op5 Monitor Administrator Manual

Introduction

There are three ways of changing the configuration of the op5 Monitor:

- Using the web UI **op5 Monitor configuration tool**.
- API
- Editing the configuration files in /opt/monitor/etc.

In this chapter we will take a look at how the **op5 Monitor Configuration tool**, from now on called only **Configure**, is used.

> ⓘ Editing the files directly is not supported and will conflict with the configuration tool and API.

Workflow

Most of the configuration in op5 Monitor is saved in configuration files (text files) in /opt/monitor/etc/. The Configure works with a database and this makes it possible to do changes in the configuration without saving it to file before all configuration is done.

The table below describes the workflow.

Step	Description
1	Configure opens and the configuration files are compared to the data in the database.
2	Edit the configuration
3	Save the changes to the Configure database by clicking **Submit** on the object you just added/changed.
4	When you are done with editing the configuration save the Configure database to the configuration files by clicking **Save**.
5	A preflight check is made on the configuration before it is exported to the configuration files.

Agents

Introduction

Most of the monitoring in op5 Monitor is used with the help of agents. The plugins are contacting the agents and let them do the job.

There are mainly four agents available for download at the op5 support site.

Agent	Environment
op5 NSClient++	Microsoft Windows
NRPE	Unix/Linux
MRTGEXT	Novell
Windows SyslogAgent	Microsoft Windows

Logger client on UNIX/Linux

Introduction

> Most UNIX/Linux systems has built-in support for syslog and hence you do not need to install any extra software to send your logs to your *op5 Monitor* server.
>
> More information covering configuration of syslog for remote logging can be found here

Novell

About

MRTGEXT was originally written as an NLM for Novell Netware to obtain values used with the widely known MRTG (predecessor of cacti), but it can also be used to poll values from op5 Monitor.

Table of Content

Installing Novell MRTGEXT

To install this extension, simply copy the MRTGEXT.NLM to each NetWare server's SYS:SYSTEM directory that you wish to gather statistics from. Then edit the server's AUTOEXEC.NCF to "LOAD MRTGEXT" so it will load each time the server is restarted.
The MRTGEXT.NLM has three command line switches available:

- -port=<port>

will change the port that MRTGEXT listens on for statistic requests. By default, MRTGEXT will use port 9999. For example, to have MRTGEXT use port 1023, add -port=1023 to the load line. If you change the port number on the command line, be sure to modify the perl script as well.

- -debug

will enable some debugging output to the System Console screen. This is only really useful when you are first configuring the extension.

- -mla=<license>

For those with an MLA license (mostly for NetWare 5), the MRTGEXT.NLM currently can not obtain a valid value for the server license count. Using this option will tell the MRTGEXT.NLM the license count max to report. This is important if you use the NWEXTCFG.PL to create configuration files or if you use the servstat.pl script. For example, if you have a NetWare 5 MLA license and you really only have a 100 user server, then you would add -mla=100 to your load command line.

Download

Novell MRTGEXT can be downloaded from the agents section in op5.com's download area.

NRPE

About

NRPE is a Unix client for executing plugins on remote hosts.
It is distributed as

- rpm-packages
- deb-packages
- portable source-code.

NRPE is used in combination with a set of local plugins. By default in op5 Monitor the plugins are placed in:

```
/opt/plugins
```

There are only a few plugins shipped with the op5 NRPE packages but you may use the ones located on the op5 Monitor server.

Table of Content

Installing NRPE

To install NRPE

- Download the package for your environment from the download section at www.op5.com
- Put the package to the host you like to install it on.
- Install the package the same way as you do normally with packages on that host.

Configuring NRPE

Before we can start use the NRPE agent for monitoring with op5 Monitor we need to configure the agent.
The NRPE agent is located in:

- `/etc/nrpe.conf`
- NRPE main configuration file settings

Setting	Description
server_port	The port NRPE should listen on. **Default**: 5666
allowed_hosts	Add the IP of you OP5 Monitor server on this line multiple addresses can be separated with , ie: allowed_hosts=1.2.3.4,1.2.3.5 Make sure you do not add any space between the comma (,). **Default**: 127.0.0.1
nrpe_user	The user the NRPE daemon is executed as. **Default**: nobody
nrpe_group	The group the NRPE daemon is executed as. **Default**: nobody
debug	Set to 1 if you need to debug the NRPE. **Default**: 0
command_timeout	The default time out, in seconds, a check shall have. **Default**: 60
dont_blame_nrpe	Set to 1 to be able to send arguments to NRPE. **Default**: 0

Adding commands to NRPE

NRPE comes with a few predefined commands. Those commands are located in:

```
/etc/nrpe.d/op5_commands.cfg
```

You may add your own commands and you should do that in your own file in:

```
/etc/nrpe.d/
```

ⓘ You must set .cfg as extension to your configuration file or else it will not be loaded into NRPE when the daemon is restarted.

NRPE command definition

The NRPE command definitions is divided into two parts.

- NRPE command parts

Part	Description
command[name]	The string between the square brackets will be the name of this command. The name is used when you executes the command with check_plugin. Do not use space in the command name.
/opt/plugins/...	This is the command line used to execute the plugin you are going to use in your command.

To add a command to NRPE

Here we will add a command that is looking for a process named smsd using the plugin check_procs, which is installed by default.

- Login to the host you have installed NRPE on as root user over ssh.
- Create a new configuration file and open it up with your favorite editor in /etc/nrpe.d/
- Add a command line looking like this:
  - `command[proc_smsd]=/opt/plugins/check_procs -w 1: -c 2:2 -C smsd`
- Save the file and restart NRPE:
  - `service nrpe restart`

Plugins used with NRPE

The only plugin used with NRPE is

- check_nrpe

To use the plugin with the command defined in the section Adding commands to NRPE, you shall use the following command line in your service definition:

```
/opt/plugins/check_nrpe -H $HOSTADDRESS$ -C proc_smsd
```

op5 NSClient++

About

This is the agent used for monitoring Windows type operating systems.

This agent has the ability to function as a drop in replacement for NSClient++ providing the same features as NSClient++ combined with the ability to execute scripts on the monitored Windows server.
op5 NSClient++ runs as a service under

- Windows 2000
- Windows XP
- Windows 2003
- Windows 7
- Windows 2008.
- Windows 2008 R2
- Windows 2012

Table of Content

Plugins used with op5 NSClient++

There are mainly two plugins that is used to communicate with op5 NSClient++:

- check_nt
- check_nrpe

check_nt

This plugin is used for all basic tests like:

- Cpu
- Memory
- Disks

But it can also be used to check

- Windows services
- Performances counters
- The perfered way is to use the check_nrpe_win commands.

check_nrpe

check_nrpe can also be used in the communication with op5 NSClient++. This one is normally used when you are performing checks on the Windows server with custom scripts.

Configuration files

NSClient++ operation is configured in a couple of plain text files called:

- NSC.ini
- op5.ini
- custom.ini

They are located in the installation directory, typically C:\Program Files\op5\nsclient++

Description of the configurations files:

File	Description
NSC.ini	This is the standard configuration file. This contains the default settings for NSClient++ This file might be overwritten during an update of NSClient++
op5.ini	This is a op5 specific configuration file. Here are the changes made by op5 entered. This file might be overwritten during an update of NSClient++
custom.ini	This is where you shall place your own configuration. It will never be overwritten during any update of NSClient++.

The default configuration provided is fully functional but there are some options that likely need to be changed.

Changing the configurationTo change the configurationTo change the configuration open the custom.ini file using your favorite text-editor (e.g. WordPad). This file is empty but take a look at NSC.ini to view all settings. Read the NSC.ini file carefully to get a complete understanding of all configuration options. Lines starting with ; (semicolon) are comments or disabled commands.

Before the changes will take effect, the op5NSClient++ service must be restarted.
Options most likely in need for configuration are described bellow, section by section.

```
[Settings]
allowed_hosts=
```

This option lists all servers that are allowed to talk to the agent. Enter the IP-address of the op5 Monitor server or servers if used in a load balanced configuration. If this option is left blank anybody will be able to communicate with the agent.

```
[log]
debug=0
```

Set debug to 1 to enable debugging. This is normally not needed but can be very useful when troubleshooting.

```
[NSClient]
port=1248
```

This is the port used for NSClient style requests, i.e. using the check_nt plugin. If any other application is already using the default port it might be necessary to change this option.

```
[NRPE]
```

port=5666

This is the port used for nrpe style requests. In order for a minimum of configuration on the op5 Monitor server it's recommended that this option is left with the default value. If this is changed new nrpe check commands using the configured port need to be created on the op5 Monitor server.

> ⓘ If a non default port is used you also need to make changes in the check_command used on the op5 Monitor server.

```
allow_arguments=0
```

Set this to 1 to enable the possibility to include arguments in nrpe requests. This could be considered a security risk so only enable this if needed. Also, make sure to set the allowed_hosts option described above if arguments are allowed.

```
[NRPE Handlers]
```

The nrpe handlers provide a way to execute any custom plugin/check command on the monitored Windows server. In this section you configure all the commands that should be available.

- *Adding a custom script/plugin to NSClient++*

```
command[my_custom]=c:\mycustomdir\my_prog.exe
```

Or the simplified syntax:

```
my_custom=c:\mycustomdir\my_prog.exe
```

Windows SyslogAgent

About

op5 SyslogAgent runs as a service under

- Windows 2000
- Windows XP
- Windows 2003
- Windows 2008.
- Windows 2008 R2
- Windows 2012

It formats all types of Windows Eventlog entries into syslog format and sends them to a syslog host (The op5 Monitor server or the op5 LogServer).

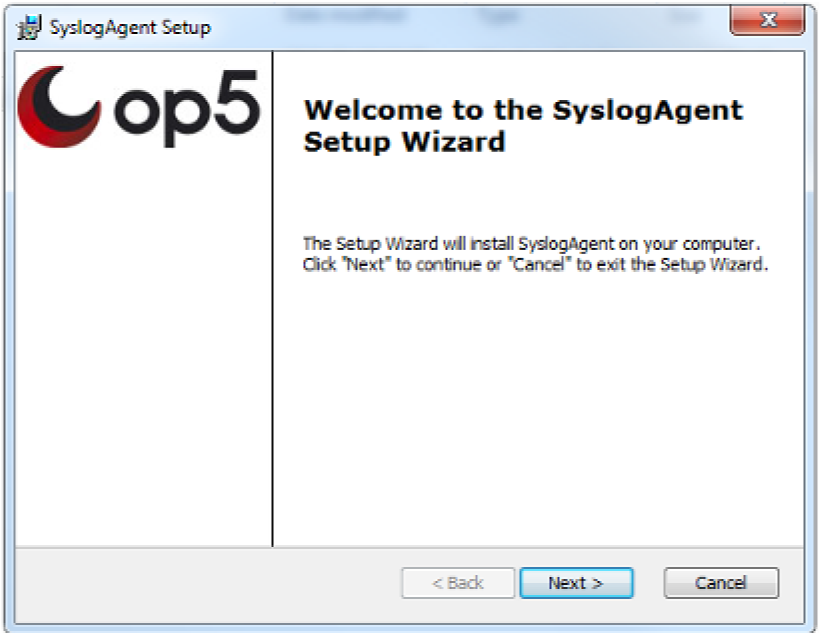
The op5 SyslogAgent can also forward plaintext log-files. Entries in the Event log are sent to the op5 Logserver or op5 Monitor server, text based application logs are also supported. It is a repackaged version of the Datagram SyslogAgent, which initially is a bug fixed version of Sabre Net's old NT_Syslog.

The op5 SyslogAgent is licenced as GPL software.

Table of Content

Installation

The op5 SyslogAgent installation package consists of an msi installer. To install simply double click the installation msi file and follow the on-screen instructions.



Welcome to the SyslogAgent Setup Wizard

The Setup Wizard will install SyslogAgent on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

By default the op5 SyslogAgent will be installed in an op5 subdirectory to the program files folder.Usually:

```
C:\Program Files\op5\SyslogAgent\
```

For configuration see the chapter Configuration

Upgrading

If a prior version of the SyslogAgent is installed it should to avoid problems, be stopped and uninstalled as a service and then uninstalled. Stopping and uninstalling the service can be done from the SyslogAgent Configuration tool.

Follow these steps to stop and uninstall the SyslogAgent service:

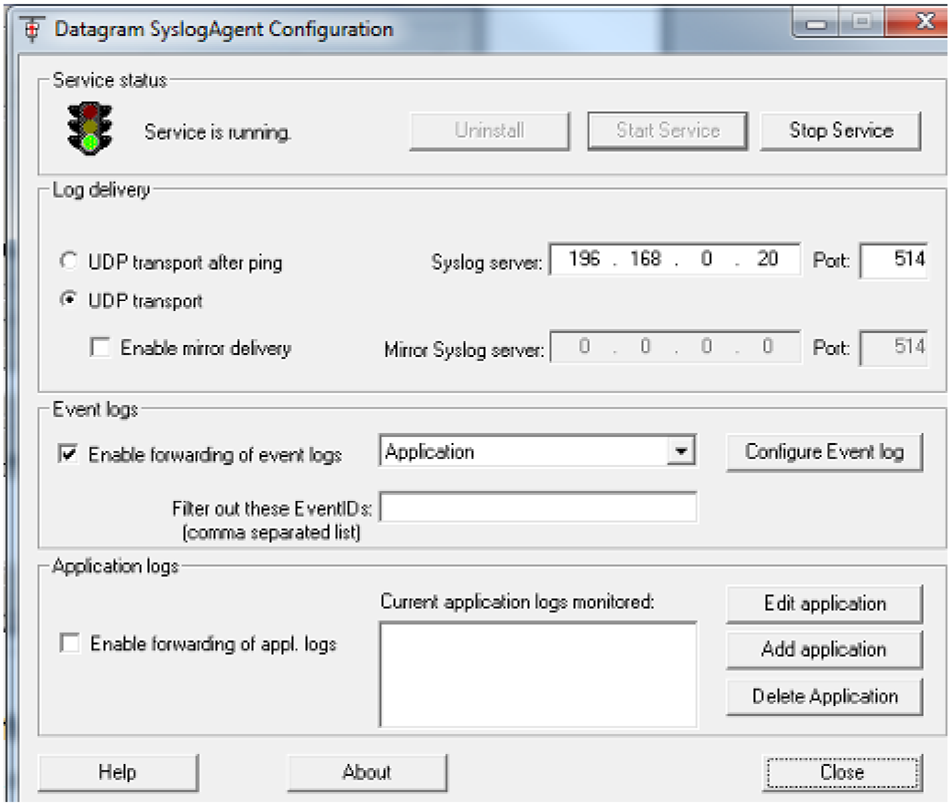
a. Start the SyslogAgent Configuration tool
b. Press the "Stop"-button (see Fig 3. in the section Configuration)
c. Press the "Uninstall"-button

After the service have been stopped and uninstalled you should uninstall the previous version of the SyslogAgent from "Add/Remove software" on the windows control panel.
Now you can proceed with the installation of the new version as usual.

Note that your previous settings will be used directly when the installation is complete.

Configuration

When the configuration tool is started the following window should be displayed:



Datagram SyslogAgent Configuration

Service status

Service is running.

Log delivery

○ UDP transport after ping

● UDP transport

□ Enable mirror delivery

Syslog server: 196 . 168 . 0 . 20 Port: 514

Mirror Syslog server: 0 . 0 . 0 . 0 Port: 514

Event logs

☑ Enable forwarding of event logs Application

Filter out these EventIDs:
(comma separated list)

Application logs

□ Enable forwarding of appl. logs

Current application logs monitored:

Configuring the elementary functions

To configure the elementary functions and start the SyslogAgent started follow the following steps:

- Enter the IP address in the field **Syslog Server:**. This IP should be the one to your op5 Logserver or op5 Monitor server.
- Make sure the check box "**Enable forwarding of event logs**" is checked.
- Press **Start Service**.

Your SyslogAgent is now configured and should be sending logs to your op5 Logserver or op5 Monitor server.

Configuration options

UDP delivery

This is the standard way of sending logs - using 'best-effort' UDP protocol. If a secondary syslog server is configured, logs are sent to both addresses.
Separate ports can be configured for the primary and mirror server. Default is 514 (UDP).

UDP with Ping Delivery

With this option, the Syslogserver will first be pinged before any logs are sent. As long as the Event log is not cleared before contact can be restored, no information will be lost. The same is not neccessarary true for Application Logs - depending on how the particular application handles the log files.
The server will be pinged every 20 seconds while connection is successful. When ping is unsuccessful, the Agent will eventually slow down to attempt a ping every minute.

Enable forwarading of event logs

By default, syslog entries are forwarded to the syslog server. If only application logging is desired, event forwarding can be disabled.
The Syslog agent is preconfigured regarding classification of different types of entries. These settings can be modified by choosing an event log and pressing the 'Configure event log' button. Please see advanced configuration for detailed description of registry settings.

Filter out EventIDs

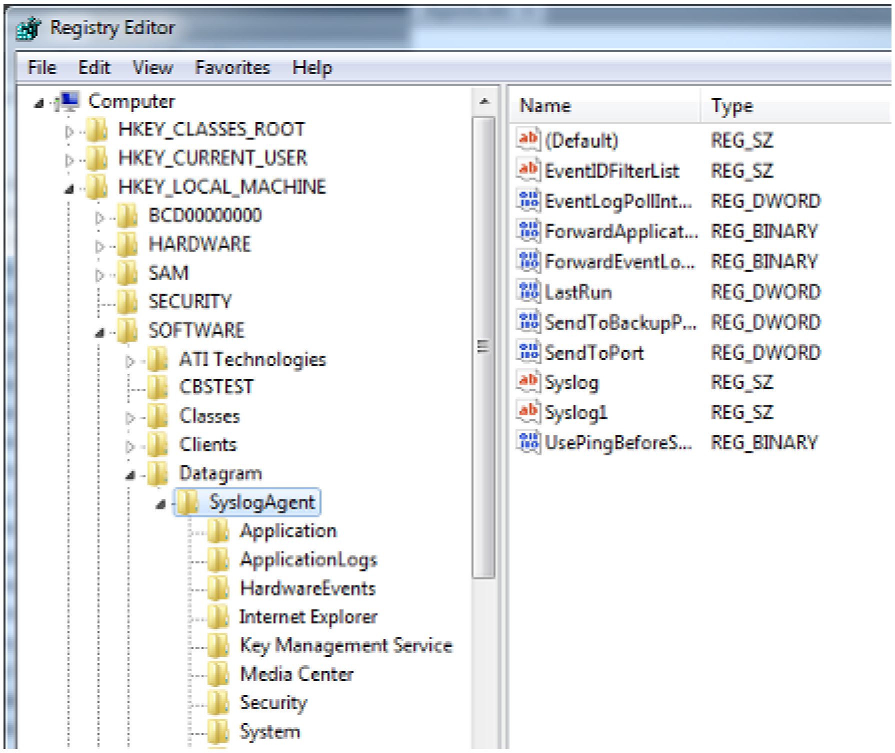
In certain cases, it can be desireable to filter out certain Event ID's. SyslogAgent supports this by entering the Event ID's to be filtered out in a comma separated list. A maximum of 30 Event ID's can be specified. For instance:

```
562,565,4132,566,836,837
```

Exporting configuration

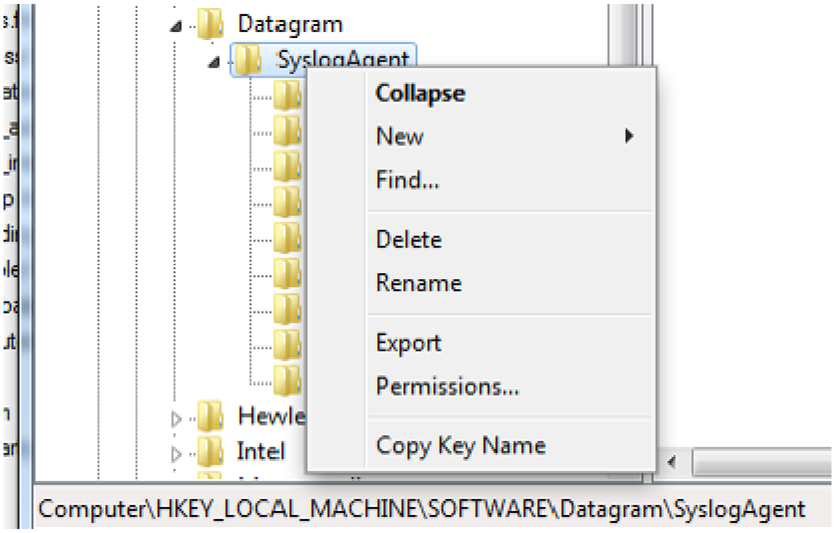
All settings are stored in the registry, and can therefore be exported to a .reg file. This way the settings can be pushed out via a group policy, scripts etc. Please observe that in such an export the key 'LastRun' should be deleted before copied to another computer - it's the key that helps each computer to know which entries has already been sent. Not deleting this field can cause computers to not send syslog entries.
To create a .reg-file simply open the regedit-tool, i.e type regedit from the command-line and follow these steps.

- Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Datagram\SyslogAgent:



Name	Type
(Default)	REG_SZ
EventIDFilterList	REG_SZ
EventLogPollInt...	REG_DWORD
ForwardApplicat...	REG_BINARY
ForwardEventLo...	REG_BINARY
LastRun	REG_DWORD
SendToBackupP...	REG_DWORD
SendToPort	REG_DWORD
Syslog	REG_SZ
Syslog1	REG_SZ
UsePingBeforeS...	REG_BINARY

- Right-click the folder and choose export.



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Datagram\SyslogAgent

- Save the file and open it by right-clicking the file and choosing edit. Remove the whole line corresponding to the keyword "LastRun"(if present).

- The line can be found under the section: " HKEY_LOCAL_MACHINE\SOFTWARE\Datagram\SyslogAgent]"

API

Documentation for the available application programming interfaces in op5 Monitor

HTTP-API

About

op5 Monitor comes with a REST API that can be used to:

- Fetch status information
- Configure system
- Get report data
- Send commands to op5 Monitor

The HTTP-API let's you configure, get status information and report data from op5 Monitor by issuing regular HTTP requests. Basically, you 'visit' an URI, which triggers op5 Monitor to do something, and you get a response telling you what happened.

For more information about the REST API go to https://your-op5-monitor/api/help/

Table of Content

HTTP Status API

Deprecation notice
Since version 6.3 of op5 Monitor, the status API has been deprecated. It's recommended to use the more flexible and powerful "filter" API instead

The HTTP Status API is used to get the information from op5 Monitor Status GUI. It can give you information about all objects used by the op5 monitor.
Creating widgets, dashboards and mobile apps are places where the HTTP Status API will come handy.
There are only a briefly documentation about that API in this manual, since the main documentation is included in the product.
Let us say that your monitor server is called op5-monitor you can reach the documentation on the following location:
https://op5-monitor/monitor/Documentation/html/index.html
It is generated by doxygen and contains information like:

- namespaces
- structures (classes and methods)

- files

HTTP Configuration API

The configure API is used to manipulate the object configuration used by op5 Monitor. It works against the configure database the same way as the op5 Monitor Configuration tool does.
You may use it to build integrations between op5 Monitor and other third party software.
Let us say that your monitor server is called op5-monitor you can reach the documentation on the following location:
https://op5-monitor/monitor/op5/nacoma/Documentation/html/index.html
It is generated by doxygen and contains information like classes and methods used in the op5 Monitor configuration tool.

HTTP Command API

The command API lets you submit the following commands to op5 Monitor using the REST API:

- Acknowledge Host Problem
- Acknowledge Service Problem
- Process Host Check Result
- Process Service Check Result
- Schedule and Propagate Host Downtime
- Schedule and Propagate Triggered Host Downtime
- Schedule Host Check
- Schedule Host Downtime
- Schedule Service Check
- Schedule Service Downtime

Acknowledge Host Problem

This command is used to acknowledge a host problem.
When a host problem is acknowledged, future notifications about problems are temporarily disabled until the host changes from its current state. If you want acknowledgement to disable notifications until the host recovers, specify the 'sticky' option. Contacts for this host will receive a notification about the acknowledgement, so they are aware that someone is working on the problem. Additionally, a comment will also be added to the host. Make sure to enter your name in the 'author' parameter and fill in a brief description of what you are doing in the 'comment' paramter. If you would like the host comment to remain once the acknowledgement is removed, specify the 'persistent' option. If you do not want an acknowledgement notification sent out to the appropriate contacts, do not specify the 'notify' option.

Acknowledge Service Problem

This command is used to acknowledge a service problem.
When a service problem is acknowledged, future notifications about problems are temporarily disabled until the service changes from its current state. If you want acknowledgement to disable notifications until the service recovers, specify the 'sticky' option. Contacts for this service will receive a notification about the acknowledgement, so they are aware that someone is working on the problem. Additionally, a comment will also be added to the service. Make sure to enter your name in the 'author' parameter and fill in a brief description of what you are doing in the 'comment' parameter. If you would like the service comment to remain once the acknowledgement is removed, specify the 'persistent' option. If you do not want an acknowledgement notification sent out to the appropriate contacts, do not specify the 'notify' option.

Process Host Check Result

This command is used to submit a passive check result for a host.

Process Service Check Result

This command is used to submit a passive check result for a service. It is particularly useful for resetting security-related services to OK states once they have been dealt with.

Schedule and Propagate Host Downtime

Schedules downtime for a specified host and all of its children (hosts).
If the "fixed" argument is set to one (1), downtime will start and end at the times specified by the "start" and "end" arguments. Otherwise, downtime will begin between the "start" and "end" times and last for "duration" seconds. The "start" and "end" arguments are specified in time_t format (seconds since the UNIX epoch). The specified (parent) host downtime can be triggered by another downtime entry if the "trigger_id" is set to the ID of another scheduled downtime entry. Set the "trigger_id" argument to zero (0) if the downtime for the specified (parent) host should not be triggered by another downtime entry.

Schedule and Propagate Triggerd Host Downtime

Schedules downtime for a specified host and all of its children (hosts).
If the "fixed" argument is set to one (1), downtime will start and end at the times specified by the "start" and "end" arguments. Otherwise, downtime will begin between the "start" and "end" times and last for "duration" seconds. The "start" and "end" arguments are specified in time_t format (seconds since the UNIX epoch). Downtime for child hosts are all set to be triggered by the downtime for the specified (parent) host. The specified (parent) host downtime can be triggered by another downtime entry if the "trigger_id" is set to the ID of another scheduled downtime entry. Set the "trigger_id" argument to zero (0) if the downtime for the specified (parent) host should not be triggered by another downtime entry.

Schedule Host Check

This command is used to schedule the next check of a host.
The monitoring process will re-queue the host to be checked at the time you specify.

Schedule Host Downtime

This command is used to schedule downtime for a host.
During the specified downtime, the monitoring process will not send notifications out about the host. When the scheduled downtime expires, the monitoring process will send out notifications for this host as it normally would. Scheduled downtimes are preserved across program shutdowns and restarts. If you specify the 'fixed' option, the downtime will be in effect between the start and end times you specify. If you do not specify the 'fixed' option, the monitoring process will treat this as "flexible" downtime. Flexible downtime starts when the host goes down or becomes unreachable (sometime between the start and end times you specified) and lasts as long as the duration of time you specify. The 'duration' parameter does not apply for fixed downtime.

Schedule Service Check

This command is used to schedule the next check of a service.
The check will be re-queued to be run at the time you specify.

Schedule Service Downtime

This command is used to schedule downtime for a service.
During the specified downtime, the monitoring process will not send notifications out about the service. When the scheduled downtime expires, the monitoring process will send out notifications for this service as it normally would. Scheduled downtimes are preserved across program shutdowns and restarts. If you specify 'fixed' option, the downtime will be in effect between the start and end times you specify. If you do not specify the 'fixed' option, the monitoring process will treat this as "flexible" downtime. Flexible downtime starts when the service enters a non-OK state (sometime between the start and end times you specified) and lasts as long as the duration of time you specify. The 'duration' parameter does not apply for fixed downtime.

HTTP Report API

The report API can be used to retrieve report data in XML or JSON format.

HTTP Filter API

The filter API can be used to ether retrieve a list of objects from a filter or do a count of objects in a filter.

Query example

To view hosts that are not OK:
`https://<op5server>/api/filter/query?query=[hosts]%20state!=0&columns=name,state,acknowledged,has_been_checked`

Count example

To get a count of the objects using the same query as above:
`https://<op5server>/api/filter/count?query=[hosts]%20state!=0&columns=name,state,acknowledged,has_been_checked`

Example

In this example we will create a new host called **my_server** with one ping service. The IP for **my_server** is **192.168.0.20**
In this example the op5 server is called **op5-server**, the username is **joe** and joe's password is **joespassword**.
By visiting the page https://op5monitor.example.com/api/help/config/host, you get more detailed information on how to create a host.

This is what needs to be done in PHP:

```
<?php
$data = json_encode(array(
'address' => '192.168.0.20',
'alias' => 'My Server',
'host_name' => 'my_server'
));
$a_handle = curl_init('https://op5monitor.example.com/api/config/host');
curl_setopt($a_handle, CURLOPT_USERPWD, 'joe:joespassword');
curl_setopt($a_handle, CURLOPT_RETURNTRANSFER, TRUE);
curl_setopt($a_handle, CURLOPT_POSTFIELDS, $data);
curl_setopt($a_handle, CURLOPT_HTTPHEADER, array('Content-Type: application/json'));
curl_setopt($a_handle, CURLOPT_SSL_VERIFYPEER, false);
$host = curl_exec($a_handle);
$data = json_encode(array(
'check_command' => 'check_ping',
'service_description' => 'ping',
'host_name' => 'my_server'
));
$a_handle = curl_init('op5-server/api/config/service');
curl_setopt($a_handle, CURLOPT_USERPWD, 'joe:joespassword');
curl_setopt($a_handle, CURLOPT_RETURNTRANSFER, TRUE);
curl_setopt($a_handle, CURLOPT_POSTFIELDS, $data);
curl_setopt($a_handle, CURLOPT_HTTPHEADER, array('Content-Type: application/json'));
curl_setopt($a_handle, CURLOPT_SSL_VERIFYPEER, false);
$service = curl_exec($a_handle);
?>
Before the changes are applied, you need to confirm them and then save them so that
they become part of your configuration. This can be done in two ways, either by Saving
changes in the op5 Monitor GUI, or by adding an additional call via the REST API:
<?php
$a_handle = curl_init('op5-server/api/config/change');
curl_setopt($a_handle, CURLOPT_USERPWD, 'joe:joespassword');
curl_setopt($a_handle, CURLOPT_CUSTOMREQUEST, 'POST');
curl_setopt($a_handle, CURLOPT_SSL_VERIFYPEER, false);
$save = curl_exec($a_handle);
?>
```

Now, visiting https://op5-server/api/config/host/my_server in a web browser should show you the live configuration.

REST and LDAP

When you have more than one auth module, for example "Local" and "LDAP", you need to specify which to authenticate against. This is done with the dollar character ('$').
Thus, this regular call:

```
curl -u user:password https://op5monitor.example.com/api/status/host
```

becomes:

```
curl -u 'user$LDAP:password' https://op5monitor.example.com/api/status/host
```

or:

```
curl -u 'user$Local:password' https://op5monitor.example.com/api/status/host
```

Notice how the dollar sign ('$') needs quoting depending on the environment (in bash, it will always need to be quoted).

The first way of calling the API: `curl -u user:password https://op5monitor.example.com/api/status/host` will still work, provided that you want to authenticate against the default driver. The default driver can always be specified from within the GUI: **Configure -> Auth Modules.**

Authentication Integration

Introduction

The authentication system is handled by authentication drivers. Each driver handles authentication of the user, and resolution of the group memberships for the given user. The groups is then mapped to permissions by the authorization layer, which is described later.

An auth driver can either use a local storage of users (Driver Default), rely on apache authentication (Driver apache), or use an external system for managing users (Driver LDAP).
The authentication system is configured through the configuration, using the **Auth Modules** option under configuration.

The configuration for the authentication system is stored in the "auth" configuration file, located in */etc/op5/auth.yml*

Child Pages

Apache

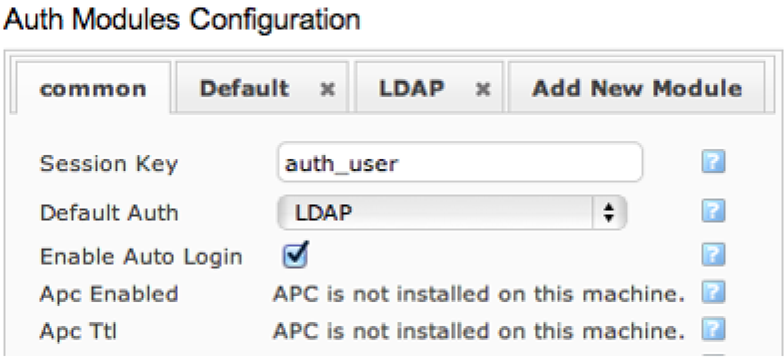
About

A system can also rely on apache to authenticate the user. In this case, it is up to the user to protect the `/monitor` path with access in the apache web server, either by an `.htaccess` file or in the apache configuration.
The apache driver makes it possible to use apache modules for single sign-on authentication solutions, or other systems, like mysql or kerberos.
The driver gets the authenticated username from apache, and adds the group `apache_auth_user` to all users logged in.

Table of Content

Setting up an authentication module that utilises the Apache driver

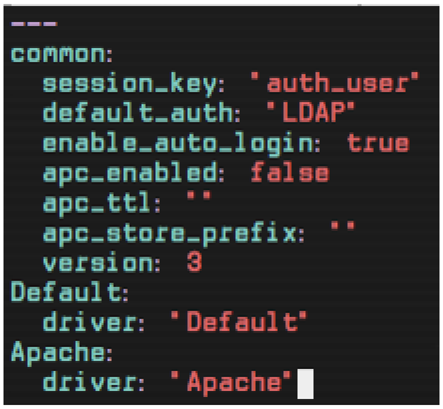
After having logged in to op5 Monitor, go to **Configure** and then select **Auth modules**.
Click the **Add new module** tab.
In the dialogue that appears, name your new module.
Choose the Apache driver from the dropdown.
Click **Add**.
In the common tab, check the checkbox for the option "**Enable Auto Login**".
Save your changes by clicking "**Submit**"..



Auth Modules Configuration

Session Key	auth_user
Default Auth	LDAP
Enable Auto Login	☑
Apc Enabled	APC is not installed on this machine.
Apc Ttl	APC is not installed on this machine.

