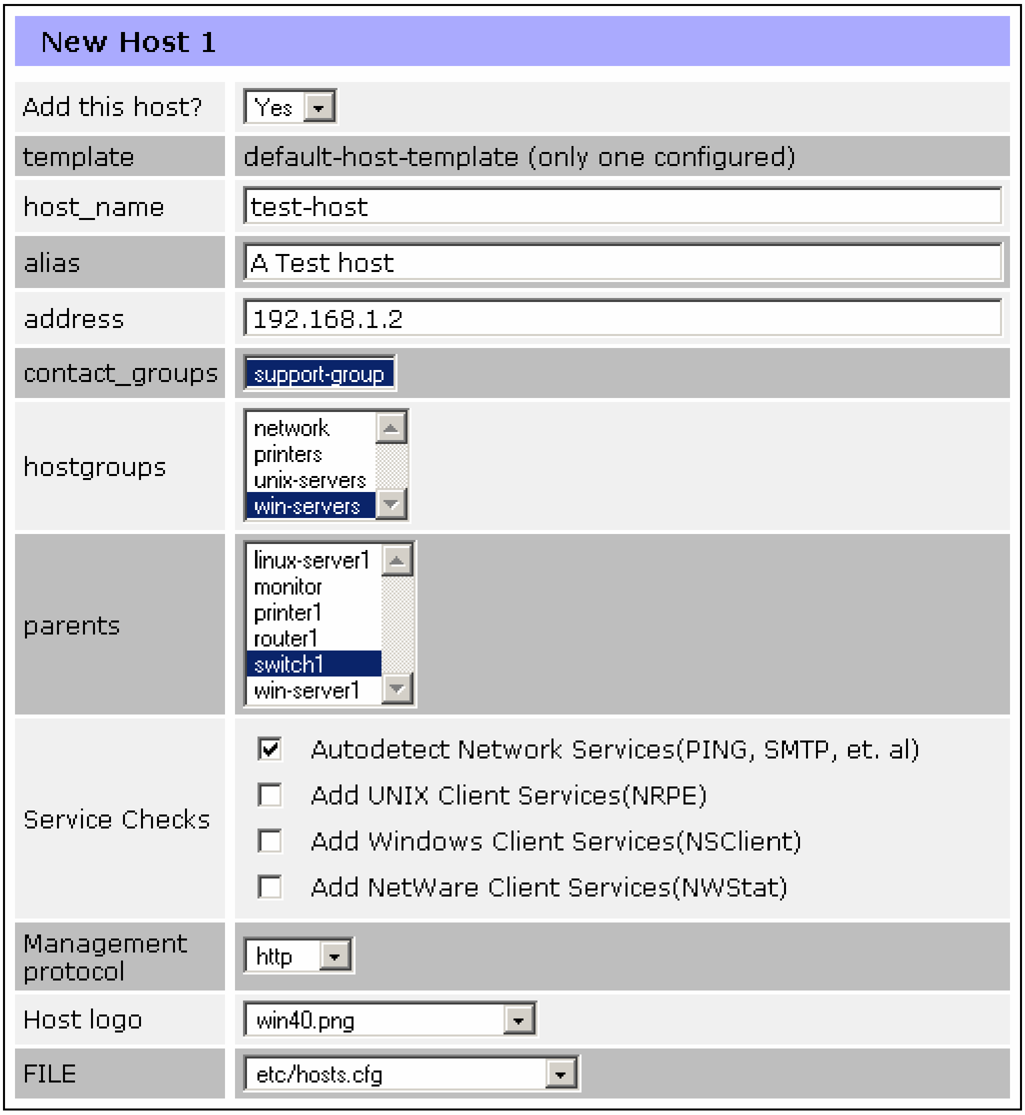
Add this host?	Yes
template	default-host-template (only one configured)
host_name	
alias	
address	
contact_groups	support-group
hostgroups	network printers unix-servers win-servers
parents	linux-server1 monitor printer1 router1 switch1 win-server1
Service Checks	☑ Autodetect Network Services(PING, SMTP, et. al) ☐ Add UNIX Client Services(NRPE) ☐ Add Windows Client Services(NSClient) ☐ Add NetWare Client Services(NWStat)
Management protocol	
Host logo	
FILE	etc/hosts.cfg

Here is an explanation of each variable.

Add this host?: If you are adding several hosts at a time, for example by using the autodetect network nodes function described earlier, you can select which hosts to add.
template: 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, usually a short but descriptive name. Example: router1
alias: Full description of the host, since the host_name is supposed to be short you can use this field to enter a more descriptive text. Example: Router for main office.
address: The IP address or host name of the host.
contact_groups: The contact group(s) this hosts notifications will be sent to, one or more groups can be selected.
hostgroups: The host group(s) that the host will be a member of. The host can be a member of several hostgroups.
parents: The parent(s) that this host is physically connected to. Example: serverA is connected to switch1 and therefore has switch1 as parent. It is possible to have several parents for redundant connections. Note: There is a limitation in the parent directive, you cannot have circular parent relationships.

Service Checks: Add 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 agent software yet.
Management Protocol: Choose the management protocol used to configure the host. E.g. telnet for routers and HTTP for switches. This will result in a URL, with the specified management protocol, next to the host in Host Detail. Example: telnet://router1/
Host Logo: Associate a logo to the host. This logo will appear in the status map and network map. When selecting a logo you will get a popup window with a preview.
FILE: The configuration file that this data will be stored in, default is hosts.cfg. Don’t change this if you’re not really sure what it does.

Example of entered data

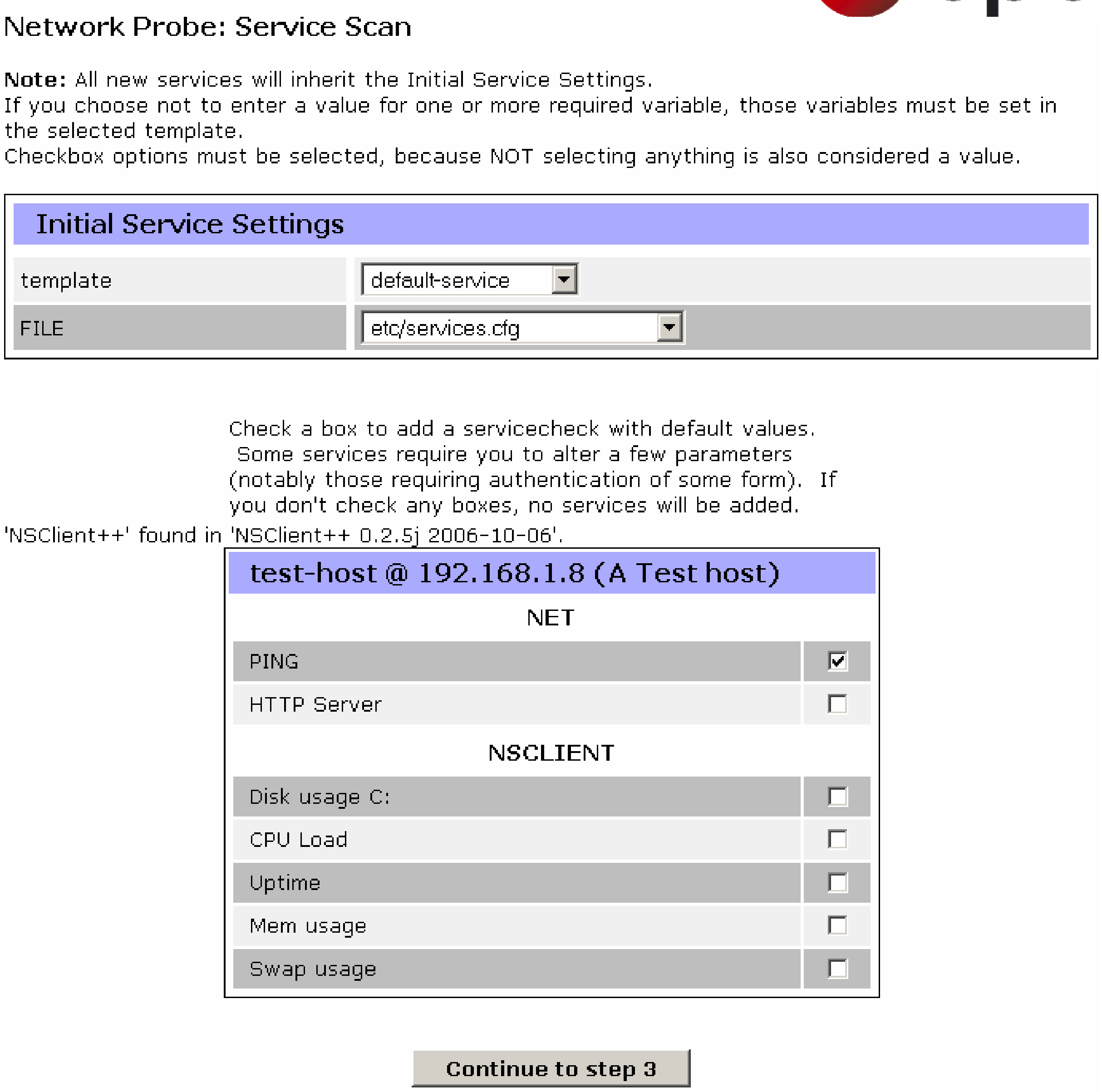


New Host 1

Add this host?	Yes
template	default-host-template (only one configured)
host_name	test-host
alias	A Test host
address	192.168.1.2
contact_groups	support-group
hostgroups	network printers unix-servers win-servers
parents	linux-server1 monitor printer1 router1 switch1 win-server1
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	http
Host logo	win40.png
FILE	etc/hosts.cfg

When you are done entering data, click on the 'Scan hosts for services' button to continue.

A port scan is now performed on the new hosts to detect common services like ftp and http on the host, the scan also searches for any installed agent.



Network Probe: Service Scan

Note: All new services will inherit the Initial Service Settings.
If you choose not to enter a value for one or more required variable, those variables must be set in the selected template.
Checkbox options must be selected, because NOT selecting anything is also considered a value.

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.

'NSClient++' found in 'NSClient++ 0.2.5j 2006-10-06'.

test-host @ 192.168.1.8 (A Test host)	
NET	
PING	☑
HTTP Server	□
NSCLIENT	
Disk usage C:	□
CPU Load	□
Uptime	□
Mem usage	□
Swap usage	□

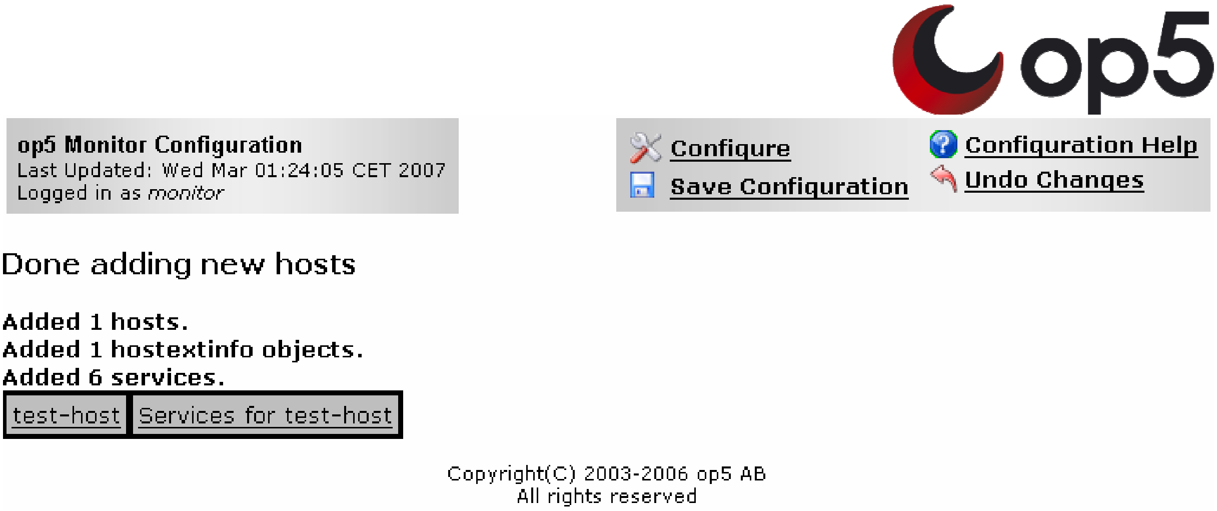
This page is displayed in two segments, first “Initial Service Settings” and below the results of the scan.

