

op5 Monitor 4.0

Manual

October 24, 2008

Contents

1	Getting Started	1
1.1	Using op5 Monitor	1
1.2	Start page	1
2	About the Main Menu	3
2.1	About	3
2.2	Simple menu or Advanced menu	3
3	Viewing Current Monitoring Information	4
3.1	Tactical Overview	4
3.2	Host Detail and Service Detail	8
3.2.1	Host Detail	8
3.3	Service Detail	13
3.3.1	op5 Monitor Simple Graphs	14
3.3.2	Extended service Information	14
3.3.3	Service commands	16
3.4	Filtering	18
3.5	Host group Summary, Overview and Grid	19
3.5.1	Host group Summary	19
3.5.2	Host group Overview	20
3.5.3	Host group Grid	20
3.6	Service group Summary, Overview and Grid	20
3.6.1	Service group Summary	21
3.6.2	Service group Overview	21
3.6.3	Service group Grid	22
4	Presentation Using Maps	23
4.1	Status Map	23
4.2	Network Map	26
4.2.1	View host group	27
4.2.2	View custom map (default)	28

4.2.3	Edit host group	28
4.2.4	Edit custom map	29
4.3	Hyper Map	30
5	Problem Views for Work Flow	31
5.1	Network Outages	31
5.2	Host Problems	32
5.3	Service Problems	32
5.4	Unhandled Problems	32
5.5	Show Host	33
5.6	Comments	33
5.7	Downtime	34
6	Runtime Status	36
6.1	Process Info	36
6.1.1	The Process Information	36
6.1.2	Process Commands	37
6.2	Performance Info	39
6.2.1	Services Actively Checked	39
6.2.2	Services Passively Checked	39
6.2.3	Hosts Actively Checked	40
6.2.4	Hosts Passively Checked	40
6.3	Scheduling Queue	41
7	Reporting Web Menu	42
7.0.1	Reporting	42
7.1	Trends	42
7.2	Availability	45
7.3	Old Availability	49
7.4	SLA Reporting	53
7.5	Alert History	55
7.6	Alert Summary	56
7.6.1	Top 25 Hard Service Alert Producers	57
7.7	Notifications	58
7.8	Event Log	58
7.9	Schedule Reports	59
8	Configuration Web Menu	61
8.0.1	View Config	61
8.1	Change Password	62
8.2	Backup / Restore	62

8.2.1	Create a backup	62
8.2.2	Restore a backup	63
8.3	Configure	63
8.3.1	Configuration basics	65
8.3.2	New Hosts	65
8.3.3	Hosts	70
8.3.4	Dependencies	72
8.3.5	Escalations	73
8.3.6	Extras	75
8.3.7	Clone	75
8.3.8	Parent/Child	76
8.3.9	Advanced	76
8.3.10	Services for host	80
8.3.11	Dependencies	82
8.3.12	Escalations	83
8.3.13	Extras	84
8.3.14	Advanced	85
8.3.15	Templates	89
8.3.16	Host Groups	90
8.3.17	Service Groups	91
8.3.18	Contacts	92
8.3.19	Contact Groups	94
8.3.20	Commands	95
8.3.21	Time Periods	96
8.3.22	Access Rights	99
8.3.23	Assign Group Rights	100
8.3.24	Export hosts to statistics	100
A	Customizing Views	102
B	Profiles and Cloning	104
B.1	Overview	104
B.2	Profiles	105
B.2.1	Creating a Profile	105
B.2.2	Use from a Profile	105
B.3	Cloning	106
B.3.1	Cloning from an Existing Host	106
B.3.2	Cloning services	106

C Basic Work Flows around Monitor	107
C.1 Getting the Contacts Right	107
C.2 Tuning Alerts	108
C.3 Updating Monitor	108
C.4 Handling Alerts	109
C.4.1 Acknowledging Alerts	109
C.5 Service Groups	110
D Index	111

Introduction

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

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

Using This Manual

This manual is written using the same structure as the Web Interface – so as to function as a reference manual where you can easily find the answers to the specific part of Monitor you are looking for.

If you can not find what you are looking for, please read through the index for any possible keywords, or look at the table of contents for the appendixes.

Targeted Audience

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.

Chapter 1

Getting Started

1.1 Using op5 Monitor

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

The interface is protected by using both authentication (username and password) and by SSL ¹ which enables a secure manner for accessing the web interface using encryption.



1.2 Start page

The start page is the first page that you access 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, shortcuts to monitor, support information and more.

¹Secure Socket Layer

To access op5 Monitor simply click on the op5 Monitor logo. This will direct you to the <https://a.b.c.d/monitor/> page 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.

Chapter 2

About the Main Menu

2.1 About

The portal 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, if you are running op5 Appliance – an easy way to install updates.

Since op5 System version 3.0 you can update all your op5 Software using yum – more information on this is available in op5 System manual.

2.2 Simple menu or Advanced menu

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.



Chapter 3

Viewing Current Monitoring Information

The monitoring section in the web menu is related to problem management and status of your network.

3.1 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: Tue Oct 21 11:06:57 CEST 2008
 Updated every 90 seconds
 op5 Monitor 4.0.0, powered by Nagios®
 Logged in as monitor

Monitoring Performance
 Service Check Execution Time: 0.01 / 0.38 / 0.135 sec
 Service Check Latency: 0.01 / 0.27 / 0.162 sec
 Host Check Execution Time: 0.01 / 0.08 / 0.023 sec
 Host Check Latency: 0.01 / 0.25 / 0.168 sec
 # Active Host / Service Checks: 6 / 29
 # Passive Host / Service Checks: 0 / 0

Network Outages
 0 Outages

Network Health
 Host Health:
 Service Health:

Hosts

0 Down	0 Unreachable	6 Up	0 Pending
--------	---------------	------	-----------

Services

0 Critical	0 Warning	0 Unknown	29 Ok	0 Pending
------------	-----------	-----------	-------	-----------

Monitoring Features

Flap Detection		Notifications		Event Handlers		Active Checks		Passive Checks	
ENABLED	All Services Enabled No 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 connected to it become unreachable from the op5 Monitor system. This will then be listed as a *Network Outage*. You can see 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. **Monitoring Features** You have the possibility to enable and disable some functionality on global basis. Just by clicking on the vertical bars labeled ENABLED 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. 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 plugin 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 see, 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.

3.2 Host Detail and Service Detail

Host and Service detail gives you a detailed status list of all hosts. The list is sorted on the hostname column by default. You can change this 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.

3.2.1 Host Detail

Current Network Status
 Last Updated: Tue Oct 21 12:53:09 CEST 2008
 Updated every 90 seconds
 op5 Monitor 4.0.0, powered by Nagios®
 Logged in as **monitor**

[View Service Status Detail For All Host Groups](#)
[View Status Overview For All Host Groups](#)
[View Status Summary For All Host Groups](#)
[View Status Grid For All Host Groups](#)

Host Status Totals				Service Status Totals				
Up	Down	Unreachable	Pending	Ok	Warning	Unknown	Critical	Pending
6	0	0	0	29	0	0	0	0
All Problems		All Types		All Problems		All Types		
0		6		0		29		

Host Status Details For All Host Groups

Host	Status	Last Check	Duration	Status Information
linux-server1	UP	2008-10-21 12:50:44	0d 2h 5m 17s	OK - 127.0.0.1 responds to ICMP. Packet 1, rtt 0.000ms
monitor	UP	2008-10-21 12:51:34	0d 2h 5m 9s	OK - localhost responds to ICMP. Packet 1, rtt 0.000ms
printer1	UP	2008-10-21 12:52:24	0d 2h 3m 29s	OK - 127.0.0.1 responds to ICMP. Packet 1, rtt 0.033ms
router1	UP	2008-10-21 12:52:24	0d 2h 2m 43s	OK - 127.0.0.1 responds to ICMP. Packet 1, rtt 0.000ms
switch1	UP	2008-10-21 12:48:54	0d 2h 4m 54s	OK - 127.0.0.1 responds to ICMP. Packet 1, rtt 0.030ms
win-server1	UP	2008-10-21 12:48:14	0d 2h 4m 46s	OK - 192.168.1.8 responds to ICMP. Packet 1, rtt 0.839ms

6 Matching Host Entries Displayed

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 are by default 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.

Host Information

Last Updated: Tue Oct 21 13:10:53 CEST 2008
Updated every 90 seconds
op5 Monitor 4.0.0, powered by [Nagios®](#)
Logged in as **monitor**

[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](#)

Host

Windows Server 2003
(win-server1)

Member of
win-servers

192.168.1.8
(Windows Server 1)

Extra Actions

Host State Information

Host Status:	UP (for 0d 2h 22m 30s)
Status Information:	OK - 192.168.1.8 responds to ICMP. Packet 1, rtt 13.203ms
Performance Data:	pkt=1;0;0;0;5 rta=13.203;2000.000;2000.000;;
Current Attempt:	1/5 (HARD state)
Last Check Time:	2008-10-21 13:08:54
Check Type:	ACTIVE
Check Latency / Duration:	0.116 / 0.062 seconds
Next Scheduled Active Check:	2008-10-21 13:13:57
Last State Change:	2008-10-21 10:48:23
Last Notification:	N/A (notification 0)
Is This Host Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	2008-10-21 13:10:52 (0d 0h 0m 1s ago)

Active Checks: **ENABLED**

Passive Checks: **ENABLED**

Obsessing: **ENABLED**

Notifications: **ENABLED**

Event Handler: **ENABLED**

Host Commands

- [Locate host on map](#)
- [Disable active checks of this host](#)
- [Re-schedule the next check of this host](#)
- [Submit passive check result for this host](#)
- [Stop accepting passive checks for this host](#)
- [Stop obsessing over this host](#)
- [Disable notifications for this host](#)
- [Send custom host notification](#)
- [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](#)

1. Useful links to status pages and reports for the selected host.
2. Base information about the host. Hostname, description, ip-address 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

1. **Locate Host On Map:** Link to status map with focus on the host
2. **Disable Active Checks Of This Host:** This can be used to temporary disable the host checks for that host.
3. **Re-schedule the next check of this host:** 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.
4. **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.
5. **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.
6. **Stop Obsessing Over This Host:** This is only used when configuring certain redundant solutions and should normally not be used.
7. **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.
8. **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.

9. **Send custom host notification:** This command is used to send a custom notification about the specified host. Useful in emergencies when you need to notify admins of an issue regarding a monitored system or service. Custom notifications normally follow the regular notification logic in op5 Monitor. Selecting the Forced option will force the notification to be sent out, regardless of the time restrictions, whether or not notifications are enabled, etc. Selecting the Broadcast option causes the notification to be sent out to all normal (non-escalated) and escalated contacts. These options allow you to override the normal notification logic if you need to get an important message out.
10. **Delay next host notification:** This alternative is only displayed if the host is in a non ok state. It lets you delay the next problem notification that is sent out for the specified host. The notification delay will be disregarded if the host changes state before the next notification is scheduled to be sent out. This command has no effect if the host is currently UP.
11. **Schedule Downtime For This Host:** This command is used to schedule downtime on the selected host.
12. **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.
13. **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.
14. **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.

15. **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.
16. **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.
17. **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.
18. **Disable Flap Detection For This Host:** This command is used to disable flap detection for the selected host.

3.3 Service Detail

Current Network Status Last Updated: Tue Oct 21 13:56:31 CEST 2008 Updated every 90 seconds op5 Monitor 4.0.0, powered by Nagios® Logged in as monitor		Host Status Totals				Service Status Totals				
		Up	Down	Unreachable	Pending	Ok	Warning	Unknown	Critical	Pending
		6	0	0	0	29	0	0	0	0
		All Problems		All Types		All Problems		All Types		
		0		6		0		29		

[View History For all hosts](#)
[View Notifications For All Hosts](#)
[View Host Status Detail For All Hosts](#)

Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
linux-server1 ★	Disk usage /	OK	2008-10-21 13:53:31	0d 3h 8m 0s	1/3	DISK OK - free space: / 4615 MB (71% inode=95%):
	HTTP	OK	2008-10-21 13:55:03	0d 3h 6m 28s	1/3	HTTP OK - HTTP/1.1 302 Found - 0.000 second response time
	NTP	OK	2008-10-21 13:51:56	0d 3h 5m 42s	1/3	NTP OK: Offset -0.003997287655 secs, jitter=5.214000
	PING	OK	2008-10-21 13:51:35	0d 3h 4m 56s	1/3	OK - 127.0.0.1: rta 0.086ms, lost 0%
	SSH	OK	2008-10-21 13:53:22	0d 2h 28m 9s	1/3	SSH OK - OpenSSH_4.3 (protocol 2.0)
	System Load	OK	2008-10-21 13:53:55	0d 3h 8m 39s	1/3	OK - load average: 0.00, 0.00, 0.00
	Total Processes	OK	2008-10-21 13:53:39	0d 3h 7m 52s	1/3	PROCS OK: 82 processes
	Users	OK	2008-10-21 13:54:25	0d 3h 7m 6s	1/3	USERS OK - 1 users currently logged in
	Zombie Processes	OK	2008-10-21 13:55:11	0d 3h 6m 20s	1/3	PROCS OK: 0 processes with STATE = Z
	cron process	OK	2008-10-21 13:55:57	0d 3h 5m 34s	1/3	PROCS OK: 1 process with command name 'crond'
	syslogd process	OK	2008-10-21 13:51:43	0d 3h 4m 48s	1/3	PROCS OK: 1 process with command name 'syslogd'

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.

3.3.1 op5 Monitor Simple Graphs

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

There are four graphs displayed – daily, weekly, monthly and yearly.

The graphs are generated using nagiosgraph from the performance data output from the plugins. If you try running a plugin such as `/opt/plugins/check.http` manually, you will see that there is the data that is presented in the webgui, followed by a pipe and more detailed numbers.

It is these detailed numbers to the right of the pipe that is saved as performance data, and later used to generate graphs.

If you wish to enable your own plugins to create graphs, you can look at our map definitions in `/opt/monitor/op5/nagiosgraph/map` and put your own definitions in the directory `map_custom/`.