The configuration file located at `/etc/op5/auth.yml` can be modified manually to enable usage of the Apache authentication driver. It should look similar to this picture:

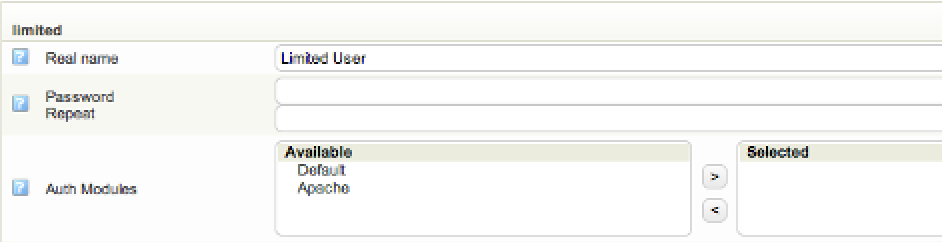


```
---
common:
  session_key: 'auth_user'
  default_auth: 'LDAP'
  enable_auto_login: true
  apc_enabled: false
  apc_ttl: ''
  apc_store_prefix: ''
  version: 3
Default:
  driver: 'Default'
Apache:
  driver: 'Apache'
```

Make sure enable_auto_login is set to true.

Users and permissions

The Apache authentication driver utilises similar configuration to the Default driver for group authorization. This means that you will have to set up additional "`Local users`" to resolve group memberships since Apache doesn't have a way to resolve them itself.
For each user one or more Auth Modules can be specified. This enables the user to log in using the Auth Modules that where chosen but not the others. Just as with ordinary Local users, groups can be specified per user to give it permissions to different parts of op5 monitor.



limited

Real name	Limited User
Password Repeat	
Auth Modules	Available: Default, Apache Selected:

Note that some Auth Modules might not need you to specify a password for the user. This is validated every time you edit your users and passwords needs to be set for every user you have given an Auth Module that depends on username and password to log in.

Default

About

For local users, the default driver can be used. This enables a local store of users at the op5 Monitor server. It is recommended that you always keep this driver configured with an admin account as a fallback if the system is primarily using LDAP.

When the Default driver is enabled, a configuration interface, named **Local Users** appears in op5 configuration.

In the local users page, each user has a real name, a password can be set, and group membership can be controlled. Groups needs to be created in advance. See *Group Rights*
This driver stores the users in the `auth_users` configuration file, located in `/etc/op5/auth_users.yml`.

Table of Content

Header Authentication Method (SSO single sign on)

Introduction

Header Authentication can be used to give single sign on (SSO) access to op5 Monitor by sending extra headers with the HTTP request. The headers must be sent on every page load meaning the authentication is performed every time a page is loaded.

> This authentication method should only be used when all requests are made through an authenticating proxy which filters all request headers. Failing to do this will enable any user to send extra headers that can grant admin privileges.

Table of Content

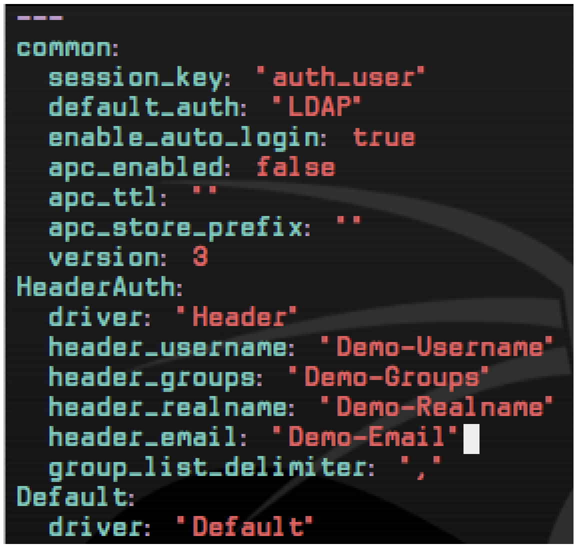
Configuration

It's possible to enable HTTP header authentication by adding a authentication module using the "Header" driver.
To configure this module, you need to manually add the following section to "/etc/op5/auth.yml":

```
HeaderAuth:
  driver: "Header"
  header_username: X-Username
  header_realname: X-Realname
  header_email: X-Email
  header_groups: X-Groups
  group_list_delimiter: ","
```

Where "X-Username", "X-Realname", "X-Email" and "X-Groups" is the corresponding headers, case insensitive.
Additionally, you must set the "enable_auto_login" option to "true" for header authentication work.

Below is an example configuration of the authentication module in Monitor (from "/etc/op5/auth.yml"):



```
---
common:
  session_key: 'auth_user'
  default_auth: 'LDAP'
  enable_auto_login: true
  apc_enabled: false
  apc_ttl: ''
  apc_store_prefix: ''
  version: 3
HeaderAuth:
  driver: 'Header'
  header_username: 'Demo-Username'
  header_groups: 'Demo-Groups'
  header_realname: 'Demo-Realname'
  header_email: 'Demo-Email'
  group_list_delimiter: ','
Default:
  driver: 'Default'
```

Permissions

Permissions are handled by the groups that are sent in the group header, which can be configured on the "Group permissions" page.

LDAP and Active Directory

About

For central user management, an LDAP server can be used, like Microsoft Active Directory or OpenLDAP. When used, op5 Monitor verifies the user with the LDAP server lookup the group membership of the users in the directory.

Table of Content

Before we start

This documentation assumes that you have:

- Administrator access to the domain
- Basic knowledge about LDAP structure

Prepare your domain

In op5 Monitor, permissions is handled by groups. Make sure you have one group available for each role in the system.
If the domain doesn't allow to bind anonymously to resolve group memberships or find users, a service account must be added. This account needs to have read access to resolve group membership and search for users in the system.

Connection parameters

Server

Address to the LDAP server, or servers. Can be a space separated list of addresses. Addresses are added for redundancy. Servers will be used in that order.

Port

TCP port to connect to. Leave blank for default. (389 for no encryption/start-tls, 636 for ssl)

Encryption

Which type of encryption to use for connection between op5 Monitor to the LDAP server. (none, start_tls or ssl). Make sure to have a valid ssl certificate for the LDAP server, and php recognizes it.

Bind DN

Distinguished name (or user principal name for active directory, which is `username@domain`) of the service account, created under "Prepare your domain" above, or empty to bind anonymously.

Bind secret

Password for the service user.
For security reasons, this can also be a path to a filename containing the password. To use this feature, enter `file:/path/to/secret/file`
It is also possible to keep the password in a separate config file, when multiple LDAP-connections is used. In this case, enter "`config:configname`", which will use config file `/etc/op5/configname.yml`. The config file should then contain one line per driver: "`driver name: secret`"

Base DN

The distinguished name for the root of the directory to access. This is usually the DN for the domain, for example: `DC=example,DC=com`

User base DN

The base DN to search for users. This is an absolute DN, and not relative to Base DN. In almost all cases, use the same value as Base DN here.

User filter

A LDAP filter used to filter out user objects. Usually this is a filter for objectClass. For Active Directory "`(objectClass=user)`" should work.

Group Base DN

The base DN to search for groups. This is an absolute DN, and not relative to Base DN. In almost all cases, use the same value as Base DN here.

Group filter

A LDAP filter used to filter out group objects. Usually this is a filter for objectClass. For Active Directory "`(objectClass=group)`" should work.

Groupkey

The name of the attribute identifying the group. For Active Directory, "`cn`" should work.

Group Recursive

If groups can be nested, so that a group can be member of another group. This is possible in Active Directory, and should there be active.
With this unchecked, only members of that group directly will be treated as members of the group. If this is the case for systems which supports nested groups. This checkbox can be unchecked for performance reasons.

UPN Suffix

When binding with UPN (user principal name), this is the suffix to use after @, which is the domain name. For example, if the UPN of a user is "`username@example.com`", the UPN suffix is "`example.com`".

Userkey

The key to select the username of a user in the system. Older versions of Active Directory uses sAMAccountName. But in later versions, use userPrincipalName

Userkey is UPN

Check this if the userkey is a UPN. In that case, the domain part of the userkey will be ignored. Check this if you are using Active Directory, and userPrincipalName as userkey.

Userkey realname

The name of the attribute in the user object describing the real name of the user. For active Directory, and most other LDAP systems, "`cn`" should work. This is used to nicely display the username of the logged in user.

Userkey email

The name of the attribute in the user object containing the the email address. For active directory, and many other systems, "`mail`" should work.

Memberkey

The name of the attribute in a group, which contains the reference to it's members.
When using LDAP with posix extensions, this should be "`memberUid`". When group is of class "`groupOfUniqueNames`", this should be "`uniqueMember`". For Active Directory, "`member`" should work.

Memberkey is DN

Check this box if Memberkey is defines the entire DN of the member user or group, not only it's name. For Active Directory, this is true. In a posix system, this is false.

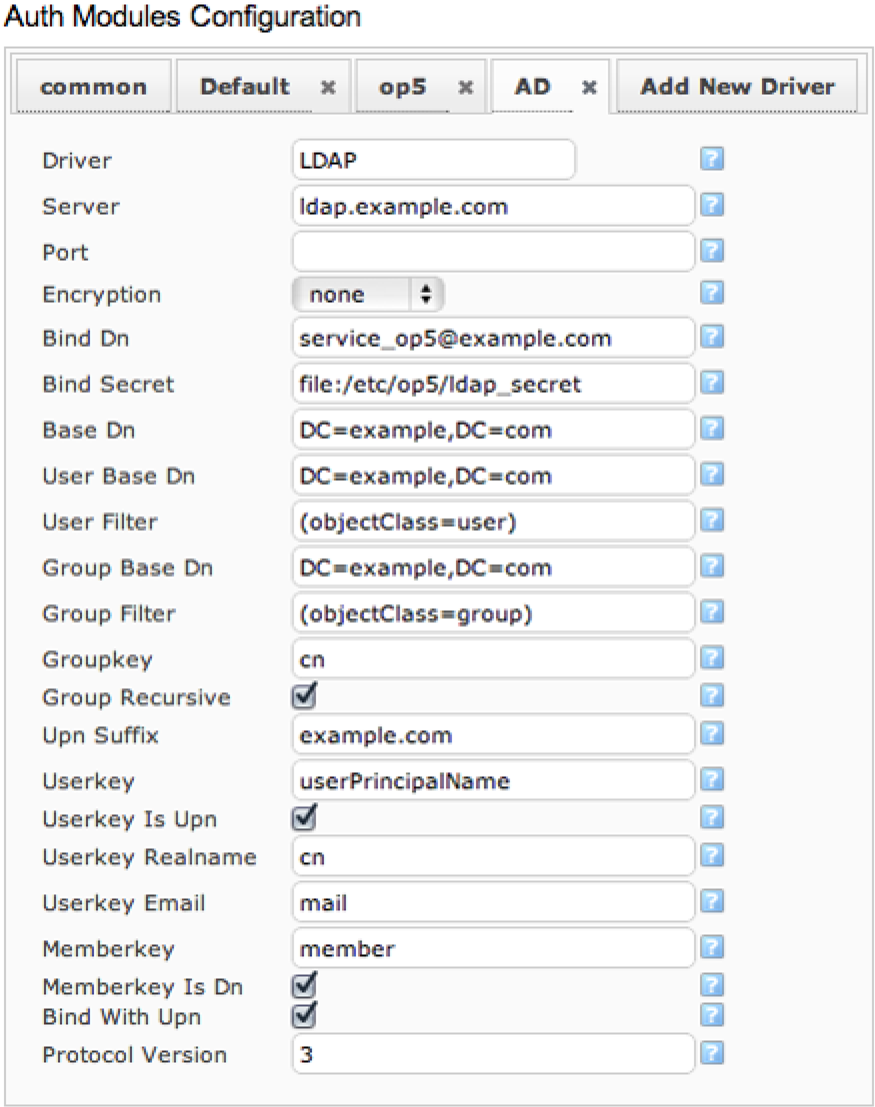
Bind with UPN

If binding to the LDAP server should be done with the user principal name instead of the DN of the user.
For Active Directory, this is true. For all other systems, this is false.
When binding with UPN, the system constructs a UPN from the username and UPN suffix, and tries to bind with the constructed UPN and given password. If bind succeeds, it resolves the groups.
When binding with DN, the system tries to bind with "Bind DN" and "Bind Secret" to look in the directory for the user. If the user is found, it tries to rebind with the user DN and password given, and if that succeeds, the group membership is resolved.

Protocol version

The LDAP protocol version to use. Almost everyone will keep this at 3.

Example configuration for Active Directory



Auth Modules Configuration

Driver: LDAP
Server: ldap.example.com
Port:
Encryption: none
Bind Dn: service_op5@example.com
Bind Secret: file:/etc/op5/ldap_secret
Base Dn: DC=example,DC=com
User Base Dn: DC=example,DC=com
User Filter: (objectClass=user)
Group Base Dn: DC=example,DC=com
Group Filter: (objectClass=group)
Groupkey: cn
Group Recursive: ☑
Upn Suffix: example.com
Userkey: userPrincipalName
Userkey Is Upn: ☑
Userkey Realname: cn
Userkey Email: mail
Memberkey: member
Memberkey Is Dn: ☑
Bind With Upn: ☑
Protocol Version: 3

Server:ldap.example.com
Port:
Encryption:none
Bind DN:service_op5@example.com
Bind Secret:file:/etc/op5/ldap_secret
Base DN:DC=example,DC=com
User Base DN:DC=example,DC=com
User filter:(objectClass=user)
Group Base DN:DC=example,DC=com
Group filter:(objectClass=group)
Groupkey:cn
Group Recursive:yes
UPN Suffix:example.com
Userkey:userPrincipalName
Userkey is UPN:yes
Userkey realname:cn
Userkey email:mail
Memberkey:member
Memberkey is DN:yes
Bind with UPN:yes
Protocol version:3

Test your connection

To test if the system can bind using "Bind DN" and "Bind Secret", go to Assign Group Rights page in op5 configuration. A column has

appeared for the driver, and the corresponding group parameters is correctly set.
If a group is successfully resolved, the corresponding cell is turned green. If it is determined that the group doesn't exist in the LDAP domain, the cell is red. In either way, a successful connection has been established.
If the connection failed, all the cells are gray.

More Information

For more information and help setting up an AD connection, please read our Active Directory Integration How-To

For information on how to use LDAP SSL (SLADP) see Certificate management for LDAP SSL (sldap) with Active Directory

Backend

The op5 Monitor backend is called Merlin (Module for Effortless Redundancy and Load balancing In Nagios). It was initially created to provide an easy way to set up distributed Nagios installations, allowing Nagios processes to exchange information directly as an alternative to the standard nagios way using NSCA.

When we started making our own GUI for op5 Monitor, called Ninja, we realized that we could continue the work on Merlin and adopt the project to function as backend for the new GUI by adding support for storing the status information in a database, fault tolerance and some other things.

Backend parts

About

This chapter describes the backend of op5 Monitor

Table of Content

Backend parts

merlin-mod

Responsible for jacking into the NEBCALLBACK_* calls and send them to a socket. If the socket is not available the events are written to a backlog and sent when the socket is available again.

merlind

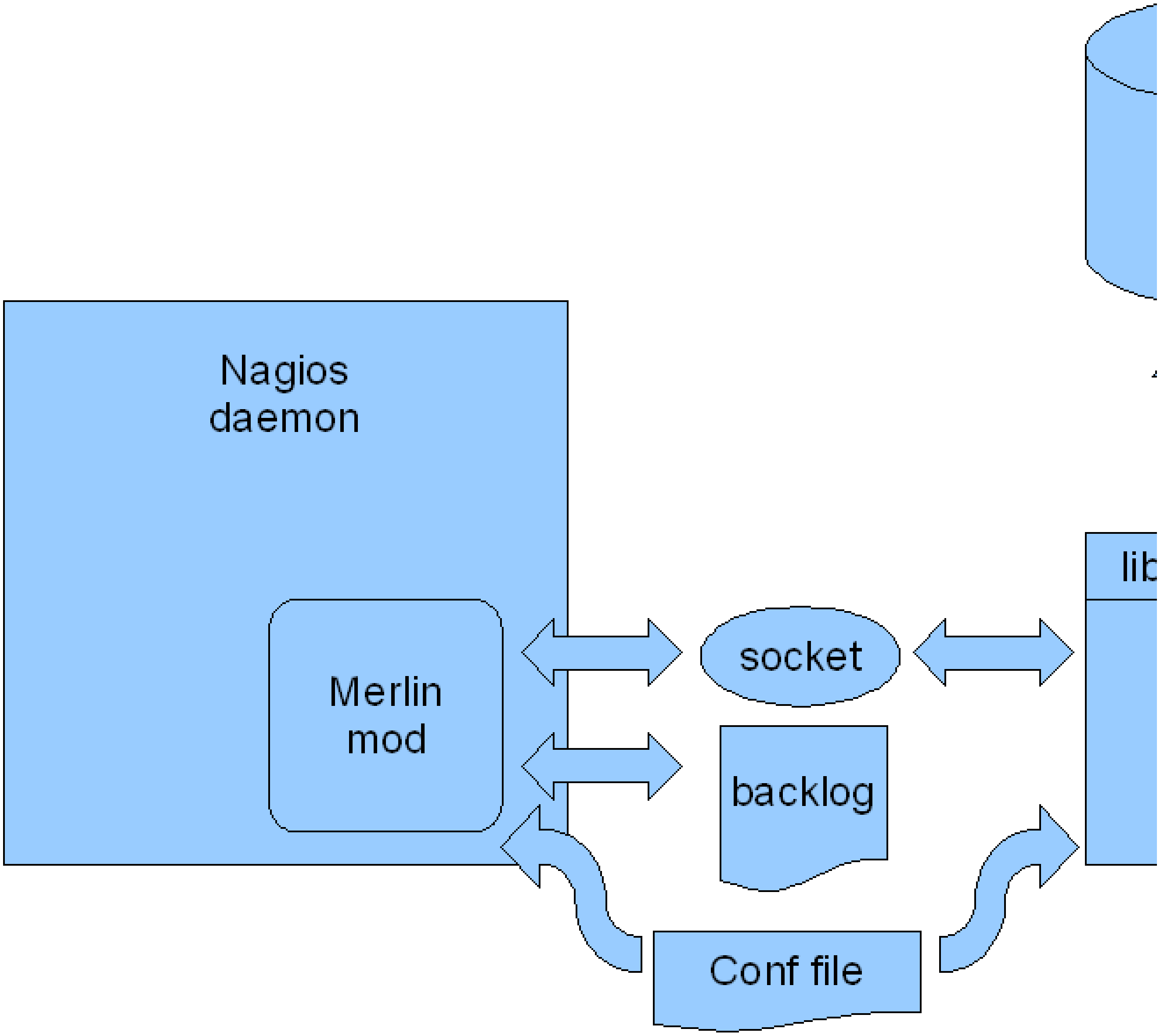
The Merlin daemon listens to the socket that merlin-mod writes to and sends all events received either to a database of your choice (using libdbi) or to another merlin daemon. If the daemon is unsuccessful in this it writes to a backlog and sends the data later.

merlin database

This is a database that includes Nagios object status and status changes. It also contains comments, scheduled downtime etc.

Backend Layout

Describes the workflow of the op5 Monitor backend



Folders and files

About

This chapter describes the different folders of your op5 Monitor system

Table of Content

Folders and files

The main parts of op5 Monitor is located in /opt/monitor in the file system.

Folder	Description
bin/	The monitor daemon binary.
etc/	The op5 Monitor configuration files.
op5/	All o5p specific add-ons.

sbin/	The old CGI files.
share/	Main parts of the old GUI based on the CGIs.
var/	Most logs and the cmd pipe all commands are sent to.

How op5 Monitor works "under the hood"

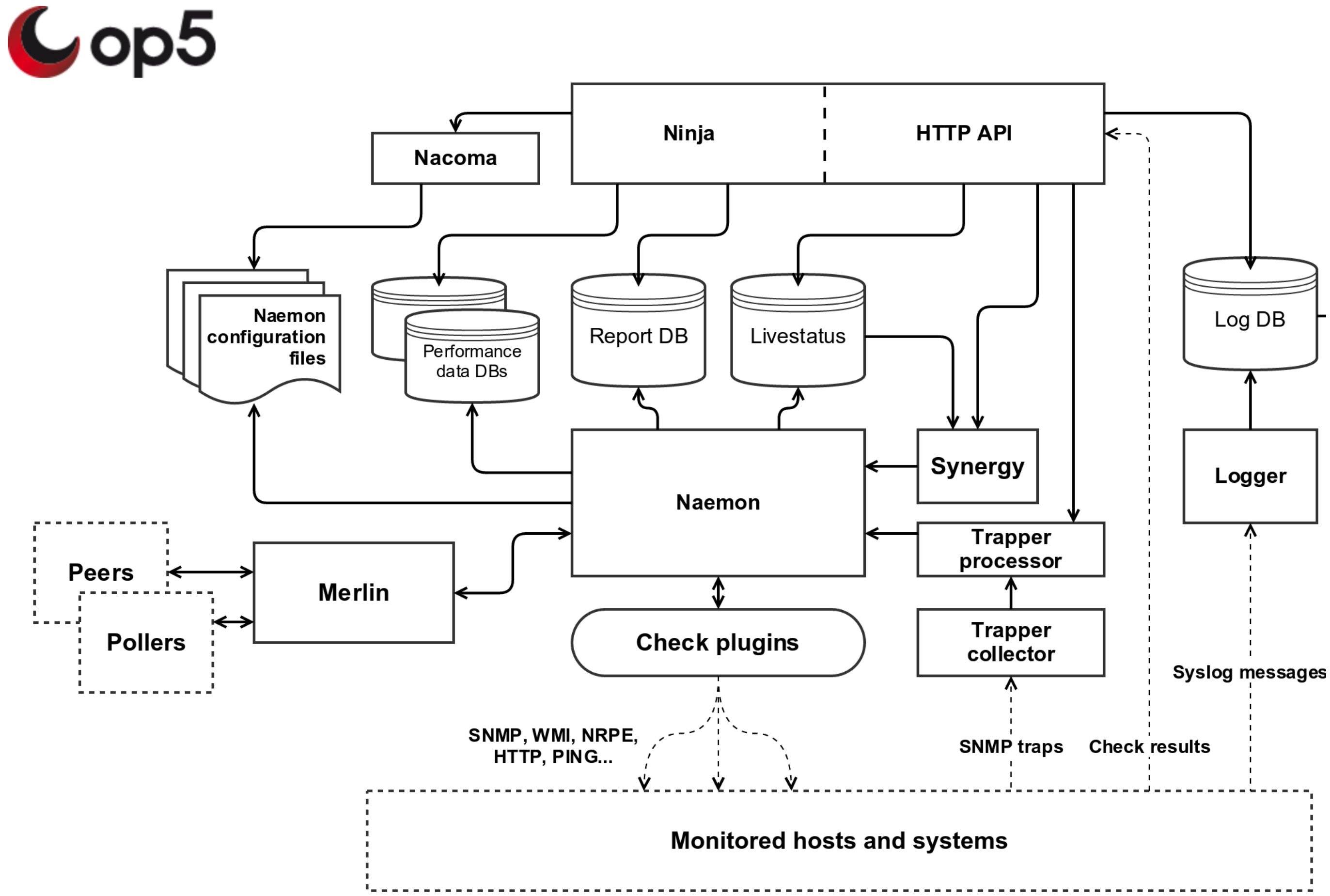
Version
This article was written for version 7.0.9 of op5 Monitor, it could work on both lower and higher version if nothing else is stated.

Articles in the Community-Space are not supported by op5 Support.

Introduction

The purpose of this article is to give the reader a high-level overview of how op5 Monitor works "under the hood".
It will cover the different components of the product and how they interact with each other.

Overview



This illustration is a simplified version of the components relationships

Components

Below are descriptions of the most critical components included in op5 Monitor:

Naemon -

Naemon is the core of Monitor, responsible for monitoring hosts and triggering notifications.
It's a community developed fork of Nagios 4 core, one of the worlds most used and trusted open source monitoring systems.

Naemon is responsible for scheduling checks, keeping blocking outages and similar,
but the actual monitoring and notifications is handled by plugins.

Monitor includes a lot of check plugins out of the box to monitor systems via common protocols like SNMP, WMI and NRPE,
but can easily be extended to support other applications, thanks to it's compatibility with the Nagios plugin API.

Additional information

- Plugins included in op5 Monitor
- HOW-TO: Developing your own check plugin
- HOW-TO: Installing third-party plugins
- Blog post: op5 on Naemon, Nagios and the future
- The Naemon project website (external)

Merlin -

Merlin is the software component in Monitor responsible for load balancing/high availability and distributed monitoring.
It takes care of tasks like splitting configuration for pollers, making sure checks get spread out over peers and synchronizing object states.

It consists of two parts - a Naemon module and a system daemon.
Merlin uses a custom protocol for exchanging state information and utilizes SSH for configuration management.

Additional information

- Merlin community space
- Distributed monitoring documentation
- Load balanced monitoring documentation
- Merlin work flow and design

Livestatus -

Monitor uses a fork Mathias Kettner's Livestatus, a Naemon module that acts like a in-memory database,
containing real-time information about the states of objects in Naemon and related data.

Livestatus is used by many components inside Monitor, but can also be queried through a UNIX socket or command line tools like "mon".

Additional information

- Livestatus community space
- Documentation for the original version of MK Livestatus (external)

Logger -

The Logger component allows Monitor to receive syslog messages for analysis and storage.
It's built on top of the syslog-ng server and stores log data in a PostgreSQL database and compressed log archives for historical data.

The logs can be viewed and searched in Ninja or queried through the HTTP API.

Additional information

- Logger documentation
- HOW-TO: Monitoring log filters in Monitor 7.0 or higher
- HOW-TO: Using Logger and custom columns for root cause analysis
- Documentation for syslog-ng OSE (external)

Trapper -

Trapper is responsible for handling incoming SNMP traps/notifications.
It consists of two parts - the collector and the processor.

The collector is built on a modified version of snmptrapd and inserts received traps into a MySQL database for processing.
The processor runs a set of user defined rules to handle the trap data and updates a service in Naemon via a passive check result with the status.

Trapper can be managed in Ninja or via the command line tool "traped".

Additional information

- Trapper documentation
- HOW-TO: Getting started with op5 Trapper
- Manual page for snmptrapd configuration (external)

Synergy -

Synergy, also known as Business Service Management (BSM),
analyze information from hosts and services in Naemon to determine a high level business/service delivery status.

It queries the Livestatus database for status information and runs a set of user defined rules to determine the state of a business object.
The business object can be "materialized" as service on a host, which will result in Synergy sending passive check results to Naemon.
This allows you to include the business objects in reports and configure alerting/event handlers for them.

Synergy can be configured in Ninja under "Business Services" or with configuration files.

Additional information

- Business Services documentation
- Business Service monitoring manual
- HOW-TO: 4 steps to turn on simple BSM in your system
- Webinar: Introduction to Business Services Management in op5 Monitor

Ninja -

Ninja is the web interface for Monitor.
It gives users the ability to view status information and monitoring metrics for hosts and service,
search for log patterns, configure business services, generate reports and similar.

Additional information

- Ninja community space

Nacoma -

Nacoma is the graphical utility for Naemon object configuration and various other aspects of Monitor,
like user permissions and management packs.
It provides tools like clone and propagate that help the users work efficiently and keeps a change log containing which users made what changes.

Nacoma stores it's settings in a MySQL database and compiles Naemon configuration files for objects after each save.

It's currently embedded inside Ninja and works as the back-end for object configuration in the HTTP API.

Additional information

- Configuration tool documentation
- Power-user tools and features in Nacoma

HTTP API -

The HTTP API provides a RESTful interface for interacting with Monitor.
It can be used to query the status of hosts and services, extract event information and performance metrics, submit check results, change configuration and similar.

The HTTP API is a great tool for build integrations with third-party systems like reporting engines, management systems and dashboards.

Additional information

- HTTP API documentation
- HOW-TO: Submitting status updates through the HTTP API

.How op5 Monitor works "under the hood" v2015.d

Version

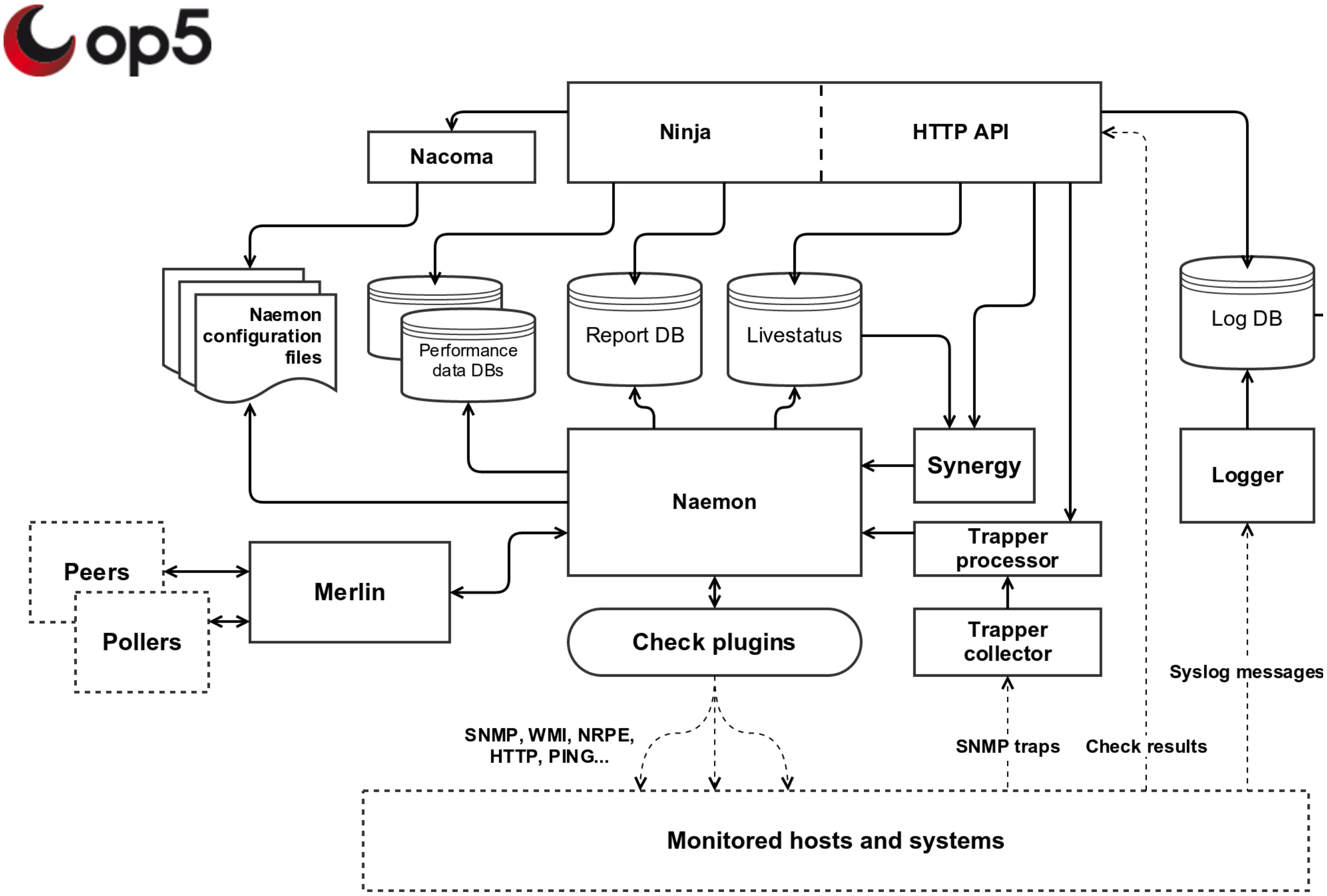
This article was written for version 7.0.9 of op5 Monitor, it could work on both lower and higher version if nothing else is stated.

Articles in the Community-Space are not supported by op5 Support.

Introduction

The purpose of this article is to give the reader a high-level overview of how op5 Monitor works "under the hood".
It will cover the different components of the product and how they interact with each other.

Overview



This illustration is a simplified version of the components relationships

Components

Below are descriptions of the most critical components included in op5 Monitor:

Naemon -

Naemon is the core of Monitor, responsible for monitoring hosts and triggering notifications.
It's a community developed fork of Nagios 4 core, one of the worlds most used and trusted open source monitoring systems.

Naemon is responsible for scheduling checks, keeping blocking outages and similar,
but the actual monitoring and notifications is handled by plugins.

Monitor includes a lot of check plugins out of the box to monitor systems via common protocols like SNMP, WMI and NRPE,
but can easily be extended to support other applications, thanks to it's compatibility with the Nagios plugin API.

Additional information

- Plugins included in op5 Monitor
- HOW-TO: Developing your own check plugin
- HOW-TO: Installing third-party plugins
- Blog post: op5 on Naemon, Nagios and the future
- The Naemon project website (external)

Merlin -

Merlin is the software component in Monitor responsible for load balancing/high availability and distributed monitoring.
It takes care of tasks like splitting configuration for pollers, making sure checks get spread out over peers and synchronizing object states.

It consists of two parts - a Naemon module and a system daemon.
Merlin uses a custom protocol for exchanging state information and utilizes SSH for configuration management.

Additional information

- Merlin community space
- Distributed monitoring documentation
- Load balanced monitoring documentation
- Merlin work flow and design

Livestatus -

Monitor uses a fork Mathias Kettner's Livestatus, a Naemon module that acts like a in-memory database,
containing real-time information about the states of objects in Naemon and related data.

Livestatus is used by many components inside Monitor, but can also be queried through a UNIX socket or command line tools like "mon".

Additional information

- Livestatus community space
- Documentation for the original version of MK Livestatus (external)

Logger -

The Logger component allows Monitor to receive syslog messages for analysis and storage.
It's built on top of the syslog-ng server and stores log data in a PostgreSQL database and compressed log archives for historical data.

The logs can be viewed and searched in Ninja or queried through the HTTP API.

Additional information

- Logger documentation
- HOW-TO: Monitoring log filters in Monitor 7.0 or higher
- HOW-TO: Using Logger and custom columns for root cause analysis
- Documentation for syslog-ng OSE (external)

Trapper -

Trapper is responsible for handling incoming SNMP traps/notifications.
It consists of two parts - the collector and the processor.

The collector is built on a modified version of snmptrapd and inserts received traps into a MySQL database for processing.
The processor runs a set of user defined rules to handle the trap data and updates a service in Naemon via a passive check result with the status.

Trapper can be managed in Ninja or via the command line tool "traped".

Additional information

- Trapper documentation
- HOW-TO: Getting started with op5 Trapper
- Manual page for snmptrapd configuration (external)

Synergy -

Synergy, also known as Business Service Management (BSM),
analyze information from hosts and services in Naemon to determine a high level business/service delivery status.

It queries the Livestatus database for status information and runs a set of user defined rules to determine the state of a business object.

The business object can be "materialized" as service on a host, which will result in Synergy sending passive check results to Naemon.
This allows you to include the business objects in reports and configure alerting/event handlers for them.