Initial Service Settings lets you change “non standard” settings for all services that you are about to add, i.e. settings that differ from the configured service templates (read more about this on Templates). The list is dynamically created depending on if you have used non standard settings before. Normally you do not need to change anything here.

The result of the scan is also displayed as two parts. First part is net related services such as PING, HTTP, FTP and so on. Second part is only displayed if an agent is installed, if that is the case a couple of default checks, such as Disk Usage, CPU Load and so on, appear.

More information about agents is available at the op5 support website.

Check the services you want to add and click 'Continue to step 3'.



op5 Monitor Configuration
Last Updated: Wed Mar 01:24:05 CET 2007
Logged in as *monitor*

Done adding new hosts

Added 1 hosts.
Added 1 hostextinfo objects.
Added 6 services.

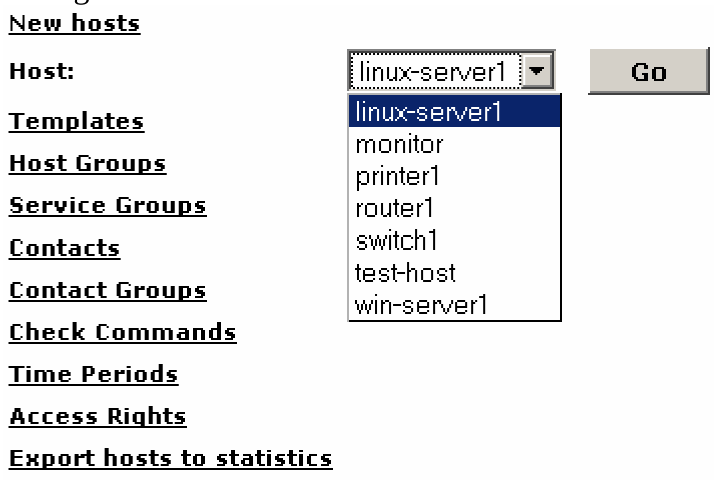
Copyright(C) 2003-2006 op5 AB
All rights reserved

That's it. You have now added a new host. You have the options to go back and do configurations on the new host or its services. If you feel you're done click save configuration. The “Pre-flight configuration check" is made, Monitor reloads the configuration and 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.

There is two ways to fix the configuration if the “Pre-flight configuration check” fails. The first is to try to fix any mistakes that you have done in the configuration gui, pay attention to any errors or warnings displayed during the “Pre-flight configuration check”. The second one is to simply restore an old backup using the Backup/Restore tool.

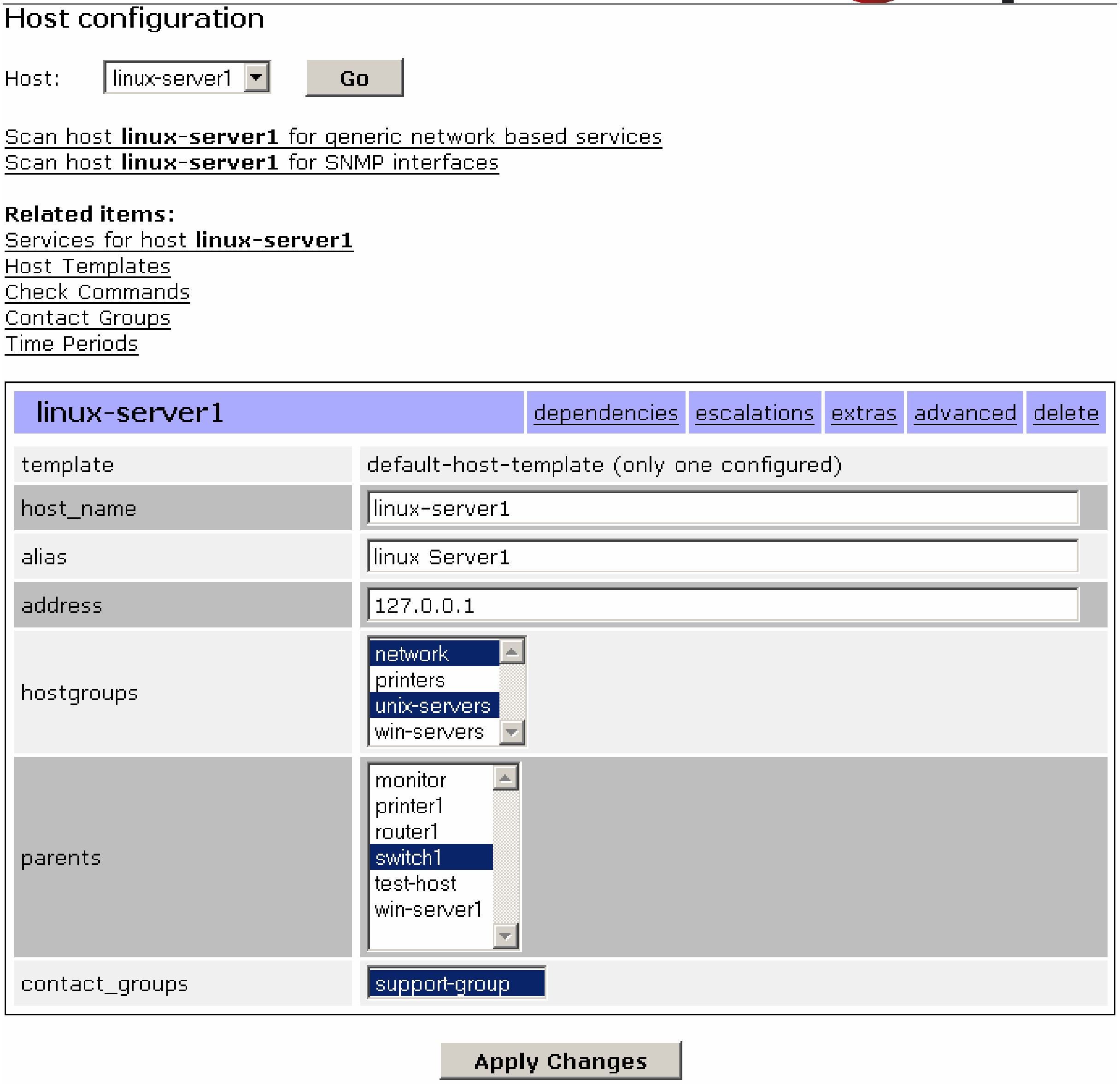
Hosts

To change the configuration of an existing host select the host in the dropdown menu and click go.



Host: linux-server1

You now have the option to configure a couple of host related variables and objects.



Host configuration

Host: linux-server1 ▾ Go

Scan host **linux-server1** for generic network based services
Scan host **linux-server1** for SNMP interfaces

Related items:
Services for host **linux-server1**
Host Templates
Check Commands
Contact Groups
Time Periods

linux-server1 | dependencies | escalations | extras | advanced | delete

template	default-host-template (only one configured)
host_name	linux-server1
alias	linux Server1
address	127.0.0.1
hostgroups	network (selected) printers unix-servers (selected) win-servers
parents	monitor printer1 router1 switch1 (selected) test-host win-server1
contact_groups	support-group (selected)

The page has 4 different functions.

At the top of the page you have a drop down menu where you quickly can switch to another hosts configuration. Below that you have two scan tools to help you with your configuration.

- Scan host for generic network based services which simply does the same scan that you do when adding new hosts.
- Scan host for SNMP interfaces which can help you adding monitoring of interfaces for a RFC1213 (MIB-II) compliant SNMP device.

Related items gives you shortcuts to, well related items. Basically, lets say that you are about to make some configuration changes to your host and discovers that you are missing the new contact_group that you needed you can simply click on the "Contact Groups" link in the related items section. It's supposed to speed up the configuration process by saving you an extra click.

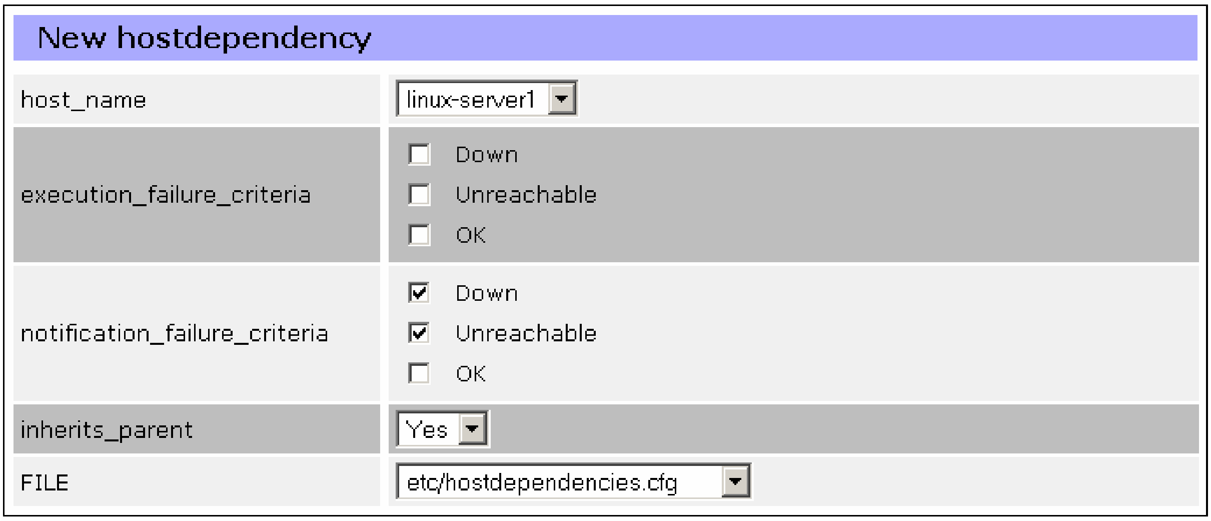
Note: to configure services for a host, click on the "services for host" link in the related items section. Read more about how to configure services on the Services for host headline.

The last part of the host configuration page is the host object box itself. Next to the name of the host in the host object box there are five links: dependencies, escalations, extras, advanced and delete.

Dependencies

Host dependencies are an advanced feature of op5 Monitor that allows you to suppress notifications and even check execution for hosts, based on the status of one or more other hosts. Host dependencies are optional and are mainly targeted at advanced users.

An easy way to get almost the same functionality would be to use the parents directive instead.