Note: Your map files putted in `map_custom/` must end with `.map` as file extension.

3.3.2 Extended service Information

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

Service Information

Last Updated: Tue Oct 21 13:50:30 CEST 2008
Updated every 90 seconds
op5 Monitor 4.0.0, powered by Nagios®
Logged in as **monitor**

[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
Memory usage
On Host
Windows Server 2003
(win-server1)
Member of
No servicegroups.
192.168.1.8


Service State Information

Current Status:	OK (for 0d 2h 54m 21s)
Status Information:	Memory usage: total:1105.79 Mb - used: 380.16 Mb (34%) - free: 725.62 Mb (66%)
Performance Data:	'Memory usage'=380.16Mb;884.63;995.21;0.00;1105.79
Current Attempt:	1/3 (HARD state)
Last Check Time:	2008-10-21 13:46:28
Check Type:	ACTIVE
Check Latency / Duration:	0.182 / 0.121 seconds
Next Scheduled Check:	2008-10-21 13:51:28
Last State Change:	2008-10-21 10:56:09
Last Notification:	N/A (notification 0)
Is This Service Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	2008-10-21 13:50:27 (0d 0h 0m 3s ago)

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](#)
-  [Send custom service notification](#)
-  [Schedule downtime for this service](#)
-  [Disable event handler for this service](#)
-  [Disable flap detection for this service](#)

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.

3.3.3 Service commands

1. **Disable Active Checks Of This Service:** This can be used to temporarily disable the checks for that service.
2. **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.
3. **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.
4. **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.
5. **Stop Obsessing Over This Service:** This is only used when configuring certain redundant solutions and should normally not be used.
6. **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.
7. **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.
8. **Delay Next Service Notification:** This alternative is only displayed if the service is in a non ok state. It 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.

9. **Schedule Downtime For This Service:** This command is used to schedule downtime on the selected service.
10. **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.
11. **Disable Flap Detection For This Service:** This command is used to disable flap detection for the selected host.

3.4 Filtering

Current Network Status
 Last Updated: Tue Oct 21 16:38:45 CEST 2008
 Updated every 90 seconds
 op5 Monitor 4.0.0, powered by Nagios®
 Logged in as **monitor**

[View History For all hosts](#)
[View Notifications For All Hosts](#)
[View Host Status Detail For All Hosts](#)

Display Filters:
 Host Status Types: Up
 Host Properties: Any
 Service Status Types: Ok
 Service Properties: Any

Host Status Totals					Service Status Totals				
Up	Down	Unreachable	Pending		Ok	Warning	Unknown	Critical	Pending
5	1	0	0		28	0	0	1	0
All Problems		All Types			All Problems		All Types		
1		6			1		29		

Service Status Details For All Hosts

Host ^v	Service ^v	Status ^v	Last Check ^v	Duration ^v	Attempt ^v	Status Information
linux-server1 ★	Disk usage /	OK	2008-10-21 16:38:31	0d 5h 50m 14s	1/3	DISK OK - free space: / 4614 MB (71% inode=95%):
	HTTP	OK	2008-10-21 16:35:03	0d 5h 48m 42s	1/3	HTTP OK - HTTP/1.1 302 Found - 0.001 second response time
	NTP	OK	2008-10-21 16:36:56	0d 5h 47m 56s	1/3	NTP OK: Offset -1.405540388e-06 secs, jitter=0.074000
	PING	OK	2008-10-21 16:36:35	0d 5h 47m 10s	1/3	OK - 127.0.0.1: rta 0.072ms, lost 0%
	SSH	OK	2008-10-21 16:38:22	0d 5h 10m 23s	1/3	SSH OK - OpenSSH_4.3 (protocol 2.0)
	System Load	OK	2008-10-21 16:33:55	0d 5h 50m 53s	1/3	OK - load average: 0.00, 0.01, 0.00
	Total Processes	OK	2008-10-21 16:38:39	0d 5h 50m 6s	1/3	PROCS OK: 84 processes
	Users	OK	2008-10-21 16:34:25	0d 5h 49m 20s	1/3	USERS OK - 1 users currently logged in
	Zombie Processes	OK	2008-10-21 16:35:11	0d 5h 48m 34s	1/3	PROCS OK: 0 processes with STATE = Z
	cron process	OK	2008-10-21 16:35:57	0d 5h 47m 48s	1/3	PROCS OK: 1 process with command name 'crond'
	syslogd process	OK	2008-10-21 16:36:43	0d 5h 47m 2s	1/3	PROCS OK: 1 process with command name 'syslogd'
monitor ★	Disk usage /	OK	2008-10-21 16:37:29	0d 5h 46m 16s	1/3	DISK OK - free space: / 4614 MB (71% inode=95%): Uptime: 83994 Threads: 16 Questions: 15790 Slow

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.

3.5 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
- Host Group Overview
- Host Group Grid



3.5.1 Host group Summary

Host Group	Host Status Summary	Service Status Summary
Routers / Switches (network)	3 UP	11 OK
Printers (printers)	1 UP	1 OK
Unix / Linux Servers (unix-servers)	2 UP	20 OK
Windows Servers (win-servers)	1 UP	6 OK

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 good view if you quickly want to get a summary of all your host groups.









3.5.2 Host group Overview





Routers / Switches (network)				Printers (printers)				Unix / Linux Servers (unix-servers)			
Host	Status	Services	Actions	Host	Status	Services	Actions	Host	Status	Services	Actions
monitor	UP	9 OK	   	printer1	UP	1 OK	   	linux-server1	UP	11 OK	   
router1	UP	1 OK	   					monitor	UP	9 OK	   
switch1	UP	1 OK	   								

Windows Servers (win-servers)			
Host	Status	Services	Actions
win-server1	UP	6 OK	   

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

3.5.3 Host group Grid

Unix / Linux Servers (unix-servers)										
Host	Services									Actions
linux-server1	Disk usage /	HTTP	NTP	PING	SSH	System Load	Total Processes	Users	Zombie Processes	   
monitor	Disk usage /	MySQL	SSH	Swap Usage	System Load	Users	Zombie Processes	cron process	syslogd process	   

Windows Servers (win-servers)										
Host	Services									Actions
win-server1	CPU usage	Disk usage C:	Disk usage E:	IIS Admin Service	Memory usage	PING				   

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

3.6 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:

3.6.1 Service group Summary

Service Group	Host Status Summary	Service Status Summary
Disk usage servicegroup (disk-usage)	3 UP	4 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.

3.6.2 Service group Overview

Disk usage servicegroup (disk-usage)			
Host	Status	Services	Actions
linux-server1	UP	1 OK	   
monitor	UP	1 OK	   
win-server1	UP	2 OK	   

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

3.6.3 Service group Grid

Disk usage servicegroup (disk-usage)		
Host	Services	Actions
linux-server1	Disk usage /	   
monitor	Disk usage /	   
win-server1	Disk usage C: Disk usage E:	   

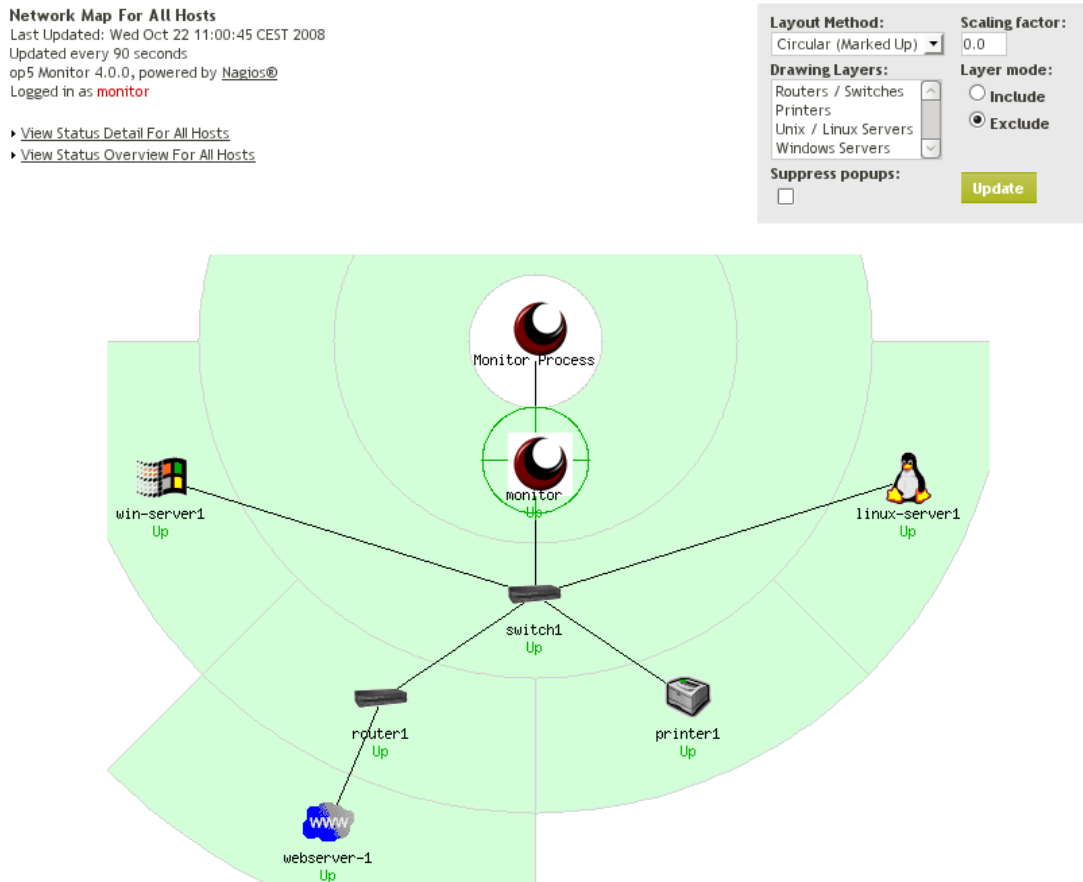
Servicegroup Grid is the most detailed view it shows one table per service group listing each host and service with colors representing status.

Chapter 4

Presentation Using Maps

4.1 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.



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

1. Layout Method, there are a couple of layout methods available
 - (a) User-supplied coords, you can configure x and y coords for your hosts (see host Extras for more information)
 - (b) Depth layers, shows only one level of the network at a time. Click on a host to display the host and the underlying layer.
 - (c) Collapsed tree, shows the network in a tree layout with everything centered towards the middle
 - (d) Balanced tree, shows the network in a tree layout but with the underlying levels centered below each parent host.

- (e) Circular, shows a circular layout.
 - (f) 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.
 - (g) 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.
2. 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.
 3. 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.

4.2 Network Map

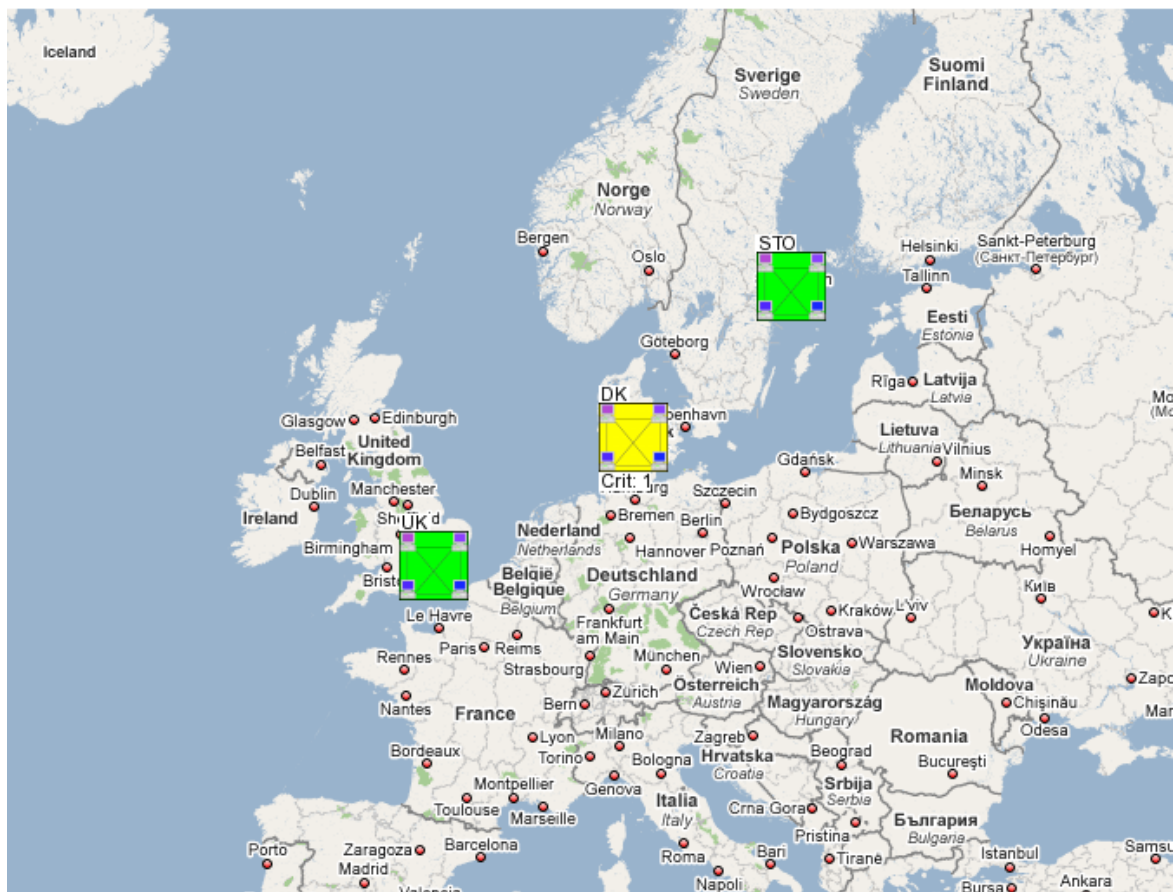
The network map is an enhanced version of the status map with possibility to create highly customized views of a network by just click and place hosts, host groups and views on a map.

Network Map

- View settings
- Global settings

Map mode Custom map

Current custom view: Root view



The image above shows an example configuration of the network map, a background image of Europe including 3 custom maps.