Synergy can be configured in Ninja under "Business Services" or with configuration files.

Additional information

- Business Services documentation
- Business Service monitoring manual
- HOW-TO: 4 steps to turn on simple BSM in your system
- Webinar: Introduction to Business Services Management in op5 Monitor

Ninja -

Ninja is the web interface for Monitor.
It gives users the ability to view status information and monitoring metrics for hosts and service,
search for log patterns, configure business services, generate reports and similar.

Additional information

- Ninja community space

Nacoma -

Nacoma is the graphical utility for Naemon object configuration and various other aspects of Monitor,
like user permissions and management packs.
It provides tools like clone and propagate that help the users work efficiently and keeps a change log containing which users made what changes.

Nacoma stores it's settings in a MySQL database and compiles Naemon configuration files for objects after each save.

It's currently embedded inside Ninja and works as the back-end for object configuration in the HTTP API.

Additional information

- Configuration tool documentation
- Power-user tools and features in Nacoma

HTTP API -

The HTTP API provides a RESTful interface for interacting with Monitor.
It can be used to query the status of hosts and services, extract event information and performance metrics, submit check results, change configuration and similar.

The HTTP API is a great tool for build integrations with third-party systems like reporting engines, management systems and dashboards.

Additional information

- HTTP API documentation
- HOW-TO: Submitting status updates through the HTTP API

Tweaks

About

Tweaking your system to improve performance can be a good way to use you hardware more efficient.

Table of Content

Ramdisk

A ramdisk can be enabled for storing spools for performance data and checkresults.
By storing these spools on a ramdisk we can lower the disk I/O significantly.

Enable ramdisk

To enabe ramdisk, see The mon command - Ramdisk in the Administrators Manual.

Backup

Backup and Restore

Configuration backup tool

About

The op5 Monitor GUI has got a built-in configuration backup feature. This is not supposed to be a replacement to op5-backup

Table of Content

ⓘ The configuration backup is only backing up the op5 Monitor configuration, nothing else.

Backup/Restore actions

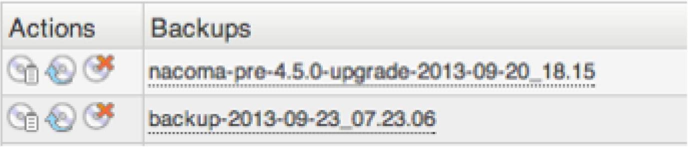
In the list of backups the first column is called **ACTIONS**. This is the functions you will find there, from the left to the right:
View what files are included in the backup.
Restore the backup
Delete the backup.

Backing up the configuration

1. Click Backup/Restore in the main menu.

2. Click **Save your current op5 Monitor configuration**.

3. Now your backup is created and can be restored at any time you like.



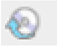
Actions	Backups
	nacoma-pre-4.5.0-upgrade-2013-09-20_18.15
	backup-2013-09-23_07.23.06

4. Click the backup archive name to download and save the backup archive somewhere else.

Restoring a configuration backup

1. Click Backup/Restore in the main menu.

2. Click restore icon on the configuration backup you like to restore.



The backup has now been restored.

op5-backup

About

The op5-backup script is a script that backs up the op5 installation.

⚠ It does not backup the operating system nor does it include logger data.

Table of Content

Configuration

The configuration for op5-backup is located in:

```
/etc/op5-backup/main.conf
```

op5-backup support local or ftp/sftp backup. Local backup can be done to a mounted share.

Create a backup

Creating a full backup

A full backup will back up the following (if installed):

- op5-system
- op5-monitor
- op5-plugins
- Docuwiki
- Logserver
- Trapper

To run a full backup of your op5 server type in the console:

```
op5-backup
```

If you like to run the interactive op5-backup, use the -i option:

```
op5-backup -i
```

The backup file will be stored in the location specified in the configuration file.

Creating a custom backup

It is possible to exclude or include different modules in a backup.
To get a list of the different modules type:

```
ls /etc/op5-backup/modules/legacy
```

To create a backup that excludes a specific module type:

```
op5-backup – -<module1> -<module2>
```

To create a backup that includes only the specified modules type:

```
op5-backup – +<module1> +<module2>
```

Creating a change arch backup

A change arch backup is used when i.e backing up a 32-bits system and restore it on a 64-bits system.
To create a change arch backup type:

```
op5-backup -m charch
```

It is also possible to combine this with the include/exclude modules option.
I.e we what to create a backup of a 32-bit system with the system configuration to restore that on a 64-bits system.

```
op5-backup -m charch – -op5-system
```

⚠ A change arch backup will convert all graphs, in a large installation with a lot of history this can take up to a couple of hours.

Restoring a backup

To restore a full backup type:

```
op5-restore -b <path to backup file>
```

ⓘ Only do a full restore when using a local terminal. Do not restore via SSH. The session will be lost if the network service is restarted.

Verify a backup

It is very good practice to verify the backups from time to time. Especially after a manual backup.
This is done using SSH or the console of the op5 server.

```
tar vft <backup-file>
```

Depending on what modules was used for the backup the list will vary. This is an example of a migration backup:

```
rw-r r- root/root 1476847 2013-05-08 08:23 dokuwiki.tar.gz
rw-r r- root/root 514982 2013-05-08 08:23 migrate.tar.gz
rw-r r- root/root 296954 2013-05-08 08:23 nagios-plugins.tar.gz
rw-r r- root/root 1052 2013-05-08 08:23 op5-geomap.tar.gz
rw-r r- root/root 26274 2013-05-08 08:23 op5-logserver-3.tar.gz
rw-r r- root/root 27206917 2013-05-08 08:24 op5-monitor.tar.gz
rw-r r- root/root 142 2013-05-08 08:24 op5-notify.tar.gz
rw-r r- root/root 409 2013-05-08 08:24 op5-synergy.tar.gz
rw-r r- root/root 203002 2013-05-08 08:24 op5-system.tar.gz
rw-r r- root/root 1917 2013-05-08 08:24 ssh.tar.gz
rw-r r- root/root 4 2013-05-08 08:24 version
rw-r r- root/root 16 2013-05-08 08:24 timestamp
rw-r r- root/root 7 2013-05-08 08:24 architecture
rw-r r- root/root 8 2013-05-08 08:24 mode
rw-r r- root/root 7 2013-05-08 08:24 archive
drwxr-xr-x root/root 0 2013-05-08 08:24 modules/
rw-r r- root/root 147 2013-05-08 08:23 modules/op5-geomap
rw-r r- root/root 3284 2013-05-08 08:23 modules/op5-monitor
rw-r r- root/root 136 2013-05-08 08:24 modules/op5-notify
rw-r r- root/root 518 2013-05-08 08:24 modules/op5-system
rw-r r- root/root 865 2013-05-08 08:23 modules/op5-logserver-3
rw-r r- root/root 5813 2013-05-08 08:23 modules/migrate
rw-r r- root/root 116 2013-05-08 08:24 modules/ssh
rw-r r- root/root 165 2013-05-08 08:24 modules/op5-synergy
rw-r r- root/root 646 2013-05-08 08:23 modules/dokuwiki
rw-r r- root/root 177 2013-05-08 08:23 modules/nagios-plugins
```

Deleting a backup

Deleting a backup is really easy. It is just a matter of deleting the backup file. If the backup files are stored on the op5-server enter

```
rm <backup-file>
```

Or if the file is stored on a network share, you can browse the network share from any computer to delete the file.

Business Service

Introduction

The business process view is designed to combine your IT monitoring and your business service management (BSM) to give an overview of the applications and/or services that your organisation is providing either to customers or internally.

Business services

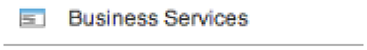
About

A business object is a group that can be populated with hosts and services from hosts and host groups.
It is also possible to add sub-groups that can have their own rule-set.

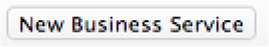
Table of Content

Creating a new group

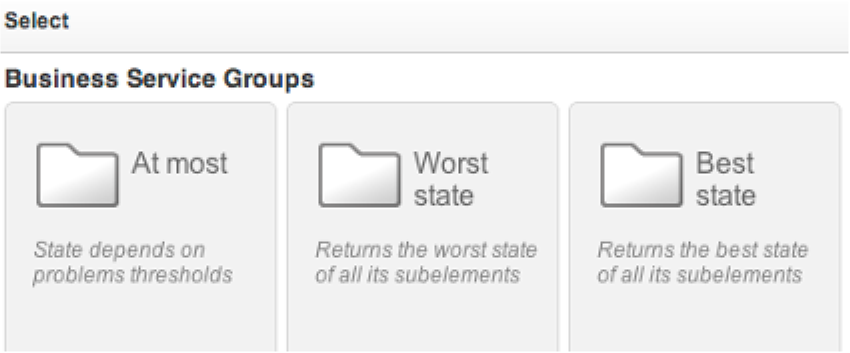
To create a new group go to "Business Process" in the menu.



Click on the "New Object" button at top-right area



Select rule for your business process group



Select

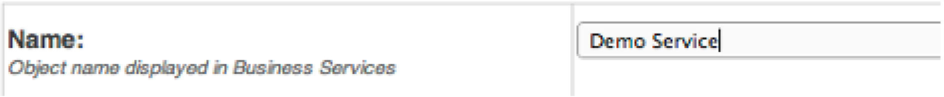
Business Service Groups

At most — State depends on problems thresholds

Worst state — Returns the worst state of all its subelements

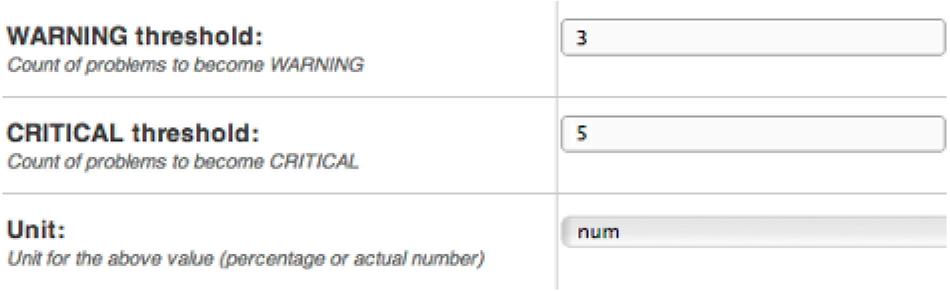
Best state — Returns the best state of all its subelements

Fill in the name of the group



Name: *Object name displayed in Business Services*: Demo Service

Enter the parameters of the rule, if any.



WARNING threshold: *Count of problems to become WARNING*: 3

CRITICAL threshold: *Count of problems to become CRITICAL*: 5

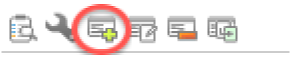
Unit: *Unit for the above value (percentage or actual number)*: num

Click on the "Create" button

Click on the "Save" icon.

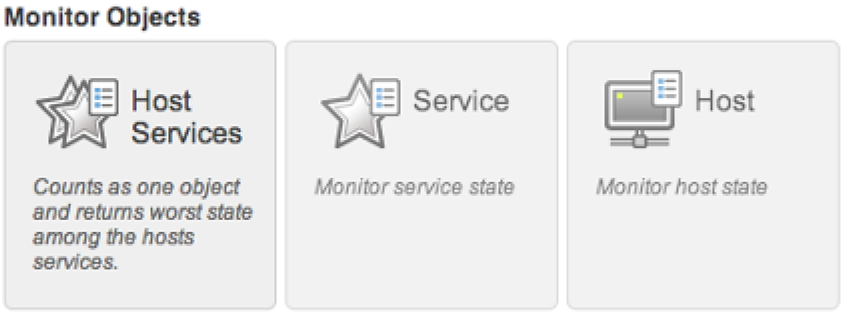
Creating a sub-element

A sub-element is either a service, a host or another group with it's own rule-set.
To add the sub-element click "add sub-element" icon in actions icons column



Add a monitored object

Select what type of object you what to add. In the example below we use **Service**



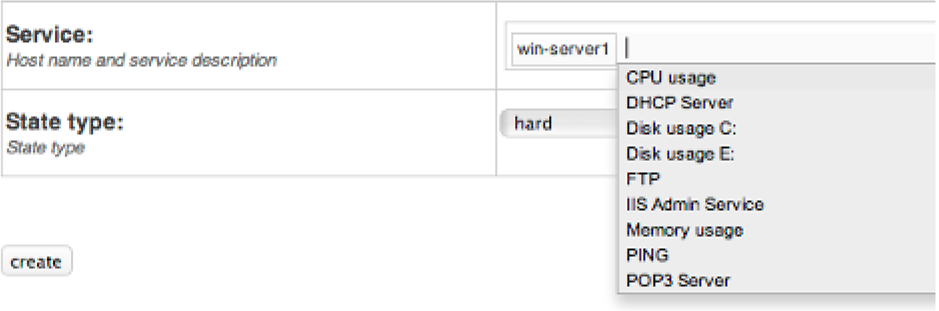
Monitor Objects

Host Services — Counts as one object and returns worst state among the hosts services.

Service — Monitor service state

Host — Monitor host state

Select which object by clicking in the empty text field and select you object from the drop-down menu.



Service: *Host name and service description* — win-server1

State type: *State type* — hard

Click on the "Save" icon.

💾

Add a group as sub-element

Select the type of rule-set the group shall have. Then follow the steps in *Creating a new group*.

Rules types

There are currently 6 different rule types to choose from, each group has their unique rule set.

Group	Description
Worst state	Returns the worst state of all its sub-elements
Best state	Returns the best state of all its sub-elements
Simple at least	Returns OK if at least one sub-element are OK
At least	Returns OK if at least X sub-elements are ok and WARNING if Y sub-elements is OK.
Scores	The state depends on the number of points scored by its sub-elements.
Custom	Custom rules sets can be created.

Worst state

Group state will be the worst state of all its sub-elements

Examples

Worst State of {OK, WARNING, CRITICAL} => CRITICAL
Worst State of {OK, WARNING, CRITICAL, UNKNOWN} => UNKNOWN

Best state

Group state will be the best state of all its sub-elements

Examples

Best State of {WARNING, CRITICAL} => WARNING
Best State of {OK, WARNING, CRITICAL, UNKNOWN} => OK

Simple At least

Means to express the idea that you need some amount of services up and running for the delivered service to be functional. The number of sub-elements that has to be OK is specified in percentage or actual amount. If the number of sub-elements that are OK are equal or more than the at-least number or percentage then the group will be OK, or else the group will get the worse state of its sub-elements.

Examples

Simple At least(2, num) of {OK, OK, CRITICAL, CRITICAL} => OK

Simple At least(3, num) of {OK, OK, WARNING, CRITICAL} => CRITICAL
Simple At least(3, num) of {OK, OK, WARNING, WARNING} => WARNING
Simple At least(50, %) of {OK, OK, WARNING, CRITICAL} => OK
Simple At least(50, %) of {OK, OK, WARNING, CRITICAL, CRITICAL} => CRITICAL

At least

Means to express the idea that you need some amount of services up and running to be functional and lesser amount to be semi-functional (e.g. with degraded performance). Two thresholds are specified, percentage or actual among is possible:
If the number of OK sub-elements is grater or equal than the OK threshold then group is OK
If the number of OK sub-elements is less then the OK threshold but greater or equal than the WARNING threshold then group is WARNING
If number of OK sub-elements is less then the WARNING threshold then group is CRITICAL

Examples

At least(2,1,num) of {OK, OK, WARNING, CRITICAL} => OK
At least(3,2,num) of {OK, OK, WARNING, CRITICAL} => WARNING
At least(3,2,num) of {OK, WARNING, WARNING, CRITICAL} => CRITICAL
At least(3,2,num) of {OK, WARNING, WARNING, WARNING} => CRITICAL

At most

Means to express the idea that you can tolerate some amount of problems. Two thresholds are specified either in percentage or actual among.
If number of problematic sub-elements is greater or equal to the CRITICAL threshold then group is CRITICAL
If number of problematic sub-elements is less than CRITICAL threshold but greater or equal to the WARNING threshold then group is WARNING
If number of problematic sub-elements is less than the WARNING threshold then the group is OK

Examples

At most(2,1,num) of {OK, OK, WARNING, CRITICAL} => OK
At most(3,2,num) of {OK, OK, WARNING, CRITICAL} => WARNING
At most(3,2,num) of {OK, WARNING, WARNING, CRITICAL} => CRITICAL
At most(3,2,num) of {OK, WARNING, WARNING, WARNING} => CRITICAL

Scores

Means to express the idea that having several WARNING sub-elements is the same as having few OKs and few CRITICALs. Groups sums the problems points of all its children using:
OK state gives 0 problems points
WARNING = 1
CRITICAL = 2
UNKNOWN = 3
Then checks it against two specified thresholds.
If sum is less than the WARNING points then group is OK
if sum is between the WARNING and CRITICAL points then group is WARNING
if sum is greater or equal than the CRITICAL points then group is CRITICAL

Examples

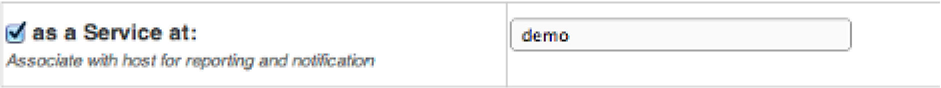
Scores(4,3,num) of {OK, OK, WARNING, CRITICAL} => WARNING
Scores(4,3,num) of {OK, WARNING, WARNING, WARNING} => WARNING
Scores(4,3,num) of {WARNING, WARNING, WARNING, WARNING} => CRITICAL
Scores(4,3,num) of {OK, OK, CRITICAL, CRITICAL} => CRITICAL

Custom rules

It is possible to create your own custom rules. This is done in a script language called LUA.
See chapter custom rules (not yet written).

Publish as a service

It is possible to publish an object as a service of a host. By doing this the object will get the same possibilities as a service in Monitor such as notifications, reports, graphs and so on.
To publish an object edit the object that you want to publish and select "as a service" and the host on which to publish the object.



☑ **as a Service at:** *Associate with host for reporting and notification*	demo

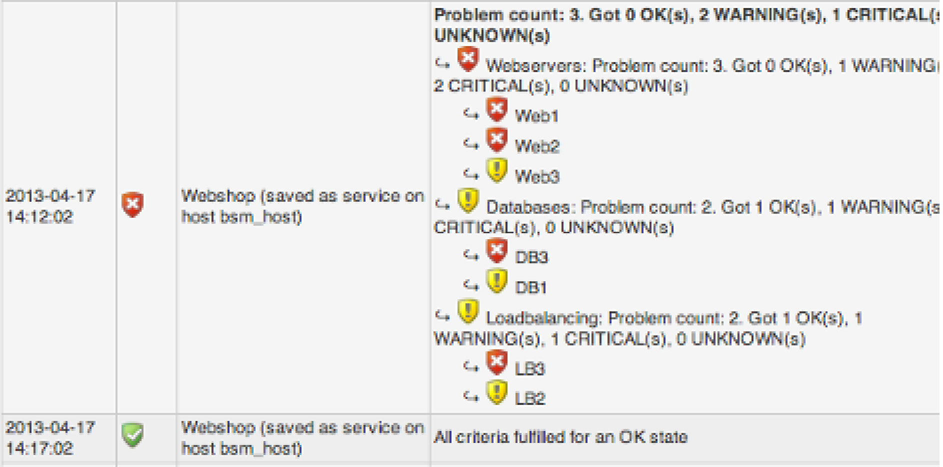
The object will now be found under the host as a service.

Reporting

When creating a SLA or Availability report out of a BSM top level element that has been published to a host it is possible to include the BSM events in that report.
This will show the underlying checks that triggered a WARNING or CRITICAL alert in the BSM.
To enable this choose to include BSM event when creating a report.
If the selected BSM service is not a top level element, no BSM events will be displayed.
To enable this choose to **include BSM event** when creating a report.

☑ Include BSM events

When the report is generated the event will be included in the report.



2013-04-17 14:12:02	☒	Webshop (saved as service on host bsm_host)	**Problem count: 3. Got 0 OK(s), 2 WARNING(s), 1 CRITICAL(s UNKNOWN(s)** ↪ ☒ Webservers: Problem count: 3. Got 0 OK(s), 1 WARNING 2 CRITICAL(s), 0 UNKNOWN(s) ↪ ☒ Web1 ↪ ☒ Web2 ↪ ! Web3 ↪ ! Databases: Problem count: 2. Got 1 OK(s), 1 WARNING(s CRITICAL(s), 0 UNKNOWN(s) ↪ ☒ DB3 ↪ ! DB1 ↪ ! Loadbalancing: Problem count: 2. Got 1 OK(s), 1 WARNING(s), 1 CRITICAL(s), 0 UNKNOWN(s) ↪ ☒ LB3 ↪ ! LB2
2013-04-17 14:17:02	✓	Webshop (saved as service on host bsm_host)	All criteria fulfilled for an OK state

Graphs

Introduction

op5 Monitor is using PNP to create the graphs available for most standard services in the user interface.

PNP is an add-on to nagios which analyzes performance data provided by plugins and stores them automatically into RRD-databases (Round Robin Databases).
PNP only processes performance data built according to the Developer Guidelines for monitoring plugins. With this limitation we want to honour the work of Nagios Plugin Developers who stick to the guidelines.
This is a short description of how to use PNP and it's functions pages and templates.

For more info please refer to the online manual for PNP
http://www.pnp4nagios.org/pnp/start
Kudos to **Joerg Linge** for letting us use his text.

Collections

About

Collections provides the opportunity to collect graphs of different hosts and services on to one page. That way - as an example - you can display the traffic rates of all tape libraries.

Table of Content

Creating a new collection

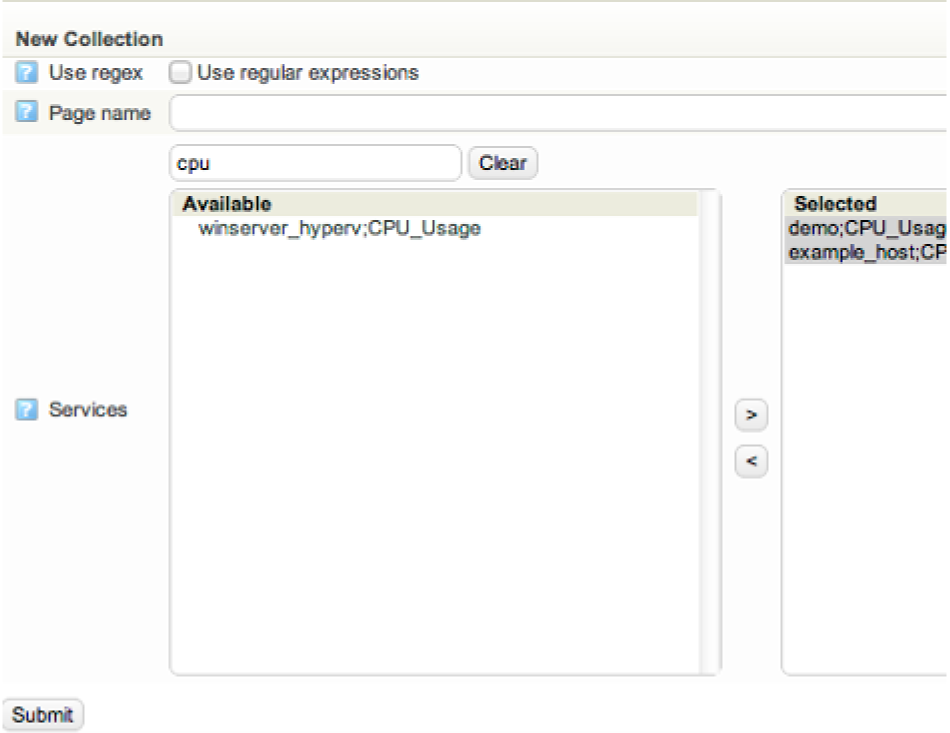
The setup of Graph Collections is done through the configuration page.
Go to Configure and click on the **Graph Collections** icon.

Graph Collections

There are two ways to select which services to show in the graph, either use the GUI to select the services from the list or use regular expressions.

GUI selection

Enter a collection name and select which services to put in the collection by selecting them from the list.


New Collection

Use regex ☐ Use regular expressions

Page name

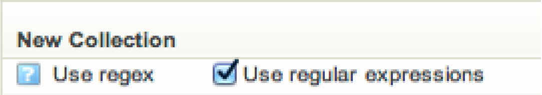
Services: cpu

Available: winserver_hyperv;CPU_Usage

Selected: demo;CPU_Usag
example_host;CP

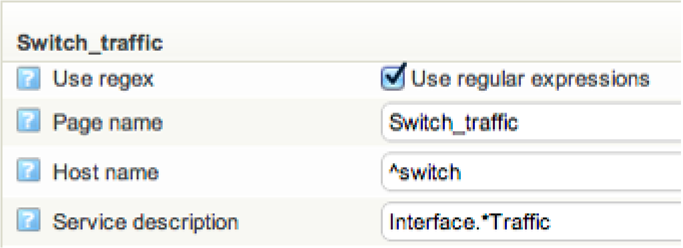
Regex selection

Check the checkbox for **Use regex**


New Collection

Use regex ☑ Use regular expressions

The host and services is now selected by a regular expression.
In the example below we select all graphs from the host which names starts with "switch" and services that contains "Interface" and "Traffic". Note that regular expressions are case sensitive.


Switch_traffic

Use regex ☑ Use regular expressions

Page name: Switch_traffic

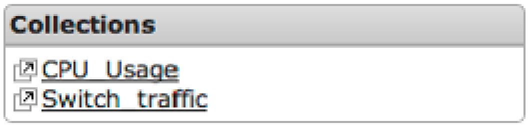
Host name: ^switch

Service description: Interface.*Traffic

Viewing Collections

The collections are found under graphs in the main menu on the left and click on the **Collection icon**

Note that his icon is only visible when at least one collection is created.
All the collections are listed in the panel to the right.



Collections

CPU_Usage
Switch_traffic

Combined Graphs

About

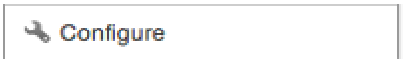
A combined graph overlays several graphs in the same graph which will give a better overview of how two different checks are performing.
It takes one or more service from one or more host and lays them on top of each other in the same graph.

Table of Content

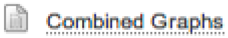
ⓘ The service checks must have the same name on all the hosts for combined graphs to work.

Creating combined graphs

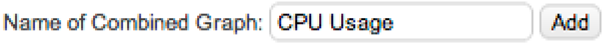
The combined graphs is created though the configuration.
Go to **Configure** in the menu



Click on **Combined Graphs**

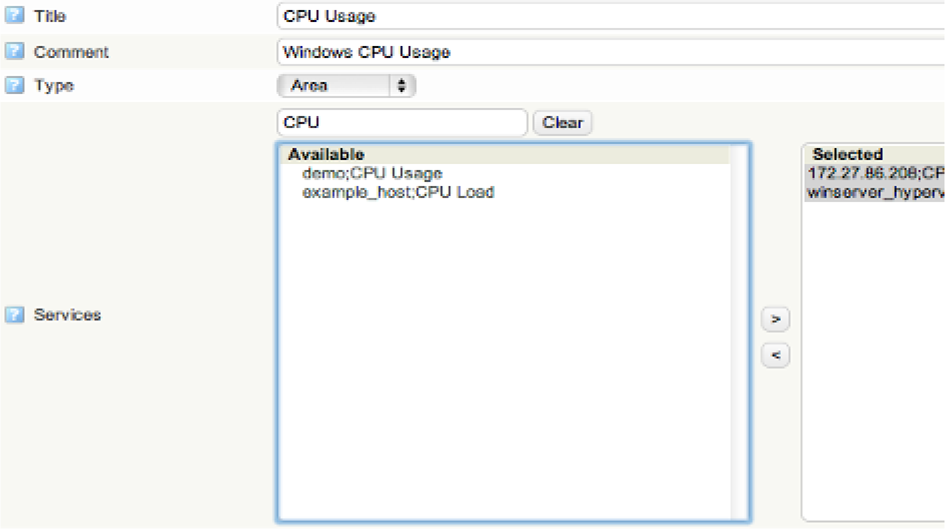


Enter a name of the combined graph and click on **Add**



Name of Combined Graph: CPU Usage

Select the service to graph and from which hosts this service should be fetched from. Also add a name and comment.



Title: CPU Usage

Comment: Windows CPU Usage

Type: Area

Services: CPU

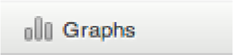
Available
- demo;CPU Usage
- example_host;CPU Load

Selected
- 172.27.86.208;CP
- winserver_hyperv

Click on **Submit**

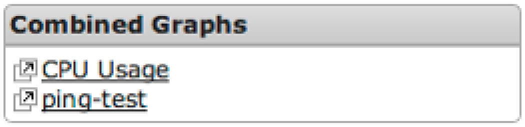
Viewing combined graphs

The combined graphs can be found under **Graphs** in the main menu



and click on the **Combined Graphs** icon.

All the combined graphs can be found under **Combined graphs** in the right side menu.

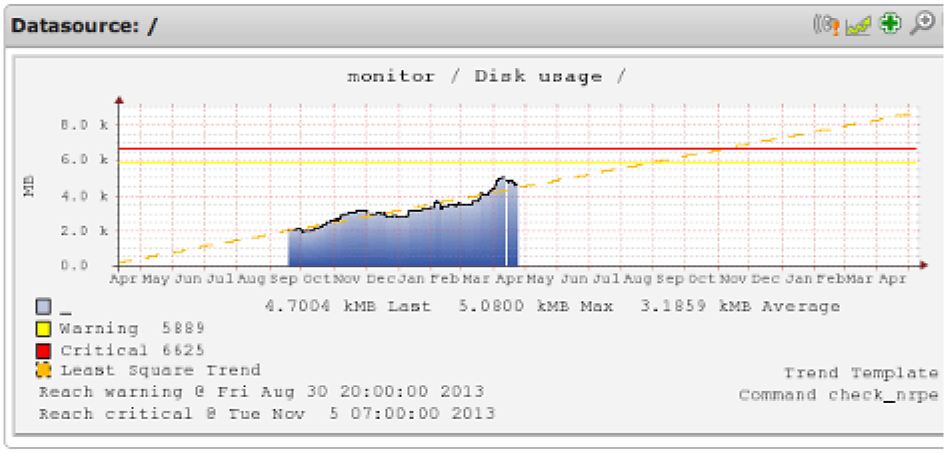


Combined Graphs
- CPU Usage
- ping-test

Graph prediction

About

A graph prediction plots a line across the graph to predict when it will cross the thresholds.

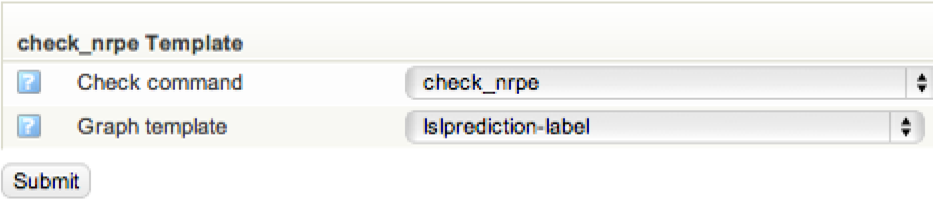


Datasource: /

```
□ _            4.7004 kMB Last   5.0800 kMB Max   3.1859 kMB Average
🟨 Warning  5889
🟥 Critical 6625
🟧 Least Square Trend
Reach warning @ Fri Aug 30 20:00:00 2013                 Trend Template
Reach critical @ Tue Nov  5 07:00:00 2013            Command check_nrpe
```

Activate graph prediction

The graph prediction is not used by default. To enable graph prediction you have to change the template that is used for the specific check command.
Edit the template for the check command, follow instructions in *Changing Graph template*.
Select the template **lslprediction-label** and click on **submit**.



check_nrpe Template

Check command: check_nrpe

Graph template: lslprediction-label

This will change the layout of your graphs.

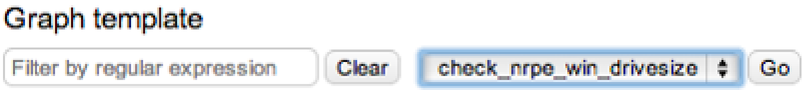
Graph templates

About

Graph templates controls how your graphs look. By changing the template for on check command you can customize how the graph for that check will look.

Changing Graph template

By default a the template default is used for drawing graphs. This can be changed for a specific check command.
To change the template for a check command go to **configuration** and select **graph templates**. Select a template that you would like to modify, then press **go**.

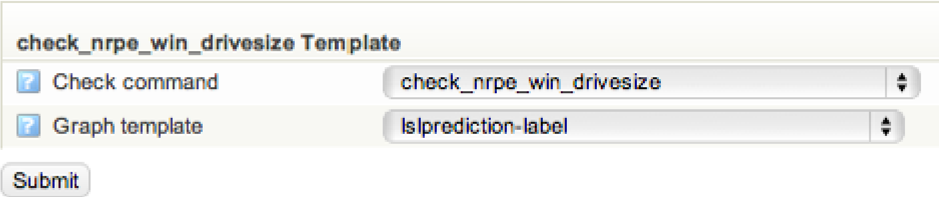


Graph template

Filter by regular expression

check_nrpe_win_drivesize

Select the check command that will use this temple and select the template. There are several templates in the system by default.



check_nrpe_win_drivesize Template

Check command: check_nrpe_win_drivesize

Graph template: lslprediction-label

Graph web front end

About

This article covers the PNP web front-end configuration.

Configuration

The behavior of the PNP web front-end can be controlled through the config file */opt/monitor/etc/pnp/config.php*. This is however not recommended as the file will be overwritten during updates of PNP as the paths and options are detected during ./configure.

If adjustments are needed they should be implemented in:

```
/opt/monitor/etc/pnp/config_local.php
```

If this file does not exist the file config.php can be used as a guideline. All variables will be inherited from config.php unless they are specifically overwritten by config_local.php, i.e. there is no need to copy the entire file in order to change one variable. The file must however always begin with "<?php". The following example shows what the code should look like in order to set the graph width to 1500:

```
<?php

$conf['graph_width'] = "1500";
```

To access the PNP web front end through the GUI click on Graphs in the menu.

Logger

License requirements
The *Pro* or *Ent+* license is required if you want to receive and process logs from external hosts

Introduction

op5 Monitor can act as centralized logging server for event correlation, pattern based alerts and audit purposes.
In this chapter we will cover configuration of the built in *Logger* functionality and look at some client configurations for remote logging.

Configuring Logger clients

Introduction

Logger acts as a syslog server, so any system with remote syslog capabilities can send its logs to your *op5 Monitor* host for storage and analysis.
This chapters covers basic configuration of syslog clients on various platforms like *Microsoft Windows* and *Cisco IOS*.