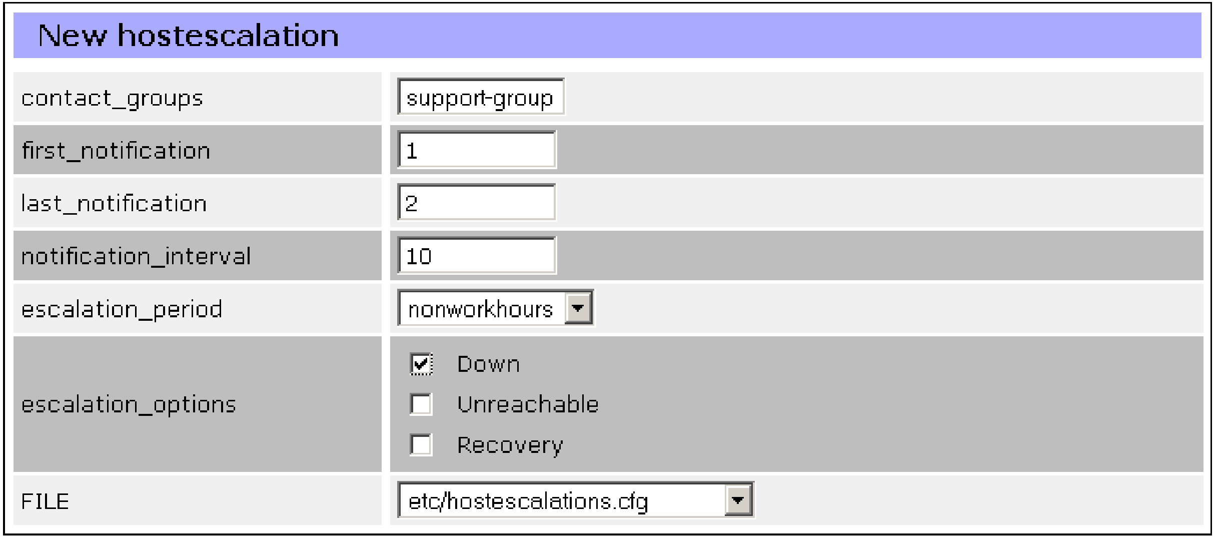
New hostdependency

host_name	linux-server1 ▾
execution_failure_criteria	□ Down □ Unreachable □ OK
notification_failure_criteria	☑ Down ☑ Unreachable □ OK
inherits_parent	Yes ▾
FILE	etc/hostdependencies.cfg ▾

host_name: This defines the host that we are depending on, the parent host.
execution_failure_criteria: If the parent host defined in ‘host_name’ is in one of the selected states this host’s status will not be checked.
notification_failure_criteria: If the parent host defined in ‘host_name’ is in one of the selected states notifications will not be sent out for this host.
inherits_parent: This indicates if this host shall inherit any existing dependencies on the parent host defined by ‘host_name’.
FILE: defines where to store the hostdependency object, do not change this if you are not absolutely sure what it does.

Escalations

Escalations let you configure escalation of notifications for this host. The idea is that if you have a really important host you can send the first notification to the default contact group in order for them to solve the problem. If the problem is not solved in lets say 30 minutes you can send the notification to a broader range of contacts.



New hostescalation

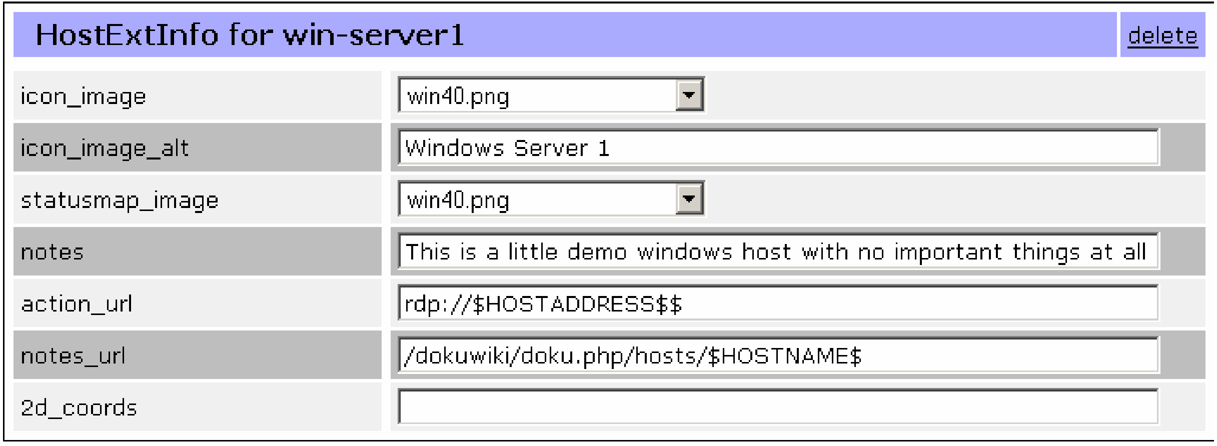
contact_groups	support-group
first_notification	1
last_notification	2
notification_interval	10
escalation_period	nonworkhours
escalation_options	☑ Down □ Unreachable □ Recovery
FILE	etc/hostescalations.cfg

contact_groups: which contact group(s) should receive the notification.
first_notification: which notification, of the total amount notifications sent, is the first to be sent out to this contact group(s)
last_notification: which notification, of the total amount notifications sent, is the last to be sent out to this contact group(s). If you specify 0 only one notification is sent out.
notification_interval: If the interval between first_notification and last_notification is more than one notification this specifies the interval in minutes between notifications.
escalation_period: during which time period is this escalation valid.
escalation_options: which notifications that should be sent out.

Note: To make escalations work you need to set 'notification_interval' to something else than 0 in the configuration for the host.

Extras

Extras let you configure cosmetic things as which logo you want to associate with the host.



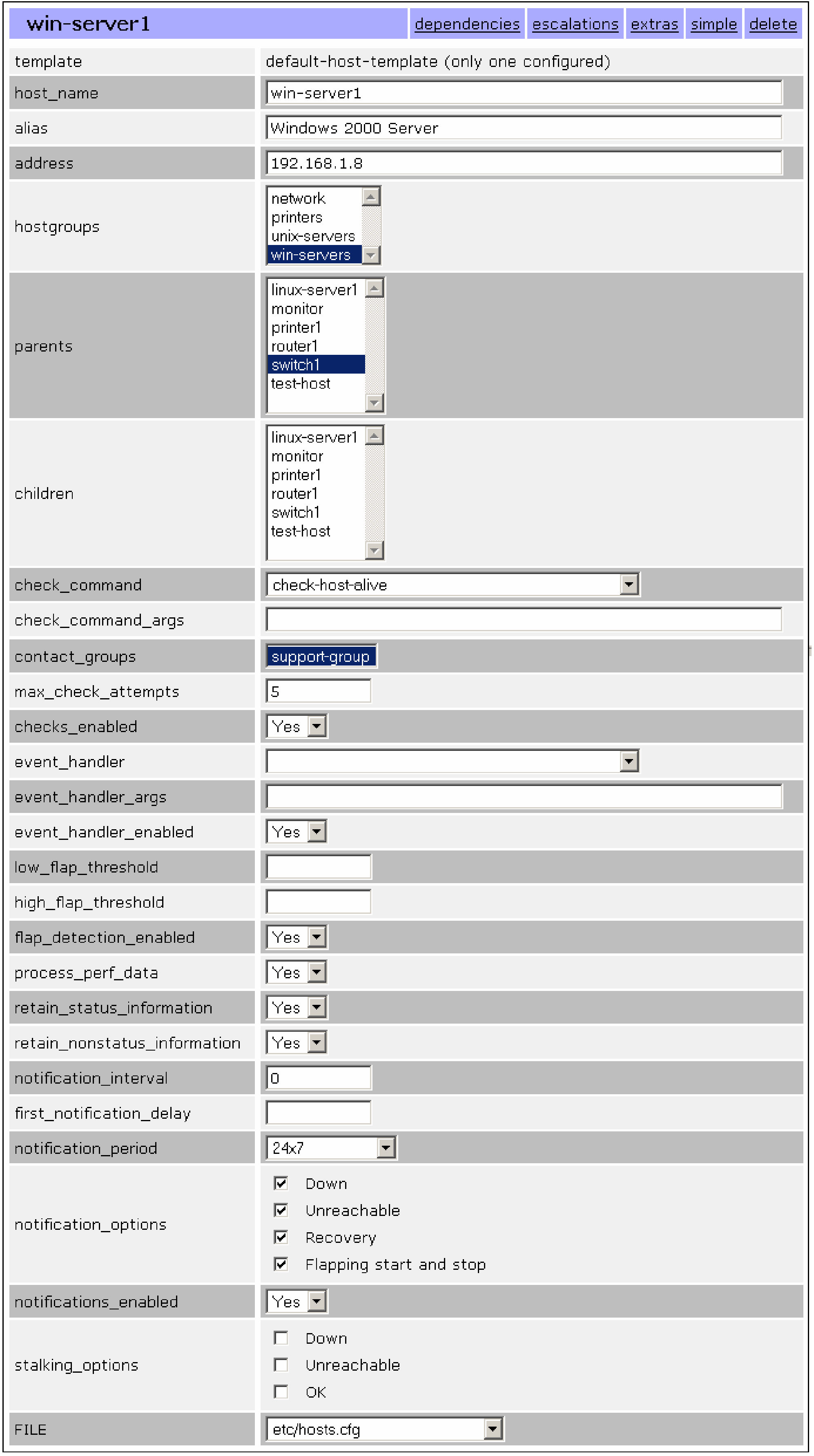
HostExtInfo for win-server1

icon_image	win40.png
icon_image_alt	Windows Server 1
statusmap_image	win40.png
notes	This is a little demo windows host with no important things at all
action_url	rdp://$HOSTADDRESS$$
notes_url	/dokuwiki/doku.php/hosts/$HOSTNAME$
2d_coords	

icon_image: The graphic file used to represent the host in the status or network map.
icon_image_alt: The alias for the host, shown in the status map
statusmap_image: The image used as a background in the status map.
notes: notes for the server
action_url: The url used to manage the host. i.e. telnet, http, ssh
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.

Advanced

There are many variables that can be configured for a host. Most of them is being set by using templates and therefore not displayed in the host configuration box. If you want to change one of those options you can click on Advanced. This will expand the host configuration box to include all variables, even those configured in the selected host template.



win-server1

template	default-host-template (only one configured)
host_name	win-server1
alias	Windows 2000 Server
address	192.168.1.8
hostgroups	network printers unix-servers win-servers
parents	linux-server1 monitor printer1 router1 switch1 test-host
children	linux-server1 monitor printer1 router1 switch1 test-host
check_command	check-host-alive
check_command_args	
contact_groups	support-group
max_check_attempts	5
checks_enabled	Yes
event_handler	
event_handler_args	
event_handler_enabled	Yes
low_flap_threshold	
high_flap_threshold	
flap_detection_enabled	Yes
process_perf_data	Yes
retain_status_information	Yes
retain_nonstatus_information	Yes
notification_interval	0
first_notification_delay	
notification_period	24x7
notification_options	☑ Down ☑ Unreachable ☑ Recovery ☑ Flapping start and stop
notifications_enabled	Yes
stalking_options	□ Down □ Unreachable □ OK
FILE	etc/hosts.cfg

template: 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, usually a short but descriptive name. Example: router1
alias: Full description of the host, since the host_name is supposed to be short you can use this field to enter a more descriptive text. Example: Router for main office.
address: The IP address or host name of the host
hostgroups: The host group(s) that the host will be a member of. The host can be a member of several hostgroups.
parents: The parent(s) that this host will is physically connected to. Example: serverA is connected to switch1 and therefore has switch1 as parent. It is possible to have several parents for redundant connections. Note: There is a limitation in the parent directive, you cannot have circular parent relationships.
children: The hosts that are connected to this host (using this host as a parent). This variable makes it easier to configure parenting. Instead of configuring the parent variable of each host connected to a switch you can use the children variable from the switch and select the child hosts.
check_command: the check command that should be run to determine status of the host. Read more about check_commands on the Check Commands headline.
check_command_args: any arguments required for the check command to work
contact_groups: The contact group(s) this hosts notifications are sent to.
max_check_attempts: The number of checks required for the host to enter HARD state and send out notifications.
checks_enabled: if checks are enabled or not, normally yes.
event_handler: Event handler is a check_command that is run every time a host changes state.
event_handler_args: any arguments needed for the event handler command.
event_handler_enabled: specifies if event handlers should be used or not.
low_flap_threshold: se below note about flap detection
high_flap_threshold: se below note about flap detection
flap_detection_enabled: if flap detection is enabled or not. Normally flap detection is enabled on global basis and not per host.
process_perf_data: Most of the plugins outputs data in two ways. The normal output which you can see in your notifications and web gui, but also performance output. Performance output is a more “machine friendly” output that can be parsed by a script or a piece of software. Currently performance data is used to create graphs of the check result for some standard checks.
retain_status_information: Retain status information between restarts of op5 Monitor
retain_nonstatus_information: Retain other information between restarts of op5 Monitor
notification_interval: The interval in minutes when the host is down or unreachable. If this is set to 0 (default) only one notification is sent out.
first_notification_delay: The amount of minutes to delay the host notification. This can be useful if you want to be able to reboot a server without notifying anyone.
notification_period: During which period notifications for this host should be sent out.
notification_options: Which notifications that should be sent out for this host.
notifications_enabled: If notifications are enabled or not, default is Yes.
stalking_options: Stalking is used mainly for troubleshooting. If you enable stalking, op5 Monitor will log everything related to the host. Note that this will probably cause the log file to grow and therefore slow down all reports. Use this with care.
FILE: Which file this host object should be saved in.