Configuration of the network map is done from the configuration

box in the upper right corner

Network Map

- View settings
- Global settings

Map mode Custom map

1. 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.
2. 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.

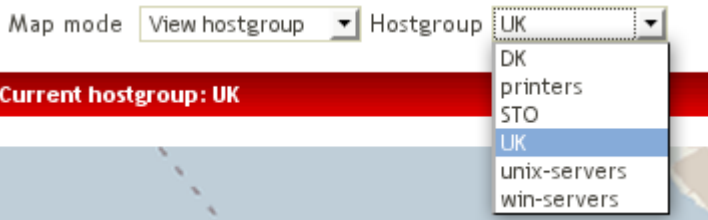
4.2.1 View host group

Network Map

- View settings
- Global settings

Map mode Hostgroup

Current hostgroup: UK



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

4.2.2 View custom map (default)

Network Map

- View settings
- Global settings

Map mode Custom map

Current custom view: Root view



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

4.2.3 Edit host group

Network Map

- View settings
- Global settings

Map mode Hostgroup Select object

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

4.2.4 Edit custom map

Network Map

- View settings
- Global settings

Map mode Custom map Select object Background

Custom view tree

Root view
 └─ Sthlm view
 └─ UK view

Select task

Create new custom view

Name

Parent

Current custom view: Root view

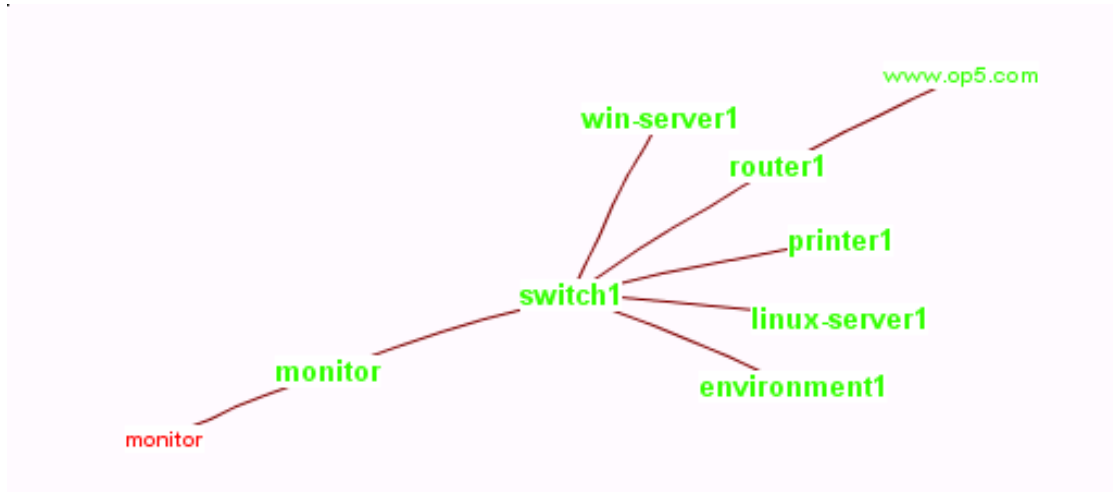
Custom maps are configured in a tree hierarchy. This makes it possible to have several network layers.

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

Available tasks are:

1. **Create new custom view:** Allows you to create new views
2. **Rename this view:** Allows you to rename the selected view
3. **Add items to this view:** Allows you to add items (host groups and hosts) to the selected view
4. **Remove items from this view:** Allows you to remove items (host groups and hosts) from the selected view
5. **Handle background images:** Allows you to upload new background images (must be .png format), Set default background and delete existing background images.

4.3 Hyper Map



Hyper Map is a java applet that draws all hosts and connections and then lets you – 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 see a status summary for the host. If you click on a host you will get to the service detail page for that host.

Chapter 5

Problem Views for Work Flow

5.1 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.

Network Outages

Last Updated: Wed Oct 22 23:01:00 CEST 2008
Updated every 90 seconds
op5 Monitor 4.0.0, powered by [Nagios®](#)
Logged in as **monitor**

Blocking Outages

Severity	Host	State	Notes	State Duration	# Hosts Affected	# Services Affected	Actions
3	router1	DOWN	N/A	0d 0h 0m 52s	2	7	    





1. **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).

2. **Host:** Name of the host causing the network outage
3. **State:** State of the host
4. **Notes:** Link to comments for the host, if there are no comments N/A is displayed
5. **State Duration:** For how long has the outage been going on
6. **Hosts Affected:** Number of hosts affected by the outage
7. **Services Affected:** Number of services affected by the outage
8. **Actions:** A couple of icons that links you to different status pages for the host causing the outage. For a full list of icons and images see **Table of Icons**.

5.2 Host Problems

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.

5.3 Service Problems

Host ^v	Service ^v	Status ^v	Last Check ^v	Duration ^v	Attempt ^v	Status Information
router1	 PING	 CRITICAL	2008-10-22 23:40:52	0d 0h 43m 1s	1/3	CRITICAL - 128.0.0.1: rta nan, lost 100%
webserver-1	 FTP	 CRITICAL	2008-10-22 23:41:27	0d 2h 18m 16s	3/3	CRITICAL - Socket timeout after 10 seconds

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.

5.4 Unhandled Problems

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 it 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.

5.5 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.

5.6 Comments

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

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 process is restarted. Acknowledgement comments are however kept over process restarts as long as the problem still persists, regardless if the comment is persistent or not.

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.

5.7 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 in scheduled downtime.

Basically the Schedule Downtime view is a summary of all currently configured scheduled downtime for hosts and services. In this view you can schedule new downtime. It is however even easier to schedule downtime from the views Host Information, Service Information, Hostgroup Information and Servicegroup Information.


All Host and Service Scheduled Downtime
Last Updated: Thu Oct 23 00:51:33 CEST 2008
Updated every 90 seconds
op5 Monitor 4.0.0, powered by Nagios®
Logged in as **monitor**

Scheduled Host Downtime

 [Schedule host downtime](#)

Host Name	Entry Time	Author	Comment	Start Time	End Time	Type	Duration	Downtime ID	Trigger ID	Actions
webserver-1	2008-10-23 00:38:31	Monitor Admin	Hardware service	2008-10-23 00:38:04	2008-10-23 02:38:04	Fixed	0d 2h 0m 0s	1	N/A	

Scheduled Service Downtime

 [Schedule service downtime](#)

Host Name	Service	Entry Time	Author	Comment	Start Time	End Time	Type	Duration	Downtime ID	Trigger ID	Actions
linux-server1	SSH	2008-10-23 00:50:32	Monitor Admin	security patch	2008-10-23 00:49:32	2008-10-23 02:49:32	Flexible	0d 0h 45m 0s	2	N/A	

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.

Chapter 6

Runtime Status

6.1 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.

6.1.1 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 were rotated.

Monitor PID: op5 Monitor's Process ID.

Notifications Enabled: (Yes or No)

Process Commands

-  [Shutdown the Monitor process](#)
-  [Restart the Monitor process](#)
-  [Disable notifications](#)
-  [Stop executing service checks](#)
-  [Stop accepting passive service checks](#)
-  [Stop executing host checks](#)
-  [Stop accepting passive host checks](#)
-  [Disable event handlers](#)
-  [Start obsessing over services](#)
-  [Start obsessing over hosts](#)
-  [Disable flap detection](#)
-  [Disable performance data](#)

Service Checks Being Executed: (Yes or No)

Passive Service Checks Being Accepted: (Yes or No)

Host Checks Being Executed: (Yes or No)

Passive Host Checks Being Accepted: (Yes or No)

Event Handlers 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)

6.1.2 Process Commands

Shutdown the Monitor process: Shutdown the Monitor program. You may do this either by the system console, or via a SSH connection.

Note: If you have an op5 Monitor Appliance system you can do this in the “Configure System”.

You can find more information about accessing the linux terminal in op5 System manual.

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.

Disable performance data: This command is used to disable the processing of performance data for hosts and services on a program-wide basis.

6.2 Performance Info

op5 Monitor gives you detailed information about its performance.

6.2.1 Services Actively Checked

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 Services Passively Checked 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:

1. 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.
2. 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.
3. Percent State Change: 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.

6.2.2 Services Passively Checked

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 actively checked so the values can be quite low or equal to zero.

6.2.3 Hosts Actively Checked

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 Hosts Passively Checked 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 only be used as a performance measurement if you have configured op5 Monitor to actively check all your hosts.

Note that if you haven't configured op5 Monitor to actively check all your hosts and still have a lot of active hosts checks being executed then you probably have an unstable network and a large "percent state change" value.

6.2.4 Hosts Passively Checked

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 actively checked.

6.3 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: Wed Oct 22 18:02:40 CEST 2008
 Updated every 90 seconds
 op5 Monitor 4.0.0, powered by Nagios®
 Logged in as **monitor**

Entries sorted by next check time (ascending)

Host ▾	Service ▾	Last Check ▾	Next Check ▾	Type	Active Checks	Actions
router1	PING	2008-10-22 17:57:45	2008-10-22 18:02:45	Normal	ENABLED	 
router1		2008-10-22 17:57:49	2008-10-22 18:02:59	Normal	ENABLED	 
webserver-1	HTTPS Server	2008-10-22 17:58:17	2008-10-22 18:03:17	Normal	ENABLED	 
linux-server1	SSH	2008-10-22 17:58:22	2008-10-22 18:03:22	Normal	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 calendar icon links you to specify a new time for check execution. The X let you disable an active check for that service and host.

Chapter 7

Reporting Web Menu

7.0.1 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.

7.1 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:

Continue to Step 2

Select the preferred report type, Host or Service.

Step 2: Select Service

Service:

[Continue to Step 3](#)

Select host or service you want the report based on.

Step 3: Select Report Options

Report period:

If Custom Report Period...

Start Date (Inclusive):

End Date (Inclusive):

Assume Initial States:

Assume State Retention:

Assume States During Program Downtime:

Include Soft States:

First Assumed Service State:

Backtracked Archives (To Scan For Initial States):

[Create Report](#)

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.

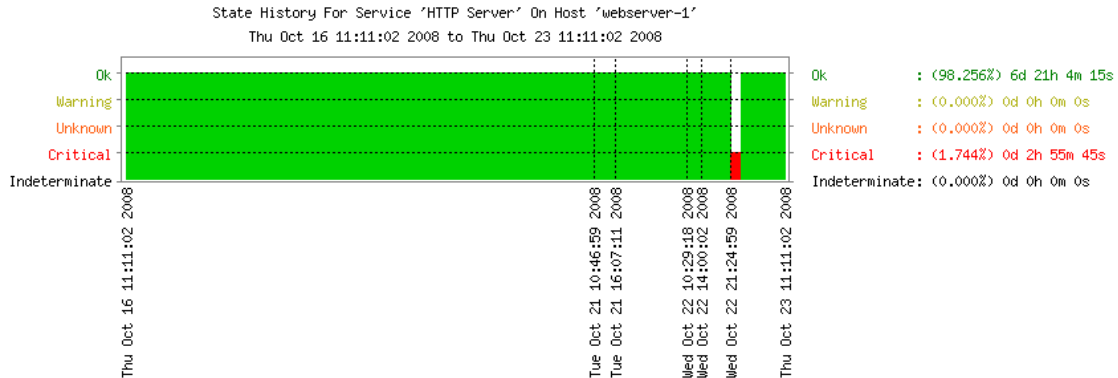
Include Soft States: A problem is classified as a SOFT problem until the number of checks has reached the configured max_check_attempts value. When max_check_attempts is reached the problem is reclassified as HARD and normally op5 Monitor will send out a notification about the problem. SOFT problem's 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.

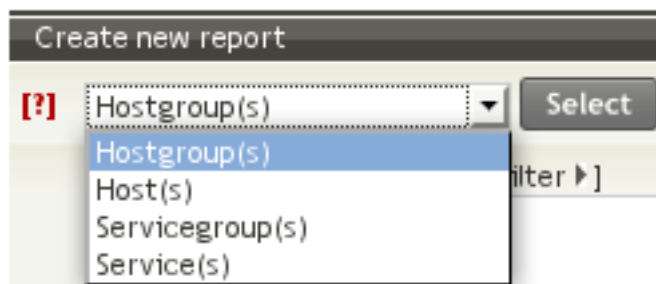


The graph that is created shows what state the host has been in over the selected report interval. You can zoom into the graph by clicking on it.

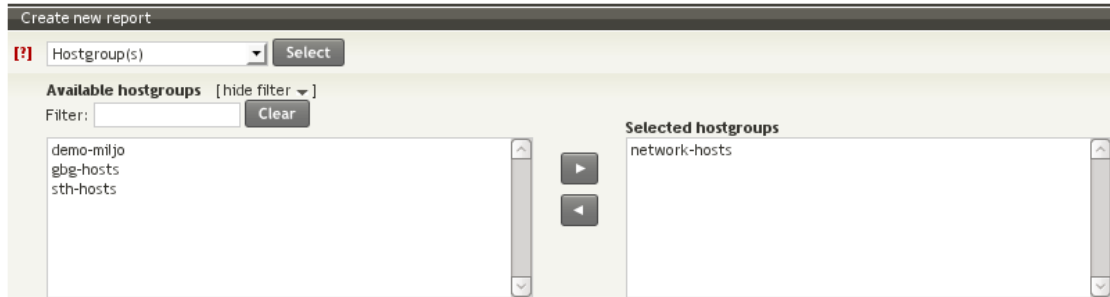
7.2 Availability

The availability report shows availability of hostgroups, service-groups, hosts or services during a selected report period.