If your system or device isn't listed in any of the included guides, please refer to the vendor's manual.

Configuring remote logging on UNIX/Linux systems

About

Most UNIX/Linux systems have built-in support for syslog and hence you do not need to install any extra software.

Table of Content

syslogd

On most systems, you will find a config file called */etc/syslog.conf* - this is where you enter the host name or IP address of your op5 Monitor host.
If your op5 Monitor host is on IP address 172.16.32.64, and you want to forward all facilities to it, append the following to /etc/syslog.conf and restart your syslog daemon:

```
. @172.16.32.64
```

Some systems do not understand the **"."** syntax - if this is the case you have to enter all facilities separatly:

auth.*	@172.16.32.64
authpriv.*	@172.16.32.64
cron.*	@172.16.32.64
daemon.*	@172.16.32.64
ftp.*	@172.16.32.64
kern.*	@172.16.32.64
lpr.*	@172.16.32.64
mail.*	@172.16.32.64
mark.*	@172.16.32.64
news.*	@172.16.32.64
security.*	@172.16.32.64
syslog.*	@172.16.32.64
user.*	@172.16.32.64
uucp.*	@172.16.32.64
local0.*	@172.16.32.64
local1.*	@172.16.32.64
local2.*	@172.16.32.64
local3.*	@172.16.32.64
local4.*	@172.16.32.64
local5.*	@172.16.32.64
local6.*	@172.16.32.64
local7.*	@172.16.32.64

Note that on some systems, notably Solaris, the blank between the facility and the receiving host has to be made up of tabs, not spaces.
For details on how to configure syslog.conf, please refer to the manual:
man syslog.conf

syslog-ng

More and more clients use syslog-ng for sending syslog messages to a loghost.
If you use syslog-ng you can benefit from the stability of using TCP connections instead of the standard UDP.
Sample /etc/syslog-ng/syslog-ng.conf to setup logging to loghost:

```
# all known message sources
source s_all {
 # messages generated by Syslog-NG
 internal();
 # standard Linux log source (this is the default place for the syslog() function to send logs to)
 unix-stream("/dev/log");
 # messages from the kernel
 file("/proc/kmsg" log_prefix("kernel: "));
};

# define the destination loghost
destination d_loghost {
 tcp("172.16.32.64" port(514));
};

# send everything to loghost
log {
 source(s_all);
 destination(d_loghost);
};
```

Sending Text Files to Logger

Some applications do not send their logs to syslog, but store them in a file on disk.
Most applications can be configured to use syslog, and changing the configuration of those applications should be your first hand choice.
Another option is using tail and logger to read the log file, and send appended lines to syslog. This command will read /var/log/myapp.log and send it to syslog as facility *daemon* and severity *info*.

```
# tail -f /var/log/myapp.log | logger -p daemon.info
```

You can use a command like the one above for your application, and make sure it is executed in reboot - on many systems this can be done by placing the command in */etc/rc.local*.

If you are running syslog-ng, you can instead of using the above workaround simply define a log source (see the example above under "messages from the kernel" for how to define a file as a log source) and add another log section with that source.

Installing the syslog agent on Microsoft Windows

To make a Windows computer send its logs to your *op5 Monitor* server you have to download and install the *Windows Syslog Agent* from the agent download page.
Windows Syslog Agent sends the Windows Event Log content to the IP address or DNS-name of your *op5 Monitor* system, and can optionally send plain text log files too – for applications that keep their own logs.

You can find the manual for *Windows Syslog Agent* here

Configuring Logger settings

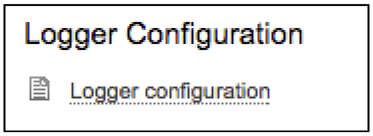
About

The Logger configuration page allows you to tweak storage settings, log rotation and similar.

Table of Content

Configuration

To access the Logger configuration go to the configuration page and click on **Logger Configuration**



Logger Configuration

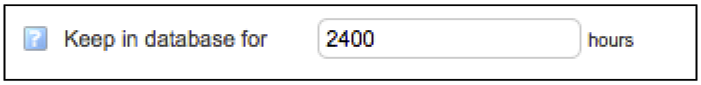
Logger configuration

In Logger configuration you can configure

- Database retention
- Log archive

Database retention

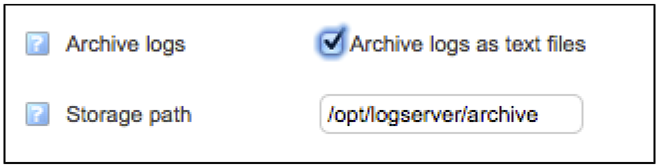
Logs are rotated out from the database when they reach a certain age.
This can be configured using the **Keep in database** option.



Keep in database for 2400 hours

Log Archive

A log archive can be set to store the logs in. The archive will not have any retention time.
To enable log archive check the **Archive logs** checkbox and specify an absolut **storage path** on the op5 Monitor server.



Archive logs ☑ Archive logs as text files

Storage path /opt/logserver/archive

Since the archive will not automatically be rotated logs will be stored indefinitely.

Log Monitoring

If you want to learn about monitoring log patterns, see the "Monitoring log filters in op5 Monitor 7.0 or later"

Notifications

Introduction

In this chapter we will take a deeper look at the notification function in op5 Monitor.
We will look at how the

- notification works
- notification skins works (mail/sms/htmlpost)
- dial up notification works

- snmp trap notification works.

Configuration

Notification can be configured by changing, or creating, the file: `/etc/op5/notify.yml`. At the moment the only possible configuration is setting hostname for notification URL:s. A configuration could look like this:

/etc/op5/notify.yml

```
hostname: 192.168.0.205
```

or like this:

/etc/op5/notify.yml

```
hostname: demo.op5.com
```

Dial-up notification

About

Many of the modern mobile phones are only giving you one tiny signal when a sms arrives. If you are on duty during the night you might not wake up or if you are in a very noisy environment it might take some time for you to notice the arrived sms. There for we have included a dial up notification in op5 Monitor.

Table of Content

Workflow

This is a very simple, but effective, notification that works like this:

Step	Action
1	op5 Monitor is scheduling a notification.
2	The notification goes through all the filters.
3	The notify_dial.pl script is called with the following command line: /opt/monitor/op5/notify/notif_dial.pl <mobilephonenumber>
4	notify_dial.pl is shutting down smsd
5	notify_dial.pl tries to call the <mobilephonenumber> If the line is busy or no one answer the call in 45 seconds notify_dial.pl will hang up and try again two more times before it quits.
6	The user answer the call and notify_dial.pl hangs up.
6	notify_dial.pl is starting up smsd again and the execution is over.

Adding a dial up notification command

This is done in two steps:

- add the command
- configure the contacts

To add a dial up notification command

1. Login to the op5 Monitor user interface and go to **Configure**.
2. Click **Commands**.
3. Add a new command with the following settings:

```
command_name notify_by_dial

command_line $USER3$/notify/notify_dial.pl "$CONTACTPAGER$"
```

4. Click **Apply**.
5. Click **Save**.

Configuring the contacts

To configure the contacts

1. Login to the op5 Monitor user interface and go to **Configure**.
2. Either open up an existing contact and create a new one.
3. On the contact set **Pager** to a phone number on the form like this (***without*** the leading '+'-sign): 46795123123
4. Set **host_notification_commands** and **service_notification_commands** to: notify_by_dial
5. Click **Apply**.
6. Click **Save**.
7. Make sure the contact is a member of the contact_group is associated with the correct objects.

How does notifications work?

About

In the op5 Monitor user manual we describe some of the basics with notifications. Let us take a closer look at how it really works.

Table of Content

Notification filters

When a notification is about to be sent it has to go through a number of filters before op5 Monitor can determine whether a notification really is suppose to be sent or not.

Notification filters

Filter	Description
Program-wide	This tells op5 Monitor if notifications are turned on or not in a program-wide basis.
Service and host filters	- Is the host or service in scheduled downtime or not? - Is the host or service in a flapping state? - Does the host or service notification options says that this type of notification is supposed to be sent? - Are we in the right time period for notifications at the moment? - Have we already sent a notification about this alert? Has the host or service remained in the same non-OK state that it was when the last notification went out?
Contact filters	- Does the contacts notifications options says that this type of notification is supposed to be sent? - Are we in the right time period for notifications at the moment, according to the notification time period set on the contact?

Notification commands

How the notifications are sent is defined in either one of the two files below:

- checkcommands.cfg
- misccommands.cfg

The commands are divided into

- host notification commands
- service notification commands

The notification commands are then using scripts in the same way as the normal check commands does.
All default scripts shipped with op5 Monitor is located in:

```
/opt/monitor/op5/notify
```

Notification macros

Many of the arguments sent to the notification commands are macros. The macros are a sort of variables containing a, in most cases, program-wide value. You can read more about macros in the Nagios manual:
http://nagios.sourceforge.net/docs/3_0/macros.html
One of the most important macro used with notifications is:
`$NOTIFICATIONTYPE$`
This macro tells you what type of notification that is supposed to be sent. The `$NOTIFICATIONTYPE$` macro can have one of the following values.
Notification types

Notification type	**Description**
PROBLEM	A service or host has just entered (or is still in) a problem state.
RECOVERY	A service or host has recovered from a problem state.
ACKNOWLEDGEMENT	A service or host in a problem state has been acknowledged by a user.
FLAPPINGSTART	The host or service has entered a flapping state.
FLAPPINGSTOP	The host or service has left a flapping state.
FLAPPINGDISABLED	The host or service flapping detection has stopped and has there fore left the flapping state.
DOWNTIMESTART	The host or service has entered a scheduled downtime.
DOWNTIMESTOP	The host or service has left a scheduled downtime.
DOWNTIMECANCELLED	The scheduled downtime for a host or service has been cancelled.

The list of macros described in the Nagios manual is very useful when you are working with new notification commands and scripts. That list can be found here: http://nagios.sourceforge.net/docs/3_0/macrolist.html

Notification e-mail sender

Notifications are by default sent from the e-mail address "op5monitor" without any domain. The MTA adds the local domain name, witch by default is "`@localhost.localdomain`".
To change the e-mail address that notification are sent from use the --from argument for the notification command.
To change the sender e-mail address from `op5monitor@localhost.localdomain` to `op5notification@mycompany.com` simply go to the check command for the host-notify and add "`--from op5notification@mycompany.com`" without the "-signs.

```
command_name=host-notify
command_line=$USER3$/notify/poller_notify_send.pl --from op5notification@mycompany.com -c
"$CONTACTNAME$" -h "$HOSTNAME$" -f "$NOTIFICATIONTYPE$" -m "$CONTACTEMAIL$" -p "$CONTACTPAGER$"
"HOSTALIAS=$HOSTALIAS$" "HOSTADDRESS=$HOSTADDRESS$" "HOSTSTATE=$HOSTSTATE$"
"HOSTSTATEID=$HOSTSTATEID$" "HOSTSTATETYPE=$HOSTSTATETYPE$" "HOSTATTEMPT=$HOSTATTEMPT$"
"HOSTLATENCY=$HOSTLATENCY$" "HOSTEXECUTIONTIME=$HOSTEXECUTIONTIME$" "HOSTDURATION=$HOSTDURATION$"
"HOSTDURATIONSEC=$HOSTDURATIONSEC$" "HOSTDOWNTIME=$HOSTDOWNTIME$"
"HOSTPERCENTCHANGE=$HOSTPERCENTCHANGE$" "HOSTGROUPNAME=$HOSTGROUPNAME$"
```

```
"HOSTGROUPALIAS=$HOSTGROUPALIAS$" "LASTHOSTCHECK=$LASTHOSTCHECK$"
"LASTHOSTSTATECHANGE=$LASTHOSTSTATECHANGE$" "LASTHOSTUP=$LASTHOSTUP$" "LASTHOSTDOWN=$LASTHOSTDOWN$"
"LASTHOSTUNREACHABLE=$LASTHOSTUNREACHABLE$" "HOSTOUTPUT=$HOSTOUTPUT$" "HOSTPERFDATA=$HOSTPERFDATA$"
"HOSTACKAUTHOR=$HOSTACKAUTHOR$" "HOSTACKCOMMENT=$HOSTACKCOMMENT$"
"NOTIFICATIONNUMBER=$NOTIFICATIONNUMBER$" "CONTACTALIAS=$CONTACTALIAS$" "DATETIME=$DATETIME$"
"SHORTDATETIME=$SHORTDATETIME$" "DATE=$DATE$" "TIME=$TIME$" "TIMET=$TIMET$"
"HOSTACTIONURL=$HOSTACTIONURL$" "HOSTNOTESURL=$HOSTNOTESURL$" "ADMINPAGER=$ADMINPAGER$"
"ADMINEMAIL=$ADMINEMAIL$" "NOTIFICATIONCOMMENT=$NOTIFICATIONCOMMENT$"
```

This has to be done for the command "`service-notify`" as well.

Notification skins

About

The three basic notifications (email, sms and htmlpost notifications) are all using something called notification skins. The notification skins are templates describing how the notification is supposed to look like when it is sent to its receiver.

Table of Content

Files

If we will take a look at the notify folder we will find the following skins folders:

- skins.htmlpost/
- skins.mail/
- skins.sms/

Each folder contains a number of notification skins divided into host and service notification filters.

- host.ACKNOWLEDGEMENT
- host.FLAPPINGSTART
- host.FLAPPINGSTOP
- host.PROBLEM
- host.RECOVERY
- service.ACKNOWLEDGEMENT
- service.FLAPPINGSTART
- service.FLAPPINGSTOP
- service.PROBLEM
- service.RECOVERY

As you can see there is one skin for the most common notification types.

The content of a notification skin

Let us take a look at what a skin looks like.

The sms service.PROBLEM skin

```
#SERVICEDESC# on #HOSTNAME# is #SERVICESTATE#. #SERVICEOUTPUT#
```

This is a very simple skin. The reason for that is that you can not send too much data with a normal sms.

The mail service.PROBLEM skin

```
From: op5Monitor To: #CONTACTEMAIL# Subject: [op5] #NOTIFICATIONTYPE#: '#SERVICEDESC#' on
'#HOSTNAME#' is #SERVICESTATE#
```

```
#extra_host_vars#
op5 Monitor
Service #NOTIFICATIONTYPE# detected #LASTSERVICESTATECHANGE#. '#SERVICEDESC#' on host '#HOSTNAME#'
has passed the #SERVICESTATE# threshold.
#STATUS_URL#
Additional info;
#SERVICEOUTPUT#
Host: #HOSTNAME# Address: #HOSTADDRESS# Alias: #HOSTALIAS# Status: #HOSTSTATE# Comment:
#NOTIFICATIONCOMMENT#
Service: #SERVICEDESC# Status : #SERVICESTATE# Latency: Check was #SERVICELATENCY# seconds behind
schedule Misc : Check took #SERVICEEXECUTIONTIME# seconds to complete
Additional links (requires configuration);
Host actions: #HOSTACTIONURL# Host notes: #HOSTNOTESURL#Service actions: #SERVICEACTIONURL#
Service notes: #SERVICENOTESURL#
```

The mail notifications can contain a lot more data and there we add a lot more to the mail skin file.
In both The sms service.PROBLEM skin and The mail service.PROBLEM skin you find text like:

- `#SERVICEDESC#`
- `#HOSTNAME#`

That text is called **keywords**.
The keywords will be replaced with the value of a command line argument looking like this:

`FOO=BAR`
So a command line argument like the one above will generate a keyword with the name FOO having the value BAR.

> ⓘ If a notification macro, or other value sent to a corresponding keyword, is missing in the notification command it will not stop the notification from being sent. It is only the replacement that will be missing.

Creating custom notification skins

Sometimes the default notification skins needs to be changed. This shall not be done in the default folders.

To create custom notification skins

Go to the notify folder: `cd /opt/monitor/op5/notify`
Create the custom-skins folder: `mkdir custom-skins`
Copy the skins.* folders to the custom-skins folder: `cp -R skins.* custom-skins/`
Make the changes you like to do and the new skins will be used at directly after you have saved the changes.

SNMP trap notifications

About

op5 Monitor is shipped with the possibility to send notifications as SNMP traps. To start use the SNMP notifications you need to

- add a few new commands
- configure the contacts

Table of Content

Adding SNMP notification commands

Here we need to add two commands one for host notifications and one for service notifications.

To add a SNMP notification command

1. Login to the op5 Monitor user interface and go to **Configure**.
2. Click **Commands**.
3. Add the following new commands with the following settings:

```
command_name host_notify_by_snmp command_line $USER3$/notify/notify_by_snmp.pl -h snmp.trap.host
-C SNMPCOMMUNITY -t nHostNotify "NOTIFICATIONTYPE=$NOTIFICATIONTYPE$"
"NOTIFICATIONNUMBER=$NOTIFICATIONNUMBER$" "HOSTACKAUTHOR=$HOSTACKAUTHOR$"
"HOSTACKCOMMENT=$HOSTACKCOMMENT$" "HOSTNAME=$HOSTNAME$" "HOSTSTATEID=$HOSTSTATEID$"
"HOSTSTATETYPE=$HOSTSTATETYPE$" "HOSTATTEMPT=$HOSTATTEMPT$" "HOSTDURATIONSEC=$HOSTDURATIONSEC$"
"HOSTGROUPNAME=$HOSTGROUPNAME$" "LASTHOSTCHECK=$LASTHOSTCHECK$"
"LASTHOSTSTATECHANGE=$LASTHOSTSTATECHANGE$" "HOSTOUTPUT=$HOSTOUTPUT$"

command_name service_notify_by_snmp command_line $USER3$/notify/notify_by_snmp.pl -h snmp.trap.host
-C SNMPCOMMUNITY -t nSvcNotify "NOTIFICATIONTYPE=$NOTIFICATIONTYPE$"
"NOTIFICATIONNUMBER=$NOTIFICATIONNUMBER$" "SERVICEACKAUTHOR=$SERVICEACKAUTHOR$"
"SERVICEACKCOMMENT=$SERVICEACKCOMMENT$" "HOSTNAME=$HOSTNAME$" "HOSTSTATEID=$HOSTSTATEID$"
"SERVICEDESCRIPTION=$SERVICEDESCRIPTION$" "SERVICESTATEID=$SERVICESTATEID$"
"SERVICEATTEMPT=$SERVICEATTEMPT$" "SERVICEDURATIONSEC=$SERVICEDURATIONSEC$"
"SERVICEGROUPNAME=$SERVICEGROUPNAME$" "LASTSERVICECHECK=$LASTSERVICECHECK$"
"LASTSERVICESTATECHANGE=$LASTSERVICESTATECHANGE$" "SERVICEOUTPUT=$SERVICEOUTPUT$"
```

   Change the following to their correct value, in both commands:

```
snmp.trap.host
SNMPCOMMUNITY
```

4. Click **Apply**.
5. Click **Save**.

Configuring the contacts

To configure the contacts

1. Login to the op5 Monitor user interface and go to **Configure**.
2. Either open up an existing contact or create a new one.
3. Set **host_notification_commands** to: host_notify_by_snmp
4. Set **service_notification_commands** to: service_notify_by_snmp
5. Click **Apply**.
6. Click **Save**.

> Make sure the contact is a member of the contact_group is associated with the correct objects.

op5 Monitor Configuration Tool

Introduction

There are two ways of changing the configuration of the op5 Monitor:

- Editing the configuration files in /opt/monitor/etc.
- Using the web UI **op5 Monitor configuration tool**.

In this chapter we will take a look at how the **op5 Monitor Configuration tool**, from now on called only **Configure**, is used.

Workflow

Most of the configuration in op5 Monitor is saved in configuration files (text files) in /opt/monitor/etc/. The Configure works with a database and this makes it possible to do changes in the configuration without saving it to file before all configuration is done.
The table below describes the workflow.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1</td><td>Configure opens and the configuration files are compared to the data in the database.
<table>
<tr><th>if</th><th>then</th><th>else</th></tr>
<tr><td>The configuration files are newer than the last change of the database</td><td>import the configuration files into the <b>Configure</b> database</td><td>Do Nothing besides open up <b>Configuration</b></td></tr>
</table>
</td></tr>
<tr><td>2</td><td>Edit the configuration</td></tr>
<tr><td>3</td><td>Save the changes to the Configure database by clicking <b>Submit</b> on the object you just added/changed.</td></tr>
<tr><td>4</td><td>When you are done with editing the configuration save the Configure database to the configuration files by clicking <b>Save</b>.</td></tr>
<tr><td>5</td><td>A preflight check is made on the configuration before it is exported to the configuration files.
<table>
<tr><th>if</th><th>then</th><th>else</th></tr>
<tr><td>the preflight check failes</td><td>an error message is displayed and nothing will be exported</td><td>the configuration in the <b>Configure</b> database is exported and op5 Monitor is reloaded.</td></tr>
</table>
</td></tr>
</table>

The basics

About

In The basics section we will take a look at the basic step you need to know when working with **Configure**

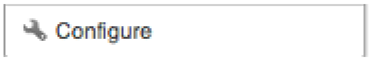
Table of Content

Start working

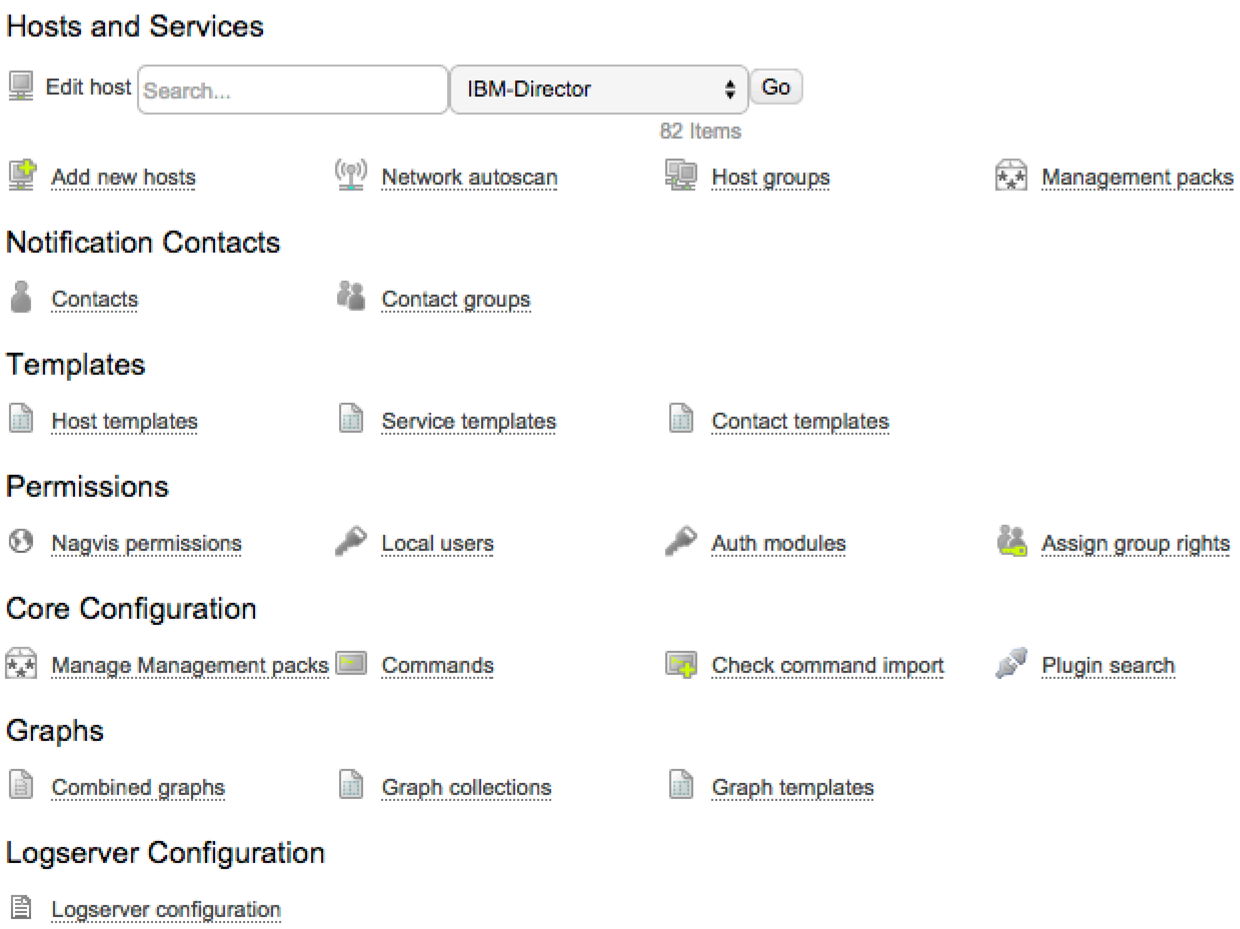
There are many ways to jump in to Configure and start working with the configuration of op5 Monitor.

To start working in Configure

Click **Configure** in the configuration menu



This will take you to the main menu of Configure.



Hosts and Services

Edit host Search... IBM-Director Go

82 Items

Add new hosts | Network autoscan | Host groups | Management packs

Notification Contacts

Contacts | Contact groups

Templates

Host templates | Service templates | Contact templates

Permissions

Nagvis permissions | Local users | Auth modules | Assign group rights

Core Configuration

Manage Management packs | Commands | Check command import | Plugin search

Graphs

Combined graphs | Graph collections | Graph templates

Logserver Configuration

Logserver configuration

Alternative

Click the **Configure** icon found on many object in the monitoring part of op5 Monitor

This will take you directly to the configuration part for the object you clicked on.

Submitting changes

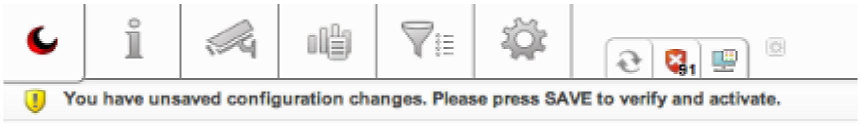
When you have made any changes to an object you have to submit it to the Configure database.

To submit the new configuration to the database

Click **Submit** at the bottom of the page

Submit

As soon as the data has been saved you will get the following warning telling you there is unsaved data in the Configure database.



You have unsaved configuration changes. Please press SAVE to verify and activate.

Continue work until your work is done for this time.

Save the changes

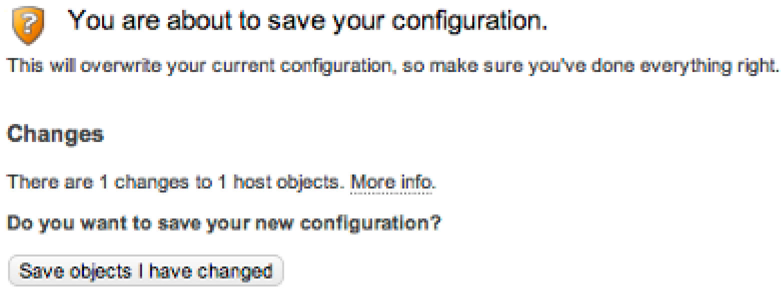
When you have finished working and consider your new configuration is ready to be used by op5 monitor you need to save the changes in

the Configure database to the configuration files.
This will also make op5 Monitor start using the new configuration.

To save the changes and reload op5 Monitor

Click **save** icon at the top of the page.

Before the configuration is saved to disk, you have the opportunity to review the changes.



You are about to save your configuration.

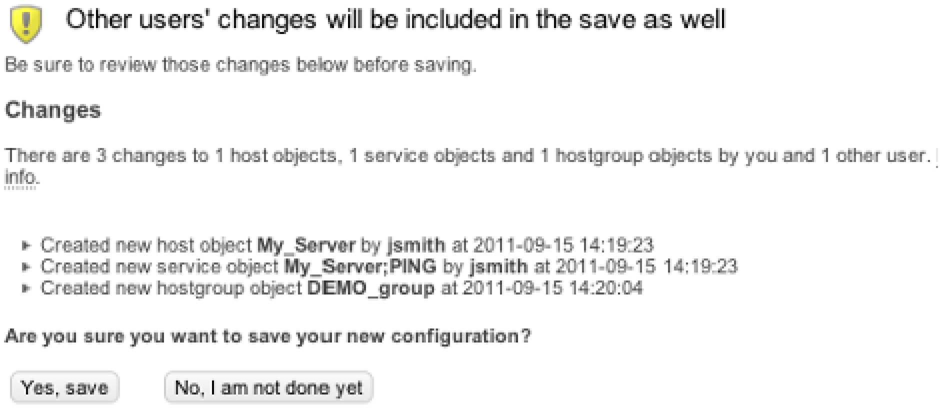
This will overwrite your current configuration, so make sure you've done everything right.

Changes

There are 1 changes to 1 host objects. More info.

Do you want to save your new configuration?

To view what changes that will be written to disk click on **More info**.
If you and another user is doing changes on the same objects that you have access to you will save the other users changes as well. The other users changes will be shown under 'More info' as well.
In the screenshot below you will see an example where we created a new host group and jsmith at the same time added a new host.



Other users' changes will be included in the save as well

Be sure to review those changes below before saving.

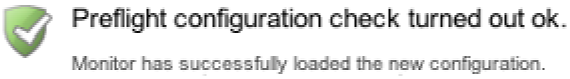
Changes

There are 3 changes to 1 host objects, 1 service objects and 1 hostgroup objects by you and 1 other user.
info.

- Created new host object **My_Server** by **jsmith** at 2011-09-15 14:19:23
- Created new service object **My_Server;PING** by **jsmith** at 2011-09-15 14:19:23
- Created new hostgroup object **DEMO_group** at 2011-09-15 14:20:04

Are you sure you want to save your new configuration?

When done click **Yes, save** to write all the changes to disk.
Now the preflight check is preformed and the data is saved to the configuration files.



Preflight configuration check turned out ok.

Monitor has successfully loaded the new configuration.

⚠ If two users with the same permissions are editing the same host all configuration regarding the host or service will be saved.

Permissions

The save the configuration the user must have export permissions. See Authorization for more information.

Undo changes

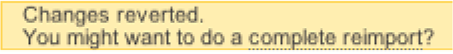
Sometimes it might be handy to reset the configuration to the state it was in where you started to work in Configure. The only thing you have to do then is to undo your changes.

⚠ The undo function will only work as long as you do not have saved the data to the configuration files.

To undo the configuration changes.

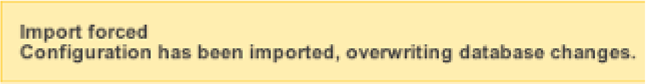
Click **undo** icon at the top of the Configure page.

This will revert the your changes since the last successful preflight check.



Changes reverted.
You might want to do a complete reimport?

To undo all users changes click on **complete reimport**. This will re-read the configuration files and all changes will be reverted. If any changes were made directly into the configurations files these changes will now be loaded in to the web configuration

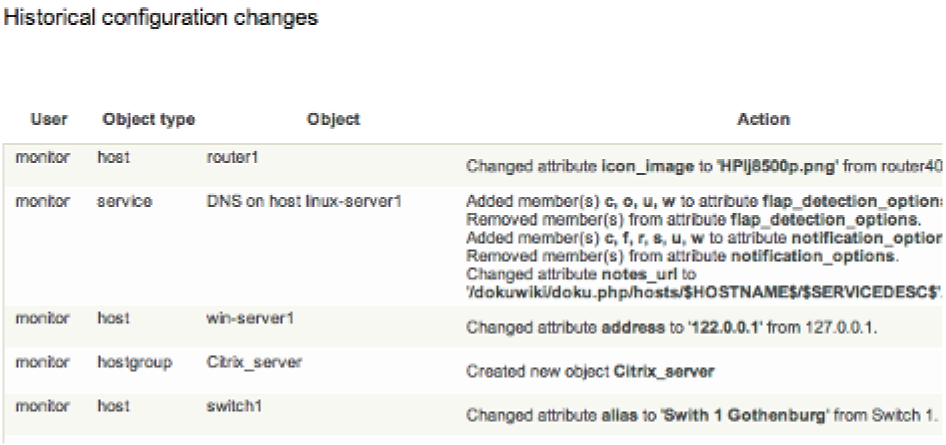


Import forced
Configuration has been imported, overwriting database changes.

Historical Configuration Changes

Historical configuration changes can be used to track changes in the configuration. In the log you will find all changes in the configuration on objects that you have access to.
To access the historical configuration changes log, go to **Configure** and click on the **Historical configuration changes** icon in the upper right corner.

Limited users will only see changes that are made to the hosts and services they are contacts for.
Full access users will see all changes.

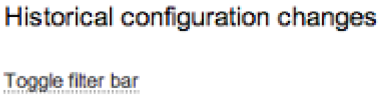


Historical configuration changes

User	Object type	Object	Action
monitor	host	router1	Changed attribute **icon_image** to '**HPlj8500p.png**' from router40
monitor	service	DNS on host linux-server1	Added member(s) **c, o, u, w** to attribute **flap_detection_option** Removed member(s) from attribute **flap_detection_options**. Added member(s) **c, f, r, s, u, w** to attribute **notification_optior** Removed member(s) from attribute **notification_options**. Changed attribute **notes_url** to '**/dokuwiki/doku.php/hosts/$HOSTNAME$/$SERVICEDESC$**'.
monitor	host	win-server1	Changed attribute **address** to '**122.0.0.1**' from 127.0.0.1.
monitor	hostgroup	Citrix_server	Created new object **Citrix_server**
monitor	host	switch1	Changed attribute **alias** to '**Swith 1 Gothenburg**' from Switch 1.

Filter config changes

To filter the configuration changes select **Toggle filter bar**

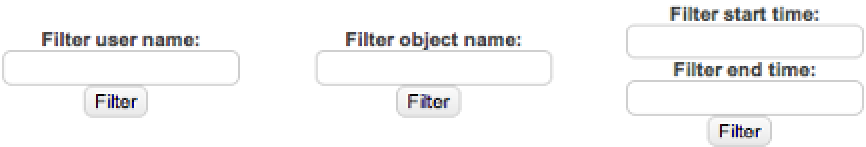


Historical configuration changes

Toggle filter bar

By using the filter bar it is possible to filter on the following:

- User
- Object Name
- Time



Main objects

About

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

- host name
- address
- notifications
- active checks
- etc.

In Configure you can

- add new objects
- modify existing objects
- remove existing objects.

A lot of objects can be cross referenced in the configuration and Configure helps you with this too.
In most of the listings you will find a small text field called **Filter by regular expression**. Use this to filter out the content you are interested in when viewing the different lists.

Table of Content

Required directives

All objects have a list of directives that are required when adding a new object. The other directives can be left out. They will then get the op5 Monitor defaults value.
This does not mean you have to set every directive for every object. One solution is called templates. They make it a lot easier to manage a large set of objects. Read more about templates in Using templates.