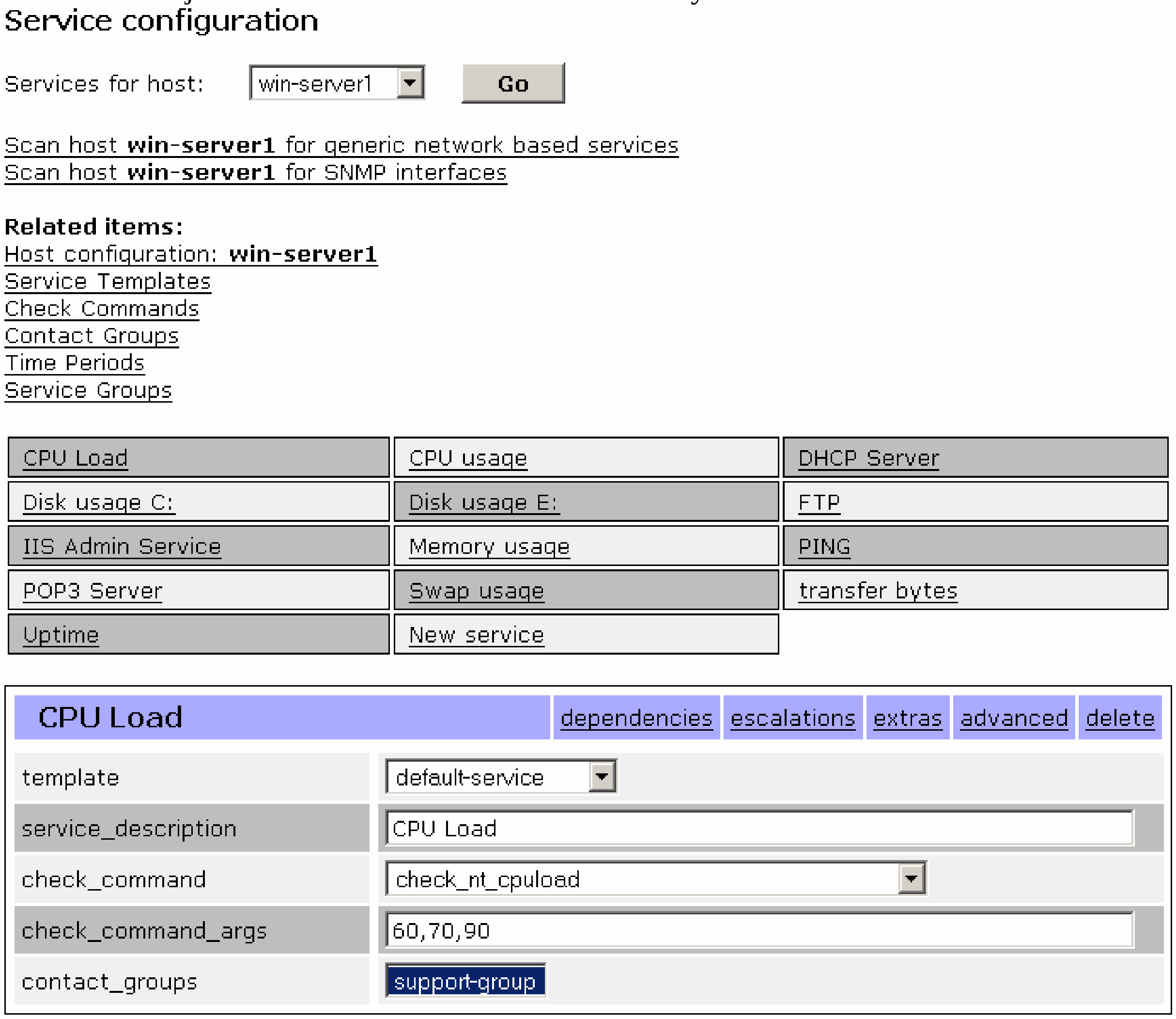
Note: Flap detection is a useful mechanism to detect reoccurring problems with a host or service. The logic works like this.

The result of the 21 last checks is saved in the memory. High_flap_threshold defines a value in percent of how much the host or service has changed its state. If the high_flap_threshold value is exceeded the host/service enters flapping state. To exit flapping state the percentage must go down to the low_flap_threshold value.

Services for host

If you click on the "Services for host" link in the Host configuration window you will be directed to the Service configuration window where you can configure services.

The service objects defines what should be checked on your host.



Service configuration

Services for host: win-server1 ▾ Go

Scan host **win-server1** for generic network based services
Scan host **win-server1** for SNMP interfaces

Related items:
Host configuration: **win-server1**
Service Templates
Check Commands
Contact Groups
Time Periods
Service Groups

CPU Load	CPU usage	DHCP Server
Disk usage C:	Disk usage E:	FTP
IIS Admin Service	Memory usage	PING
POP3 Server	Swap usage	transfer bytes
Uptime	New service	

CPU Load — dependencies | escalations | extras | advanced | delete

template	default-service ▾
service_description	CPU Load
check_command	check_nt_cpuload ▾
check_command_args	60,70,90
contact_groups	support-group

The page is modeled almost the same way as the host configuration page with the exception that several service objects is shown in the same page.

The drop down lets you select another host for which services you want to change, this makes it easier if you need to configure services on several hosts.

You have the option to scan the host for new services, and also to scan for available Interfaces using SNMP.

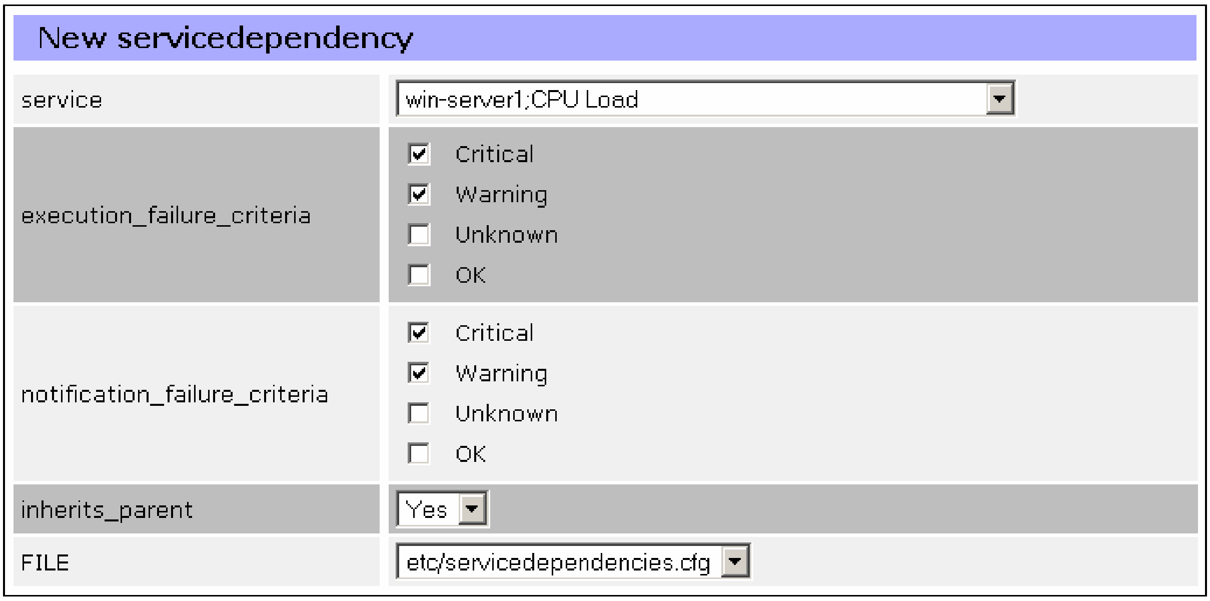
To edit a existing service simply edit the fields for that service and press the <Enter> key or scroll down to the bottom of the page and press Apply Changes.

At the bottom of the page there is always an empty service called "New service", this is for adding new services.

In the header of each service objects you have the following options:

Dependencies

Service dependencies are an advanced feature of op5 Monitor that allows you to suppress notifications and even check execution for services, based on the status of one or more other services. Service dependencies are optional and are mainly targeted at advanced users.



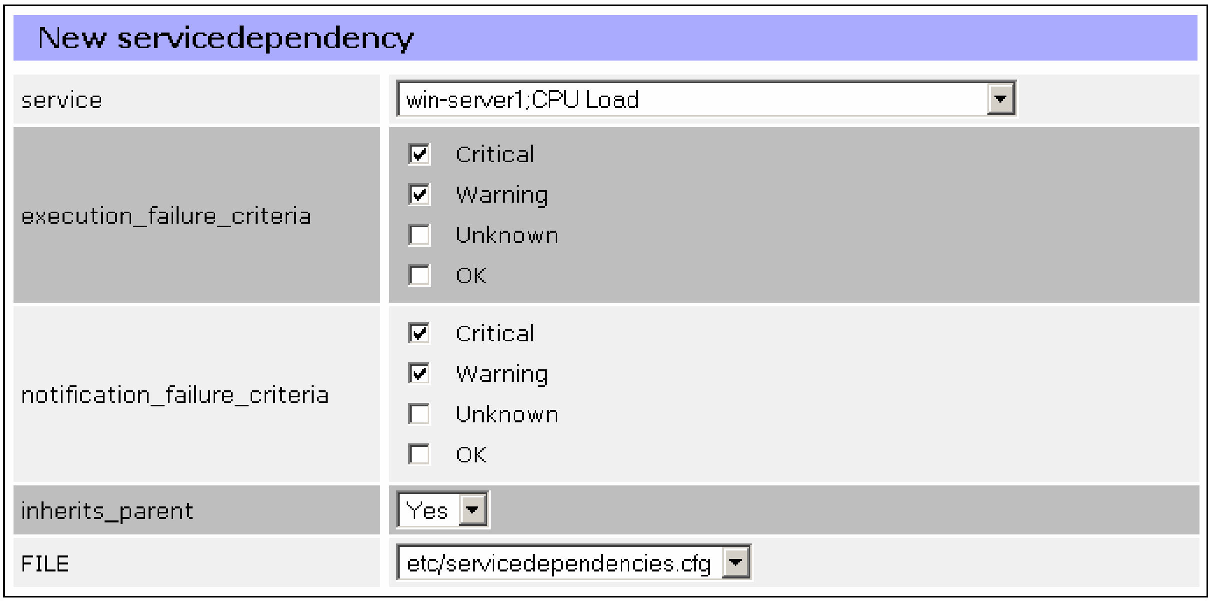
New servicedependency

service	win-server1;CPU Load
execution_failure_criteria	☑ Critical ☑ Warning □ Unknown □ OK
notification_failure_criteria	☑ Critical ☑ Warning □ Unknown □ OK
inherits_parent	Yes
FILE	etc/servicedependencies.cfg

service: This defines the service that we are depending on.
execution_failure_criteria: If the dependent service defined in 'service' is in one of the selected states this services status will not be checked.
notification_failure_criteria: If the dependent service defined in 'service' is in one of the selected states notifications will not be sent out for this service.
inherits_parent: This directive indicates whether or not the dependency inherits dependencies of the service that is being depended upon (also referred to as the master service). In other words, if the master service is dependent upon other services and any one of those dependencies fail, this dependency will also fail.