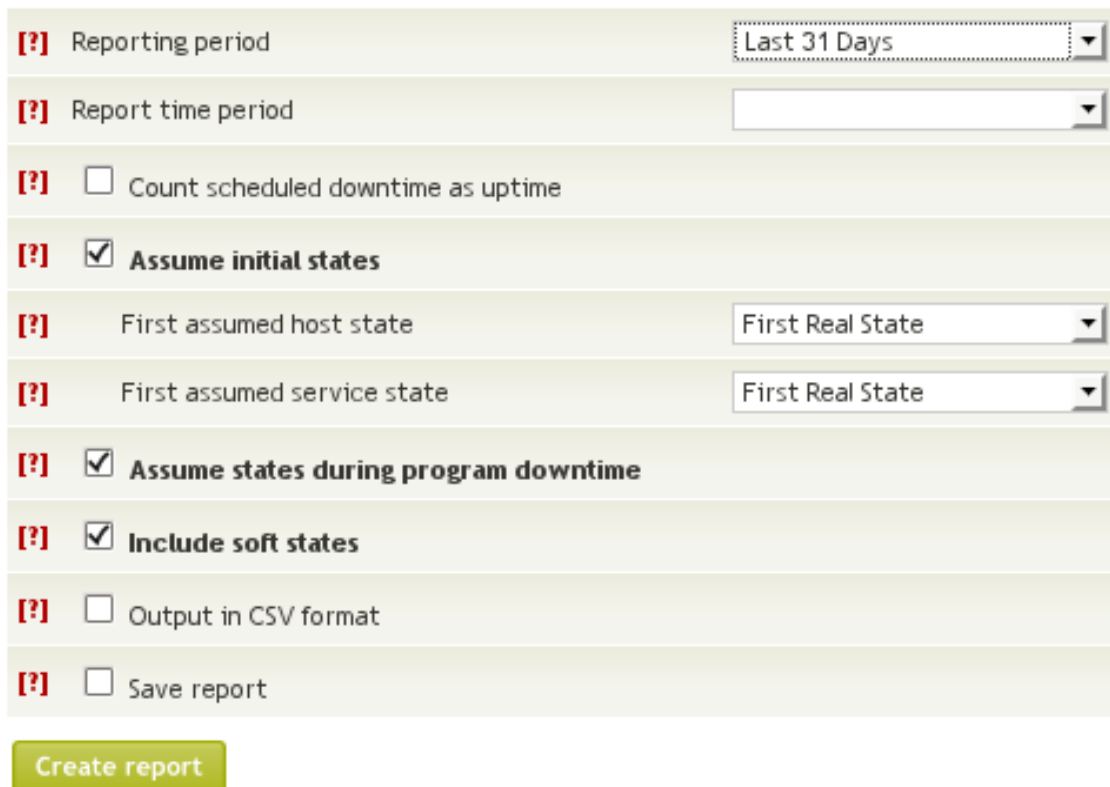
op5 Monitor comes with two different kinds of availability reports. The standard one that comes with Nagios and a new one with extended functionality and nicer presentation. As default the new availability report is used but you can always reach the old reports by clicking on the Old Availability link.



Select the preferred report type, Hostgroup(s), Host(s), Service-group(s) or Service(s).



Select the object / objects for which you want to produce your report.



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

Reporting 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 the report should be created for. The default blank selections means no filtering will be performed and the report will be created for *all* time within the selected Reporting Period. Tip: This can be used for SLA reporting.

Count scheduled downtime as uptime: Select if downtime that occurred during scheduled downtime should be counted as uptime or not.

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.

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 First Real 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 First Real State.

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.

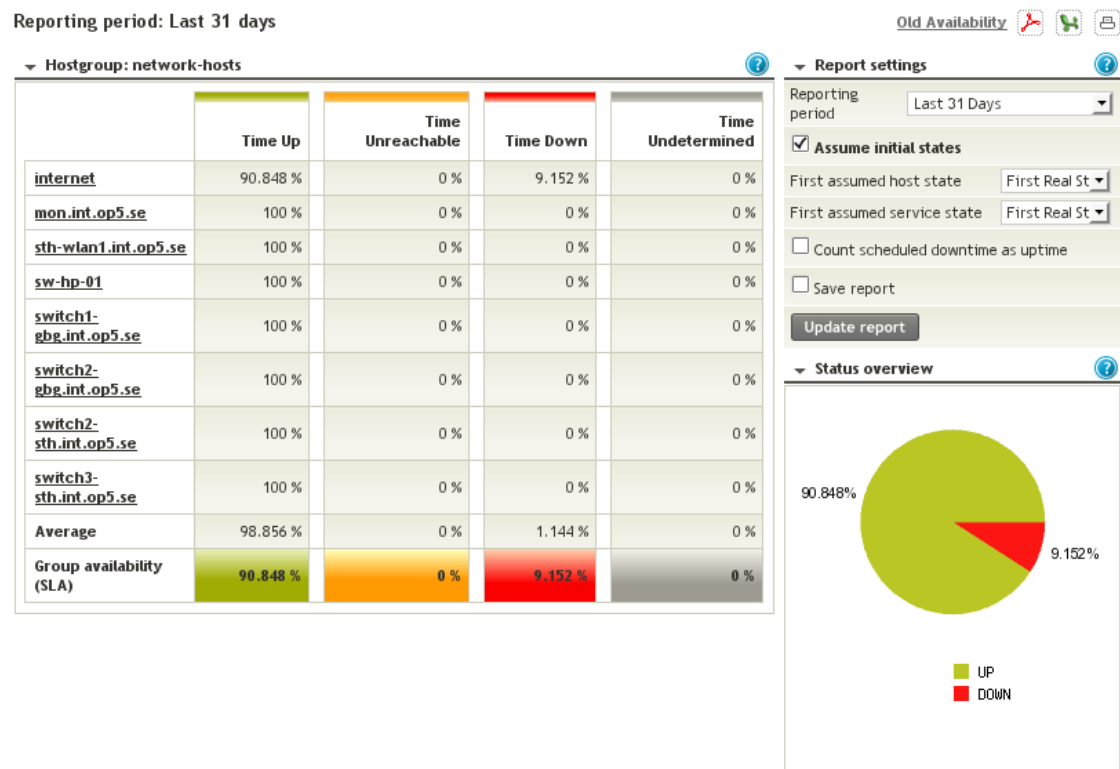
Include Soft States: A problem is classified as a SOFT problem until the number of checks has reached the configured `max_check_attempts` value. When `max_check_attempts` is reached the problem is reclassified as HARD and normally op5 Monitor will send out a notification about the problem. SOFT problems 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.

Output in CSV format: The CSV (comma-separated values) format is a file format that stores tabular data. This format is supported by many applications such as MS Excel, OpenOffice and Google Spreadsheets.

Save report: Checking this checkbox gives you the possibility to

save your report for later re-use. You will need to supply a name for your report if you select to save it. Tip: To be able to later schedule your report for automatic reoccurring e-mail delivery, you need to save the report.

Click on Create report to create the availability report



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

% Time Up: The amount of time the host has been in the state UP during the report period.

% Time Unreachable: The amount of time the host has been in the state UNREACHABLE during the report period.

% Time Down: The amount of time the host has been in the state DOWN 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 Monitors configuration during the whole report period.

There are two summary values in each report

Average: This is the average value for a group of hosts/services. It is calculated by adding the % Time for each host/service and then divide the total value with the amount of hosts/services in the group.

Group Availability (SLA): This value is only calculated for UP and PROBLEM states (for services OK and PROBLEM states). It displays the amount of time where all hosts/services in the group has been UP/OK or in a PROBLEM state at the same time.

Example:

If you have five hosts and one of the has been up in 80% of the chosen period, the rest of the 100%. Then the Average is 96%.

As you can see we only have all servers UP in 80% during the chosen period therefor we get 80% UP in the Group Availability (SLA).

Note: PROBLEM states includes all states except UP/OK.

7.3 Old Availability

The availability report shows availability of hostgroups, service-groups, 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):

network-hosts ▾

[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 31 Days ▾

If Custom Report Period...

Start Date (Inclusive):

October ▾ 1 2008

End Date (Inclusive):

October ▾ 23 2008

Report Time Period:

▾

Count scheduled downtime as uptime:

No ▾

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

[Create Availability Report!](#)

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 Availability Report” to create the availability report.

Hostgroup 'network-hosts' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
internet	90.716% (90.716%)	9.284% (9.284%)	0.000% (0.000%)	0.000%
mon.int.op5.se	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
sth-wlan1.int.op5.se	99.989% (99.989%)	0.011% (0.011%)	0.000% (0.000%)	0.000%
sw-hp-01	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
switch1-gbg.int.op5.se	99.995% (99.995%)	0.005% (0.005%)	0.000% (0.000%)	0.000%
switch2-gbg.int.op5.se	99.989% (99.989%)	0.011% (0.011%)	0.011% (0.011%)	0.000%
switch2-sth.int.op5.se	99.989% (99.989%)	0.011% (0.011%)	0.000% (0.000%)	0.000%
switch3-sth.int.op5.se	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average	98.835% (98.835%)	1.164% (1.164%)	0.001% (0.001%)	0.000%
Group Availability	90.691%	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. The values without parenthesis represent the part of the report period where op5 Monitor for certain can determine what state the host has been in. The values within parathesis is the part of the report period where op5 Monitor has assumed a certain state. In other words the value within parathesis includes the certain time plus parts of the undetermined time based on qualified guesses.

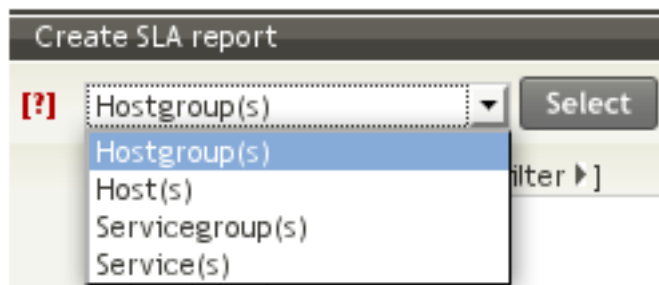
There are also two summary values for each hostgroup report.

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.

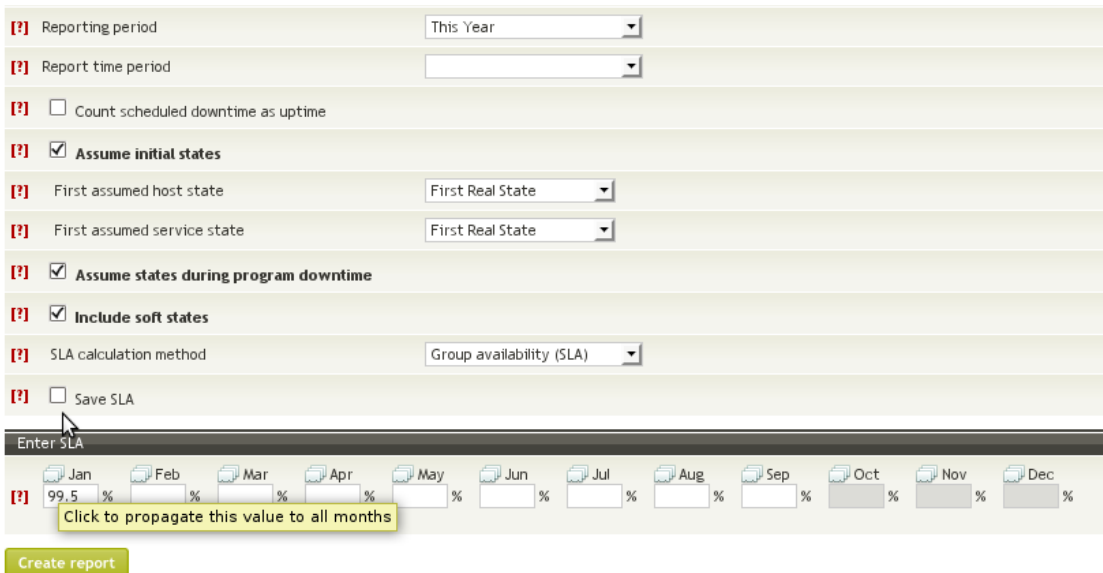
Group Average: This value is only calculated for UP/OK states. It displays the amount of time where all hosts in the group has been UP/OK at the same time.

7.4 SLA Reporting

SLA (Service Level Agreement) reporting is a report that visualizes if we met the agreed level of service, i.e. uptime, or not.



Start by selecting the preferred report type, Hostgroup, Host, Servicegroup or Service.



Now you have the ability to configure report settings

Reporting 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.

Count scheduled downtime as uptime: Select if downtime that occurred during scheduled downtime should be counted as uptime or not.

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.

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.

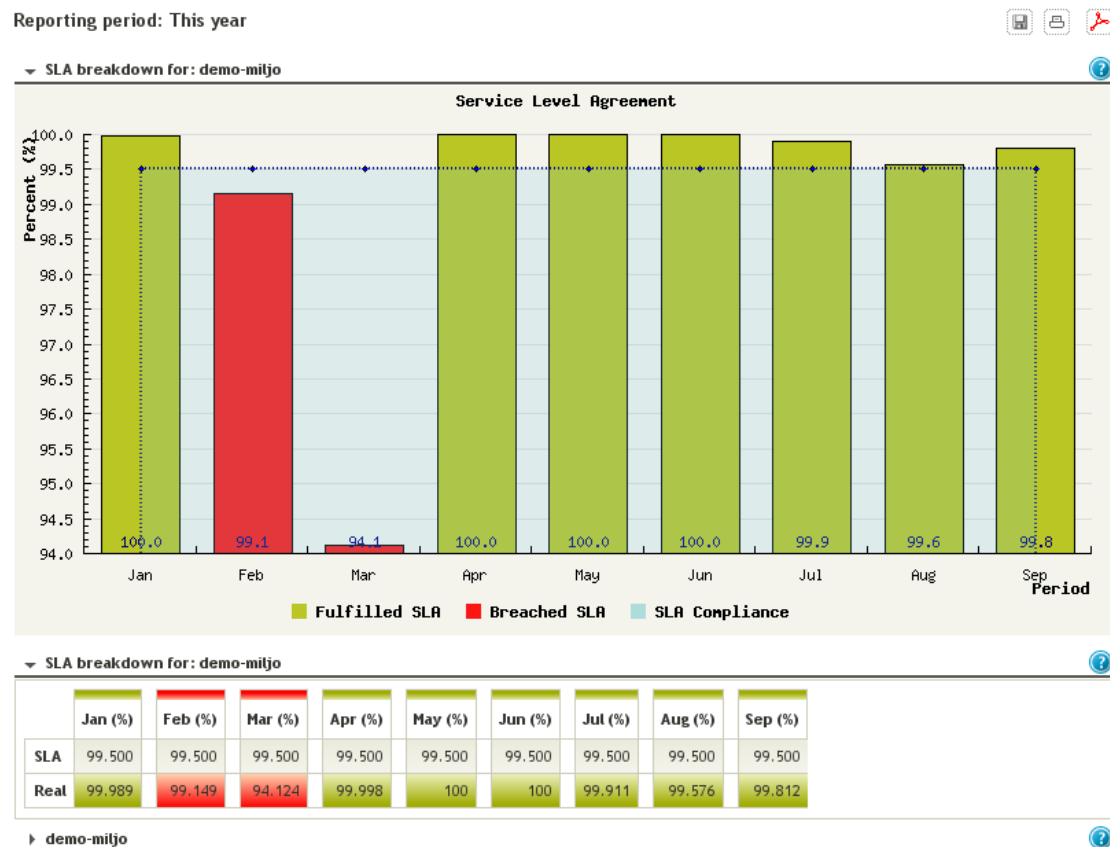
Assume States During Program Downtime: If op5 Monitor is not running for some time during a report period we can by this option decide to assume states for hosts and services during the downtime. Default value is YES.