Hosts

Hosts are one of the central objects in the monitoring logic. Important attributes of hosts are as follows:

- Hosts are usually physical or virtual devices on your network (servers, workstations, routers, switches, printers, etc) but it could be practically anything you can reach and monitor from the op5 Monitor server.
- Hosts have an address of some kind, IP address or host name.
- Hosts does not need a service directly associated to them, the services can be inherited from a hostgroup. A host can also exist without services.
- Hosts can have parent/child relationships with other hosts, often representing real-world network connections, which is used in the network reachability logic.

Required directives

The following directives are required for a host object.

- host_name
- address
- max_check_attempts
- check_period
- contacts
- contact_groups
- notification_interval

- notification_period

The table below describes the required directives for the host object

Directive	Type	Description
host_name	string	This is the id of the object. I may not contain any space in the value.
alias	string	A more describing name for the object.
address	string	The address the host is reached by, preferably an IP address to make sure the host is reachable even if the DNS is down.
max_check_attempts	integer	Is used to define the number of times op5 Monitor will retry checking the host if it returns any kind of problem state. Setting this value to 1 will cause op5 Monitor alert directly without any retry.
check_period	time_period	During this period the host is checked. It can be any time period defined in op5 Monitor.
contacts	contact	Single contacts used to send notifications to and gives access to this host for users who do not have access to all hosts.
contact_groups	contact_group	Contact groups used to send notifications to and gives access to this host for users who do not have access to all hosts.
notification_interval	integer	Number of minutes between renotifications. Set this to 0 if you only want to have one notification sent out.
notification_period	time_period	During this period the notifications are sent out if any alerts are created. It can be any time period defined in op5 Monitor.

Services

A service can be practically any thing that you can measure and monitor on a host. It is almost only your imagination and programming skills that sets the limit for what you can monitor with a service.
A service

- must be connected to a host
- can check things by tcp, agents, snmp etc.
- use a check command (Commands) to communicate with the plugin (Plugins) that gets all the data.

Required directives

The following directives are required for a service object.

- host_name
- service_description
- check_command
- max_check_attempts
- check_interval
- retry_interval
- check_period
- notification_interval
- notification_period
- contacts
- contact_groups

The table below describes the required directives for the host object

Directive	Type	Description
host_name	host_name object	The host the service is connected to.
service_description	string	This is the id of the object. It must be unique on a host but may be reused on other hosts.
check_command	command object	This is the short name of the command that is executed during service checks.
max_check_attempts	integer	Is used to define the number of times op5 Monitor will retry checking the host if it returns any kind of problem state. Setting this value to 1 will cause op5 Monitor alert directly without any retry.

check_interval	integer	The number of minutes between normal service checks.
retry_interval	integer	The number of minutes between retry checks when a service has gone into a problem state before the state becomes hard.
check_period	time_period	During this period the service is checked. It can be any time period defined in op5 Monitor.
contacts	contact	Single contacts used to send notifications to and gives access to this host for users who do not have access to all hosts.
contact_groups	contact_group	Contact groups used to send notifications to and gives access to this host for users who do not have access to all hosts.
notification_interval	integer	Number of minutes between renotifications. Set this to 0 if you only want to have one notification sent out.
notification_period	time_period	During this period the notifications are sent out if any alerts are created. It can be any time period defined in op5 Monitor.

Contacts

A contact is used for two purposes:

- to send notifications to
- permissions to view a objects in the monitoring part of op5 Monitor.

A contact is not the same as the login account given access rights to the system.

Required directives

The following directives are required for a service object.

- contact_name
- host_notifications_enabled
- service_notifications_enabled
- host_notification_period
- service_notification_period
- host_notification_options
- service_notification_options
- host_notification_commands
- service_notification_commands

The table below describes the required directives for the host object

Directive	**Type**	**Description**
contact_name	string	The id of the contact object.
host_notifications_enabled	yes/no	Used to determine whether or not the contact will receive notifications about host problems and recoveries.
service_notifications_enabled	yes/no	Used to determine whether or not the contact will receive notifications about service problems and recoveries.
host_notification_period	time_period object	The time period when the contact will receive any host notifications.
service_notification_period	time_period object	The time period when the contact will receive any service notifications.
host_notification_options	Down, Unreachable,Recovery, Flapping start and stop, Scheduled downtime start and stop	Used to set what type of host notifications the contact shall receive.
service_notification_options	Critical, Warning, Unknown, Recovery, Flapping start and stop, Scheduled downtime start and stop	Used to set what type of service notifications the contact shall receive.
host_notification_commands	command object	The command used to send the host notifications

service_notification_commands	command object	The command used to send the service notifications.
notification_period	time_period	During this period the notifications are sent out if any alerts are created. It can be any time period defined in op5 Monitor.

Local users

Local users are user accounts that makes it possible to login to the op5 Monitor GUI using the default driver. For more information about drivers see Authentication Integration chapter
Local users does not have any thing to do with notifications or the permissions of viewing objects in op5 Monitor.
Local users can be connected to a contact by giving the username the same name as the id (contact_name) of a contact.
A local user can also be created by checking the box "Configure access rights for this contact" when creating a contact.

Required directives

The following directives are required for a access rights object.

- username
- password

The table below describes the required directives for the host object.

Directive	Type	Description
username	string	The username is the id of the access rights and also used as login username.
password	string	The password is used for the login.

Group Rights

Group rights determents the permission the user will have. For more information about group right, see Authorization.

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

A time period in detail

The following tables describes the directives of a time period and how to use them.
The table below describes the first part of directives of a time period.

Directive/option	Description
timeperiod_name	short name of the time period
alias	descriptive name of the time period
Monday to Sunday	which time to include for each day. you can define multiple times by separating them with comma. Example 00:00-01:00,03:00-06:00
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.
The table below describes the exception part of a time period.

Directive/option	Description
exclude	Other predefined time period definitions that should be excluded from this time period.
Exception type	Specify what type of exception you want to use; Date or Day

The table below describes exception by **Date**:

Directive/option	Description
Interval	Choose Single ate or Date range
Date	Choose the date that is supposed to be used in this Exception.
From date	If you chosen date range you will here set the start date To date.
To date	If you chosen 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 "2012-01-01 - 2012-12-31 / 5" means every fifth day of 2012. • 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 "2012-06-01 / 14" means every 14th day from first of june 2012. 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

The table below describes exception by **Day**:

Directive/option	Description
Interval	Choose Single day or a Day range
Weekday	Choose the weekday that is supposed to be used in this Exception.
From weekday	If you chosen Day range you will here set the start day.
To weekday	If you chosen 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 "2012-01-01 - 2012-12-31 / 5" means every fifth day of 2012. • 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 "2012-06-01 / 14" means every 14th day from first of june 2012. 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

Commands

A command is exactly what it sounds like. It can use macros and arguments. Mostly they are used with services but they can actually be used as

- service or host check command

- notification command
- event handler
- obsession.

Directives

A command has got only two directives

- command_name
- command_line

Directive	Description
command_name	This is the id of the command and also the name shown in Configure.
command_line	is the actual command line used by the services, notifications, event handlers and obsession.

Plugins

Plugins are compiled executable or scripts that can be run from a command line to check the status of a host or service.
There are many plugins included in the op5 Monitor software. A list of the plugins can be found in the **list-of-plugins** at the support section at www.op5.com.
If you are looking for a plugin not found in op5 Monitor by default there are a bunch of other places to look

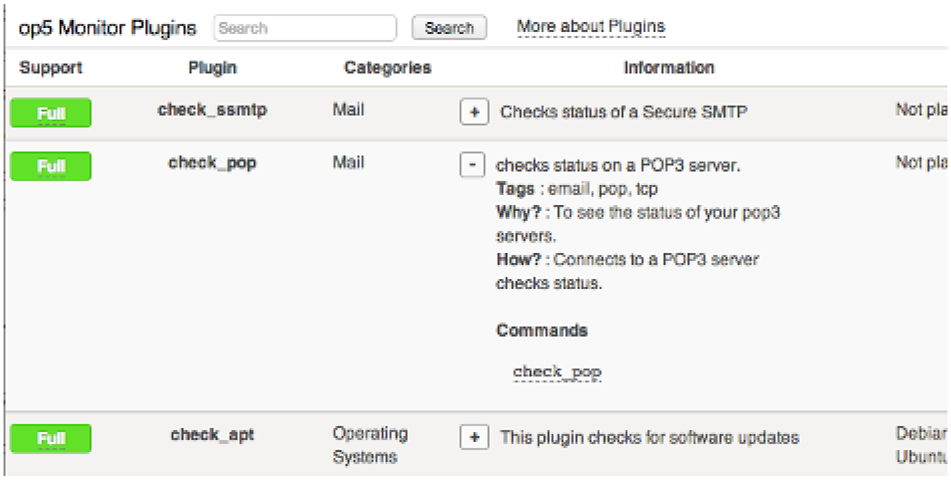
- contact op5 for a specific development
- www.op5.org
- exchange.nagios.org

You can use any plugin written for Nagios but you might need to modify them a bit before they work in the op5 Monitor environment.

Plugin search

To search the plugins that are shipped with op5 Monitor or added afterwards to to **Plugin Search** on the main configuration page

From this page you may
See the support levels of the plugins and see descriptions of the plugins.
The support levels are described in Support levels.



Support	Plugin	Categories	Information	
Full	check_ssmtp	Mail	+ Checks status of a Secure SMTP	Not pla
Full	check_pop	Mail	- checks status on a POP3 server. **Tags** : email, pop, tcp **Why?** : To see the status of your pop3 servers. **How?** : Connects to a POP3 server checks status. **Commands** check_pop	Not pla
Full	check_apt	Operating Systems	+ This plugin checks for software updates	Debiar Ubuntu

Groups

About

The groups in op5 Monitor is used to group objects of the same type. There are three types of groups in op5 Monitor

- host groups
- service groups
- contact groups

They are all good to use to get things a bit more organized and they have also special functions op5 Monitor.
The following subsections will give you a brief description about how they can be used.

Table of Content

Host groups

Host groups can be used group hosts together in any way you like.

- A host can be connected to any number of hosts.
- A host group can be connected to an other host group.

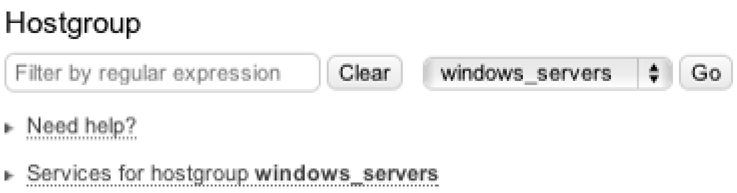
There are a few host groups included in the initial setup of op5 Monitor but you can create your own matching your own needs.
There are a infinite ways of using host groups and here are a couple of examples.
Grouping hosts by

- geographic placements
- what company they belongs to
- who owns the hosts
- who should be able to see the hosts in the group
- function or operating system.

The list can be long.

Services on Host groups

A host group can contain service checks. These service checks will be inherited on all hosts connected to the host group.
A service on a host group work in the same way as a service for a host.
To add a service to a host group go to 'Configure' and 'Host Groups'. Choose the host group you want to add services to then select 'Services for hostgroup'


Hostgroup
Filter by regular expression
Clear
windows_servers
Go
Need help?
Services for hostgroup windows_servers

For example a windows servers host group could contain the checks that are common for all windows servers. By doing this you will only need to change command arguments on the service in the host group instead of changing the arguments on all windows host.
If you add new checks to the service group all hosts in the host group will get the new service once you save your configuration.
If a host group service and a host service should get the same name, the host group service will be used, the host service will still be visible in the configuration and if the host is lifted out from the host group the host service will become active.

Nested host groups

Host groups can be connected to each other.

When nesting host groups together the services on host groups also will inherited to the nested host group. This only work one way.
For example:Host group A has service X and host 1 is a member of host group A Host group B has service Y and host 2 is a member of host group BIf host group B is added as a member of host group A then host 1 will get service Y but host 2 will not get service X.
A good way to use this feature is to have i.e a Windows host group and then a MSSQL host group. When adding the Windows host group as a member to the MSSQL host group the hosts added to MSSQL will get both the service checks that are standard for all Windows host and the default MSSQL service checks.

Service groups

The service groups are used to group services together in the same way as for host groups. On the other hand there is almost no useful at all to for example group service groups by geographic placements.
One good way to use service groups is to create groups containing services needed for a service you deliver to your customers.

- *An email service group*

Let us take a simplified email service and show how the service groups can be used.
To be able to deliver an email service to our customers the following services need to be working:

- *DNS*
- *SMTP*
- *IMAP / POP3*
- *WAN Connection*
- *File Storage*

We take al those services and place them in a service group called Customer email.
If we get a problem with any of the services in the Customer email group we can easily see that the whole email service has got a problem.
The service group in the example above is perfect to use in Service Level Agreement reports (SLA in the op5 Monitor user manual) to make sure we deliver the service as we promised.

Contact groups

Contact groups are mainly used to setup where to send service and host notifications. It can also be used to setup permissions about who should be able to see what object in the op5 Monitor GUI.
The members of a contact group associated with a certain host and/or service are the one that will get all notifications for that object.
A Contact group can be populated with a contact or another contact group.

Permission to host and services

If a user does not has the access rights to see all hosts that user need to have a contact connected to the contact group associated with the host or service the user should be able to see.

Show partial hostgroups

If an unprivileged user is not a contact for all hosts in a hostgroup, he will not be able to see the host group in the "Hostgroup summary/overview/grid" views.
To enable viewing of partial host group edit follow these steps logged in as root:

1. Create and edit the file /opt/monitor/op5/ninja/application/config/custom/groups.php with your favorite editor.
2. Put the following into the file:

```
<?php defined('SYSPATH') OR die('No direct access
allowed.');$config['see_partial_hostgroups'] = true;
```

3. Save the file.

Authorization

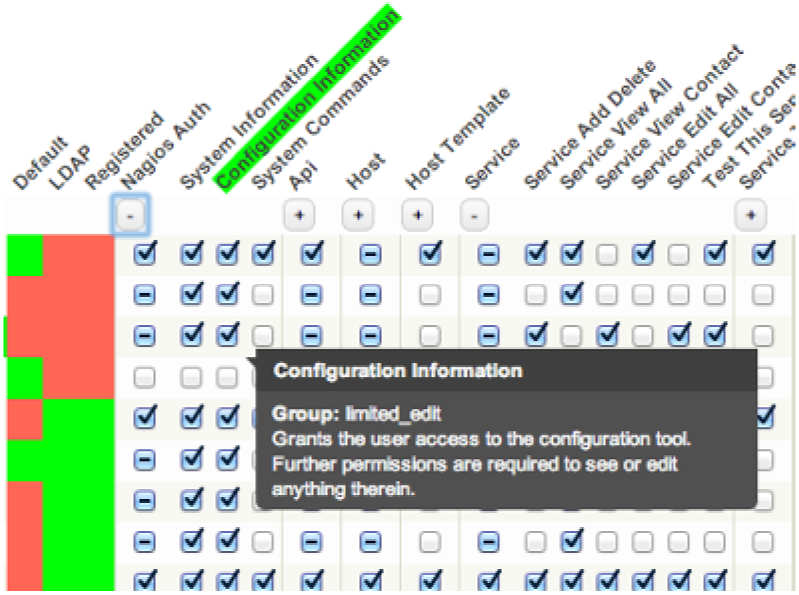
About

The authorization is set under **Assign Group Rights** under configuration.

Table of Content

Group rights

Authorizations are only set on group(s). When an authorization point is hovered a tooltip will appear explaining what the setting does and the corresponding group and setting will be highlighted

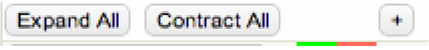


Configuration Information

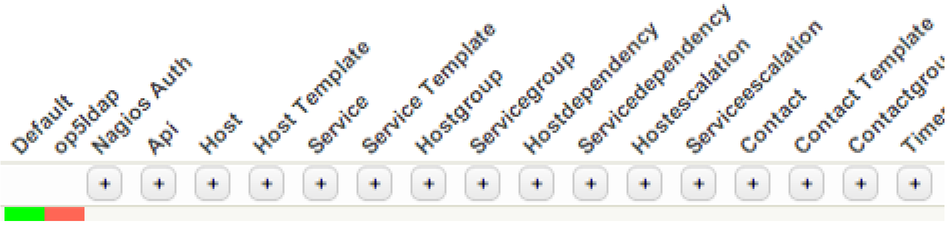
Group: limited_edit
Grants the user access to the configuration tool.
Further permissions are required to see or edit anything therein.

Expand/Contract authorization categories

The authorization categories are contracted by default. You can either choose to expand or contract all categories simultaneously by clicking the **Expand All** and **Contract All** buttons

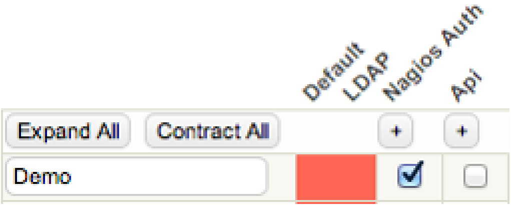


or expand or contract them individually by clicking the +/- sign underneath each category.



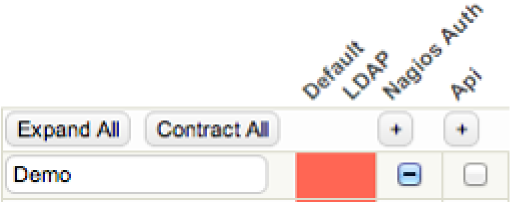
Select/Deselect all rights

To select or de-select all the rights in a group of rights, for example "Host" check the checkbox below the group of rights that you would like to add or remove.



Demo	🟥	☑	☐

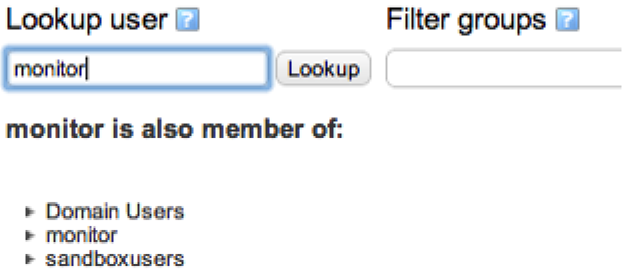
The minus sign ⊟ in the checkbox means that the group of rights is partially selected. Some rights in the group are checked.



Demo	🟥	⊟	☐

Lookup user

You can find out which groups a user is a member of by entering a username in the Lookup user text box and clicking the Lookup button.

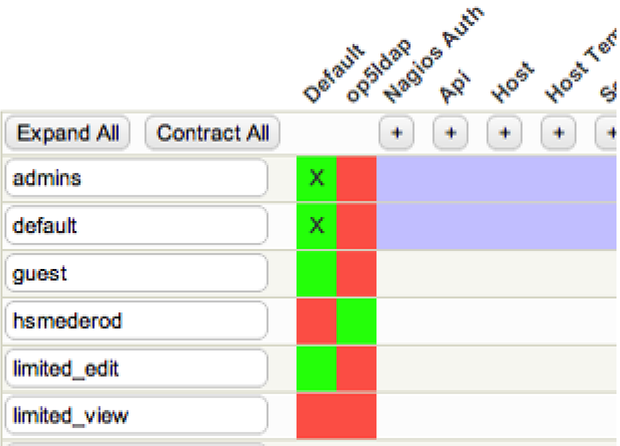


Lookup user: monitor

monitor is also member of:

- Domain Users
- monitor
- sandboxusers

The groups that the user is a member will be highlighted and the authentication driver that they belong to will be indicated with an **X**.

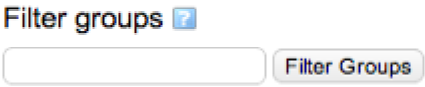


	Default	op5ldap
admins	🟩 X	🟥
default	🟩 X	🟥
guest	🟩	🟥
hsmederod	🟥	🟩
limited_edit	🟩	🟥
limited_view	🟥	🟥

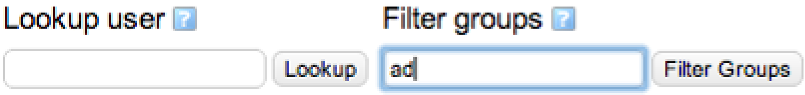
You will also get a list of additional groups the user is a member of underneath the Lookup user text box. An empty search string will hide the list and remove the highlights.

Filter groups

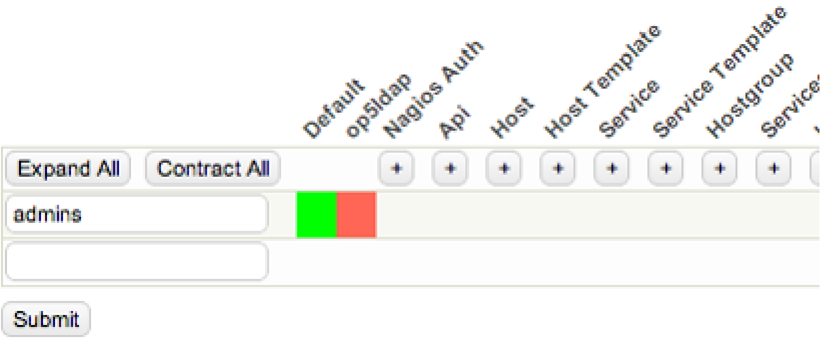
By adding a filter text in the Filter groups text box and clicking Filter groups you can set a filter on the visible groups.



Wildcard characters are neither supported nor needed. For example the filter strings "ad", "a" and "min" will all match a group called "admins".



Filter groups: ad



	Default	op5ldap
admins	🟩	🟥

An empty filter string will reset the filter.

Add, delete, rename groups

Renaming groups is done by typing a new name in the group name text box at the bottom of the table.
In the GUI you can create one new group each submit by filling the blank text box with the group name you want to create.To add a LDAP or AD group type in the name of the group as it is named in your LDAP or AD.
Deletion of groups is done by removing the group name from the text box and leaving it blank when submitting your changes.

Configuration files used by authorization

The file /etc/op5/auth_groups.yml consists of all defined groups and their respective permissions.
The GUI does not have to be used to edit authorization but we recommend that you use it to avoid syntax problems.

Authorization points

System Information

Gives the user access to the system/process information.

Configuration Information

Gives the user access to view and change configuration

System Commands

Gives the user access to issuing commands in the web gui.

Api Command

Gives the user access to the HTTP-API commands interface which allows users to send external to Nagios. Authorized commands are dependent on if the user has 'system_commands' for system wide commands, 'host edit' and 'service edit' for host/service specific commands.

Api Config

Gives the user access to the HTTP-API configuration interface. Requires edit rights on corresponding object type.

Api Status

Gives the user access to the HTTP-API status interface. Requires edit rights on corresponding object type.

Api Report

Grants the user access to the HTTP-API report interface which allows users to fetch report data in a raw and uncorrupted way. Requires edit rights on corresponding object type.

Host Add Delete

Gives the user right to add and delete hosts.

Host View All

Gives the user right to view all hosts.

Host View Contact

Gives the user right to view hosts that he/she is contact for.

Host Edit All

Gives the user right to edit all existing hosts.

Host Edit Contact

Gives the user right to edit hosts that he/she is contact for.

Test This Host

Gives the user right to test the host that is being configured.

Service Add Delete

Gives the user right to add and delete services.

Service View All

Gives the user right to view all services.

Service View Contact

Gives the user right to view services that he/she is contact for.

Service Edit All

Gives the user right to edit all existing services.

Service Edit Contact

Gives the user right to edit services that he/she is contact for.

Test This Service

Gives the user right to test the service that is being configured.

Hostgroup Add Delete

Gives the user right to add and delete hostgroups.

Hostgroup View All

Gives the user right to view all hostgroups.

Hostgroup View Contact

Gives the user right to view hostgroups that he/she is contact for.

Hostgroup Edit All

Gives the user right to edit all existing hostgroups.

Hostgroup Edit Contact

Gives the user right to edit hostgroups that he/she is contact for.

Servicegroup Add Delete

Gives the user right to add and delete servicegroups.

Servicegroup View Al

Gives the user right to view all servicegroups.

Servicegroup View Contact

Gives the user right to view servicegroups that he/she is contact for.

Servicegroup Edit All

Gives the user right to edit all servicegroups.

Servicegroup Edit Contact

Gives the user right to edit servicegroups that he/she is contact for.

Hostdependency Add Delete

Gives the user right to add and delete hostdependencies.

Hostdependency View All

Gives the user right to view hostdependencies.

Hostdependency Edit All

Gives the user right to edit hostdependencies.

Servicedependency Add Delete

Gives the user right to add and delete servicedependencies.

Servicedependency View All

Gives the user right to view servicedependencies.

Servicedependency Edit All

Gives the user right to edit servicedependencies.

Hostescalation Add Delete

Gives the user right to add and delete hostescalations.

Hostescalation View All

Gives the user right to view hostescalations.

Hostescalation Edit All

Gives the user tight to edit hostescalations.

Serviceescalation Add Delete

Gives the user right to add and delete serviceescalations.

Serviceescalation View All

Gives the user right to view serviceescalations.

Serviceescalation Edit All

Gives the user right to edit serviceescalations.

Contact Add Delete

Gives the user right to add and delete contacts.

Contact View All

Gives the user right to view contacts.

Contact Edit All

Gives the user right to edit contacts.

Contactgroup Add Delete

Gives the user right to add and delete contactgrops.

Contactgroup View All

Gives the user right to view contactgroups.

Contactgroup Edit All

Gives the user right to edit contactgroups.

Timeperiod Add Delete

Gives the user right to add and delete timeperiods.

Timeperiod View All

Gives the user right to view timeperiods.

Timeperiod Edit All

Gives the user right to edit timeperiods.

Command Add Delete

Gives the user right to add and delete commands.

Command View All

Gives the user right to view commands.

Command Edit All

Gives the user right to edit commands.

Test This Command

Gives the user right to execute commands.

Template

Gives the user right to view and change templates.

Wiki

Gives the user right to view, create and change docuwiki pages for objects he/she is authorized to see.

Wiki Admin

Gives the user right to access the docuwiki admin panel.

File

Gives the user right to change file in which an object is stored.

Access Rights

Gives the user right to edit access rights.

PNP

Gives the user right to access graphs.

Saved Filters Global

Gives the user right to create and delete global filters for listviews.

Export

Gives the user right to export or save it's own configuration.

Host Template View All

Gives the user right to view host templates.

Host Template Edit All

Gives the user right to edit host templates.

Host Template Add Delete

Gives the user right to add and delete host templates.

Service Template View All

Gives the user right to view service templates.

Service Template Edit All

Gives the user right to edit service templates.

Service Template Add Delete

Gives the user right to add and delete service templates.

Contact Template View All

Gives the user right to view contact templates.

Contact Template Edit All

Gives the user right to edit contact templates.

Contact Template Add Delete

Gives the user right to add and delete contact templates.

Configuration All

Gives the user right to export and import all configuration.

Nagvis Add Delete

Global permission to add and delete all nagvis maps.

Nagvis View

Global permission to view all nagvis maps.

Nagvis Edit

Global permission to edit all nagvis maps.

Nagvis Admin

Get full permission for nagvis, including global configuration

Logger Access

Givs user access to view Logger interface

Logger Configuration

Gives user access to modify Logger configuration

Logger Schedule Archive Search

Gives user access to schedule Logger searches in archived logs

Using templates

About

Even though Configure makes it easy for you to add and change the configuration of op5 Monitor it is still a lot of things to edit and tweak.
To make the software even more easy to use templates have been built in.
There are three types of templates to use:

- host templates
- service templates
- contact templates

op5 Monitor comes with a couple of predefined templates for each object type described above. They are just there to be examples and you should really create your own.

Table of Content

How they work

- Any directive set in a template will be used in the objects using the template. But if you set a directive explicit on an object that value will override the templates.
- Any directive not set in neither a template or directly on the object will have the op5 Monitor default value.
- If you change any value on a directive in a template it will only be valid on the objects where the same directive is not set explicit.

Managing objects

About

Now let us be a bit more hands on. In this section we will take a look at how to add/edit/delete objects using the Configure.
There are sometimes many ways to do things in op5 Monitor but we will only show a few examples.
In the subsections to Managing objects we will assume that you start from the main page of Configure.

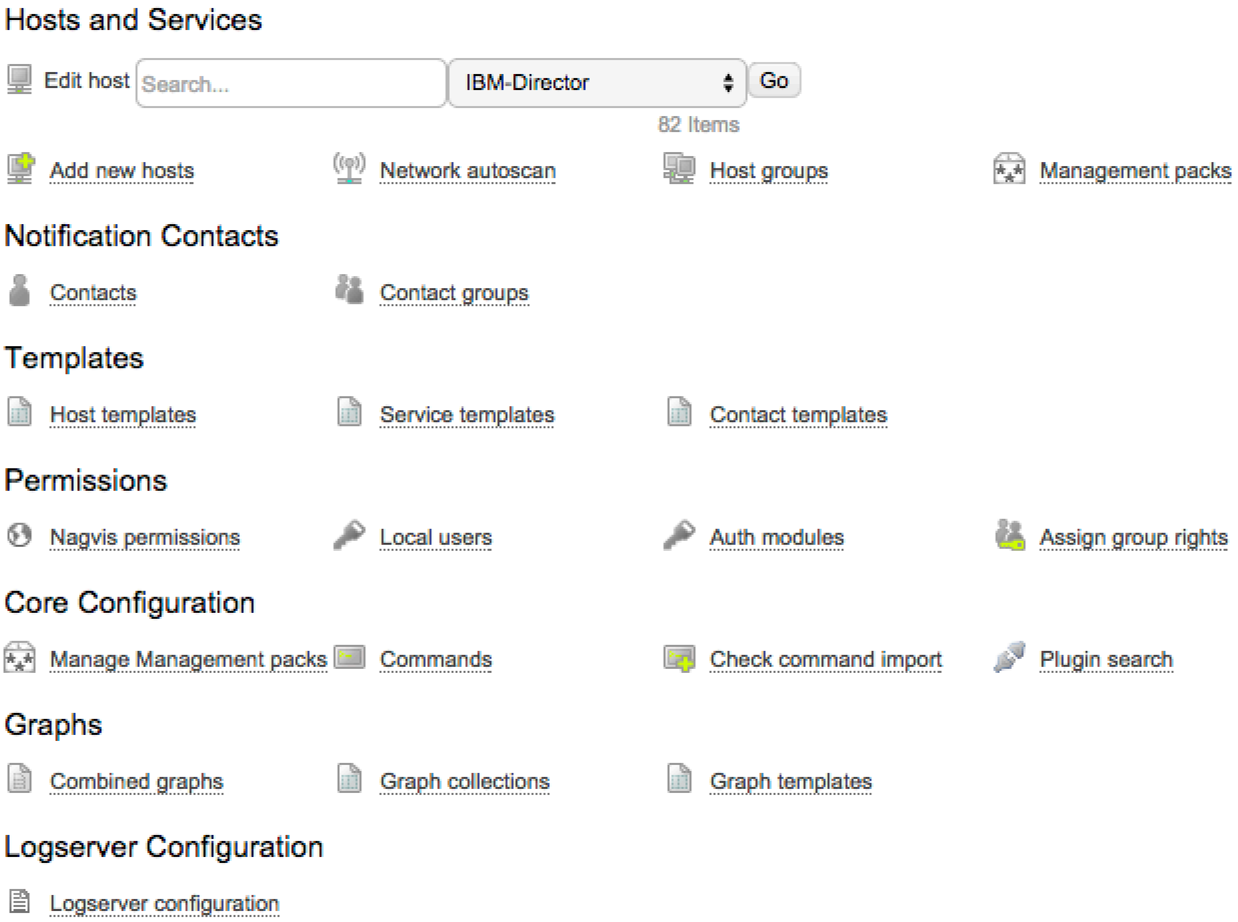


Table of Content

Before you start

Add new

Every time you comes to a page where you can handle an object you will have the **Add new...** dialog ready for you to add a new object.

Configuration files

Every object is placed in a configuration file. You may change what file the object is placed in at the bottom of every configuration page. This is normally not necessary and only used in special cases.

Help

In the guides we will only describe the directive that are differ from the default value. Click the **help icon**

Templates

Because handling templates is the same for all kind of templates, only the directives differ, we will only add a template in *Contacts*.

Contacts

Adding a contact template

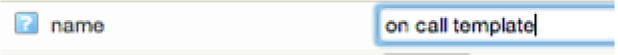
Before we start to add any new contacts we will create a contact template to use with the contact in the next section. In this guide we only describes the directive we will not use the default value in.

To add a contact template

- Click **Contact templates**.

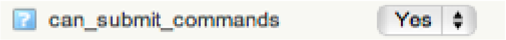
  Contact templates

- Give the contact template a name

  name: on call template

- Change **can_submit_commands** to yes.

  can_submit_commands: Yes

  This gives this the user connected to this contact the possibility to execute commands like acknowledge problems etc.

- Click **Submit**.
- Click **Save**.

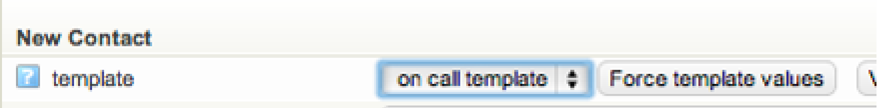
Adding a contact

To add a contact

- Click **Contacts** on the main page.

  Contacts

- Use the template on call template we created in *Adding a contact template.*

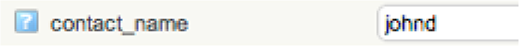
  

  New Contact

  template: on call template

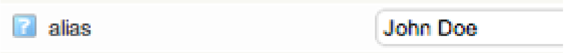
  .