Escalations

Service escalations can be used to escalate notifications for certain services. The idea is that if you have a really important service you can send the first notification to the normal contact group in order for them to solve the problem. If the problem is not solved in lets say 30 minutes you can send the notification to a broader range of contacts.



New servicedependency

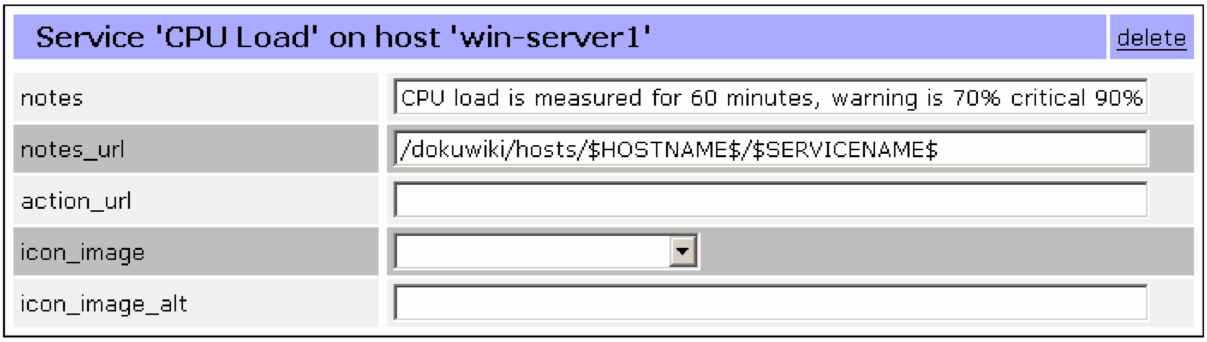
service	win-server1;CPU Load
execution_failure_criteria	☑ Critical ☑ Warning ☐ Unknown ☐ OK
notification_failure_criteria	☑ Critical ☑ Warning ☐ Unknown ☐ OK
inherits_parent	Yes
FILE	etc/servicedependencies.cfg

contact_groups: which contact group(s) should receive the notification.
first_notification: which notification, of the total amount notifications sent, is the first to be sent out to this contact group(s)
last_notification: which notification, of the total amount notifications sent, is the last to be sent out to this contact group(s). If you specify 0 only one notification is sent out.
notification_interval: If the interval between first_notification and last_notification is more than one notification this specifies the interval in minutes between notifications.
escalation_period: during which time period is this escalation valid.
escalation_options: which notifications that should be sent out.

Note: To make escalations work you need to set ‘notification_interval’ to something else than 0 in the configuration for the service.

Extras

Extras let you configure cosmetic things as which logo you want to associate with the service.



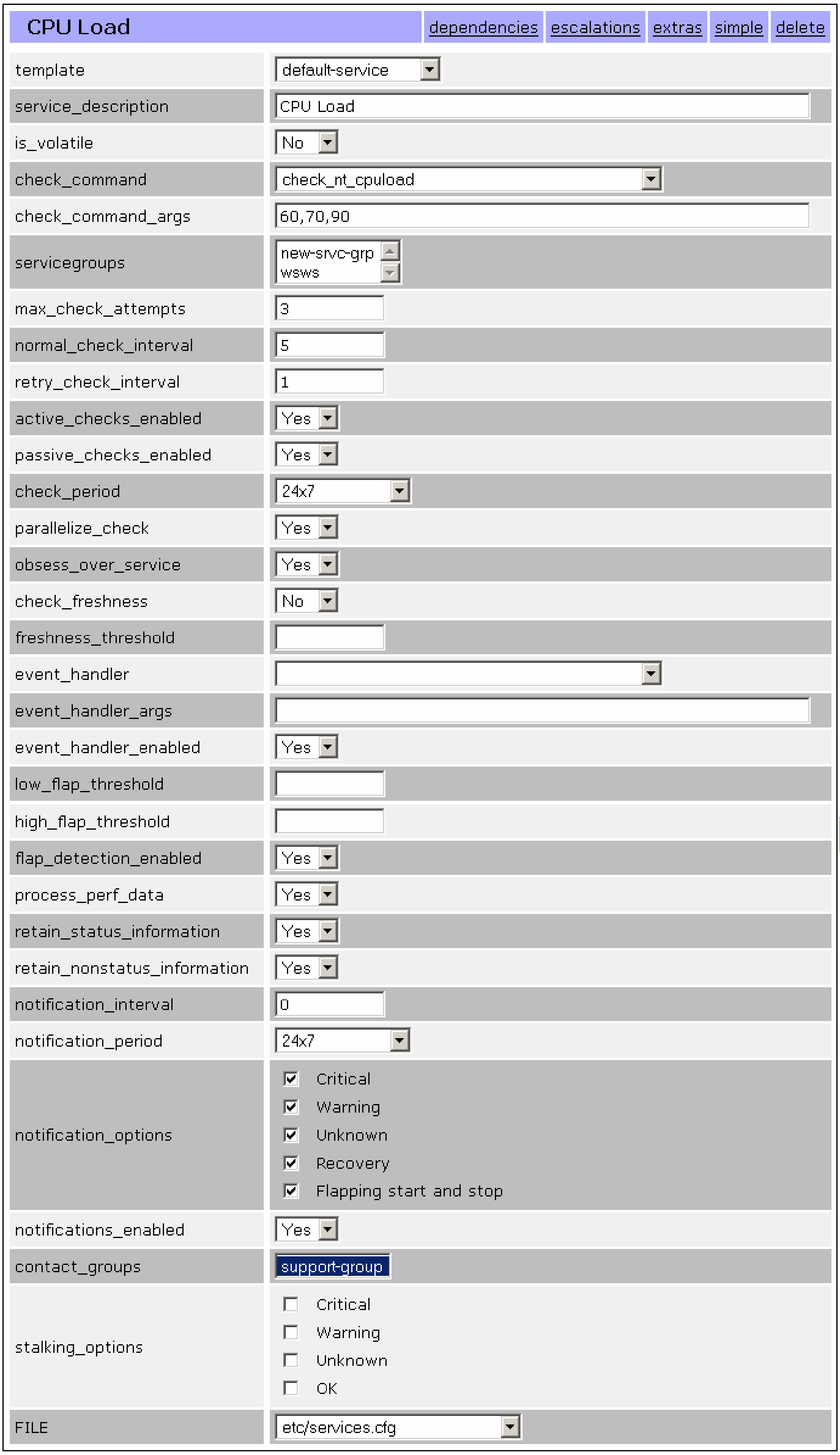
Service 'CPU Load' on host 'win-server1' delete

notes	CPU load is measured for 60 minutes, warning is 70% critical 90%
notes_url	/dokuwiki/hosts/$HOSTNAME$/$SERVICENAME$
action_url	
icon_image	
icon_image_alt	

notes: notes for the service.
notes_url: The documentation URL for this service.
action_url: The url used to manage the service.
icon_image: The graphic file used to represent the service in the Service Detail view.
icon_image_alt: The alias for the service.

Advanced

There are many variables that can be configured for a service. Most of them is being set by using templates and therefore not displayed in the service configuration boxes. If you want to change those options you can click on Advanced. This will expand the service configuration box to include all variables, even those configured in the selected service template.



template	default-service
service_description	CPU Load
is_volatile	No
check_command	check_nt_cpuload
check_command_args	60,70,90
servicegroups	new-srvc-grp wsws
max_check_attempts	3
normal_check_interval	5
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_args	
event_handler_enabled	Yes
low_flap_threshold	
high_flap_threshold	
flap_detection_enabled	Yes
process_perf_data	Yes
retain_status_information	Yes
retain_nonstatus_information	Yes
notification_interval	0
notification_period	24x7
notification_options	☑ Critical ☑ Warning ☑ Unknown ☑ Recovery ☑ Flapping start and stop
notifications_enabled	Yes
contact_groups	support-group
stalking_options	□ Critical □ Warning □ Unknown □ OK
FILE	etc/services.cfg

template: Which template to use for this service.
service_description: The description of the Service.
is_volatile: A volatile service is a service that notifies contacts every time the check is run if the check is in a hard non OK state. This can be useful when utilizing passive service checks when the check result is received from an external source.
check_command: Which check command that shall be run to determine status of the service.
check_command_args: any arguments required for the check command to work.
servicegroups: defines membership in any service group.
max_check_attempts: The amount of checks required for the service to enter HARD state and send notifications.
normal_check_interval: The interval, in minutes, between checks of the service.
retry_check_interval: The interval, in minutes, between checks if the previous check failed.
active_checks_enabled: Active checks enabled, default is Yes.
passive_checks_enabled: Passive checks enabled, default is Yes.
check_period: During which time period this service should be checked.
parallelize_check: Allow this check to be run in parallel with other checks. Default is Yes . Changing this can drastically influence performance.
obsess_over_service: This command can be used to tell op5 Monitor to run a script after each service check. It can be used for certain redundant configurations. Don't use this if you're not sure about what it does.
check_freshness: op5 Monitor supports a feature that does "freshness" checking on the results of host and service checks. This feature is useful when you want to ensure that passive checks are being received as frequently as you want.
freshness_threshold: This directive is used to specify the freshness threshold (in seconds) for this service. If you set this directive to a value of 0, op5 Monitor will determine a freshness threshold to use automatically.
event_handler: Command that should be run in case of a state change.
event_handler_args: Arguments needed for the event handler command.
event_handler_enabled: Enable or disable Event handlers. Default value is Yes.
low_flap_threshold: se below note about flap detection
high_flap_threshold: se below note about flap detection
flap_detection_enabled: if flap detection is enabled or not. Normally flap detection is enabled on global basis and not per service.
process_perf_data: Most of the plugins outputs data in two ways. The normal output which you can see in your notifications and web gui, but also performance output. Performance output is a more "machine friendly" output that can be parsed by a script or a piece of software. Currently performance data is used to create graphs of the check result for some standard checks.
retain_status_information: Retain status information between restarts of op5 Monitor. This is a good thing to enable, otherwise the status will be lost when you save your new configuration.
retain_nonstatus_information: Retain other information between restarts of op5 Monitor. This is also a good thing to enable to not loose status data when saving new configurations.
notification_interval: The interval in minutes between notifications, when the service is Critical, Warning, or Unknown. If this is set to 0 (default) only one notification is sent out.
notification_period: During which period notifications for this service should be sent out.
notification_options: Which notifications that should be sent out for this service.
notifications_enabled: If notifications are enabled or not, default is Yes
contact_groups: The contact group(s) this service notifications is sent to.

stalking_options: Stalking is used mainly for troubleshooting. If you enable stalking, op5 Monitor will log everything related to the host. Note that this will probably cause the log file to grow and therefore slow down all reports. Use this with care.
FILE: Which file this host object should be saved in.

Note: Flap detection is a useful mechanism to detect reoccurring problems with a host or service. The logic works like this.

The result of the 21 last checks is saved in the memory. High_flap_threshold defines a value in percent of how much the host or service has changed its state. If the high_flap_threshold value is exceeded the host/service enters flapping state. To exit flapping state the percentage must go down to the low_flap_threshold value.