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 problems 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.

Enter SLA: Here you specify the expected availability for each month.
Tip: If you enter a value for the first month and click outside the form you will get the option to autofill the other months as well.

If you want to use this report at later date you can click Save SLA and select a name for the report. Only saved reports can be scheduled for automatic e-mail delivery. You can however save the report after you have created it.

Click on Create report to create the SLA report



Once you have created the report you can save it, print it, view it as pdf and schedule it for automatic recurring e-mail delivery using the icons on the top right side.

7.5 Alert History

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

Log.

September 30, 2008
22:00

✓ [2008-09-30 22:56:21] SERVICE ALERT: sugar.op5.se;Process bacula-fd;OK;HARD;3;PROCS OK: 1 process with command name 'bacula-fd'
✓ [2008-09-30 22:55:17] SERVICE ALERT: sugar.op5.se;WebInject - SugarCRM;OK;HARD;3;WebInject OK - All tests passed successfully in 5.112 seconds
⚠ [2008-09-30 22:50:55] SERVICE ALERT: sugar.op5.se;WebInject - SugarCRM;WARNING;HARD;3;WebInject WARNING - All tests passed successfully but global timeout (25 seconds) has been reached

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.

7.6 Alert Summary

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

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

Standard Reports:Report Type: [Create Summary Report!](#)**Custom Report Options:**Report Type: Report Period:

If Custom Report Period...

Start Date (Inclusive): End Date (Inclusive): Limit To Hostgroup: Limit To Servicegroup: Limit To Host: Alert Types: State Types: Host States: Service States: Max List Items: [Create Summary Report!](#)

With the custom reports you can create a various amount of report types. This user-manual does not cover them all, but one very usefull is mentioned below.

7.6.1 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.

Displaying top 25 of 201 total matching alert producers

Rank	Producer Type	Host	Service	Total Alerts
#1	Service	mail.op5.se	System Load	53
#2	Service	sugar.op5.se	WebInject - SugarCRM	20
#3	Service	mon.int.op5.se	UPS - Time	19
#4	Service	rt.op5.com	Cron process	15
#5	Service	demo.op5.com	Disk usage /	15
#6	Service	env1-sth.int.op5.se	Temperature - Cooling unit	14
#7	Service	sugar.op5.se	Disk usage /	13
#8	Service	sugar.op5.se	Cron process	13
#9	Service	sugar.op5.se	Syslog process	13
#10	Service	sugar.op5.se	Zombie processes	11

7.7 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.

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.

7.8 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.

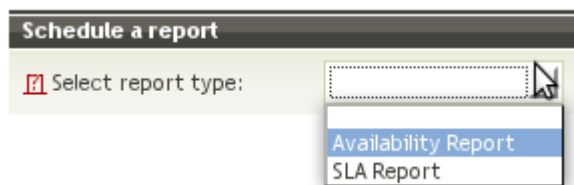
7.9 Schedule Reports

Schedule reports provides possibility to schedule automatic recurring e-mail delivery of the reports produced by **Availability** and **SLA Reporting**. The reports are sent out as pdf email attachments to one or several recipients. The reports can be sent out on a monthly or weekly basis.

To be able to schedule a report you first have to create and save it using **Availability** or **SLA Reporting**.

To configure a scheduled report do following

Select the preferred report type, Availability Report or SLA Report.



Select the saved report you want to schedule. A filename for the e-mail-attachment will be automatically suggested.

Select report	network-avail-report-test ▾
Select report interval	Weekly ▾
Select recipients	<input type="text"/>
Filename	network-avail-report-test_Weekly.pdf
Description	<input type="text"/>

Save

Now enter the email addresses of the recipients of the report. To enter multiple addresses, separate them by commas. If you want to you can also add a description to this schedule. This may be any information that could be of interest when editing the schedule and the report at a later time. The description-field is optional.

Chapter 8

Configuration Web Menu


8.0.1 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.

Select Type of Config Data You Wish To View

Object Type:

Hosts 



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

8.1 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.

Note that changing the password will log you out.

Enter your current password

Current password:

Enter your new password

New password:

Retype password:

8.2 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.

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

8.2.1 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.

Creating tarball from the Monitor home directory.

This will take a few seconds. Please be patient.

Backup file **[monitor_backup.081022.08.31.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](#).

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

8.2.2 Restore a backup

To restore a backup simply click on the “restore an older configuration” link and select one of the available backups. The numbers of the files is formatted like this:

yymmdd.hh.mm

- [monitor_backup.081022.08.31.tar.gz](#)
- [monitor_backup.081014.06.05.tar.gz](#)
- [monitor_backup.081010.10.05.tar.gz](#)
- [monitor_backup.080914.03.45.tar.gz](#)

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 lose 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.

8.3 Configure

There are two ways to configure op5 Monitor. One is to edit the text files 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 tell the server about any changes you’ve made on the current page, you should click the Apply button at the bottom of each page when you are done with your changes.

To then save the configuration to disk, click the button “Save”. This will result in an export of the new configuration to the text files, after which op5 Monitor reloads the new configuration.



This is the op5 Monitor Configuration tool. This is the place where you add new hosts, change notification settings and more. Basically almost everything configuration related is managed from this tool.

To get started, select the preferred action in the menu below.

→ **New hosts**

→ **Host**

Filter by regular expression:

Clear

monitor ▼

Go

→ **Templates**

→ **Host Groups**

→ **Service Groups**

→ **Contacts**

→ **Contact Groups**

→ **Commands**

→ **Profiles**

→ **Time Periods**

→ **Access Rights**

Tip: If you need help you can always click on the "HELP" link in the upper right corner, you can also click on the **[?]** for each configurable variable.

Note: Be careful when using Configure since it does not yet have multi user support.

The main menu consists of four menu selections:

1. Configure: returns to the configure start page listed above
2. Save Configuration: Verifies the configuration made, saves the configuration and reloads the monitor process with the new configuration
3. Undo Changes: If you haven't clicked 'Save Configuration' the 'Undo Changes' link takes you back to the configuration you had before doing changes
4. Configuration Help: Help window

8.3.1 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.

In most of the listings you will find a small textfield called “Filter by regular expression:”. Use this to filter out the content you are interested in when viewing the different lists.

8.3.2 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.

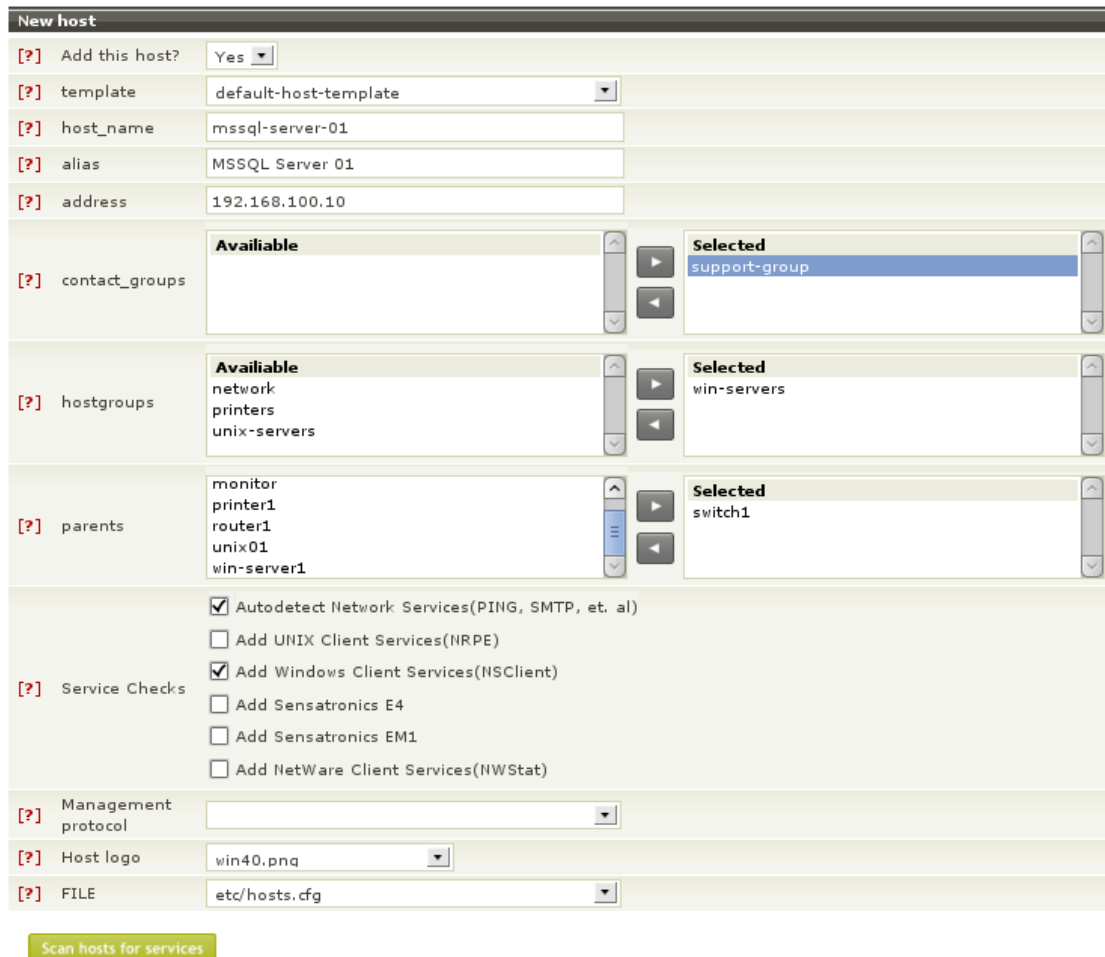
To add several hosts at a time you have two options.

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 use the profile funktion wich is described in [B Profiles and Cloning](#) on page [104](#).

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
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.



New host

[?] Add this host? Yes ▾

[?] template default-host-template ▾

[?] host_name mssql-server-01

[?] alias MSSQL Server 01

[?] address 192.168.100.10

[?] contact_groups

Available: (empty list)

Selected: support-group

[?] hostgroups

Available: network, printers, unix-servers

Selected: win-servers

[?] parents

Available: monitor, printer1, router1, unix01, win-server1

Selected: switch1

[?] Service Checks

☒ Autodetect Network Services(PING, SMTP, et. al)

☐ Add UNIX Client Services(NRPE)

☒ Add Windows Client Services(NSClient)

☐ Add Sensatronics E4

☐ Add Sensatronics EM1

☐ Add NetWare Client Services(NWStat)

[?] Management protocol ▾

[?] Host logo win40.png ▾

[?] FILE etc/hosts.cfg ▾

Scan hosts for services

Here is an explanation of each variable.

Add this host?: If you are adding several hosts at a time, for ex-

ample 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.