- Type in a contact_name

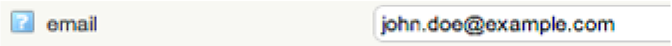
  contact_name: johnd

- Type in an alias

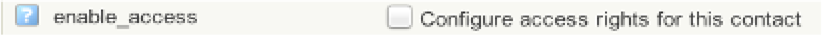
  alias: John Doe

- Type in the email address

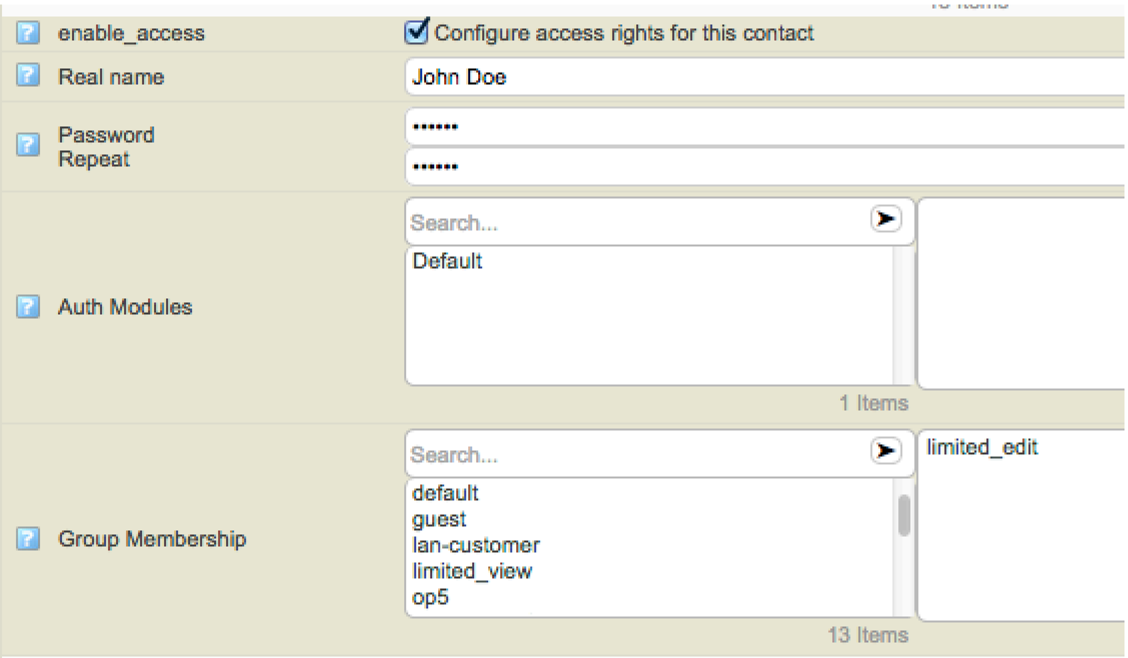
  email: john.doe@example.com

- Click **Submit**.
- If you want to create access check the "Configure access rights for this contact" box, otherwise save changes

  enable_access: □ Configure access rights for this contact

- When Configuring access right for this contact select the access rights the contact should have, after that save the changes.



enable_access ☑ Configure access rights for this contact

Real name: John Doe

Password: ••••••
Repeat: ••••••

Auth Modules: Search... Default — 1 Items

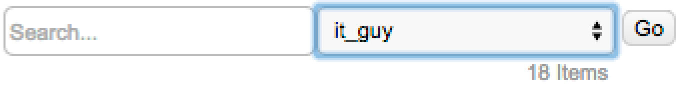
Group Membership: Search... default, guest, lan-customer, limited_view, op5 — 13 Items; limited_edit

Modify a contact

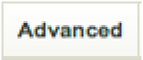
To modify a contact

- Click **Contacts** on the main page.

- Choose the contact you like to modify in the drop down list.



- Click **Go**.
- In the view you will get only directives differ from the template will be shown. To change the other directives click **Advanced**.

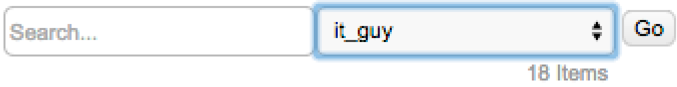


- Make your modifications and click **Submit**.
- Click **Save**.

Delete a contact

- Click **Contacts** on the main page.

- Choose the contact you like to modify in the drop down list.



- Click **Go**.
- Click on **Delete**.

- Click **Save**.

Hosts

There are many ways to add a host. A host can be added by

- **Host Wizard**
- **new host** option
- a **network scan**
- cloning of a host
- using a profile

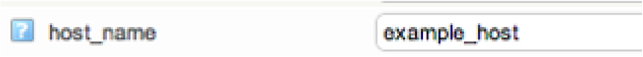
In this guide we only describes the directive we will not use the default value in.

Adding a host with new host option

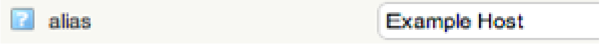
To add a new hosts using the new host option - Part 1

- Click **New host** on the main page.

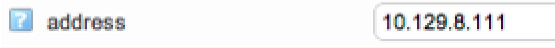
- Type in a host_name.


host_name example_host

- Type in an alias.

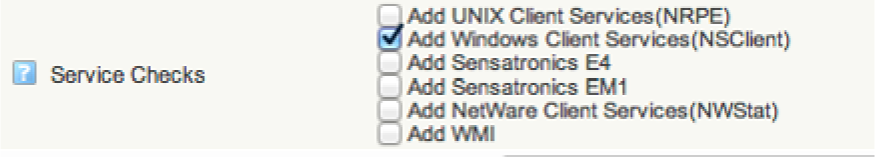

alias Example Host

- Type in the address to the host, IP address is mostly the best choice.

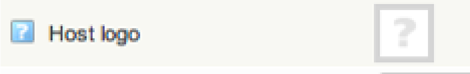

address 10.129.8.111

- We assume this is a Microsoft windows server and that NSClient++ has been installed. Check for the following service checks.

> When using WMI a administrators account must be selected. It is also possible to create a user with less privileges, see how-to https://kb.op5.com/x/K4IK


Service Checks
□ Add UNIX Client Services(NRPE)
☑ Add Windows Client Services(NSClient)
□ Add Sensatronics E4
□ Add Sensatronics EM1
□ Add NetWare Client Services(NWStat)
□ Add WMI

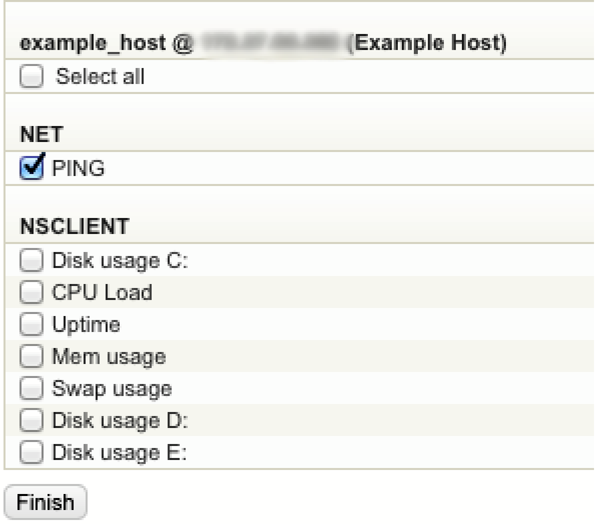
-
- Click host logo to set the icon that will be displayed for this host in lists and maps.



- Click the icon you like to use.
- Click **Add services**.

To add a new host using the new host option - Part 2

- Leave the initial settings All new services will inherit the Initial Service Settings. If you choose not to enter a value for one or more required variable, those variables must be set in the selected template.
as it is and scroll down to the services.
- The scan has found out that NSClient++ is installed plus two other services that can be added to this host.



example_host @ [redacted] (Example Host)

□ Select all

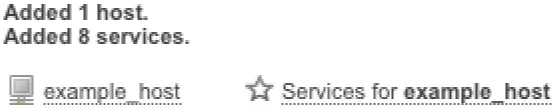
NET

☑ PING

NSCLIENT

□ Disk usage C:
□ CPU Load
□ Uptime
□ Mem usage
□ Swap usage
□ Disk usage D:
□ Disk usage E:

- Check Select All to add all services found or select the one you like to add for this host.
- Click **Continue to step 3**.
- Now either click the host or service links or click **Save**.



Added 1 host.
Added 8 services.

Adding hosts with network scan

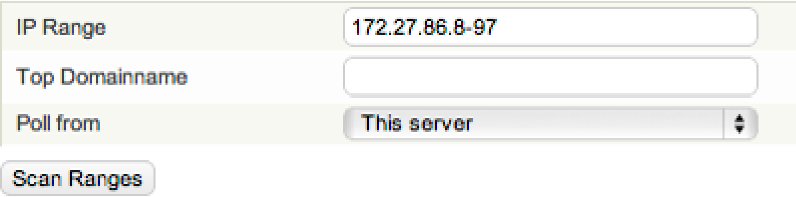
Network ranges can be specified in a very free form. Each of the four parts of the IP-address may contain any combination of comma-separated numbers, 'from-to' ranges and single numbers, as such: `10.1,2.0,4-10.1-50`.
You can specify multiple ranges, separated by spaces, if you like.

To add hosts with network scan

- Click **New host** on the main page.

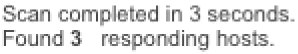
- Click **Network scan**.

- Fill in the desired network range. We will scan for hosts in the range from `172.27.86.8 - 172.27.86.97`



IP Range	172.27.86.8-97
Top Domainname	
Poll from	This server

- Click **Scan Ranges**.
- In this case we found Only hosts that aren't previously configured will be listed three hosts.



Scan completed in 3 seconds.
Found **3** responding hosts.

- Repeat *To add a new hosts using the new host option - Part 1* for each host, except for the last step. If here is one or more host you do not like to add choose **No** in **Add this host?** When you are finished click **Scan hosts for services**.
- Repeat *To add a new host using the new host option - Part 2* for each host, except for the last step.When you are finished click **Continue to step 3**
- Click **Save**.

Modifying a host

To modify a host

- On the start page choose the host you like to modify in the drop down list.

- Click **Go**.
- In the view you will get only directives differ from the template will be shown. To change the other directives click **Advanced**.

- Make your modifications and click **Submit.**
- Click **Save**.

Deleting a host

To modify a host

- On the start page choose the host you like to delete in the drop down list.

- Click **Go**.
- Click **Delete**.

- Click **Delete all affected objects**.
- Click **Save**.

Renaming a host

When renaming a host in the web GUI it will only rename the host and will not rename the host name in log-files, meaning that the history logs for the host is lost.
To rename the host name in log-files as well a script has to be run manually. The script will rename the host in log-files. If this is not done the host will lose all its alert history.
To run the script logon to the op5 monitor via SSH as root user and execute the following command:

```
mon stop; /opt/monitor/op5/merlin/rename --rename-all; mon start
```

If there is a lot of history this script can take a while to execute and during this time the op5 monitor service will not be running.

> Note that this does not yet work on schedule downtime objects. If a host is renamed that has a scheduled downtime the scheduled downtime will be lost.

Network autoscan

It might get handy to let op5 Monitor scan and notify you if there are any new hosts on a particular network range.
The network autoscan function will

- scan certain range for new hosts
- notify you when new are found
- be executed every night by cron on the op5 Monitor server.

> No host will be automatically added. The network autoscan function will only find the hosts for you.

Adding a new autoscan configuration

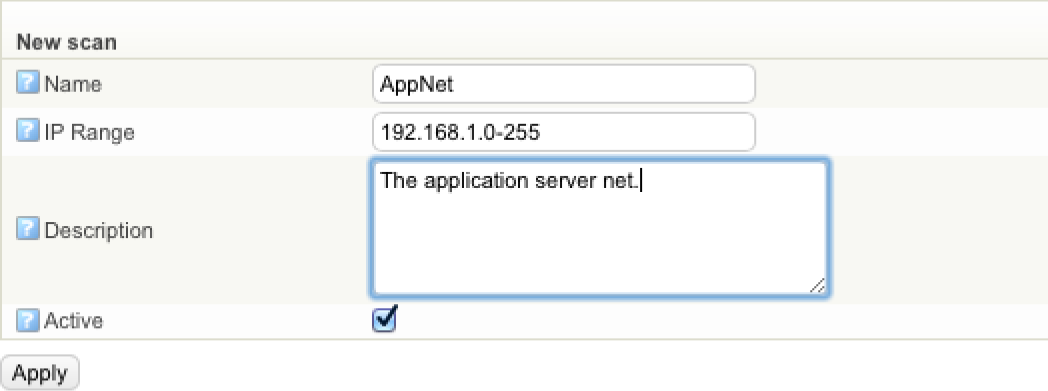
You may add as many autoscan configuration as you wish. When adding a your network range you may use the same syntax as when you manually scans a network from the Add new host wizard.

To add a new autoscan configuration

- Click **Configure** in the main menu.
- Click **Network Autoscan**.

Network Autoscan

- Fill in the **New scan** form



New scan

Name	AppNet
IP Range	192.168.1.0-255
Description	The application server net.
Active	☑

- **Name**: The identifier of this autoscan configuration
- **IP Range**: In this case a complete C net.
- **Description**
- **Activate**: Make this autoscan configuration active and in use.
- Click **Save**.

Adding a host to blacklist

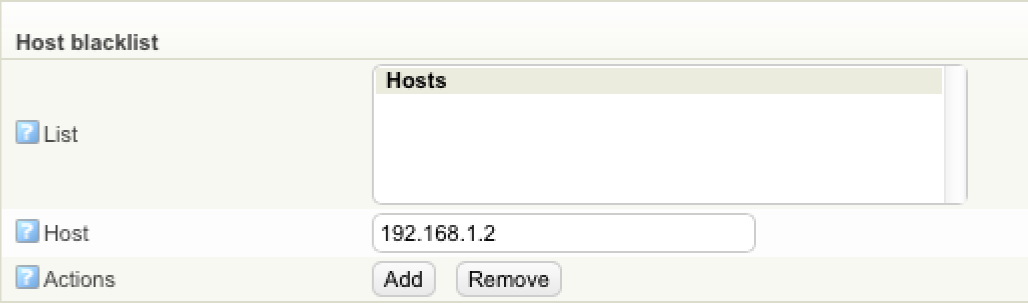
In certain ranges you are scanning with the network autoscan there might be hosts you do not want to include in the result. Then you should add that host or hosts to the blacklist.

To add a host to the blacklist

- Click **Configure** in the main menu.
- Click **Network Autoscan**.

Network Autoscan

- Add a host (IP address) in the **Host** field



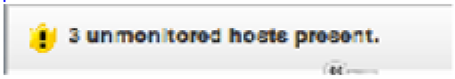
Host blacklist

List	Hosts
Host	192.168.1.2
Actions	Add Remove

- Click **Add**.

The result

After the networks scan has been executed a small result will be shown in the upper left corner of the op5 Monitor GUI



3 unmonitored hosts present.

To add the hosts that has been found you only need to click on the text to the right of the icon. You will then come to the Add new host wizard the same as when you have done a manual network scan.

Services

Services can be added in a few different ways in Configure. You may add a service by using

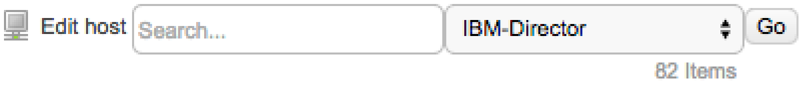
- **add service for this host**
- **scan host for network services**
- **scan host for snmp interfaces**
- **scan host for windows services with agent**
- **scan host for windows services using WMI**

We will take a look at the **add service for this host.**
In this guide we only describes the directive we will not use the default value in.
The default service template will used.

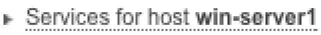
Adding a service

To add a service using add service for this host

- On the start page choose the host you like to add a new service to in the drop down list.

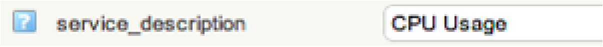


- Click **Go**.
- Click **Services for host....**under related items menu to the right.

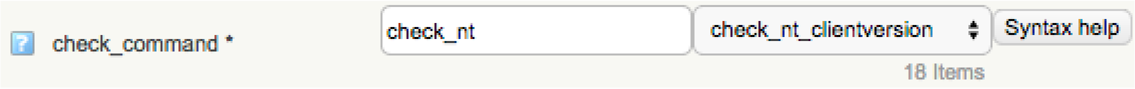


The add new service pages is shown.

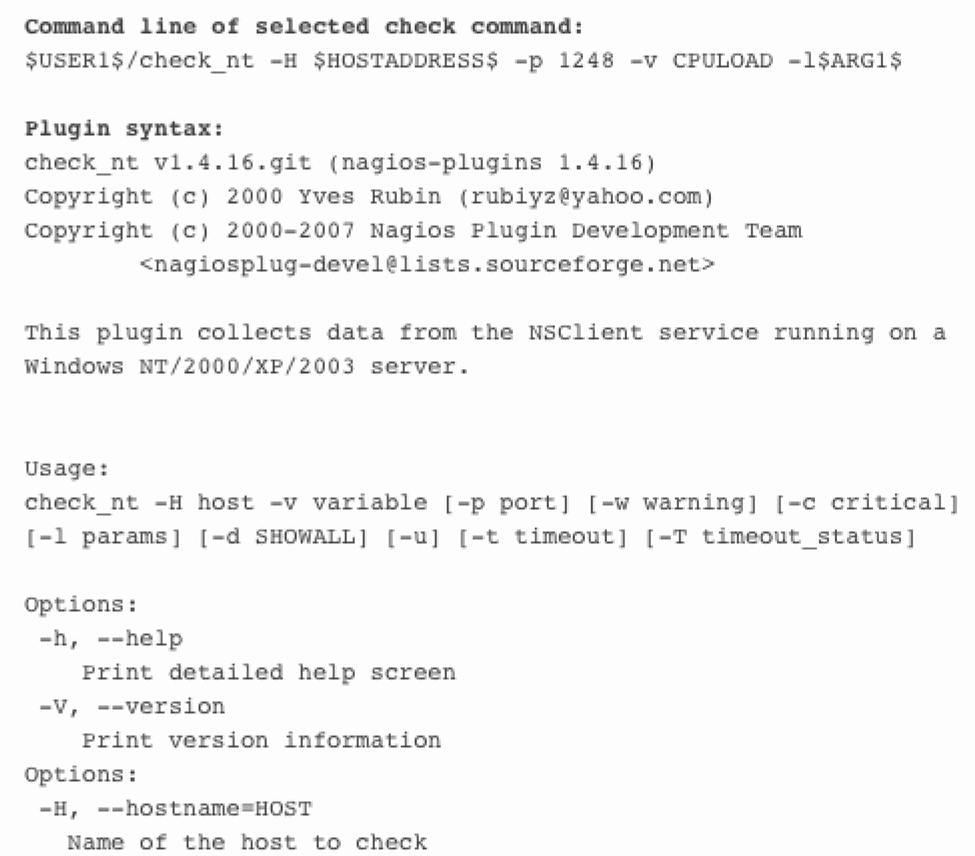
- Type in a service_description.


service_description: CPU Usage

- We will use the check_nt_cpuload command for this service.Type in as many characters you need in the filter by regular expression field until the command shows up.


check_command *: check_nt — check_nt_clientversion

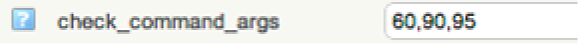
- Click **Syntax help** to see what arguments are needed for this command.



```
Command line of selected check command:
$USER1$/check_nt -H $HOSTADDRESS$ -p 1248 -v CPULOAD -l$ARG1$

Plugin syntax:
check_nt v1.4.16.git (nagios-plugins 1.4.16)
Copyright (c) 2000 Yves Rubin (rubiyz@yahoo.com)
Copyright (c) 2000-2007 Nagios Plugin Development Team
        <nagiosplug-devel@lists.sourceforge.net>

This plugin collects data from the NSClient service running on a
Windows NT/2000/XP/2003 server.


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

Options:
 -h, --help
    Print detailed help screen
 -V, --version
    Print version information
Options:
 -H, --hostname=HOST
   Name of the host to check
```

You can see that we have a macro called **$ARG1$**. This is the first, and in this case the only, argument we need to give to this command.

- Click **Syntax help** again to hide the help text.
- Type in the argument If more than one the shall be separated by a ! like this: argone!argtwo..



check_command_args: 60,90,95

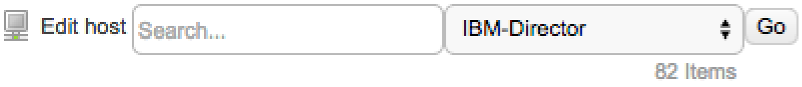
- Click **Submit**.
- Click the **Save** icon.

If the arguments include an exclamation mark "!" this has to be escaped with an back slash (). Example:
username!crypticpassword!!warning!critical
This will out put "crypticpassword!"

Modifying a service

To modify a service

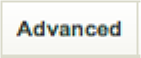
- On the start page choose the host you like to modify a service on in the drop down list.



- Click **Go**.
- Click **Services for host ...** .

- Choose the service you like to modify in the drop down list.

- Click **Go**.
- In the view you will get only directives differ from the template will be shown. To change the other directives click **Advanced**.



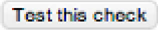
- Make your modifications and click **Submit**.
- Click **Save**.

Test this check

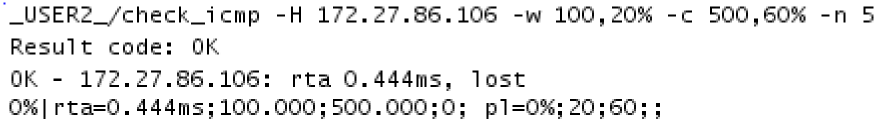
Test this check makes it possible for you to test the service you added or modified before you save the new configuration and reload monitor. This is a nice way to make sure the service works as it is supposed to.
In the guide below we will work with the service created in *Adding a service*.

To test a check

- Pick up the service you like to test as it is done in *Modifying a service*.
- Click **Test this check**, at the bottom of the page.



- The output looks like the one below. If you get any errors it will be shown here in the output

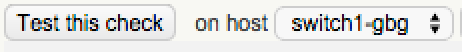


```
_USER2_/check_icmp -H 172.27.86.106 -w 100,20% -c 500,60% -n 5
Result code: OK
OK - 172.27.86.106: rta 0.444ms, lost
0%|rta=0.444ms;100.000;500.000;0; pl=0%;20;60;;
```

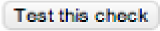
- Click **Hide check** to hide the output.

To test a hostgroup check

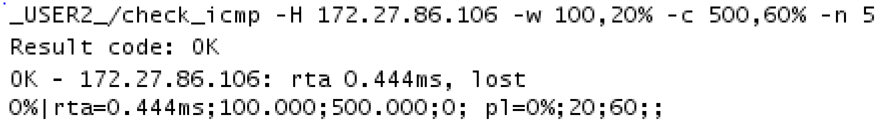
- Pick up the service you like to test as it is done in *Modifying a service*.
- Select the host that you would like the test to run on from the drop down menu.



- Click **Test this check**, at the bottom of the page.



- The output looks like the one below. If you get any errors it will be shown here in the output



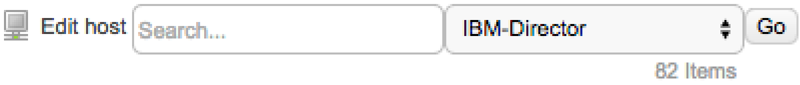
```
_USER2_/check_icmp -H 172.27.86.106 -w 100,20% -c 500,60% -n 5
Result code: OK
OK - 172.27.86.106: rta 0.444ms, lost
0%|rta=0.444ms;100.000;500.000;0; pl=0%;20;60;;
```

- Click **Hide check** to hide the output.

Deleting a service

To delete a service

- On the start page choose the host you like to delete a service from in the drop down list.



- Click **Go**.
- Click **Services for host ...** .

- Choose the service you like to delete in the drop down list.

- Click **Delete**.

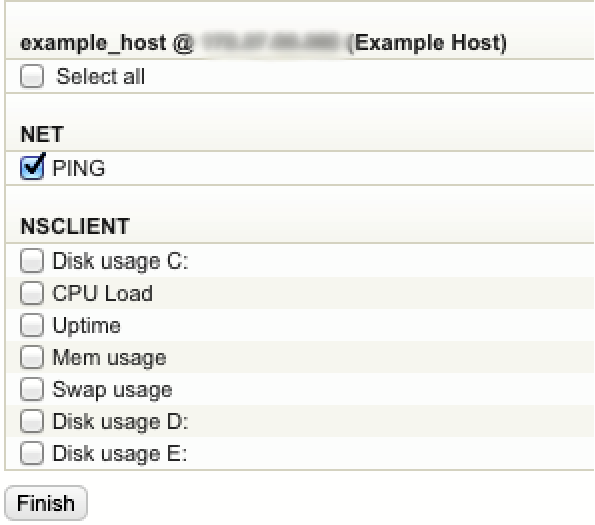
- Click **Save**.

Scanning host for network services

When you added your host you had the opportunity to add services found during the scan for network services. This scan function can also be reached afterwords.

To scan a host for network services

- Open up the host, in **Configure**, you like to add new services on.
- Click **Scan host for network services**.
- Select the new services found and click **Continue to step 3**.



example_host @ [redacted] (Example Host)

□ Select all

NET

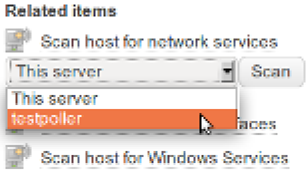
☑ PING

NSCLIENT

□ Disk usage C:
□ CPU Load
□ Uptime
□ Mem usage
□ Swap usage
□ Disk usage D:
□ Disk usage E:

- Click either the host or service link to go back to the place where you started.
- Click **Save**.

Additional information: In a distributed environment a selectbox will appear when hovering over the menu item "Scan host for network services" where you can select from which op5 Monitor system that should preform the scan.



Related items

Scan host for network services

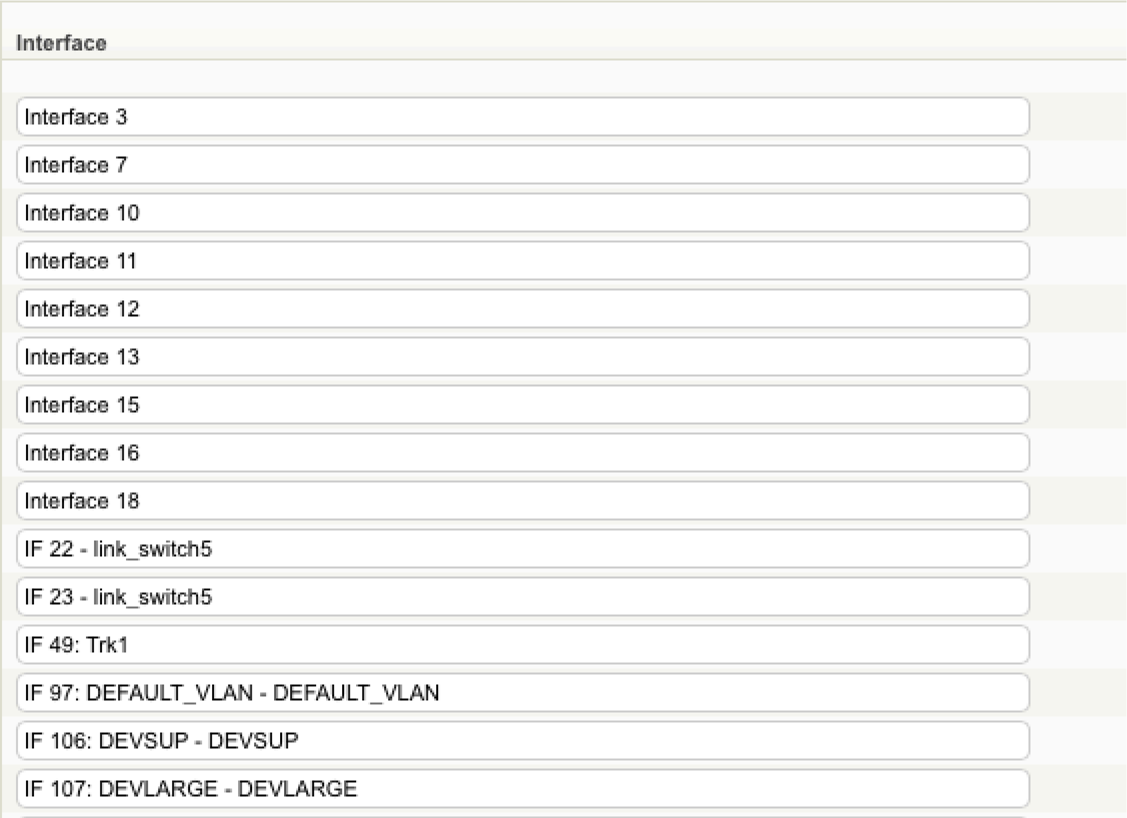
This server

Scanning a host for snmp interfaces

In many times when you are about to monitor a switch or a router you need to setup a lot of services. It is hard work and takes a lot of time to add them one by one.
Instead of adding all interface services one by one you should use the scan for snmp interfaces function.

To add snmp interfaces

- Open up the host, in **Configure**, you like to add new services on.
- Click **Scan host for SNMP interfaces**.
- Set the SNMP community.
- Chose SNMP version.
- Click **Scan host**.



Interface

Interface 3

Interface 7

Interface 10

Interface 11

Interface 12

Interface 13

Interface 15

Interface 16

Interface 18

IF 22 - link_switch5

IF 23 - link_switch5

IF 49: Trk1

IF 97: DEFAULT_VLAN - DEFAULT_VLAN

IF 106: DEVSUP - DEVSUP

IF 107: DEVLARGE - DEVLARGE

- Select the services you like to add.
- Click either the host or the service link to get back.
- Click **Add selected services**.
- Click **Save**.

Scanning host for windows services

There are two ways to scan a windows host for services:

- Using the windows agent NSclient++
- Using WMI, Windows Management Instrumentation

The following sections will describe how to accomplish this using the different techniques.

Scan for services using agent

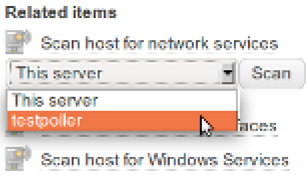
Adding a service that checks a windows services is many times harder than you think. You need to

- have access to the windows server
- know the exact name of the windows service

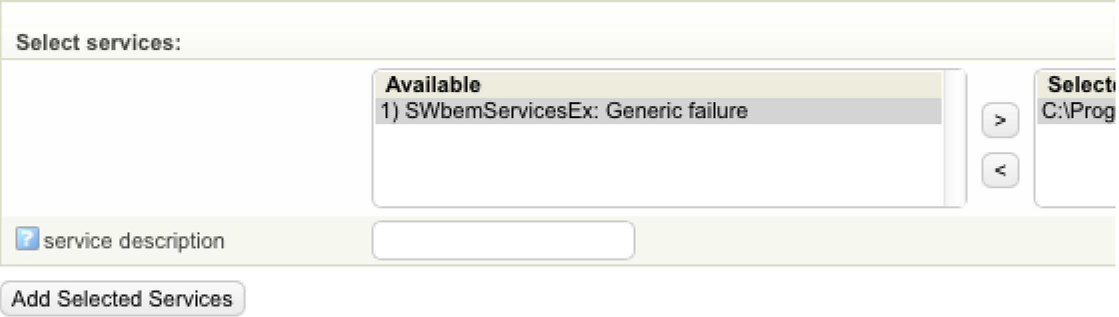
With op5 Monitor you do not need to do anything more than make sure the latest agent (NSClient++) is installed and follow the next few steps.

To add windows services

- Open up the host, in **Configure**, you like to add new services on.
- Click **Scan host for Windows Services**.
- Choose which server to preform the scan:


Related items
Scan host for network services
This server
Scan
This server
testpoller
aces
Scan host for Windows Services

- Select the Windows Services you like to add as a new service in op5 Monitor.



1) SWbemServicesEx: Generic failure

C:\Prog

service description:

- Give the new service a **Service description**.
- Click **Add Selected Services**.
- Click either the service link or the **Scan for more service** button.
- Click **Save**.

Scan for service using WMI

Scan for services using Windows Management Instrumentation has a number of dependencies to be able to work:

- WMI enabled on the windows server
- User account on the windows server with sufficient privileges

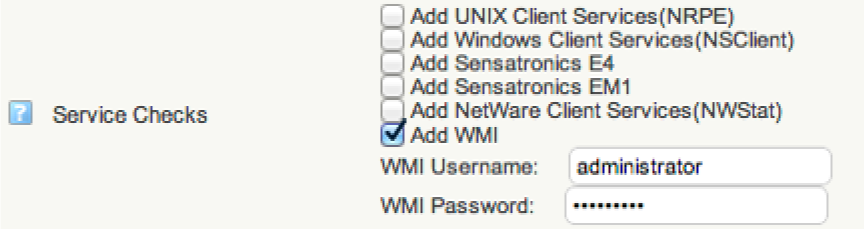
There are two ways to scan for WMI on a windows host:

- When adding a new host
- Scanning a existing host

Scanning for WMI when adding a new host

To scan a host for WMI-counters and services upon adding the host to your op5 Monitor configuration as partly described in: *Adding a host with new host option*.
To scan for WMI counters when adding a new host:

- Select **Configure** in the main menu
- Click on **New Hosts**
- Enter the information about the host
- Select the checkbox **Add WMI**



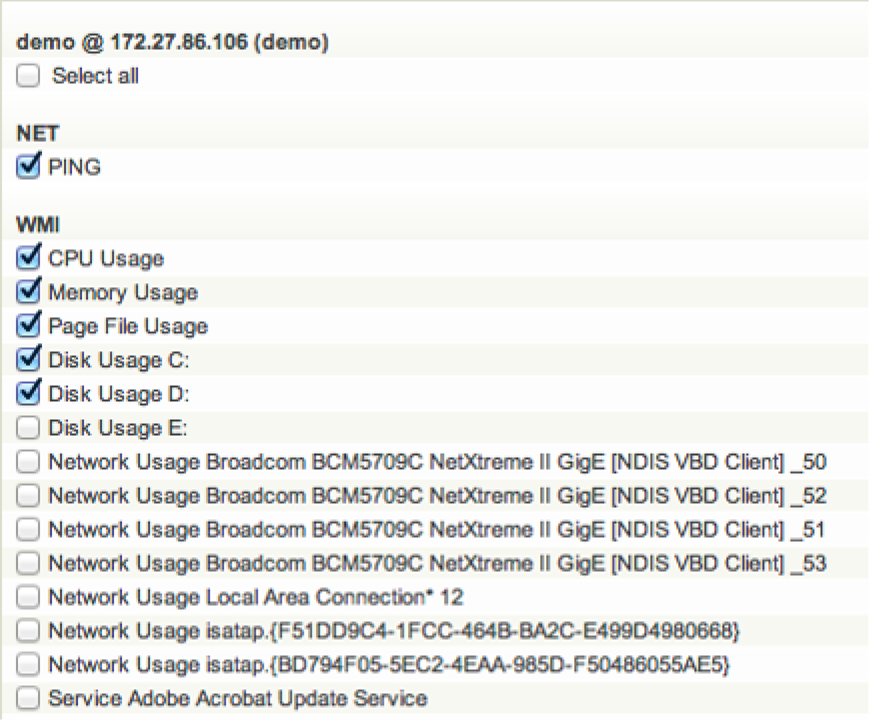
☐ Add UNIX Client Services(NRPE)
☐ Add Windows Client Services(NSClient)
☐ Add Sensatronics E4
☐ Add Sensatronics EM1
☐ Add NetWare Client Services(NWStat)
☑ Add WMI

WMI Username: administrator

WMI Password: ••••••••••

- Enter username and password
- Press **Add Services**

- Select the services you wish to add from the list



demo @ 172.27.86.106 (demo)

□ Select all

NET

☑ PING

WMI

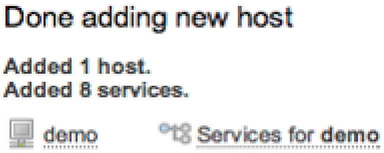
☑ CPU Usage
☑ Memory Usage
☑ Page File Usage
☑ Disk Usage C:
☑ Disk Usage D:
□ Disk Usage E:
□ Network Usage Broadcom BCM5709C NetXtreme II GigE [NDIS VBD Client] _50
□ Network Usage Broadcom BCM5709C NetXtreme II GigE [NDIS VBD Client] _52
□ Network Usage Broadcom BCM5709C NetXtreme II GigE [NDIS VBD Client] _51
□ Network Usage Broadcom BCM5709C NetXtreme II GigE [NDIS VBD Client] _53
□ Network Usage Local Area Connection* 12
□ Network Usage isatap.{F51DD9C4-1FCC-464B-BA2C-E499D4980668}
□ Network Usage isatap.{BD794F05-5EC2-4EAA-985D-F50486055AE5}
□ Service Adobe Acrobat Update Service

:

- Press **Finish**

  at the end of the page.