Templates

There are three kinds of templates available.

- Host Templates for hosts objects.
- Service Templates for service objects.
- Contact Templates for contact objects.

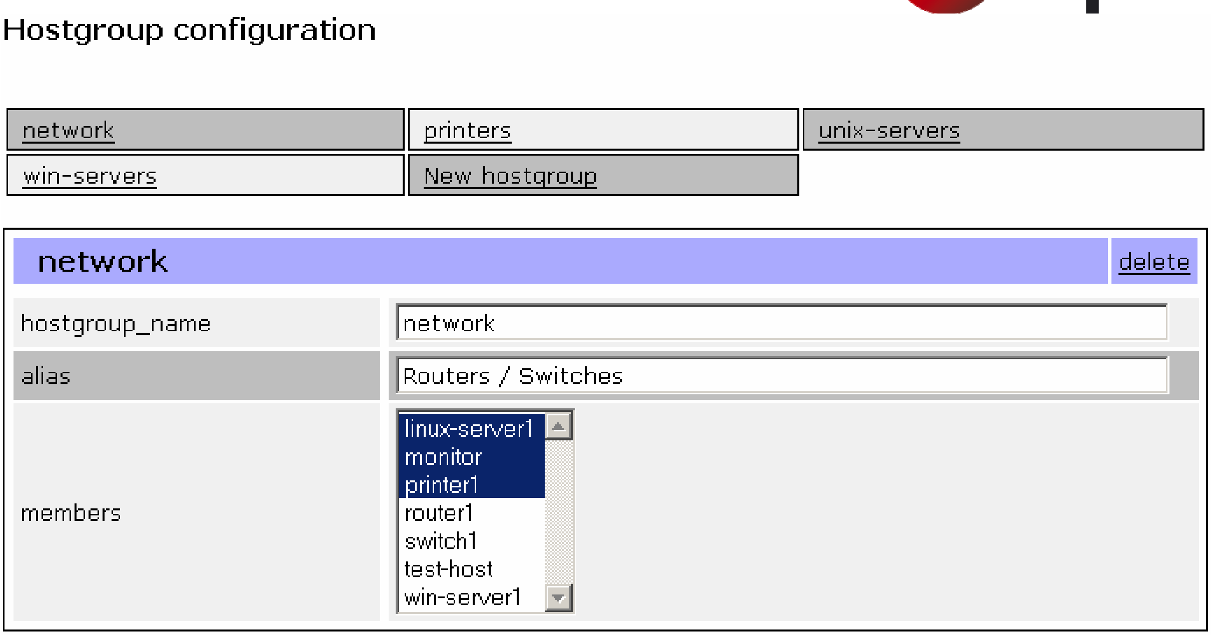
Above mentioned objects needs to have several variables configured, most of those variables are the same for each object. To avoid unnecessary work you can simply define your most common settings in templates and then use those templates when configuring the objects.

Three different templates are shipped with the default configuration for op5 Monitor, default-service, critical-service and noncritical-service. The variables that differs between those templates are, ‘normal_check_interval’, ‘retry_check_interval’ and ‘max_check_attempts’. Services that use the critical-service are monitored more often and notifies quicker than services that uses the noncritical-service.

Host Groups

A hostgroup definition is used to group one or more hosts together for display and / or reporting purposes.

To add, change or delete a host group choose the host group link from the start page.


Hostgroup configuration

network — delete

hostgroup_name: network

alias: Routers / Switches

members: linux-server1, monitor, printer1, router1, switch1, test-host, win-server1

All host groups are listed after each other, represented with a shortcut 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 a single host group.

hostgroup_name: Name of Host group.
alias: Description of Host group.
members: Hosts that are members of this host group, to select several hosts press and hold the <Ctrl> key.

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

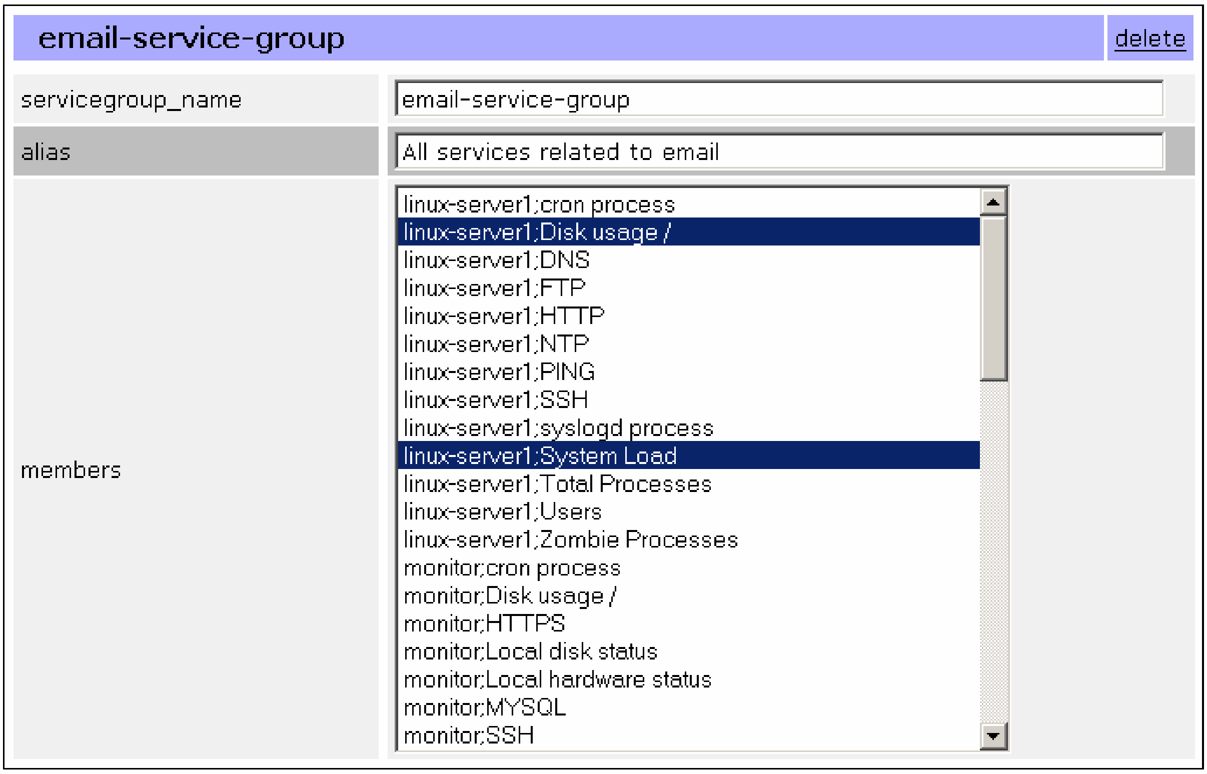
Note: Membership in hostgroups can also be configured when adding new hosts or from the Hosts configuration page.

Service Groups

A servicegroup definition is used to group one or more hosts together for display and / or reporting purposes.

To add, change or delete a servicegroup choose the host group link from the start page.

Servicegroup configuration



email-service-group

servicegroup_name	email-service-group
alias	All services related to email
members	linux-server1;cron process linux-server1;Disk usage / linux-server1;DNS linux-server1;FTP linux-server1;HTTP linux-server1;NTP linux-server1;PING linux-server1;SSH linux-server1;syslogd process linux-server1;System Load linux-server1;Total Processes linux-server1;Users linux-server1;Zombie Processes monitor;cron process monitor;Disk usage / monitor;HTTPS monitor;Local disk status monitor;Local hardware status monitor;MYSQL monitor;SSH

All service groups are listed after each other represented with a shortcut 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 service group configuration window you can click delete to delete chosen service group.

servicegroup_name: Name of the service group
alias: Description of service group
members: Services that are members of this service group

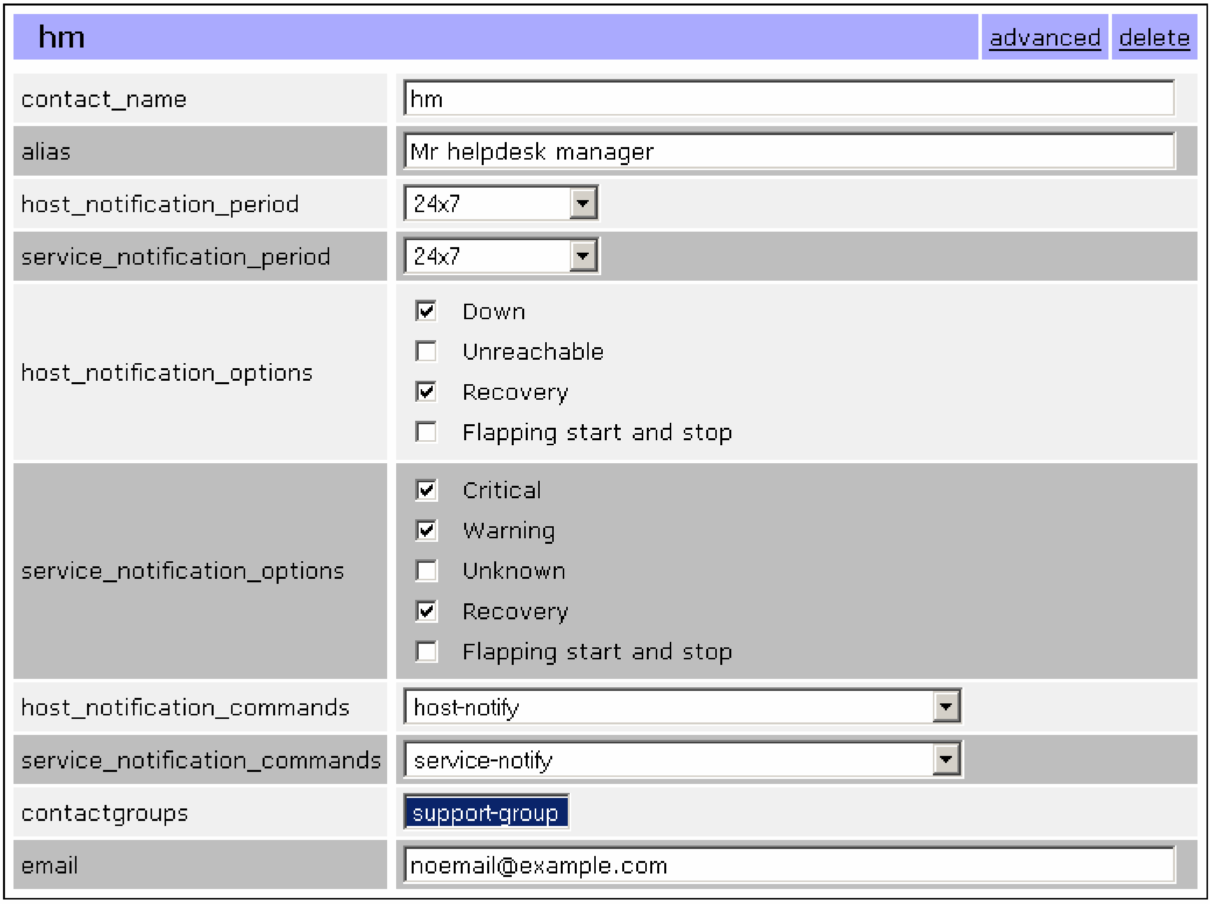
Click 'Apply changes' in the bottom of the window. Click 'Save Configuration' for the changes to take effect.

Servicegroups can be specifically useful to visualize business processes. In the image above a servicegroup named ‘email-service-group’ is configured. If you put all service checks that are related to email in that group, i.e. DNS, internet connections, POP3, SMTP and so on, you will get a good view of how your email service is working in total.

This information can be used for real-time troubleshooting but also for reports.

Contacts

To add, change or delete a contact choose the contacts link from the start page.