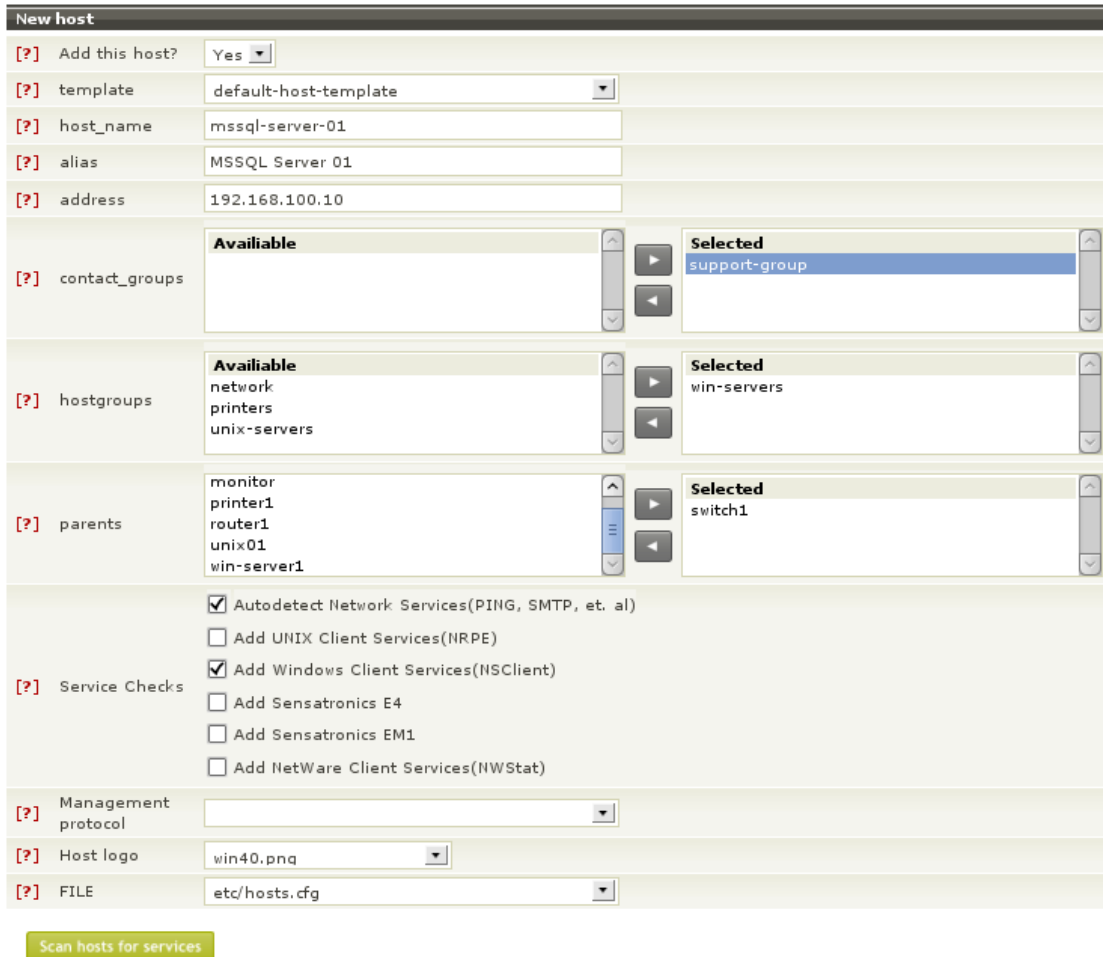
Management Protocol: Choose the management protocol used to configure the host. E.g. telnet for routers and HTTP for switches. This will result in a URL, with the specified management protocol, next to the host in Host Detail. Example: telnet://router1/

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	
[?] Add this host?	Yes ▾
[?] template	default-host-template ▾
[?] host_name	mssql-server-01
[?] alias	MSSQL Server 01
[?] address	192.168.100.10
[?] contact_groups	<div>Available</div> <div>Selected: support-group</div>
[?] hostgroups	<div>Available: network, printers, unix-servers</div> <div>Selected: win-servers</div>
[?] parents	<div>monitor, printer1, router1, unix01, win-server1</div> <div>Selected: switch1</div>
[?] Service Checks	<input checked="" type="checkbox"/> Autodetect Network Services(PING, SMTP, et. al) <input type="checkbox"/> Add UNIX Client Services(NRPE) <input checked="" type="checkbox"/> Add Windows Client Services(NSClient) <input type="checkbox"/> Add Sensatronics E4 <input type="checkbox"/> Add Sensatronics EM1 <input type="checkbox"/> Add NetWare Client Services(HWStat)
[?] Management protocol	▾
[?] Host logo	win40.png ▾
[?] FILE	etc/hosts.cfg ▾
<div>Scan hosts for services</div>	

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.

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

Initial Service Settings lets you change the `service_template` supposed to be used for the services added when you add the initial services.

Initial service settings	
[?] template	default-service
[?] FILE	etc/services.cfq

The result of the scan is 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 web-site.

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

unix01 @ 10.10.10.2 (First Unix Host)
<input type="checkbox"/> Select All
NET
<input checked="" type="checkbox"/> PING
<input type="checkbox"/> FTP
<input type="checkbox"/> SSH Server
<input type="checkbox"/> SMTP
<input type="checkbox"/> Nameserver
<input type="checkbox"/> HTTP Server
NRPE
<input type="checkbox"/> Current users
<input type="checkbox"/> System Load
<input type="checkbox"/> Disk usage /
<input type="checkbox"/> Disk usage /var

Added 1 host.

Added 7 services.

unix01 Services for unix01

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.

8.3.3 Hosts

To change the configuration of an existing host select the host in the dropdown menu and click go. If you have a long list of hosts you may use the “Filter by regular expression” to easier find the host you are interested in.

→ **Host**

Filter by regular expression:

Clear

linux-server1 ▼

Go

→ **Templates**

Host Selector

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

Filter by regular expression:

linux-server1

* Need help?
 * Services for host **linux-server1**

host

RELATED ITEMS

- * Scan host for network services
- * Scan host for SNMP interfaces
- * Services for host **linux-server1**
- * Host Templates
- * Check Commands
- * Contact Groups
- * Time Periods
- * Add new host

linux-server1		dependencies	escalations	extras	done	advanced	delete
[?] template	default-host-template						
[?] host_name	linux-server1						
[?] alias	linux Server 1						
[?] address	127.0.0.1						
[?] hostgroups	Available network printers win-servers			Selected unix-servers			
[?] parents	Available monitor printer1 router1 unix01			Selected switch1			
[?] contact_groups	Available			Selected support-group			

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.

If you want to choose from a less extensive list of hosts, you can select what hosts to include using the Filter by regular expression field.

Related Items

1. Scan host for generic network based services which simply does the same scan that you do when adding new hosts.
2. 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.

Host Object Box

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 six links:

- dependencies
- escalations
- extras
- clone
- advanced
- delete

8.3.4 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	monitor
[?] dependency_period	
[?] execution_failure_criteria	<input type="checkbox"/> Down <input type="checkbox"/> Unreachable <input type="checkbox"/> OK
[?] notification_failure_criteria	<input checked="" type="checkbox"/> Down <input checked="" type="checkbox"/> Unreachable <input type="checkbox"/> OK
[?] inherits_parent	Yes
[?] FILE	etc/hostdependencies.cfg

Apply changes

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.

8.3.5 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 Host Escalation for host linux-server1

[?] contacts	<div>Available</div> <div>monitor</div>	<div>Selected</div>
[?] contact_groups	<div>Available</div> <div>support-group</div>	<div>Selected</div>
[?] first_notification		
[?] last_notification		
[?] notification_interval		
[?] escalation_period		
[?] escalation_options	<input checked="" type="checkbox"/> Down <input type="checkbox"/> Unreachable <input type="checkbox"/> Recovery	
[?] FILE	etc/hostescalations.cfq	

Apply changes

contacts: which contact should receive the notification. Normally you use contact_groups but sometimes it is needed to only add a single contact.

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.

Note: When you start using escalations no notifications will be sent to the contacts and contact_groups set on the service.

8.3.6 Extras

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

Extended info for host linux-server1		delete
[?] icon_image	redhat.png	
[?] icon_image_alt	Linux Server	
[?] statusmap_image	redhat.png	
[?] notes		
[?] action_url	http://\$HOSTADDRESS\$	
[?] notes_url		
[?] 2d_coords		

Apply changes

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.

8.3.7 Clone

Using the Clone button you can create a profile based on the host you are configuring.

This profile can later be used to create new hosts.

For more information, read [B Profiles and Cloning](#) on page [104](#).

8.3.8 Parent/Child

When op5 Monitor realize that a child host is down it will test if the parent host is down. If the parent host is down op5 Monitor will set the childhost to unreachable state. The notifications sent out later on will be:

- Parent host: down
- Child host: unreachable

To avoid notifications about unreachable hosts you should change either the contact, host or host template.

Contact:

Make sure unreachable is unchecked in `host_notification_options`

Host / Host template:

Make sure unreachable is unchecked in `notification_options`

8.3.9 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.



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.

display_name: This option will define a alternative name that will be displayed in the web interface.

Note: This option is not used by the CGIs at the moment but it will be used in later versions of the web interface.

address: The IP address or host name of the host.

initial_state: By default op5 Monitor will assume that all hosts are in UP states when in starts. You can override the initial state for an object by using this directive.

Note: This has no effect if state retention is enabled, which is the default on op5 installations.

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.

If `switch1` is DOWN then `serverA` will be UNREACHABLE.

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

contacts: The contact(s) this hosts notifications are sent to.

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.

check_interval: The interval, in minutes, between checks of this host.

retry_interval: The amount of checks required for the service to enter HARD state and send notifications.

check_period: During which time period this host should be checked.

obsess_over_host: This directive tells whether or not to obsess for commands run for this host. Obsessing in this case means, run a command after each host check. The command that is defined as a normal “command” and is then added in /opt/monitor/etc/nagios.cfg.

check_freshness: Here you can configure the freshness threshold for passive checks in seconds. If you set this to 0, op5 Monitor will automatically determine the threshold.

active_checks_enabled : if checks are enabled or not, normally yes.

passive_checks_enabled: Passive checks enabled, default is 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: see below note about flap detection

high_flap_threshold: see 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.

flap_detection_options: This directive is used to determine what host states the flap detection logic will use for this object.

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.

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.

The options below is also found in the Extras section.

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.

8.3.10 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.

Filter by regular expression:
Clear

Go

Filter by regular expression:
Clear

Add new service
Go

Need help?

CONFIGURE
SAVE
UNDO
HELP

service
▼

RELATED ITEMS

- ✦ Scan host for network services
- ✦ Scan host for SNMP interfaces
- ✦ Host configuration: **linux-server1**
- ✦ Service Templates
- ✦ Check Commands
- ✦ Contact Groups
- ✦ Time Periods
- ✦ Service Groups

New service on host "linux-server1"

[?] template
default-service ▼

[?] service_description

[?] check_command

Filter by regular expression:
Clear

Syntax help
Edit check command

[?] check_command_args

[?] contacts

Available

monitor

▲
▶
◀
▼

Selected

▲
▶
◀
▼

[?] contact_groups

Available

support-group

▲
▶
◀
▼

Selected

▲
▶
◀
▼

[?] FILE
etc/services.cfq ▼

Test this service

The page is modeled almost the same way as the host configuration page with other options.

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.

When you have selected host you will have a drop down list where you can see the existing services for this host. There will also be an option called "Add new service" which you should chose to create a new service.

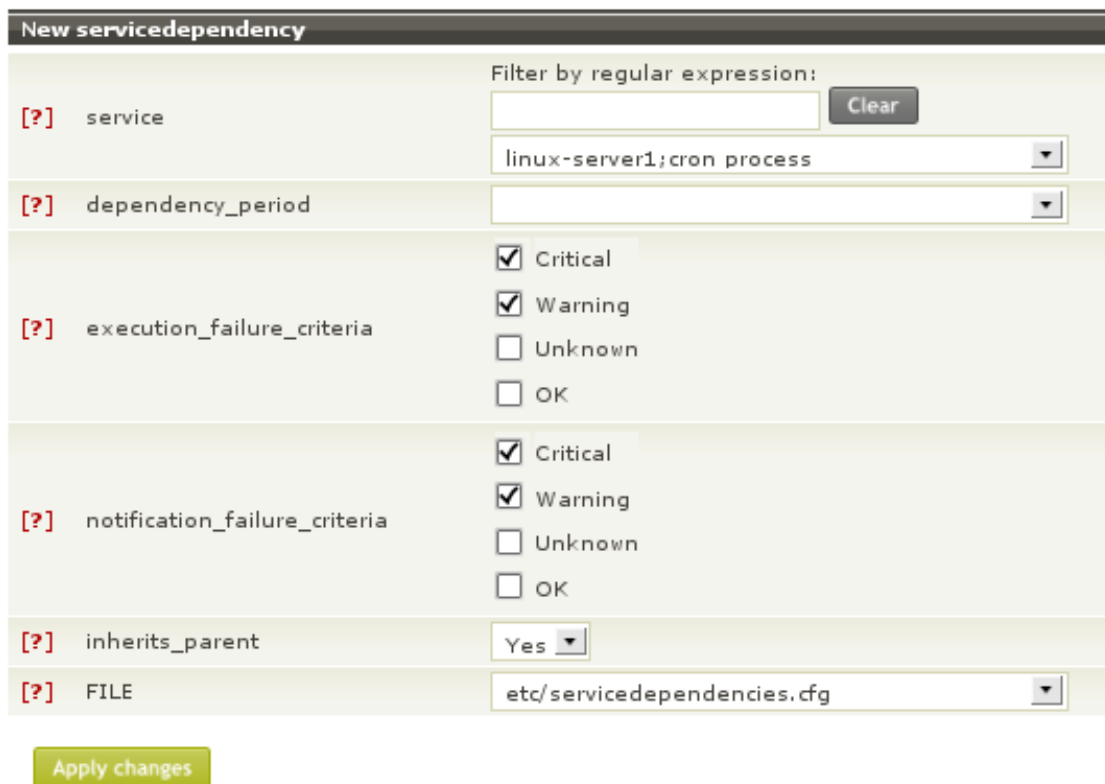
To edit a existing service simply edit the fields for that service and press the <Enter> key or scroll down to the bottom of the page and press Apply Changes.

At the bottom of the page you also have a button called “Test this service”. If you click on that button op5 Monitor execute a test so you may see if your service works as it is supposed to.

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

8.3.11 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	Filter by regular expression: <input type="text"/> <input type="button" value="Clear"/> linux-server1;cron process
[?] dependency_period	
[?] execution_failure_criteria	<input checked="" type="checkbox"/> Critical <input checked="" type="checkbox"/> Warning <input type="checkbox"/> Unknown <input type="checkbox"/> OK
[?] notification_failure_criteria	<input checked="" type="checkbox"/> Critical <input checked="" type="checkbox"/> Warning <input type="checkbox"/> Unknown <input type="checkbox"/> OK
[?] inherits_parent	Yes
[?] FILE	etc/servicedependencies.cfg
<input type="button" value="Apply changes"/>	

service: This defines the service that we are depending on.

dependency_period: This defines under what time periods this dependency will be used.

execution_failure_criteria: If the dependent service defined in ‘ser-

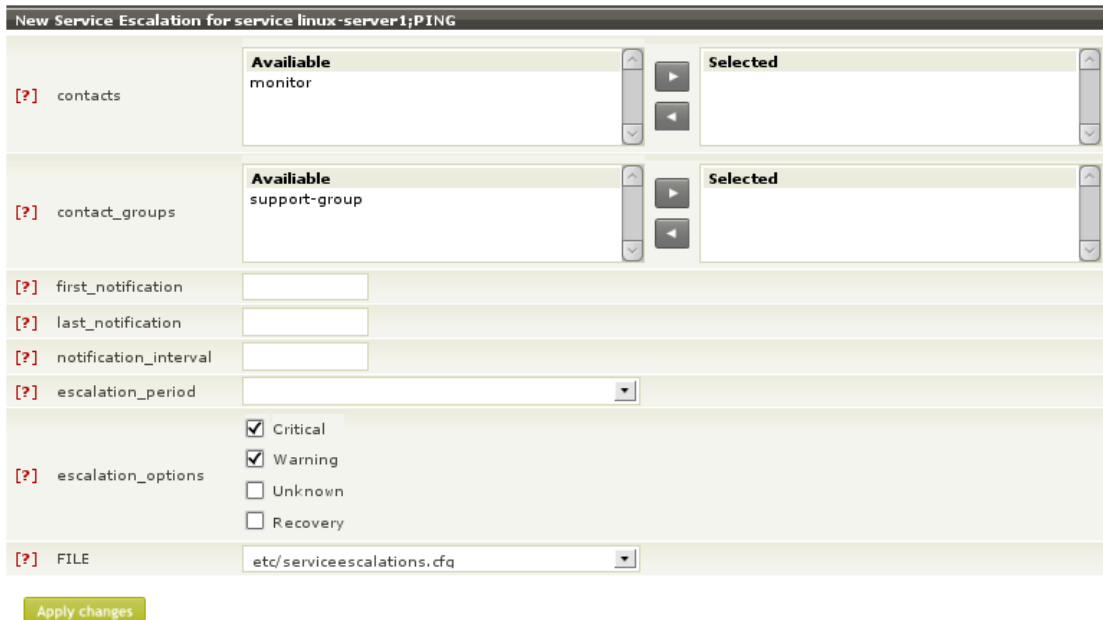
vice' is in one of the selected states this services status will not be checked.