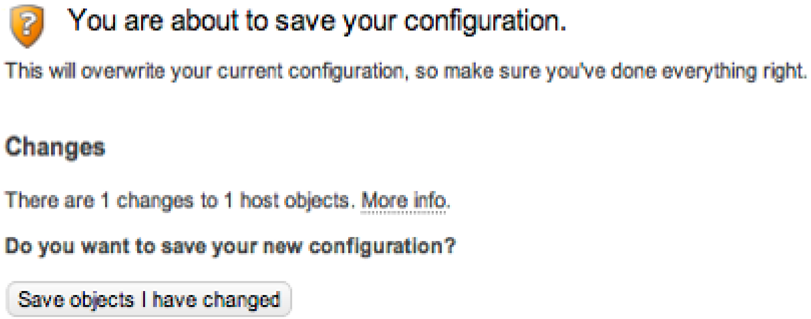
The host is added and you can save your configuration.



Done adding new host

Added 1 host.
Added 8 services.

- Press **Save** in the top right corner
- Review your changes then by clicking on **More info** press **Save objects I have change**d



You are about to save your configuration.

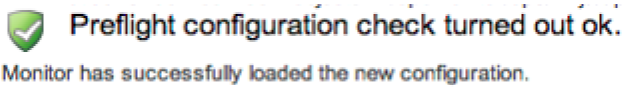
This will overwrite your current configuration, so make sure you've done everything right.

Changes

There are 1 changes to 1 host objects. More info.

Do you want to save your new configuration?

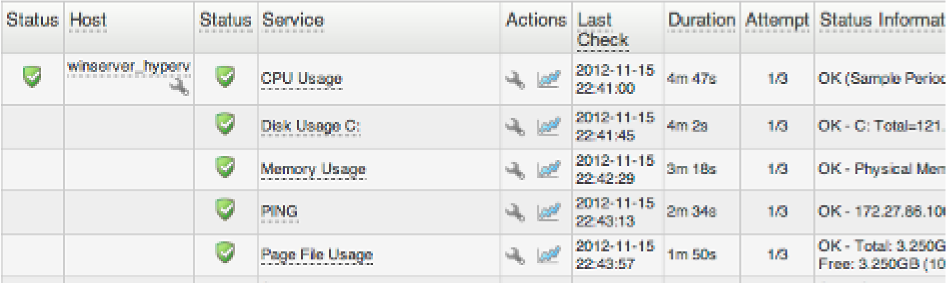
After this the configuration will be saved and i final preflight configuration check has been performed.



Preflight configuration check turned out ok.

Monitor has successfully loaded the new configuration.

Your configuration is saved and the host and its services are ready to be monitored.



Status	Host	Status	Service	Actions	Last Check	Duration	Attempt	Status Informat
✓	winserver_hyperv	✓	CPU Usage		2012-11-15 22:41:00	4m 47s	1/3	OK (Sample Perio
		✓	Disk Usage C:		2012-11-15 22:41:45	4m 2s	1/3	OK - C: Total=121.
		✓	Memory Usage		2012-11-15 22:42:29	3m 18s	1/3	OK - Physical Mem
		✓	PING		2012-11-15 22:43:13	2m 34s	1/3	OK - 172.27.86.10
		✓	Page File Usage		2012-11-15 22:43:57	1m 50s	1/3	OK - Total: 3.250G Free: 3.250GB (10

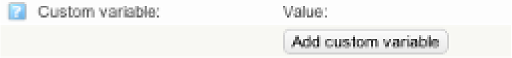
Custom Variables

Custom variables can be used to store custom information for hosts, services and contacts in the configuration. These variables can be used as a macro in command arguments and notifications for example.
All custom variables will automatically get a underscore "_" as a prefix to prevent name collisions with the standard variables.
The custom variable will also automatically be converted to upper case.
In order to prevent name collision among custom variables from different object types, Nagios prepends "_HOST", "_SERVICE", or "_CONTACT" to the beginning of custom host, service, or contact variables, respectively, in macro and environment variable names.
These variables can be used as macros in same way as the standards macros in op5 Monitor.
When using a custom variable as a macro a "$"-sign is always used before and after the variable name.

Entered Name	Variable name	Macro name
snmp_community	_SNMP_COMMUNITY	$_SNMP_COMMUNITY$
location	_LOCATION	$_LOCATION$

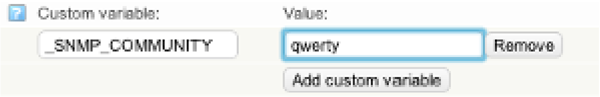
Creating a new custom variable

Go to the configuration for a host, service or contact and click on **add custom variable**.



Custom variable: Value:

Enter a variable name and the value of the variable. Note that the prefix underscore and conversion to upper case is done automatically.

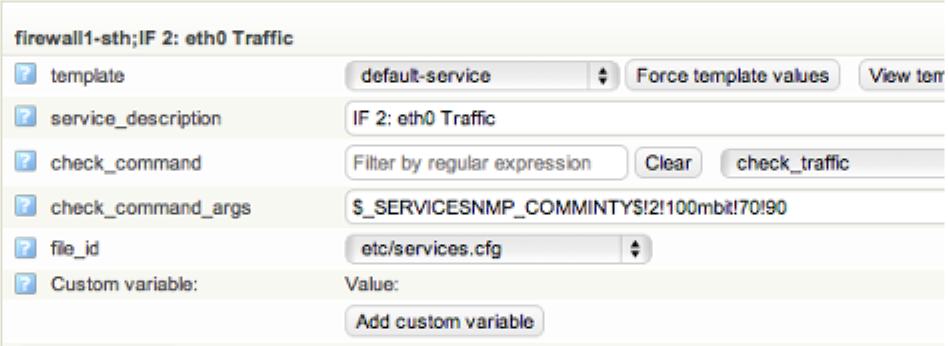


Custom variable: Value:
_SNMP_COMMUNITY qwerty

Click on **submit** and save the configuration.

Example

Instead of using the SNMP community name hardcoded in the check command or in the command arguments in the service check we will create a custom variable that we will use as a macro in the command arguments.
In this example we will move the SNMP community name on a traffic check on a switch port from being in the command arguments to a custom variable.
First we create a custom variable on a switch traffic check, see *Creating a new custom variable*.
Name the variable: `snmp_community` (the prefix and upper case conversion will be done automatically).
Enter the name of your SNMP community as a value. Let's say for this example that the community name is "qwerty"
Change the command argument of the command argument from "`qwerty!2!100mbit!70!90`" to "`$_SERVICESNMP_COMMUNITY$!2!100mbit!70!90`"



firewall1-sth;IF 2: eth0 Traffic

template	default-service
service_description	IF 2: eth0 Traffic
check_command	Filter by regular expression / check_traffic
check_command_args	$_SERVICESNMP_COMMINTY$!2!100mbit!70!90
file_id	etc/services.cfg
Custom variable:	Value:

Click on **submit** and save the configuration.

Dynamic Button

The dynamic button is a customizable button which any script can be added to.
If defined, a link in the service information page will appear under "Service Commands" on the service ext info page.

Configuration

To configure the dynamic button two custom variables has to be created on the service which the button should be added to.
The first one is the command line and the second one is the permissions.
The prefix _OP5 symbolizes that this is a dynamic button variable. If an H is added to the prefix (_OP5H) the custom variables will not be visible in the Service State Information table.
`_OP5H__ACTION__NAME`
`_OP5H__ACCESS__NAME`

> ⓘ Note that there are two underscores!

Action

The action has the variable name **`_OP5H__ACTION__NAME`**
The value of the action is the path to the script that should be executed.
The name of the button is set by replacing "NAME" in the variable name. When using spaces in the name, this should be replaced by one underscore.
Example:
To name the dynamic button "Restart Service" and it will execute the script /opt/plugins/custom/restart_service.sh. The variable name should be:
Variable name:`_OP5H__ACTION__RESTART_SERVICE`
Value:`/opt/plugins/custom/restart_service.sh`

Access

The *OP5HACCESS*_NAME sets who will be able to use the dynamic button. This is set on contact-groups only.
If a user is not in a group that is specified in the access variable the button will not be visible for the user.
The access variable name must have the same name as the action name.
Example
If you want to give access to the "Restart Service" action to the support-group and windowsadmins groups the setup should look like this:
Variable name: `_OP5H__ACCESS__RESTART_SERVCE`
Value: `support-group,windows-admins`

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.

Host and service escalations works exactly in the same way so we will only take a look at host escalations from now on.

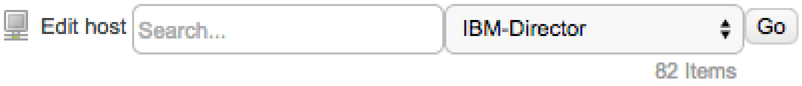
Adding a host escalation

In this guide we will add a small escalation chain that does the following

- First notification is sent to the support-group
- After 10 minutes the second (the last one) is sent to the sysadmins group.

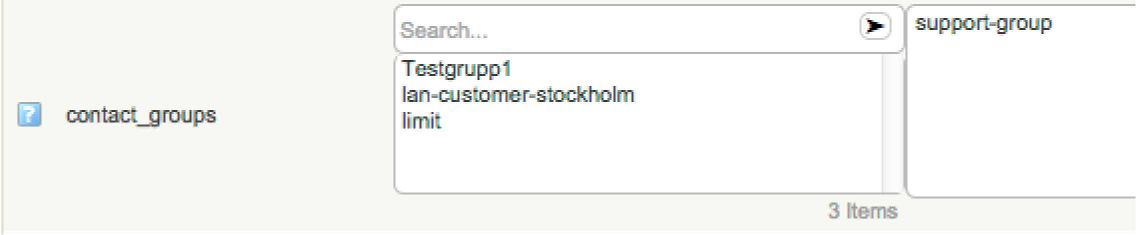
To add a host escalation

- On the **Edit Host** page, choose the host you like to add an escalation to in the drop down list.


Edit host Search... IBM-Director Go
82 Items

- Click **Go**.
- Click **Escalations**.

- Add the escalation number one.
- Choose the contact group that shall have the notification.


contact_groups

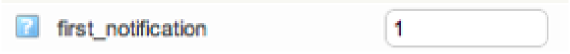
Search...

Testgrupp1
lan-customer-stockholm
limit

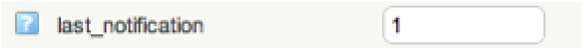
3 Items

support-group

- Set the start number in the escalation chain.

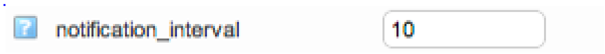

first_notification 1

- Set the end number in the escalation chain If the start number is 1 and the end number is two it means that the first and the second notification will be handled by this escalation.

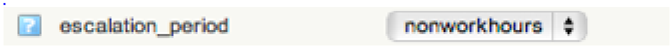

last_notification 1

.

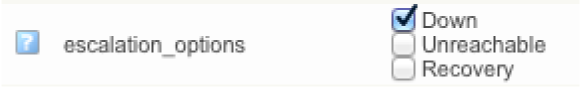
- Set the notification interval which is the number of minutes to wait to the next notification.


notification_interval 10

- Choose the time period when this escalation will be in use.


escalation_period nonworkhours

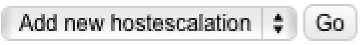
- Choose what states this escalation will be valid for.


escalation_options

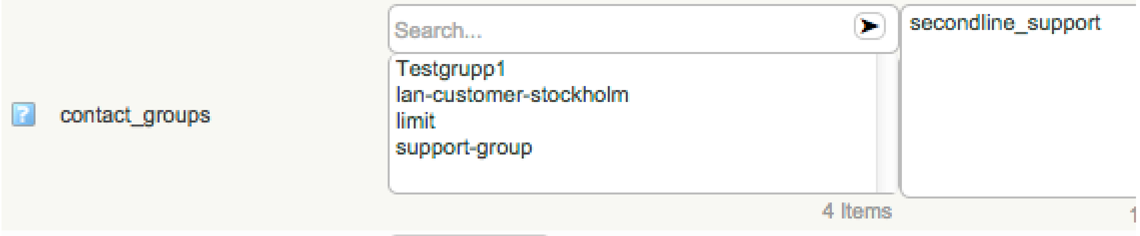
☑ Down
☐ Unreachable
☐ Recovery

In this case we do not use the escalation for unreachable or recovery which means that unreachable and recovery notifications will be sent to the contact group set on the host.

- Click **Submit**.
- Choose Add new host escalation



- Click **Go**.
- Add the escalation number two.
- Choose the contact group that shall have the notification.


contact_groups

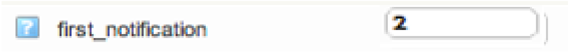
Search...

Testgrupp1
lan-customer-stockholm
limit
support-group

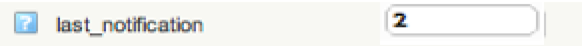
4 Items

secondline_support

- Set the start number in the escalation chain.


first_notification 2

- Set the end number in the escalation chain We have set the first notification and the last notification to 2 because this escalation will only be used once.



last_notification: 2

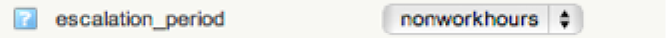
.

- Set the notification interval which is the number of minutes to wait to the next notification.

notification_interval: 10

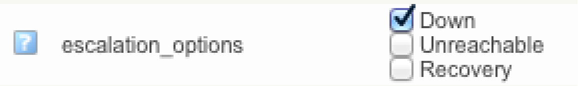
The escalation interval is set to 0 because there will be no more escalations when this one is done.

- Choose the time period when this escalation will be in use.



escalation_period: nonworkhours

- Choose what states this escalation will be valid for.



escalation_options

☑ Down
☐ Unreachable
☐ Recovery

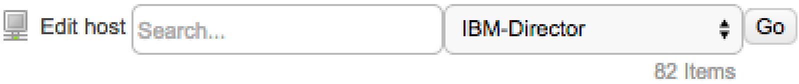
In this case we do not use the escalation for unreachable or recovery which means that unreachable and recovery notifications will be sent to the contact group set on the host.

- Click **Submit**.
- Click **Save**.

Modifying a host escalation

To modify a host escalation

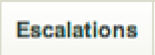
- On the start page choose the host you like to modify an escalation on in the drop down list.



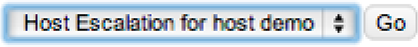
Edit host: Search... | IBM-Director | Go

82 Items

- Click **Go**.
- Click **Escalations**.



- Choose the escalation you like to modify.



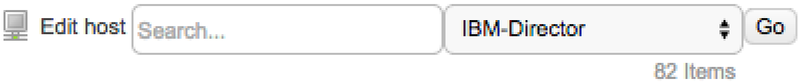
Host Escalation for host demo | Go

- Click **Go**.
- Make the modifications you like to do and click **Submit**.
- Click **Save**.

Deleting a host escalation

To delete a host escalation

- On the start page choose the host you like to delete an escalation from in the drop down list.

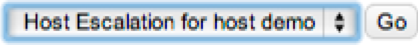


Edit host: Search... | IBM-Director | Go

82 Items

- Click **Go**.
- Click **Escalations**.

- Choose the escalation you like to modify.



Host Escalation for host demo | Go

- Click **Go**.
- Click **Delete**.

- Click **Save**.

Access rights and contacts

To be able to login to op5 Monitor you need to have a user, described in *Local users on page Main Objects*. But you need to have a contact, described in *Contacts on page Main Objects*, to be able to receive notifications and in some cases even be able to see any hosts or services.
By connecting access rights to a contact you will be able to login and get notifications with the user created in access rights.
So basically what you need to do is to configure a new contact. Add the contact to an existing contact group or create a new contact group specific for the new contact. If you created a new contact group make sure to add the contact group for the hosts and services that you want to make available in the customized view.
Add new access rights and connect it to the contact you created earlier.

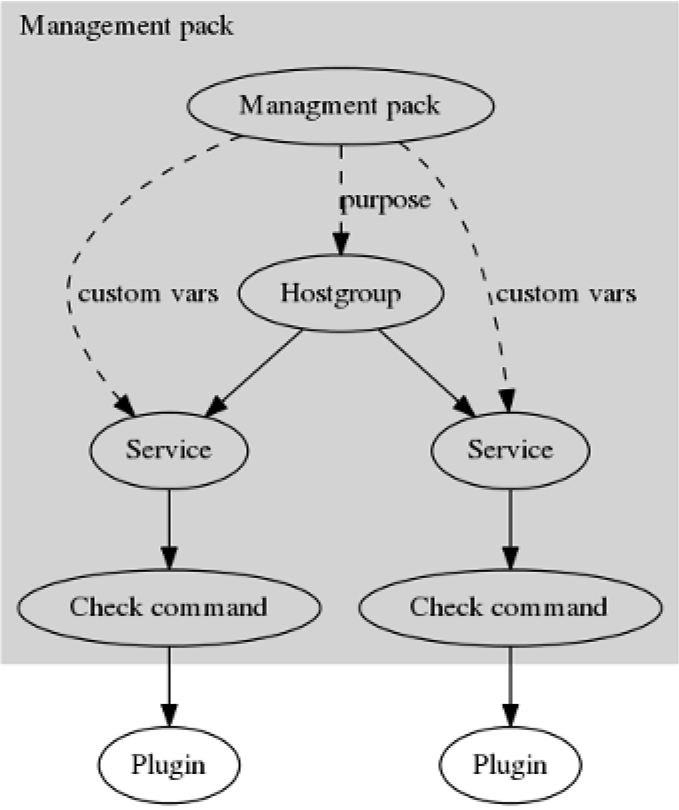
Connecting access rights to contacts

To connect access rights to a contact

- Configure a new contact.
- 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.
- Configure a user in access rights with the exact same name as the contact you created.
- Set the options for the new access right.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.

Management packs

A management pack is essantially a group of services connected to a hostgroup with the possibility to add custom variables. These are then used by the Host Wizard.
The benefit with using management packs is that the monitoring will be more homogenous.
The picture below shows how management packs integrates into op5 monitor.

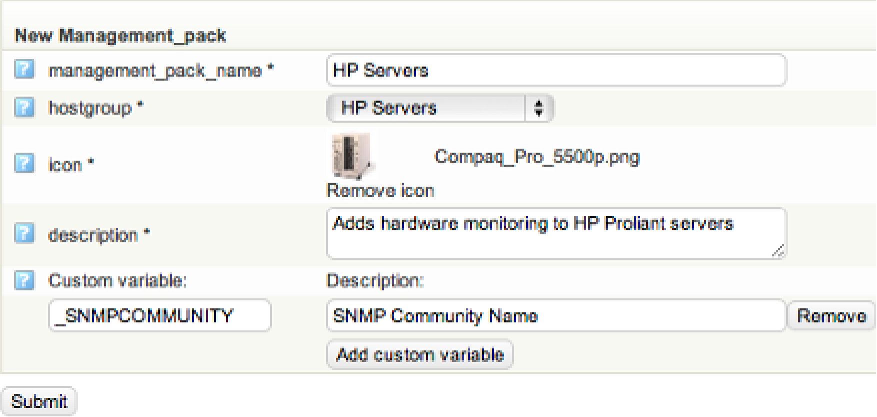


Creating management packs

To create a management pack a hostgroup must be created and the services that should be included in the management pack should be added to that hostgroup. See *Services on Host groups on page Groups* for more information.
After the hostgroup with services has been created the hostgroup can be converted into a management pack.
To create a new management pack from a hostgroup go to **Management Packs** in the configuration.

- Enter a name for the management pack.
- Select whitch hostgroup that should be used for the management pack.
- Select an icon (a larger icon looks better in the host wizard).
- Enter a description.

It is also possible to add custom variables, these can be used for information that needs to be entered when using the host wizard. Such as username, password and SNMP community names.



New Management_pack

management_pack_name *	HP Servers
hostgroup *	HP Servers
icon *	Compaq_Pro_5500p.png Remove icon
description *	Adds hardware monitoring to HP Proliant servers
Custom variable:	Description:
_SNMPCOMMUNITY	SNMP Community Name

In this example we create a management pack for HP Servers with one custom variable for SNMP community name.
Click on **Submit** to save the management pack.

Group in Group with Management Packs

It is possible to use the group in group with management packs. This works in the same way as it does for normal hostgroups.

Example

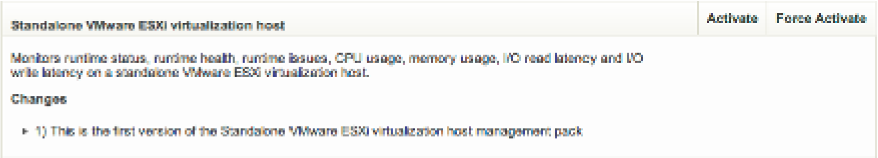
The hostgroup fruits includes the hostgroup '`apples`'.
If a management pack i associated with '`fruits`' will the host be added to the hostgroup '`fruits`' and it will get all the services that is on the hostgroup '`fruits`', but it will not be affected by the '`apples`' hostgroup.
If a management pack is associated with apples the host will be added to the hostgroup apples and get all the services that is in the hostgroup '`apples`' AND all the services that is in the hostgroup '`fruits`'.
More concrete; A hostgroup '`linux`' is created with the check '`check_ssh_cpu`' A hostgroup '`generic`' is created with the check '`check_ping`'
Management pack '`generic server'` is associated with the hostgroup '`generic`'. Hosts that are added with the management pack '`generic server`' will get the '`check_ping`' service.
Mangement pack '`linux servers`' is associated with the hostgroup '`linux`'. Hosts added with the '`linux servers`' will get both the '`check_ssh_cpu`' and the '`check_ping`' checks.

Activate Management Packs

Management packs that is not created by the user, provided by op5 or a third party, needs to be activeted.
To activate a management pack go to **Mangement Pack Management** in the configuration.

Manage Management packs

Click on **Activate** to activate a management pack.



Standalone VMware ESXi virtualization host	Activate	Force Activate
Monitors runtime status, runtime health, runtime issues, CPU usage, memory usage, I/O read latency and I/O write latency on a standalone VMware ESXi virtualization host. Changes 1) This is the first version of the Standalone VMware ESXi virtualization host management pack		

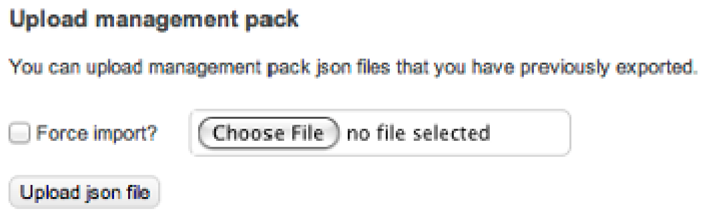
Force Activate will override any management pack with the same name.

Import Management Packs

To import a management pack from a json-file go to Management Pack Management.

Management packs

Click on **Choose File** to select the json-file that should be imported.



Upload management pack

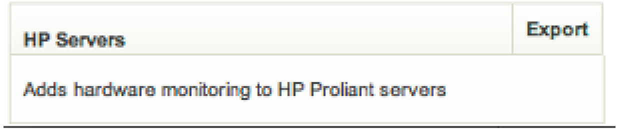
You can upload management pack json files that you have previously exported.

Click on **Upload json file** to import the management pack.

Export Management Packs

Export management packs makes it possible to share your management pack with others or upload it to another op5 Monitor server. Go to Mangement Pack Mangement under configuration.

Click on Export on the management pack to export this to a json-file. The file will be downloaded to you computer.



HP Servers	Export
Adds hardware monitoring to HP Proliant servers	

Host Wizard

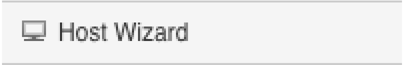
About

Host wizard is a tool to create a new host based on management packs (preconfigured services).

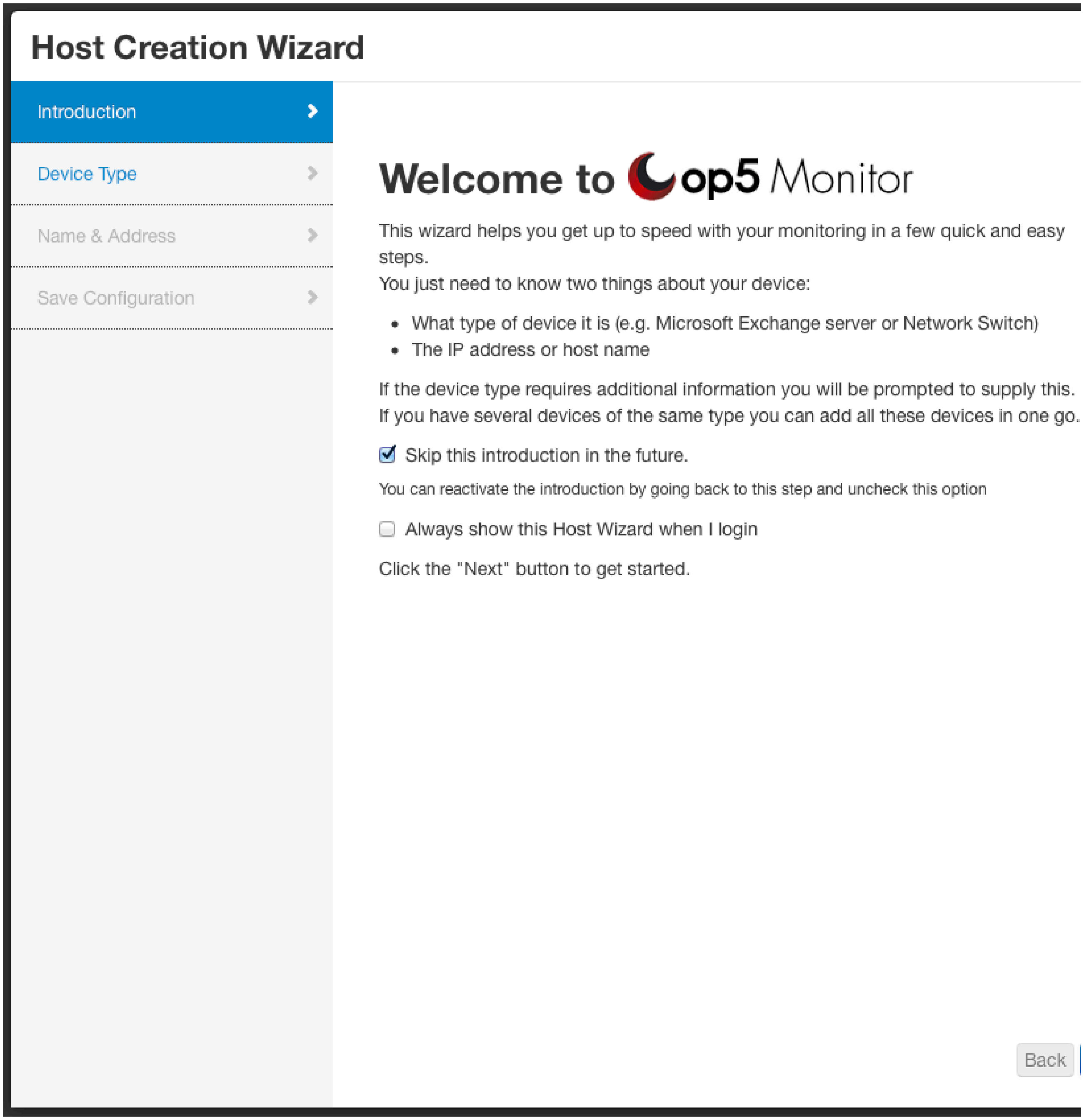
Table of Content

Adding a host using Host wizard

- Go to the **Configuration** menu and select **Host Wizard**

  This will open the Host Wizard popup
- On the first page you will find some information about the wizard and two options. **Skip this introduction in the future** will enable/disable the introduction page in the future. **Always show Host Wizard when I login** will enable/disable the wizard popup on each login.



This wizard helps you get up to speed with your monitoring in a few quick and easy steps.
You just need to know two things about your device:

- What type of device it is (e.g. Microsoft Exchange server or Network Switch)
- The IP address or host name

If the device type requires additional information you will be prompted to supply this.
If you have several devices of the same type you can add all these devices in one go.

☑ Skip this introduction in the future.

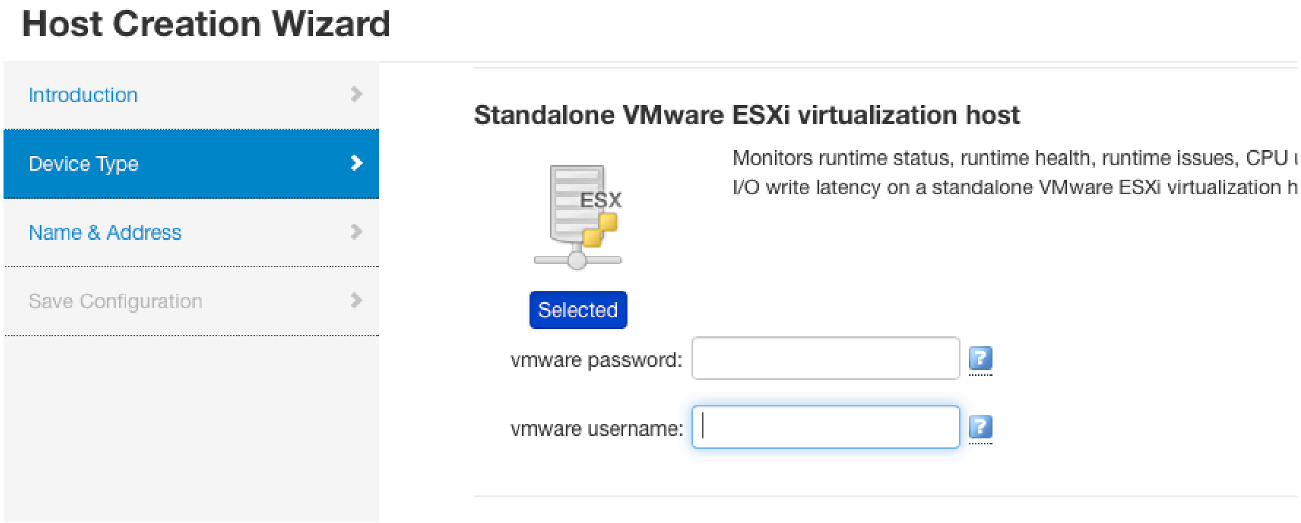
You can reactivate the introduction by going back to this step and uncheck this option

☐ Always show this Host Wizard when I login

Click the "Next" button to get started.

Click on **Next** to go to Device type selection

- Select the device type that corresponds to the host that you are adding. Multiple types can be selected.In this example we will add a ESXi host.



Host Creation Wizard

Standalone VMware ESXi virtualization host

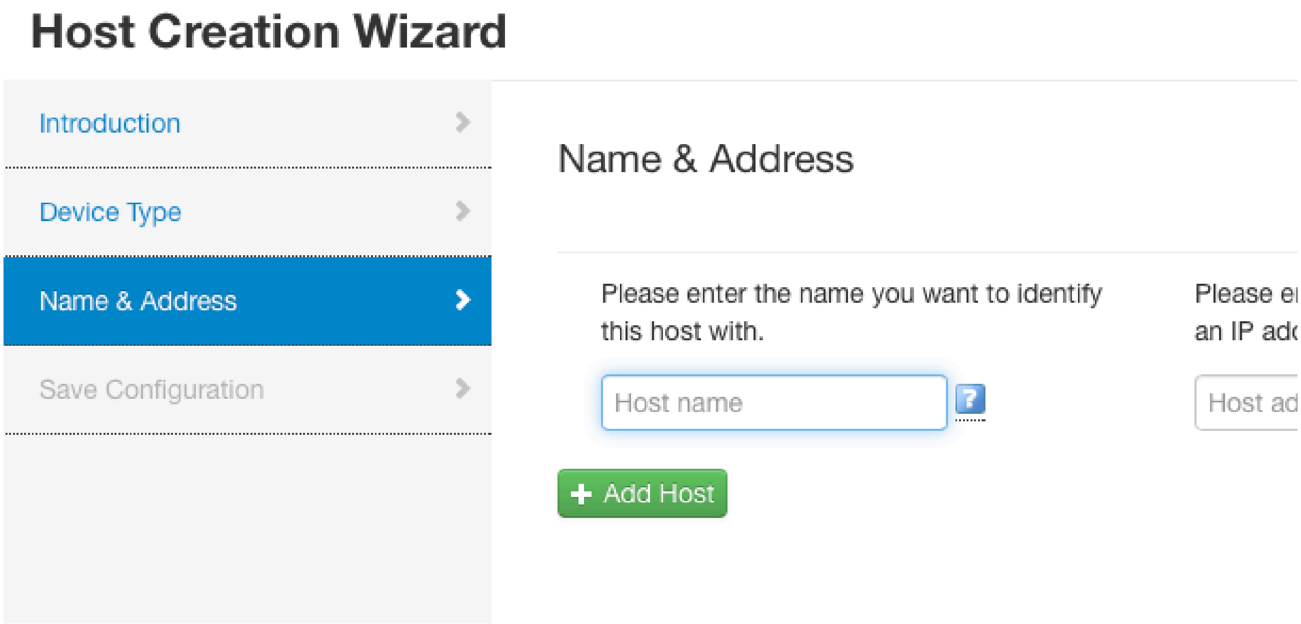
Monitors runtime status, runtime health, runtime issues, CPU u
I/O write latency on a standalone VMware ESXi virtualization h

vmware password:

vmware username:

Some device types might require some input, these are mandatory.When the correct device types has been selected click on **Next** to continue.

- Enter the host address (either the DNS-name or IP number) to the host and a hostname.



Host Creation Wizard

Name & Address

Please enter the name you want to identify this host with.