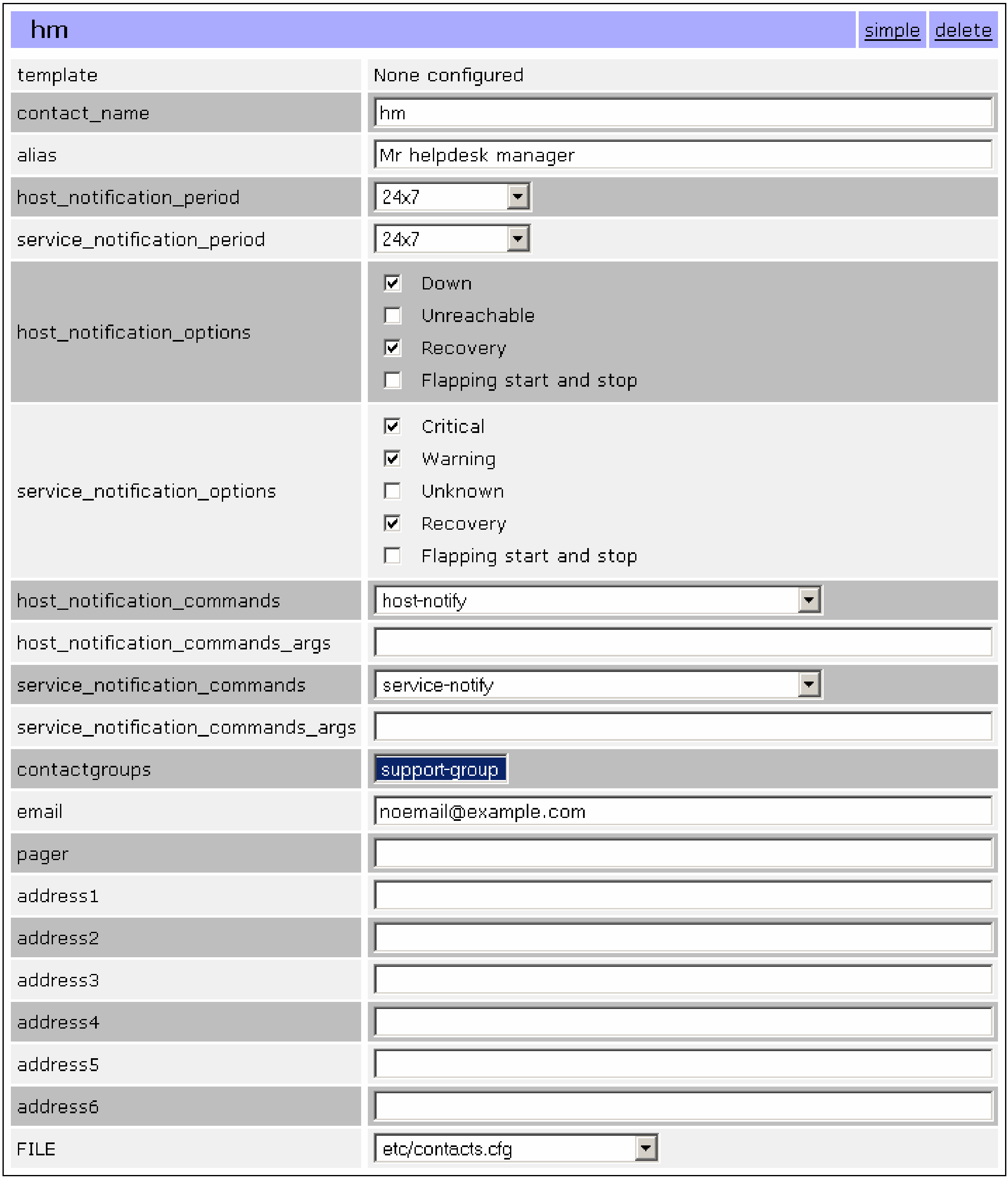
hm | advanced | delete

contact_name	hm
alias	Mr helpdesk manager
host_notification_period	24x7
service_notification_period	24x7
host_notification_options	☑ Down □ Unreachable ☑ Recovery □ Flapping start and stop
service_notification_options	☑ Critical ☑ Warning □ Unknown ☑ Recovery □ Flapping start and stop
host_notification_commands	host-notify
service_notification_commands	service-notify
contactgroups	support-group
email	noemail@example.com

Read more about the variables you can configure for contacts below.

Advanced

Contacts are one of the three objects that can use templates. To expand the contact click on Advanced.



hm simple delete

template	None configured
contact_name	hm
alias	Mr helpdesk manager
host_notification_period	24x7
service_notification_period	24x7
host_notification_options	☑ Down □ Unreachable ☑ Recovery □ Flapping start and stop
service_notification_options	☑ Critical ☑ Warning □ Unknown ☑ Recovery □ Flapping start and stop
host_notification_commands	host-notify
host_notification_commands_args	
service_notification_commands	service-notify
service_notification_commands_args	
contactgroups	support-group
email	noemail@example.com
pager	
address1	
address2	
address3	
address4	
address5	
address6	
FILE	etc/contacts.cfg

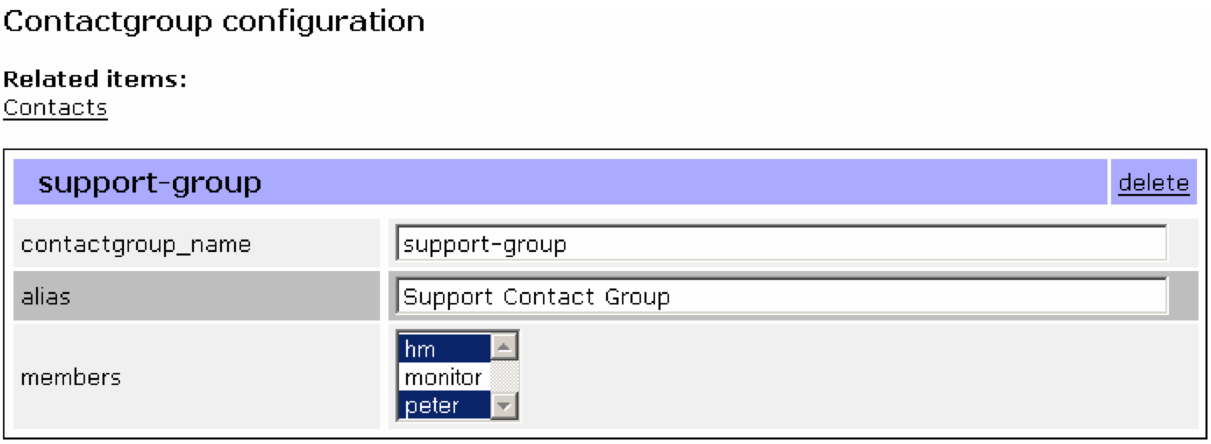
template: Which template to use for this contact.
contact_name: Short name of the contact, it is recommended to use the login name that you normally use.
alias: Full name of the contact, i.e. Mr. Dummy User.
host_notification_period: Time period for which this contact shall receive host notifications.
service_notification_period: Time period for which this contact shall receive service notifications.
host_notification_options: Which host notifications that this contact shall receive.
service_notification_options: Which service notifications that this contact shall receive.
host_notification_commands: Command that is executed to send out host notifications. Op5 Monitor comes with a default host_notification_command, host-notify. This command can

send notifications using email and sms. You can also add your own notification commands if you like.
host_notification_commands_args: Arguments that might be needed for the host_notification_command.
service_notification_commands: Command that is executed to send out service notifications. Op5 Monitor comes with a default service_notification_command, service-notify. This command can send notifications using email and sms. You can also add your own notification commands if you like.
service_notification_commands_args: Arguments that might be needed for the service_notification_command.
contactgroups: The contact group(s) this contact is a member of.
email: This contacts email address, for receiving email notifications.
pager: This contacts cell phone number, for receiving SMS notifications. Note: The number must include country code. Example for a Swedish number, 46701123456.
address1 - 6: These variables are reserved for other kind of notification options. If you create your own notification script you can use these variables to specify notification data.

Tip 1: If you want to notify an individual with both email and SMS we recommend to define two separate contacts with different host and service notification options since you normally want to define different settings for email and SMS.

Contact Groups

A contact group definition is used to group one or more contacts together for the purpose of sending out notifications. When a host or service has a problem or recovers, op5 Monitor will find the appropriate contact groups to send notifications to, and notify all contacts in those contact groups.



Contactgroup configuration

Related items:
Contacts

support-group	delete
contactgroup_name	support-group
alias	Support Contact Group
members	hm monitor peter

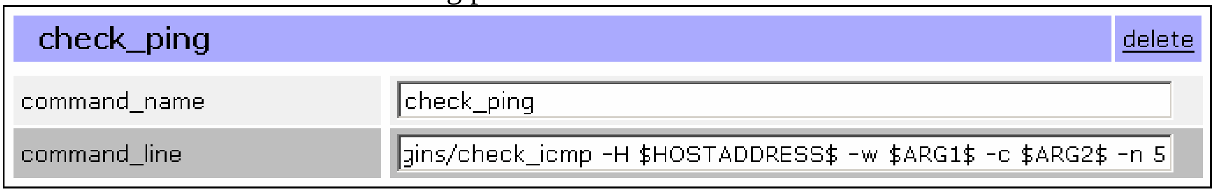
contactgroup_name: Name of the contactgroup.
alias: Description of the contact group.
members: Hosts that are members of this host group, to select several hosts press and hold the <Ctrl> key.

When done configuring click 'Apply changes'. For the changes to take effect choose the 'Save Configuration' from the start page.

Check Commands

A checkcommand is an object that defines a command. Checkcommands are a very vital part of op5 Monitor. Commands are used to do the actual monitoring, send notifications, external scripts such as eventhandler scripts and so on.

The command consists of following parts.



command_name	check_ping
command_line	gins/check_icmp -H $HOSTADDRESS$ -w $ARG1$ -c $ARG2$ -n 5

command_name: A descriptive name of the command.
command_line: the actual command that should be executed.

The command line first defines the search path to the script or program that should be run. The scripts / programs are called plugins. Read more about plugins in the op5 plugins manual, available on op5 support web.

Then any necessary variables are defined. Depending on what input the plugin might need, different variables can be specified. The check_icmp plugin above demands the variable '-H <ipaddress>' where <ipaddress> should be the IP Address of the host that should be checked. To make checkcommand definitions more flexible there are a subset of macros that can be used.