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.

8.3.12 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 Service Escalation for service linux-server1;PING

[?] contacts	Available monitor	Selected
[?] contact_groups	Available support-group	Selected
[?] first_notification		
[?] last_notification		
[?] notification_interval		
[?] escalation_period		
[?] escalation_options	<input checked="" type="checkbox"/> Critical <input checked="" type="checkbox"/> Warning <input type="checkbox"/> Unknown <input type="checkbox"/> Recovery	
[?] FILE	etc/serviceescalations.cf	

Apply changes

contacts: which contact(s) should receive the notification.

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.

Note: When you start using escalations no notifications will be sent to the contacts and contact_groups set on the service.

8.3.13 Extras

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

New Extended Serviceinfo Configuration for service 'PING' on host 'linux-server1'	
[?] notes	<input type="text"/>
[?] notes_url	<input type="text"/>
[?] action_url	<input type="text"/>
[?] icon_image	<input type="text"/>
[?] icon_image_alt	<input type="text"/>
[?] FILE	<input type="text" value="etc/serviceextinfo.cfg"/>

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.

8.3.14 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.

Note: If you change any options to a value other than the one defined in the template in use this option will not be changed on the service if it is changed in the template.

linux-server1;PING		depend
[?] template	default-service	
[?] service_description	PING	
[?] display_name		
[?] is_volatile	No	
Filter by regular expression:		
[?] check_command	check_ping	Clear
[?] check_command_args	100.0,20%!500.0,60%	
[?] servicegroups	None configured (multiple selection possible)	
[?] initial_state	<input type="radio"/> Critical <input type="radio"/> Warning <input type="radio"/> Unknown <input checked="" type="radio"/> OK	
[?] max_check_attempts	3	
[?] check_interval	5	
[?] retry_interval	1	
[?] active_checks_enabled	Yes	
[?] passive_checks_enabled	Yes	
[?] check_period	24x7	
[?] parallelize_check	Yes	

template: Which template to use for this service.

service_description: The description of the Service.

display_name: This option will define a alternative name that will be displayed in the web interface.

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.

initial_state: By default op5 Monitor will assume that all services are in OK states when in starts. You can override the initial state for an object by using this directive.

Note: This has no effect if state retention is enabled, which is the default on op5 installations.

max_check_attempts: The amount of checks required for the service to enter HARD state and send notifications.

check_interval: The interval, in minutes, between checks of the service.

retry_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: see below note about flap detection.

high_flap_threshold: see 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.

flap_detection_options: This directive is used to determine what service states the flap detection logic will use for this object.

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.

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 lose 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.

first_notification_delay: This defines how long, in minutes, op5 Monitor should wait before it sends out the first notification. Default is 0. For services you have the choice to delay the first notification, this can be useful if you don't want to be notified for problems that only last a short time

notification_period: During which period notifications for this ser-

vice 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.

contacts: The contact(s) this service notifications is sent to.

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.

The options below is also found in the Extras section.

FILE: Which file this host object should be saved in.

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.

8.3.15 Templates

There are three kinds of templates available.

1. Host Templates for hosts objects.
2. Service Templates for service objects.
3. 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

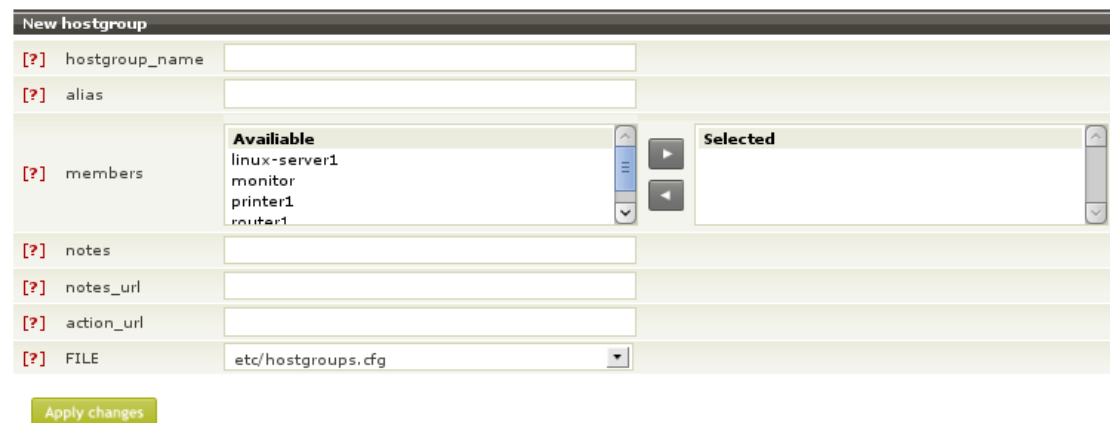
unnecessary work you can simply define your most common settings in templates and then use those templates when configuring the objects.

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.

8.3.16 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.



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.

notes: notes for the host_group.

notes_url: The documentation URL for this host_group.

action_url: The url used to manage the host_group.

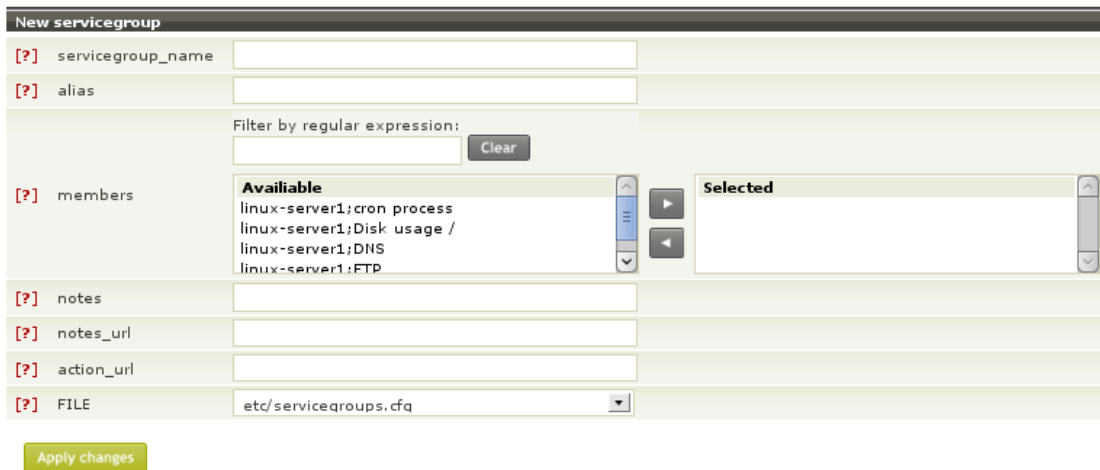
Click 'Apply changes' in the bottom of the window. Click 'Save Configuration' for the changes to take effect.

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

8.3.17 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.



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

notes: notes for the service_group.

notes_url: The documentation URL for this service_group.

action_url: The url used to manage the 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.

8.3.18 Contacts

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

New contact	
[?] template	<input type="text"/>
[?] contact_name	<input type="text"/>
[?] alias	<input type="text"/>
[?] host_notification_period	24x7
[?] service_notification_period	24x7
[?] host_notification_options	<input checked="" type="checkbox"/> Down <input type="checkbox"/> Unreachable <input checked="" type="checkbox"/> Recovery <input type="checkbox"/> Flapping start and stop
[?] service_notification_options	<input checked="" type="checkbox"/> Critical <input checked="" type="checkbox"/> Warning <input type="checkbox"/> Unknown <input checked="" type="checkbox"/> Recovery <input type="checkbox"/> Flapping start and stop
[?] host_notification_commands	host-notify
[?] host_notification_commands_args	<input type="text"/>
[?] service notification commands	service-notifv

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

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.

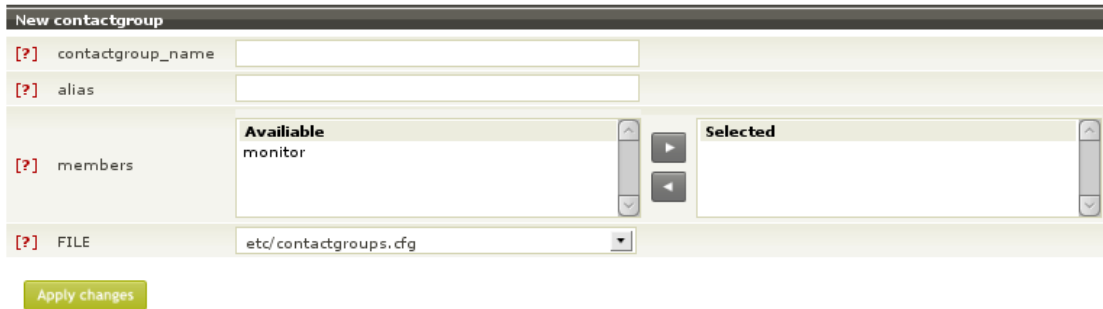
address1 - 6: These variables are reserved for other kind of notification options. If you create your own notification script you can use these variables to specify notification data.

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.

8.3.19 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 name: Name of the contactgroup.

alias: Description of the contact group.

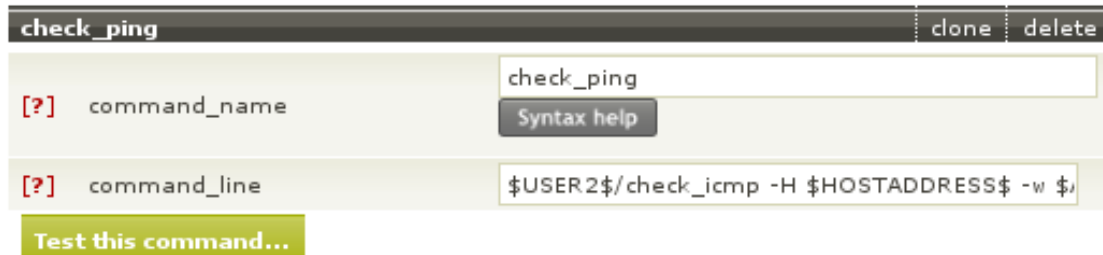
members: Hosts that are members of this host group, to select several hosts press and hold the <Ctrl> key.

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

8.3.20 Commands

A command is an object that defines who op5 monitor executes scripts and binaries such as plugins etc. Commands are a very vital part of op5 Monitor. Commands are used to do the actual monitoring, send notifications, execute event_handlers, external scripts such as eventhandler scripts and so on.

The command consists of following parts.



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 command 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 command is run for.

A full list of available macros is available from the Nagios manual at <http://nagios.sourceforge.net/docs/3.0/macros.html>

8.3.21 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.

You can also:

- use already defined time periods as excludes
- add exceptions based on dates and ranges of days

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.

Filter by regular expression:

[Need help?](#)

nonworkhours		clone	delete
[?] timeperiod_name	<input type="text" value="nonworkhours"/>		
[?] alias	<input type="text" value="Non-Work Hours"/>		
[?] exclude	Available 24x7 none workhours	<input type="button" value="▶"/> <input type="button" value="◀"/>	Selected
[?] sunday	<input type="text" value="00:00-24:00"/>		
[?] monday	<input type="text" value="00:00-08:00,17:00-24:00"/>		
[?] tuesday	<input type="text" value="00:00-08:00,17:00-24:00"/>		
[?] wednesday	<input type="text" value="00:00-08:00,17:00-24:00"/>		
[?] thursday	<input type="text" value="00:00-08:00,17:00-24:00"/>		
[?] friday	<input type="text" value="00:00-08:00,17:00-24:00"/>		
[?] saturday	<input type="text" value="00:00-24:00"/>		
[?] Exception type	<input checked="" type="radio"/> Date <input type="radio"/> Day		
[?] Interval	<input checked="" type="radio"/> Single date <input type="radio"/> Date range		
[?] Date	<input type="text" value="Every year"/> <input type="text" value="Every month"/> <input type="text" value="Every day"/>		
[?] Hours	<input type="text" value="00:00-24:00"/>		
[?]	<input type="button" value="Add"/>		
[?] Added exceptions	<input type="text"/> <input type="button" value="Remove"/> <input type="button" value="Edit"/>		

timeperiod name: short name of the time period

alias: descriptive name of the time period

exclude: Other timeperiod definitions that should be excluded from this timeperiod.

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

Exception type: Specify what type of exception you want to use; Date or Day

Depending on what kind of exception type you have chosen you will

get different settings choices. The two lists below describes them all.

Date

Interval: Chose Single date or Date range

Date: Choose the date that is supposed to be used in this Exception.

From date: If you chose date range you will here set the start date

To date: If you chose date range you will here set the end date

Frequency: How often the exception is repeated. Valid values are positive integers greater than one. E.g:

Date range "2008-01-01 - 2008-12-31 / 5" means every fifth day of 2008.

Day range "1 monday march - 3 sunday may / 3" means every third day between the first monday and the third sunday every month.

Date range "2008-06-01 / 14" means every 14th day from first of june 2008. Note that this exception has no end.

Hours: which time to include for this exception. You can define multiple times by separating them with comma. Example:

00:00-01:00,03:00-06:00

Day

Interval: Chose Single day or a Day range

Weekday: Choose the weekday that is supposed to be used in this Exception.

From weekday: If you chose Day range you will here set the start day

To weekday: If you chose Day range you will here set the end day

Frequency: How often the exception is repeated. Valid values are positive integers greater than one.

E.g:

Date range "2008-01-01 - 2008-12-31 / 5" means every fifth day of 2008.

Day range "1 monday march - 3 sunday may / 3" means every third day between the first monday and the third sunday every month.

Date range "2008-06-01 / 14" means every 14th day from first of june 2008. Note that this exception has no end.

Hours: which time to include for this exception. You can define multiple times by separating them with comma. Example: 00:00-01:00,03:00-06:00

Click on the Add button to add your exception.

Added exceptions: Shows a list of the exceptions added to this time period.

8.3.22 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	<input type="password"/>	
Verify password	<input type="password"/>	
authorized_for_system_information	<input checked="" type="checkbox"/>	
authorized_for_configuration_information	<input checked="" type="checkbox"/>	
authorized_for_system_commands	<input checked="" type="checkbox"/>	
authorized_for_all_services	<input checked="" type="checkbox"/>	
authorized_for_all_hosts	<input checked="" type="checkbox"/>	
authorized_for_all_service_commands	<input checked="" type="checkbox"/>	
authorized_for_all_host_commands	<input checked="" type="checkbox"/>	

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.

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, see Customizing views below for more information.

authorized for all hosts: Gives the user access to view all hosts, see Customizing views below for more information.

authorized for all service commands: Gives the user access to issue commands for all services, see Customizing views below for more information.

authorized for all host commands: Gives the user access to issue commands for all hosts, see 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.

8.3.23 Assign Group Rights

LDAP and Active Directory only.

If you are using LDAP based authentication you will be able to assign rights per entire group of users.

Tick the box for the different types of rights available. See **Access Rights** above for a descriptive list.

When you have added the rights you want to use, they will take effect when you press Apply.

Take good care to not accidentally lock yourself out.

8.3.24 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.

SNMP Community:	<input type="text" value="public"/>
Host template to use for exported hosts:	<input type="text" value="Unix NRPE"/>
op5 Monitor host identifier to use for Statistics 'Host Description' field:	<input type="text" value="host name"/>

Hostgroups to export	
Available network printers win-servers	Selected unix-servers

Hosts to export	
Available linux-server1 / linux Server1 monitor / OP5 Monitor Server printer1 / Printer 1 router1 / Router 1	Selected

Export hosts

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.

Appendix A

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 four 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.php` and `frame_menu.php` 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 fourth step is optional and only for advanced users.

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

Appendix B

Profiles and Cloning

B.1 Overview

Profiles and Cloning was a feature new to Monitor 3.2.x. It is a feature aimed at solving the task of configuring many similar servers without having to repeat many steps.

A profile is essentially a stored copy of a host. The profile can then be used when creating new hosts, creating an initial setup with services.

The profile will include services from the original host – when you create the profile you are presented with a choice of which services to include.

B.2 Profiles

B.2.1 Creating a Profile

- Choose the Configure web menu
- Choose Go for the host you wish to copy
- Click the Clone button
- Select the services you wish to include
- Select Save as Profile
- Enter name and description for the profile you are creating
- Click Clone

You are then presented with the option of creating clones based on this new profile. If you do not wish to do this now, you can simply use the left hand web menu to return to Configure or another part of op5 Monitor.

B.2.2 Use from a Profile

- Choose the Configure web menu
- Click Profiles
- Click use next to the profile
- Select what parts of the profile you want to include
- Fill in the number of copies and click Continue...
- Fill out host details for the clones and click Create

B.3 Cloning

B.3.1 Cloning from an Existing Host

Follow the instructions from [B.2.1](#) Creating a Profile above, except do not click Save as Profile.

B.3.2 Cloning services

The services are a bit special when it comes to cloning in op5 Monitor. When you clone a service you will copy it to an other host instead of creating a new service.

To clone a service to an other host follow the list below:

- Choose the Configure web menu.
- Choose Go for the host you wish to copy.
- Click Services for host... in the “RELATED ITEMS” menu.
- Select the service you want to clone to other hosts click on Go and then on Clone.
- Select the hosts or host_groups you want to clone the service to and click on Clone.
- Now the service has been cloned to the hosts you selected. Click on Save to export to the configurations files.

Appendix C

Basic Work Flows around Monitor

The need for an IT department to follow up on user questions is quite obvious and most organisations use some sort of trouble ticket system for this.

The need to administer faults and preventive maintenance, however, is often forgotten about and that work is then performed as a part of general server and network maintenance.

Anybody who has worked using a trouble ticket system will recognize how it makes it easy to make sure that the work gets done even if someone is on holiday, and how it makes it easier to keep track of how time is spent.

In theory, an op5 Monitor notification equals a problem and could generate a trouble ticket. It is not always that easy though, so we will present an example scenario to illustrate how you can integrate op5 Monitor in your organisation.

C.1 Getting the Contacts Right

If the notifications are annoying, they will be ignored. This is a very important rule of thumb - enabling notifications is better done slowly.

Most Monitor users have both email and mobile phone text messages for notifications. Typically, you should only send messages to mobile phones out of work hours, and only for the most important services and hosts. To throughout the workday receive text messages perhaps because of planned work does not tend to go down well.

You can also start off only sending critical notifications and host down messages via email, until you've seen that this works well and people know how to deal with the messages they receive.

C.2 Tuning Alerts

It is very important to not have “false” alerts – meaning alerts that the administrators do not think of as faults.

For instance - a ping response time of 100ms is unacceptable if it is in the same switch, but on a WAN link it might be normal.

It is very important that anything red or orange on your op5 Monitor – perhaps you have your op5 Monitor on a wall mounted TV – should be trustworthy as an important issue to deal with. Therefore, one of the highest priorities for having a successful network monitoring is adjusting the levels so that the normal state of things is that everything is green.

C.3 Updating Monitor

When you have a new installation of Monitor, it should be up to date with regards to your servers and network structure.

A common mistake is to forgetting to update as new servers are added or changes are made.

To prevent your system from degrading over time, you should not only have at least one person with the dedicated responsibility of making sure op5 Monitor is up to date – but also it needs to part of the protocol for anyone installing servers to configure it in Monitor

aswell. The web interface makes it easy for everyone in your IT department to manage their own servers and other devices.

C.4 Handling Alerts

It is essential that all notifications are dealt with. **If you have a false alarm it still needs action – the action is to change the service settings.**

If you have a trouble ticket system already, alerts can be registered in this. op5 can offer integrations to make this automatic with some trouble ticket systems – ask us if you want to know about your possibilities. Automatically having a ticket opened for every notification is sometimes a very good idea.

Another option is having a mailbox that is shared by several system administrators, where all notifications are sent. An unread notification in the inbox would then mean that it has to be dealt with.

C.4.1 Acknowledging Alerts

Monitor has strong features built-in to let your administrators work together. Acknowledging alerts is such a feature.

When you receive an alert, you can acknowledge it using the web interface and make a comment to inform your colleagues about what you are planning to do.

Using the web view Unhandled Problems you can then overview alerts that have not been acked yet – a great way of knowing what has been dealt with or not.

Sometimes it is a good idea to have Unhandled Problems displayed on the wall near the NOC or System Administrators.

C.5 Service Groups

The administrators often know exactly what it means when the CPU usage on a specific server is high or a disk on a database server is nearing full.

People working less closely with the infrastructure might not know this though, and this is one of the reasons why using Service Groups is a good idea.

You can create a group of services for every actual function delivered by your IT staff – for instance grouping email services provides a great overview: If everything is green your email ought to be working properly.

It is also great to quickly find the problem if you know there is one - you just have to look in the right service group instead of having to look through everything.

Appendix D

Index

You can use the index on the following pages if you want to know about a keyword that is not to be found in the table of contents.

Index

- 2d_coords, [75](#), [80](#)
- action_url, [75](#), [80](#), [85](#), [89](#), [91](#), [92](#)
- Active Checks, [7](#)
- active_checks_enabled , [78](#)
- Add this host?, [66](#)
- address, [1](#), [61](#), [65–67](#)
- Advanced menu, [3](#)
- alias, [61](#), [66](#), [67](#), [77](#), [85](#), [89](#), [90](#),
[92](#), [93](#), [95](#), [97](#)
- Assume Initial States, [43](#), [51](#)
- Assume State Retention, [44](#), [51](#)
- Assume States During Program Down-
time, [44](#)
- authorized_for_all, [102](#)
- authorized_for_all_host_commands, [100](#)
- authorized_for_all_hosts, [100](#)
- authorized_for_all_service_commands,
[100](#)
- authorized_for_all_services, [99](#)
- authorized_for_configuration_information,
[99](#)
- authorized_for_system_commands, [99](#)
- authorized_for_system_information,
[99](#)
- Autodetect network nodes, [65](#)
- Backtracked Archives, [44](#), [51](#)
- Check Execution Time, [39](#)
- Check Latency, [39](#)
- check_command, [77](#), [78](#), [86](#)
- check_command_args, [77](#), [86](#)
- check_freshness, [78](#), [87](#)
- check_interval, [78](#), [87](#)
- check_period, [78](#), [87](#)
- checks_enabled, [87](#)
- children, [77](#)
- cloning, [104](#)
- contact, [74](#)
- contact_groups, [66](#), [67](#), [74](#), [77](#), [84](#),
[89](#)
- contact_name, [93](#)
- contactgroup_name, [95](#)
- contactgroups, [94](#)
- contacts, [74](#), [77](#), [83](#), [89](#)
- Critical, [5](#)
- Dependencies, [72](#)
- display_name, [77](#)
- Down, [5](#)
- email, [94](#)
- escalation_options, [74](#), [84](#)
- escalation_period, [74](#), [84](#)
- Escalations, [73](#)
- event correlation, [31](#)
- Event Handlers, [7](#)
- event_handler, [78](#), [87](#)
- event_handler_args, [78](#), [87](#)
- event_handler_enabled, [78](#), [87](#)
- Exception type, [97](#)
- exclude, [97](#)
- execution_failure_criteria, [73](#), [82](#)
- exthostinfo, [75](#)
- Extras, [75](#)
- FILE, [67](#), [73](#), [79](#), [89](#)

- First Assumed Host State, [51](#)
- First Assumed Service State, [51](#)
- first_notification, [74](#), [79](#), [84](#)
- Flap Detection, [7](#)
- Flap detection, [78](#), [88](#)
- flap_detection_enabled, [78](#), [88](#)
- freshness_threshold, [87](#)
- graphical view, [23](#)
- Group Average, [53](#)
- high_flap_threshold, [78](#), [79](#), [88](#)
- Host Logo, [67](#)
- Host State Information, [9](#)
- host_name, [67](#), [73](#), [76](#), [77](#)
- host_notification_commands, [94](#)
- hostgroup_name, [90](#)
- hostgroups, [27](#), [49](#), [66](#), [67](#), [77](#), [91](#)
- icon_image, [75](#), [80](#), [85](#), [89](#)
- icon_image_alt, [75](#), [80](#)
- Include Soft States, [51](#)
- inherits_parent, [73](#), [83](#)
- initial_state, [77](#)
- Interval, [98](#)
- is_volatile, [86](#)
- last_notification, [74](#), [84](#)
- Layout Method, [24](#)
- low_flap_threshold, [78](#), [79](#), [88](#)
- Management Protocol, [67](#)
- max_check_attempts, [44](#), [51](#), [78](#), [87](#), [90](#)
- members, [90](#), [92](#), [95](#)
- Monitoring Performance, [7](#)
- Network Health, [7](#)
- Network Outage, [5](#)
- normal_check_interval, [90](#)
- notes, [75](#), [80](#), [85](#), [89](#), [91](#), [92](#)
- notes_url, [75](#), [80](#), [85](#), [89](#), [91](#), [92](#)
- notification_failure_criteria, [73](#), [83](#)
- notification_interval, [74](#), [79](#), [84](#), [88](#)
- notification_options, [79](#), [89](#), [93](#)
- notification_period, [79](#), [88](#), [93](#)
- Notifications, [7](#)
- notifications_enabled, [79](#), [89](#)
- obsess_over_host, [78](#)
- obsess_over_service, [87](#)
- Ok, [6](#)
- pager, [94](#)
- parallelize_check, [87](#)
- parents, [67](#), [72](#), [77](#)
- Passive Check, [7](#)
- passive_checks_enabled, [78](#)
- Password, [99](#)
- Pending, [5](#), [6](#)
- Pre-flight configuration check, [70](#)
- process_perf_data, [79](#), [88](#)
- profiles, [104](#)
- Report Time Period, [51](#)
- retain_nonstatus_information, [79](#), [88](#)
- retain_status_information, [79](#), [88](#)
- retry_check_interval, [90](#)
- retry_interval, [78](#), [87](#)
- scheduled_downtime, [34](#)
- search box, [33](#)
- Service Checks, [67](#)
- service_description, [86](#)
- service_notification_commands, [94](#)
- service_notification_commands_args, [94](#)
- servicegroup, [20](#)
- servicegroup_name, [91](#)
- servicegroups, [86](#)
- Severity, [31](#)
- Simple menu, [3](#)
- Soft States, [44](#)
- SSL, [1](#)
- stalking_options, [79](#), [89](#)

statusmap_image, [75](#), [80](#)

template, [67](#), [76](#), [86](#), [93](#)

timeperiod_name, [97](#)

Unknown, [6](#)

Unreachable, [5](#)

Up, [5](#)

User-supplied coords, [24](#)

Warning, [5](#)