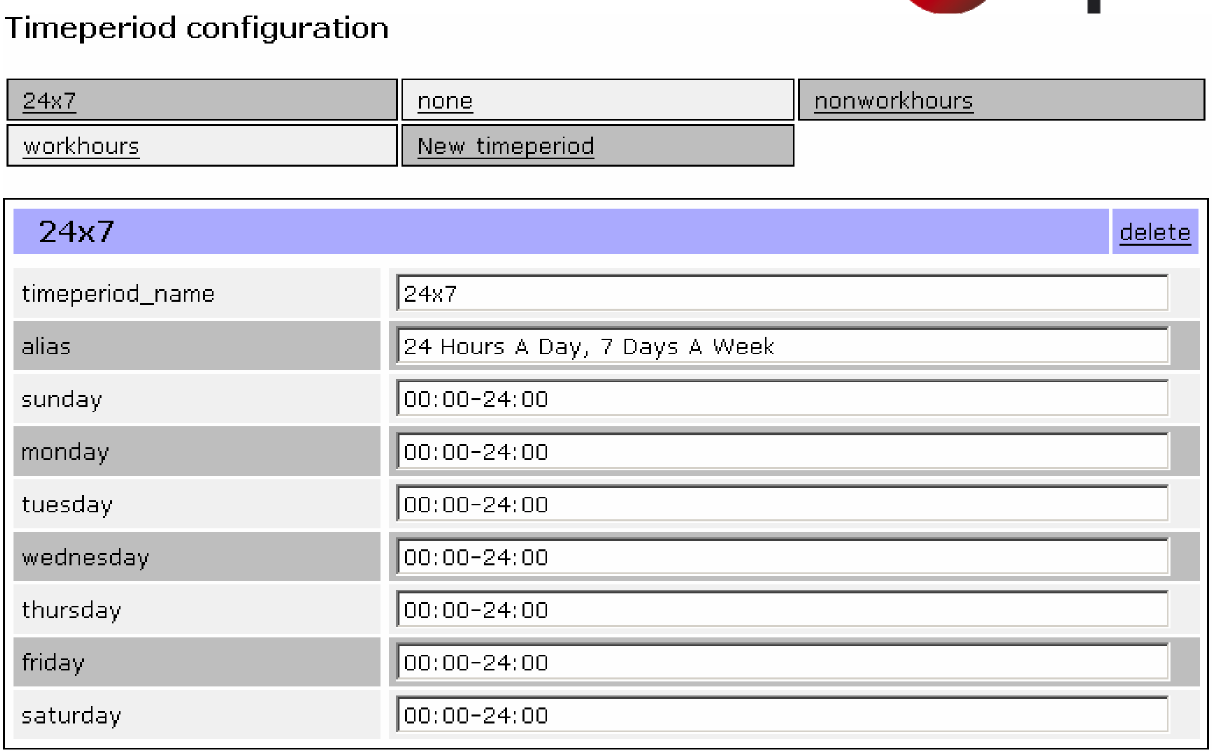
In this case we use the $HOSTADDRESS$ macro which will automatically be translated to the IP Address of the host that the checkcommand is run for.

A full list of available macros is available from the Nagios manual at
http://nagios.sourceforge.net/docs/2_0/macros.html

Time Periods

Time periods is time defining objects that span over a week. You can define "included" time for each day of the week in the time period definition.

The timeperiod objects are used at many places in the configuration. Most noticeably are in the contact objects where the timeperiods defines when notifications should be sent out. You can also use timeperiods to define when a service or a host should be monitored or when you are creating availability reports.



Timeperiod configuration

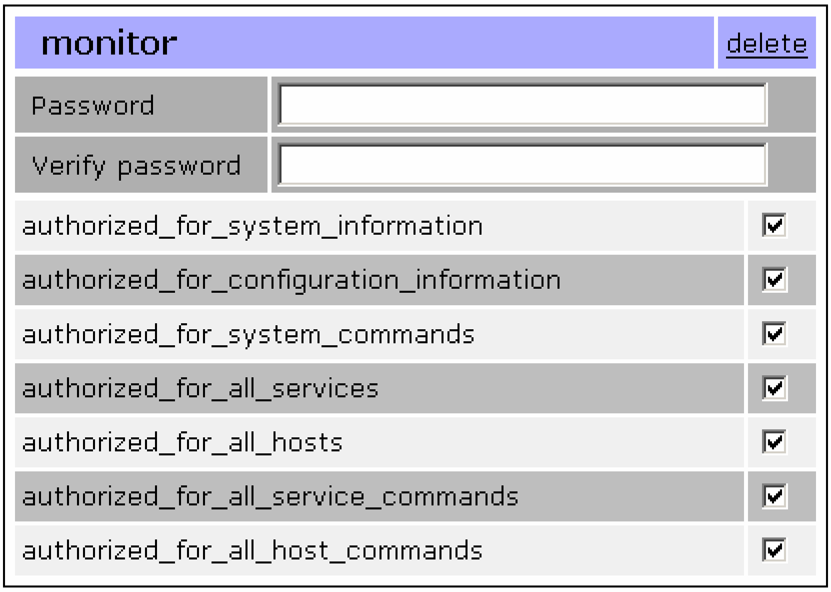
24x7 — delete

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

timeperiod_name: short name of the time period
alias: descriptive name of the time period
Monday to Sunday: which time to include for each day. you can define multiple times by separating them with comma. Example 00:00-01:00,03:00-06:00

Access Rights

Users of op5 Monitor web gui needs to provide a username and password to gain access. There are seven different variables that control what level of access a user has.



monitor — 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	☑

Password: Password for the user, hidden by default.
Verify password: type the password a second time to verify
authorized_for_system_information: Gives the user access to the system / process information, most of the views in op5 Monitor can not be accessed.

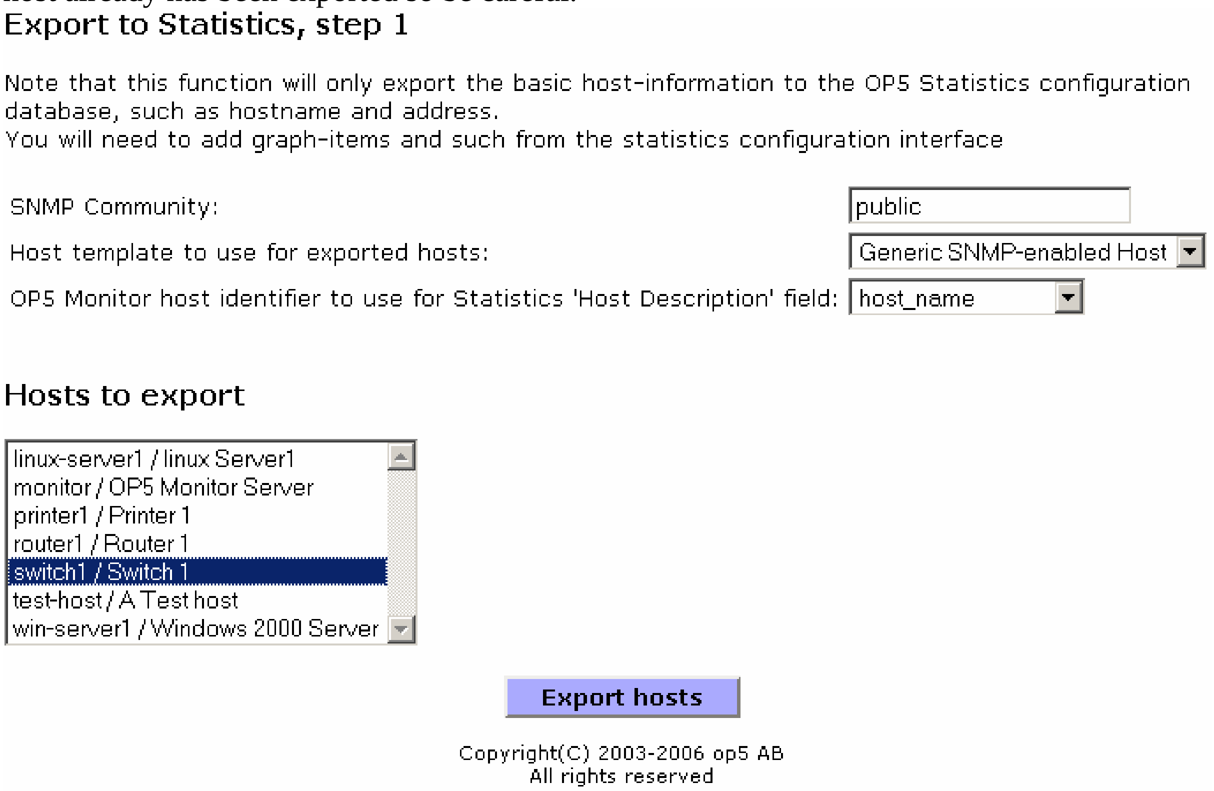
authorized_for_configuration_information: Gives the user access to view and change configuration.
authorized_for_system_commands: Gives the user access to issuing commands in the web gui. With commands you can control certain functions in op5 Monitor, for example: enable/disable notifications, scheduled downtime, acknowledge problems and so on.
authorized_for_all_services: Gives the user access to view all services, se Customizing views below for more information.
authorized_for_all_hosts: Gives the user access to view all hosts, se Customizing views below for more information.
authorized_for_all_service_commands: Gives the user access to issue commands for all services, se Customizing views below for more information.
authorized_for_all_host_commands: Gives the user access to issue commands for all hosts, se Customizing views below for more information.

Recommended settings for an administrator would be to check all boxes. For helpdesk staff it could be ‘authorized_for_system_information’ and ‘authorized_for_system_commands’, that way they can acknowledge problems but not change the configuration.

Export hosts to statistics

This function allows you to export hosts from op5 Monitor to op5 Statistics in order to save time when configuring op5 Statistics.

For now this is fairly simple export functionality and does not do any checks to detect if the host already has been exported so be careful.



Export to Statistics, step 1

Note that this function will only export the basic host-information to the OP5 Statistics configuration database, such as hostname and address.
You will need to add graph-items and such from the statistics configuration interface

SNMP Community: public

Host template to use for exported hosts: Generic SNMP-enabled Host

OP5 Monitor host identifier to use for Statistics 'Host Description' field: host_name

Hosts to export

linux-server1 / linux Server1
monitor / OP5 Monitor Server
printer1 / Printer 1
router1 / Router 1
switch1 / Switch 1
test-host / A Test host
win-server1 / Windows 2000 Server

Copyright(C) 2003-2006 op5 AB
All rights reserved

Select which host(s) you want to export, change the SNMP Community if needed and select which Host template to use in statistics. You can also specify which host identifier in op5 Monitor that shall be used as Host Description in statistics.

Click Export hosts and you are done.

Customizing views

It is possible to configure a user with limited access to the system not only by denying access to certain views using Access Rights but also by only letting the user see a selected choice of hosts and services.

In smaller companies or organizations this might not be needed but for larger enterprises it can be quite useful to be able to customize the objects op5 Monitor displays for each user or team of users. This function can also be useful if you are a hosting provider.

Customization of the gui can be done in three steps where the last step is optional and only for advanced users since it requires editing html or php files on the op5 Monitor system.

1. Configure a new contact.
2. Add the contact to an existing contactgroup or create a new contactgroup specific for the new contact. If you created a new contactgroup make sure to add the contact group for the hosts and services that you want to make available in the customized view.
3. Configure a user in access rights with the exact same name as the contact you created. When selecting options do not use the last fore options, authorized_for_all_. By doing this the new user will only see the hosts and services that uses the contactgroup that he is a member of.
4. Create a directory in /opt/monitor/share/ with the same name as the contact and user you just configured. Create your own index.html and side.html files, you can use the files available in /opt/monitor/share as start. Make sure to set the right permissions on the directory and the files so that the web server can read the files.

Remember the third step is optional and only for advanced users.

To test your new “limited” simply log on as the new user you just created.

Index

Appendix 1 - Icons

Icon	Description
🛠	Indicates that a host / service problem is acknowledged.
★	Link to action_url
🕹	Indicates a executed command in the Event Log
📝	Indicates that comments are available for a host / service
●	Indicates a critical log entry in the Event Log
⏱	Affect the time a check is executed
🗑	Remove comments or downtime
🔍	View extended information
✗	Disable
▼	Entries sorted decending
☾	Host / Service is in scheduled downtime
✓	Enable
🗒	Link to notes_url, external source with host / service documentation
⇅	Host / service is flapping
🕒	View alert history for this host
ℹ	Indicates an information log entry in the Event Log
«	Back
🔄	Indicates logfile rotation in the Event Log
🔇	Notifications disabled
🛠	Remove problem acknowledgement
📝	Add new comment
🔊	Notifications enabled
👤	Only passive checks are processed
OK	Status OK
🔄	Restart op5 Monitor
»	Forward
⚙	An eventhandler has been executed for this service
▶	Monitor was started
🚦	Show status
🔍	View status details for this host, ie all services
📍	Locate on status map
⏻	Stop op5 Monitor
📊	Show Trend
?	Status Unknown
!	Status Warning
▲	Entries sorted ascending