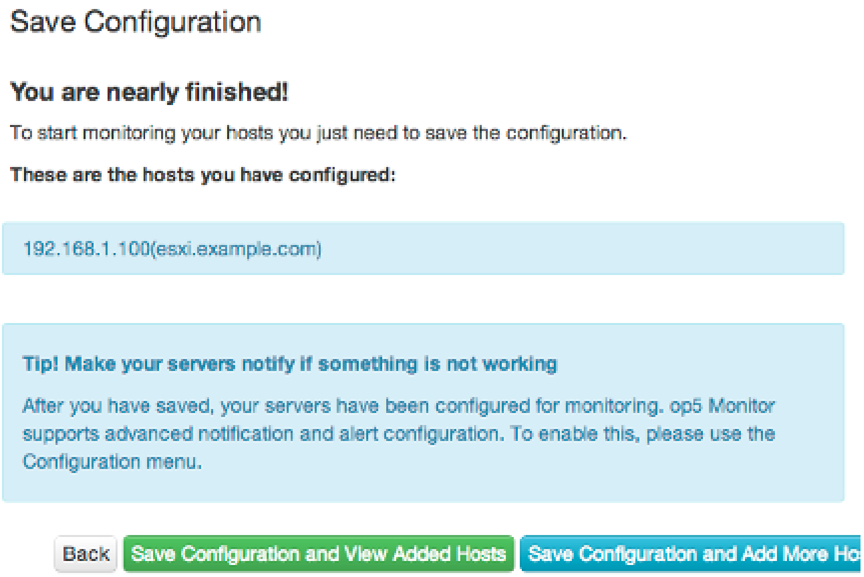
Host name

Please e
an IP adc

Host ad

If you would like to add more than one host using the same device type click on **+ Add Host** to get more address and name fields. Click on **Next** to continue.

- Review the information and click on **Save Configuration and View Added Hosts**. It is possible to
- the configuration and go back to adding more host, with different device types, by selecting **Save Configuration and Add More Hosts**



Save Configuration

You are nearly finished!

To start monitoring your hosts you just need to save the configuration.

These are the hosts you have configured:

192.168.1.100(esxi.example.com)

Tip! Make your servers notify if something is not working

After you have saved, your servers have been configured for monitoring. op5 Monitor supports advanced notification and alert configuration. To enable this, please use the Configuration menu.

Back
Save Configuration and View Added Hosts
Save Configuration and Add More Ho

Groups rights for Host Wizard

The Host Wizard requires the following rights for a user:
configuration_information

- Misc > FILE
- Api > API config
- Host > Host add delete
- Host Template > Host template view all
- Hostgroup > Hostgroup view all
- Management Pack > Management pack view all
- Configuration > Export

For more information on group rights and how to use them see Group Rights.

Make things easy

About

Making things easier to handle with op5 monitor.

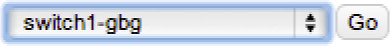
Table of Content

Cloning objects

Cloning from an existing Host

To clone a host follow these steps:

- On the start page choose the host you like to create a profile of in the drop down list.



switch1-gbg

- Click **Go**.
- 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**

Cloning services

If you want to create the same service check on multiple host first create the service check on the host, then clone the service check to one or more hosts.
It is also possible to clone multiple services to one or more hosts or hostgroups.

To clone a service to an other host

- Choose the Configure web menu.
- Choose your host you want to copy from, then click **Go**
- Click **Services for host...** in the 'RELATED ITEMS' menu.
- Select the service (or one of the services) you want to clone then click on **Go** and then on **Clone**.
- Select the service(s) you want to clone.
- You can chose to clone the service(s) to a list of hosts, a hostgroup or all hosts in a hostgroup.
- Click **Clone**.

Copy objects

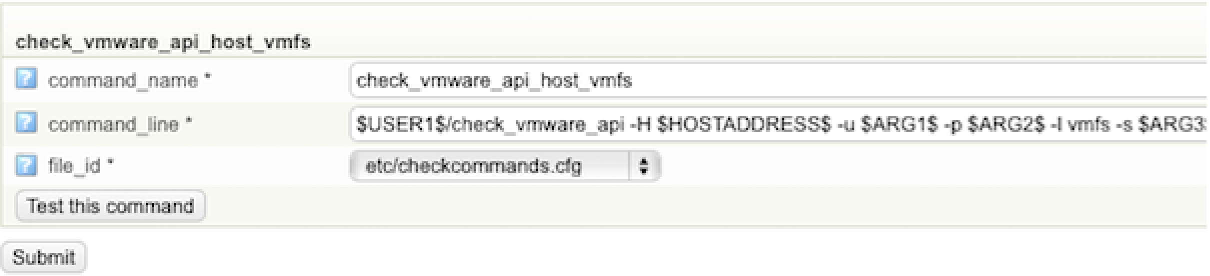
There are a number of objects that can be copied in the configuration tool and make a exact copy of the object, besides the name that must be unique.
These are the objects that is possible to make a copy of:

- Hosts
- Services
- Hostgroups
- Servicegroups
- Check commands
- Contacts
- Contactgroups
- Templates
- Timeperiods
- Host Dependencies
- Service Dependencies
- Host Escalations
- Service Escalations

The copy will inherit all the values set on a object except the name.
To illustrate this let us make a copy of a check command and modify it slightly:

- Click on **Configure** in the main menu:
- Select **Commands** in the configuration menu

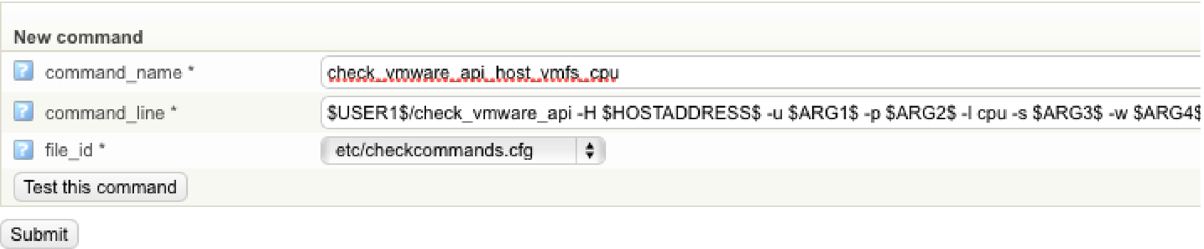
- Search for a command to copy:



check_vmware_api_host_vmfs

command_name *	check_vmware_api_host_vmfs
command_line *	$USER1$/check_vmware_api -H $HOSTADDRESS$ -u $ARG1$ -p $ARG2$ -l vmfs -s $ARG3
file_id *	etc/checkcommands.cfg

- Click **Copy**
- Make the changes you want. A new name is required. and i.e create a listing of the attached VMFS-storages:



New command

command_name * check_vmware_api_host_vmfs_cpu

command_line * $USER1$/check_vmware_api -H $HOSTADDRESS$ -u $ARG1$ -p $ARG2$ -l cpu -s $ARG3$ -w $ARG4$

file_id * etc/checkcommands.cfg

- Click **Submit**

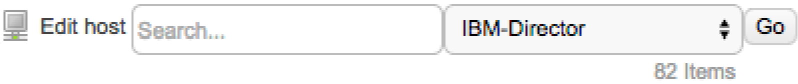
This approach should apply to the most objects that are possible to copy.

Propagate settings

To change the same directive on many objects of the same type can be a really time consuming work. This is where the propagate function in op5 Monitor is very handy.
With the propagate function you can copy the value of a directive from one object to one or many other objects of the same type.
In the guide below we will use the propagate function to copy the parents from one host to a couple of other hosts.

To propagate a value of a directive

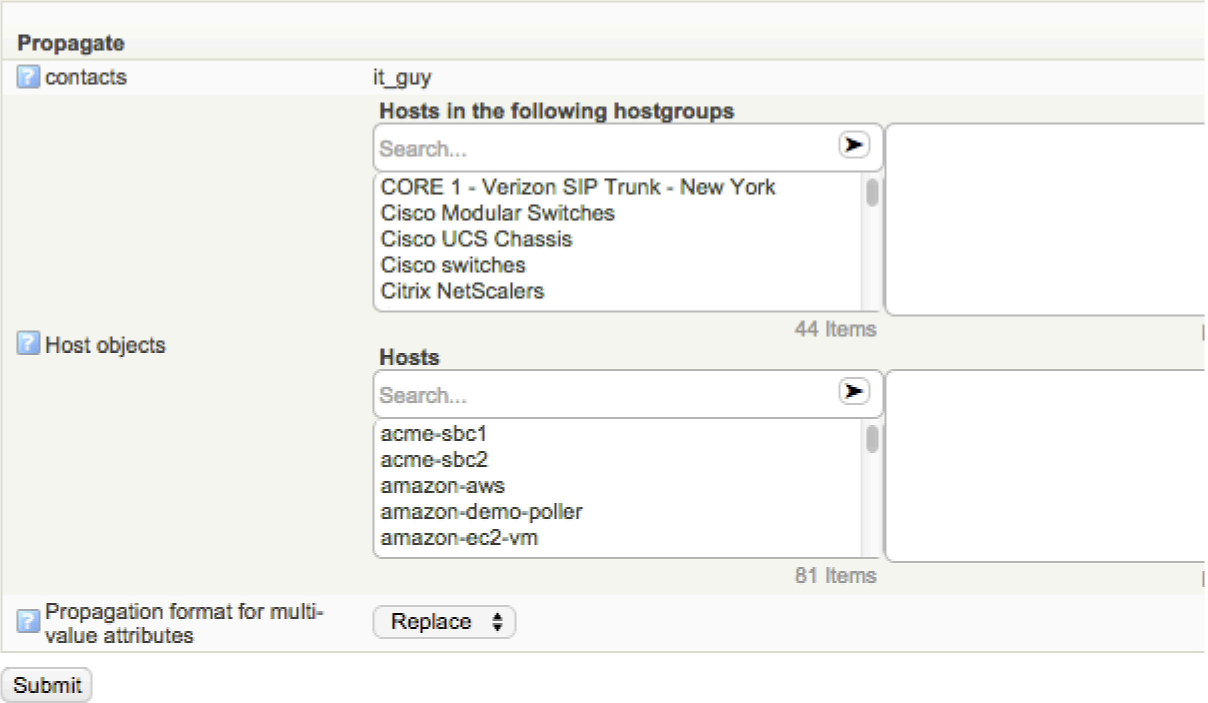
- On the start page choose the host you like to propagate a directive value from in the drop down list.



Edit host: Search... | IBM-Director

- Click **Go**.
- Click **Propagate**.

- Check the check box for parents and click **Propagate selected settings**.
- Select the host objects (host or whole host groups) you like to propagate the settings to.



Propagate

contacts: it_guy

Host objects

Hosts in the following hostgroups

Search...

CORE 1 - Verizon SIP Trunk - New York
Cisco Modular Switches
Cisco UCS Chassis
Cisco switches
Citrix NetScalers

44 Items

Hosts

Search...

acme-sbc1
acme-sbc2
amazon-aws
amazon-demo-poller
amazon-ec2-vm

81 Items

Propagation format for multi-value attributes: Replace

- In order to select more than one item at a time the following options are available:
  - Hold down the primary mouse button when selecting a series of items and all items will be moved to the other box.
  - Click on the arrow next to the search box and all items matching the current filter will be moved to the right-hand box.
- To remove all items from the right-hand box, click "Deselect all"
- Select how you want to propagate your settings with the **Propagation format for multi-value attributes option**. This option is only available when propagating multi-value options such as contacts and hostgroups for example. You can choose the following

options

Option	Description
Replace	Replace the destination values.
Append	Append the source values to the destination values.
Subtract	Subtract the source values from the destination values.

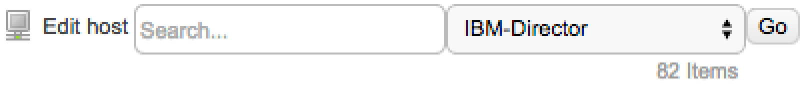
- Click **Submit**.
- Click **Save**.

Bulk delete

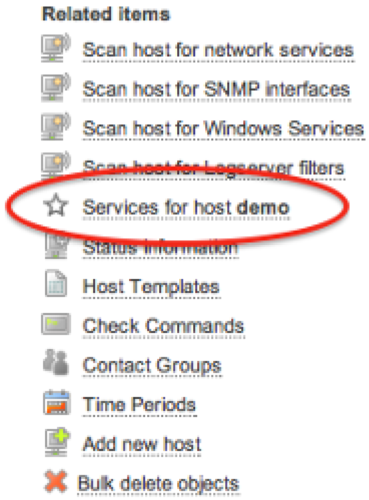
Bulk delete is powerful tool to remove several host or services at once.
Bulk delete support the following objects:

- Hosts
- Services
- Hostgroups
- Servicegroups
- Contacts
- Contactgroups
- Commands
- Time Periods

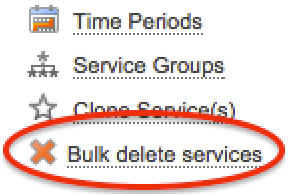
As an example, we will delete two services "Ping" on two different hosts, but the process is similar on all objects listed above.
To delete multiple services this is preformed trough Configure



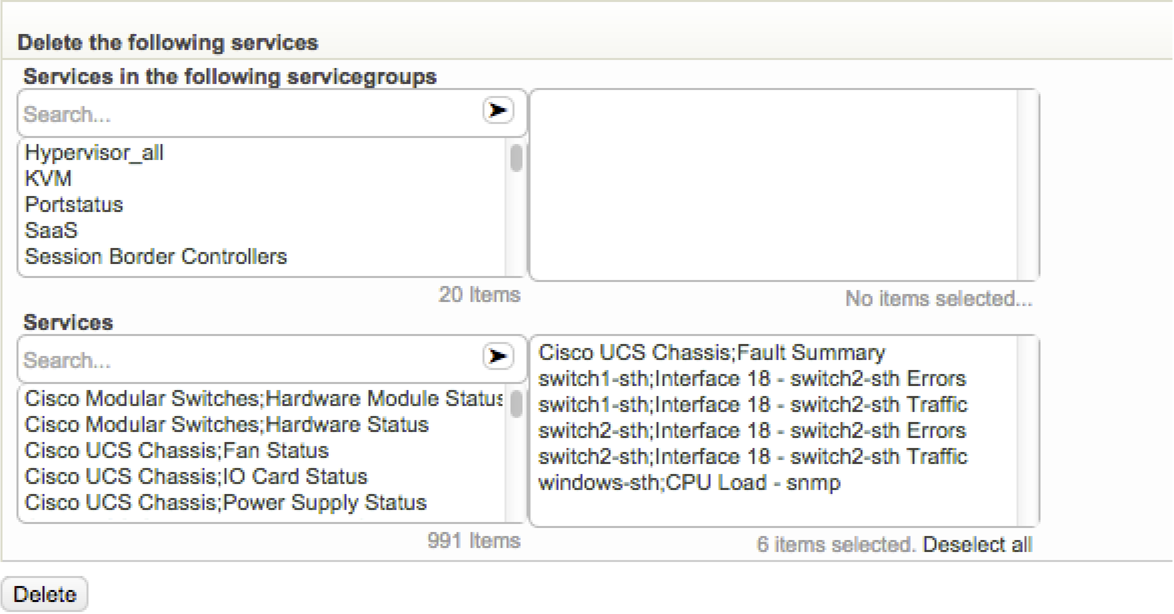
- Select a host which services you want to delete and click **GO**
- Click **Services for host** in the right menu.



- Click on **Bulk delete objects**



- Select the services that you want to delete and click **Delete**



Delete the following services

Services in the following servicegroups

Search...

Hypervisor_all
KVM
Portstatus
SaaS
Session Border Controllers

20 Items

No items selected...

Services

Search...

Cisco Modular Switches;Hardware Module Status
Cisco Modular Switches;Hardware Status
Cisco UCS Chassis;Fan Status
Cisco UCS Chassis;IO Card Status
Cisco UCS Chassis;Power Supply Status

991 Items

Cisco UCS Chassis;Fault Summary
switch1-sth;Interface 18 - switch2-sth Errors
switch1-sth;Interface 18 - switch2-sth Traffic
switch2-sth;Interface 18 - switch2-sth Errors
switch2-sth;Interface 18 - switch2-sth Traffic
windows-sth;CPU Load - snmp

6 items selected. Deselect all

- Click **Delete**

Time periods

About

In this section we will take a look at time periods.

Table of Content

Add a time period

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

Macros

About

Macros can be used to a lot of things. It can for example be used for paths, passwords and retrieving information from op5 monitor.
You can read more about notification commands in *Notification macros in the Notifications chapter*.

Table of Content

Pre-defined macros

By default op5 monitor has a number pre-defined macros. All from path to plugin folder to retrieving information about the last state of service check.
Below is a list of some macros a complete lite of macros can be found at nagios home page: http://nagios.sourceforge.net/docs/3_0/macroli

st.html

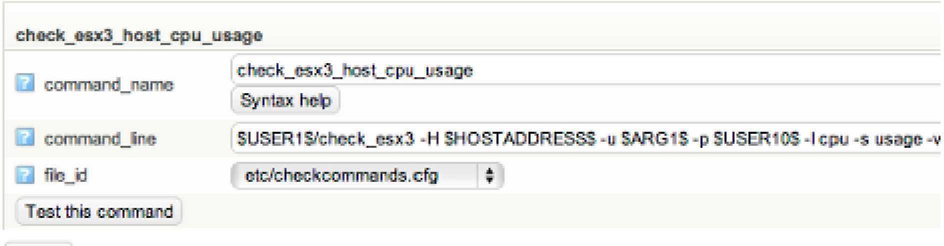
MACRO	DESCRIPTION
$USER1$	Path to /opt/plugins.
$ARGn$	The nth argument passed to the command
$HOSTNAME$	Short name for the host.
$HOSTADDRESS$	Address of the host.
$HOSTSTATE$	A string indicating the current state of the host ("UP", "DOWN", or "UNREACHABLE").
$SERVICEDISPLAYNAME$	An alternate display name for the service.
$SERVICESTATE$	A string indicating the current state of the service ("OK", "WARNING", "UNKNOWN", or "CRITICAL").

Custom macros

It is possible to create your own macros. This can be used to store passwords or user names for example.
All custom macros should be put in the file `/opt/monitor/etc/resource.cfg`
A custom macro should use the $USERn$ macro.
To define a password for a check, first add the macro in `resource.cfg`

```
# Password for vmware user
    $USER10$=secretpassw0rd
```

After that add the macro to check command, in this example we use the `check_esx3_host_cpu_usage` check command.



check_esx3_host_cpu_usage

command_name: check_esx3_host_cpu_usage

command_line: $USER1$/check_esx3 -H $HOSTADDRESS$ -u $ARG1$ -p $USER10$ -l cpu -s usage -v

file_id: etc/checkcommands.cfg

```
command_name=check_esx3_host_cpu_usage
command_line=$USER1$/check_esx3 -H $HOSTADDRESS$ -u $ARG1$ -p $USER10$ -l cpu -s usage -w $ARG2 -c $ARG3$
```

This check will use the following macros:
$HOSTADDRESS$ - Will get the address of the host from the configuration
$ARG1$ - Use the fist argument from the check command.
$USER10$ - Use the argument specified in resources.cfg with the same name.
$ARG2$ - Use the second argument from the check command.
$ARG3$ - Use the third argument from the check command.

Writeprotected configuration files

About

By making a file write-protected it cannot be changed by op5 Configuration. This is equivalent to the nagios function called **notouch.**

Table of Content

Writing the file

Create the file `/opt/monitor/op5/nacoma/custom_config.php`

Add the following content:

```
<?php
$notouch_file_prefix = 'static_';
?>
```

If a configuration file in is renamed with the *`static_`* prefix op5 configuration will not be able to change this file.

Features not supported by Configure

About

Even though some features are not supported by the op5 Monitor configuration tool you can still use them.
The `hostgroup_name` is one of them.
What you have to do is to add a separate configuration file not read by the import function in Configure. Then you add your other configuration tricks into that file.

Table of Content

To add a configuration file not read by Configure

- Open up a ssh connection to the op5 Monitor server and login as root.
- Create the following file with an editor of your choice:

  `/opt/monitor/op5/nacoma/custom_config.php`

- Add the following code to the file you just created:

  ```
  <?php
  $notouch_file_prefix = "_";
  ?>
  ```

- Create a configuration file with "_" as a prefix to the file name like this:

  `touch /opt/monitor/etc/_custom_objects.cfg`

- Add the file to the /opt/monitor/etc/nagios.cfg with by adding the following line below the other cfg_file variables in nagios.cfg:

  `cfg_file=/opt/monitor/etc/_custom_objects.cfg`

- Restart op5 Monitor.

  `service monitor restart`

Now you may add your objects to the new configuration file and they will not be loaded into Configure. But you can still see the objects using View config as it is described in the op5 Monitor user manual.

Plugins

Introduction

op5 Monitor is shipped with many plugins that cover most monitoring needs. But what to do if one of your corporate applications can not be monitored straight out of the box?
Often you can find a plugin at www.nagiosexchange.org, and since op5 Monitor and Nagios uses the same plugin format you can often simply

download a plugin, put it in /opt/plugins/custom/ and start using it.
However, if you can not find a suitable plugin anywhere you might have to write your own plugin. Since the plugin interface is very straight-forward, anyone with a fair amount of UNIX scripting experience can do this.
If you need help developing a plugin you may also contact a op5 sales representative to get a quote.

Adding your first plugin to op5 Monitor

About

In this section we will create a very simple check plugin in the bash programming language to demonstrate *op5 Monitor*'s plugin interface. The plugin will not be very useful, but we will use it to describe the steps needed to create your own monitoring plugins.

This tutorial requires you to have shell access to the server running *op5 Monitor* and some basic UNIX/Linux knowledge.

Table of Content

Creating the plugin

1. Open a SSH session to the host running *op5 Monitor*
2. Move to the custom plugins directory, create the example plugin "helloworld" and make it executable:

```
$ cd /opt/plugins/custom
# touch helloworld
# chmod 755 helloworld
```

3. Open the plugin with your favorite text editor and add the following code to the empty file:

```
#!/bin/sh
echo 'WARNING: Hello world!'
exit 1
```

4. Save and exit your text editor
5. The bash script is now a usable check plugin. You can test it by executing it in the terminal and verify that it exits with the return code "1" (warning state):

```
$ ./helloworld
WARNING: Hello world!
$ echo $?
1
```

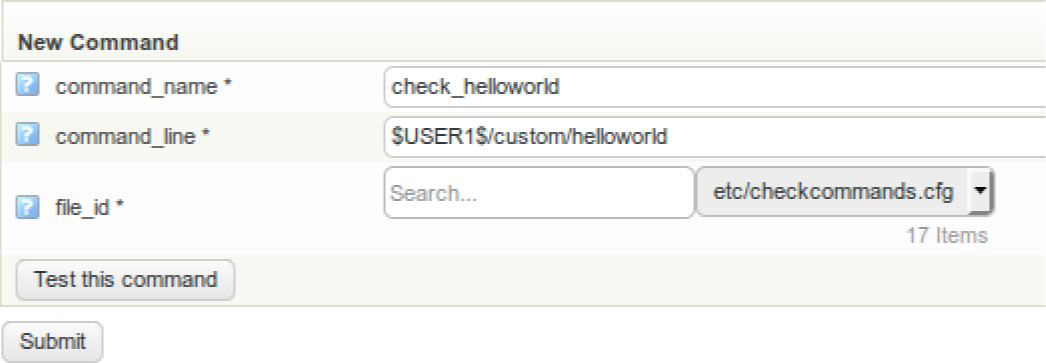
Using the plugin in op5 Monitor

Configuring the plugin as a check command

1. Go to the configuration page and enter the "Commands" section:
   Add a new command with the following parameters:

```
command_name: check_local_helloworld
command_line: $USER1$/custom/helloworld
```

It should look like this in the configuration dialog:

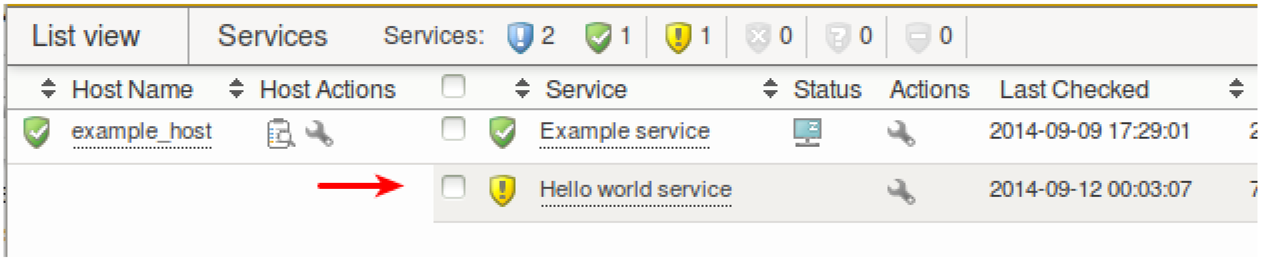


New Command

command_name *	check_helloworld
command_line *	$USER1$/custom/helloworld
file_id *	Search... etc/checkcommands.cfg 17 Items

2. Click "Submit" and save the configuration

Now you may use your check command with a service as described in *Services*



Host Name	Host Actions	□	Service	Status	Actions	Last Checked
example_host		□	Example service			2014-09-09 17:29:01
		□	Hello world service			2014-09-12 00:03:07

Before you start

About

Before you can start developing you own plugins you need to make sure you have SSH access or terminal access to your op5 server orthe possibility to transfer files to your op5 Monitor server. Any kind of editor can be used, vim and jed are installed by default on your op5 Monitor server.

Table of Content

⚠ Microsoft Windows users may use PuTTY for terminal access via SSH and WinSCP for file transfers via SFTP (SSH).
Macintosh or UNIX/Linux users may use the commands ssh or scp from a local terminal window.

Creating a more complex plugin

About

In this section we will create a more complex and useful plugin compared to the one we created in *Adding your first plugin to op5 Monitor*.
We will stick to bash, because of the simplicity.
We will create a plugin that checks that the storage path specified in `/etc/op5backup.conf` exists, to make sure that `op5backup.sh` is configured properly for local operation.

Table of Content

To create a more complex plugin

1. Create the script and edit it:

```
$ cd /opt/plugins/custom
# touch check_op5backup
# chmod 755 check_op5backup
```

2. Open up the script with your favorite text editor and type in the following code:

```
#!/bin/bash
# Create a function to print the storage path
storagepath() {
grep ^storagepath /etc/op5backup.conf |
tail -1 |
sed 's/^[^"]*"//g' | sed 's/"$//g'
}

# Put the storage path in an environmental variable
STORAGEPATH=`storagepath`

# Test if the storagepath exists and is a directory
if [[ ! -d "$STORAGEPATH" ]]; then
# Print a warning message for the web gui
echo op5backup.sh is not properly configured for local operation
# Exit with status Warning (exit code 1)
exit 1
fi

# If the script reaches this point then the test passed
# Print an OK message
echo $STORAGEPATH exists
# Exit with status OK
exit 0
```

3. Add a check_command like this using the op5 Monitor web gui:
   command_name: `check_op5backup`
   command_line: `$USER1/custom/check_op5backup`

4. Enter the service configuration for your monitor server, and add a service with `check_op5backup` as the check_command.
5. Save configuration.

More information

About

This chapter has only scratched on the surface of how to write your own plugins.
To read more about plugin development take a look at the **Monitoring plugin development guidelines**:
https://www.monitoring-plugins.org/doc/guidelines.html

Table of Content

Paths and macros

Paths and macros

All standard plugins shipped with op5 Monitor are installed in:

```
/opt/plugins
```

The macro you use to reach the plugins folder is:

```
$USER1$
```

The plugins you add to the system by your own must be placed in:

```
/opt/plugins/custom
```

And they will then be reached with the following macro/path:

```
$USER1$/custom
```

The reason for placing your own plugins in /opt/plugins/custom is because then they will not be touched by any upgrade from op5.

Table of Content

Support levels

About

Plugins that are shipped with op5 Monitor will have different support levels.
There are four levels.

Table of Content

Full

This plugin is fully supported.
The plugin is continuously tested by op5. A fully compatible test environment for the plugin is in place to verify its functionality.

Bug support

The plugin is not continuously tested by op5. op5 probably do not have a compatible test environment in place and/or resources to test the plugin. If an issue with the plugin is found, op5 will examine the importance and prioritize according to impact and level of effort. op5 monitors the upstream project (if any) and updates the shipped plugin regularly.
Best effort

Best effort

The plugin is shipped as a courtesy to op5 customers. Dependencies are resolved and the plugin is executed without runtime errors. The plugin has normally only been installed and tested at a customer site.
op5 support helps out with command syntax.

Unsupported

This plugin is unsupported by op5.

The plugin interface

About

A plugin is a small executable that takes optional command line parameters as input and

1. Performs a test
2. Reports a diagnostic message on stdout (will be shown in the web GUI)
3. Returns an exit code.

Table of Content

Example

Execute `check_tcp` to test the port 80/tcp on 193.201.96.136

```
monitor!root:~# /opt/plugins/check_tcp -H 193.201.96.136 -p 80
TCP OK - 0.043 second response time on port
80|time=0.042824s;0.000000;0.000000;0.000000;10.000000
monitor!root:~# echo $?
0
monitor!root:~# /opt/plugins/check_tcp -H 193.201.96.136 -p 143
Connection refused
monitor!root:~# echo $?
2
monitor!root:~#
```

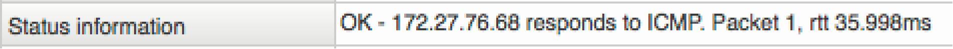
In the *Example* we first execute `check_tcp` to test that port 80/tcp on 193.201.96.136 responds, which it does, hence the exit code of 0.
Then we check port 143/tcp on the same host and that port is not open, hence the result is Critical - exit code 2.
The result output is actually built upon two parts divided by a | sign (pipe). The text on the

- left hand side of the | is the status information
- right hand side of the | is the performance data.

The performance data is not mandatory but you need it if you want your plugin to be able to produce graphs for you in op5 Monitor.

Status information

The Status information is the text describing the result in human readable form. The plugin must print the status output to stdout when your plugin is executed.
You will see it in the Status state information on the Service or Host information page.



Status information	OK - 172.27.76.68 responds to ICMP. Packet 1, rtt 35.998ms

This text can be anything, you like to use to describe the status situation for your plugin, including HTML.

Performance data

The performance data is data displaying the result in numbers. The plugin must print the status output to stdout when your plugin is executed. It is also to produce performance graphs in op5 Monitor.
So if you want graphs from your plugin you need to have performance data in your output.
The performance data is setup like this:

```
'label'=value[UOM];[warn];[crit];[min];[max]
```

Performance parts with descriptions*:*

Part	Description
label	The label can contain any characters. If space is included quotes are needed.
value	The plugin was able to check the service, but it appeared to be above some "warning" threshold or did not appear to be working properly
UOM	Can be any of: • no unit assuming an integer as a value • s - seconds (also us, ms) • % - percentage. • B- Bytes (also KB, MB, GB and TB) • c - A continuous counter like bytes transmitted on an interface.
warn, crit, min, max	• Can all be null and trailing unfilled semicolons can be dropped. • min and max is not needed if UOM is %. • value, warn, crit, min and max must be of the same UOM.

Example 2

Performance data output:

```
time=0.218901s;;;0.000000 size=42236B;;;0
```

The *Example2* shows a performance data output from a plugin with two values separated with one space in the output.

Return code

The return code is the one that op5 Monitor uses to determine what state the services is in. It may be one of the following:

```
0, 1, 2, 3
```

Any return code above 0 is to be known as **problem states**.
The return codes in detail*:*

Nr	Name	Description
0	Ok	The check did ok and everything seems to be working fine.
1	Warning	The plugin was able to check the service, but it appeared to be above some "warning" threshold or did not appear to be working properly
2	Critical	The plugin detected that either the service was not running or it was above some "critical" threshold
3	Unknown	Something unknown happened during the check. Things like invalid command line arguments or low-level failures internal to the plugin shall **not** be reported as Unknown state.

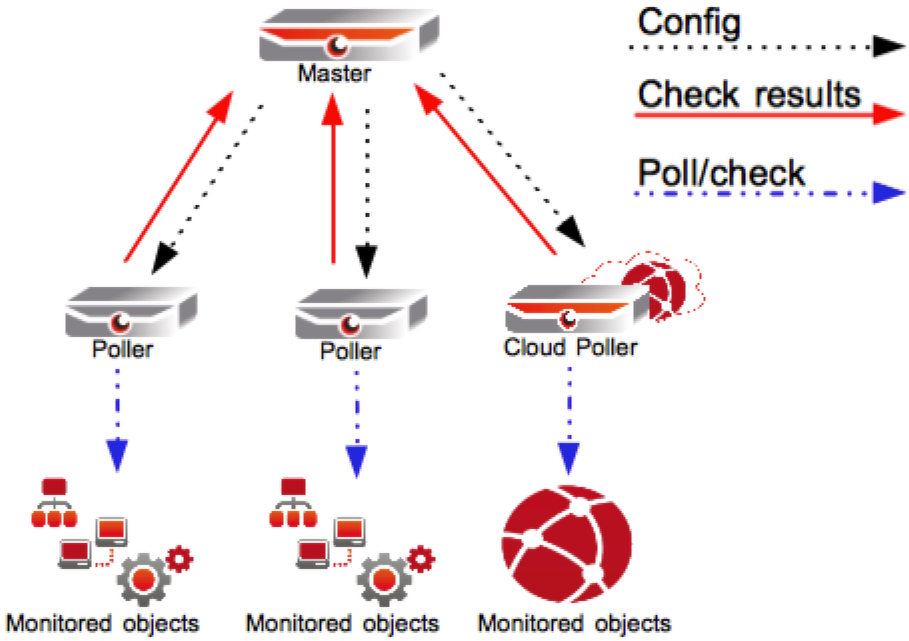
Scalable Monitoring

Scalable Monitoring

Distributed Monitoring

Introduction

The op5 Monitor backend can easily be configured to be used as a distributed monitoring solution. The distributed model looks like this.



In the distributed monitoring solution:

- All configuration is performed on the master node.
- All new configuration is distributed to the pollers.
- Each poller node is responsible for its own host group (site).
- The master node has all the status information.

Table of Content

Before we start

Prerequisites

There are a few things you need to take care of before you can start setting up a distributed monitoring solution. You need to make sure you have at least two servers of **the same architecture** (32/64 bit), both running the **same** version of op5 Monitor.

More specifically, make sure that:

- op5 Monitor version >=5.2 is installed and running on all servers.
- The following TCP ports must be opened on the poller nodes, to allow master nodes to successfully communicate with poller nodes:
    - 22 (SSH), used for distributing configuration from master to poller nodes.
    - 15551 (merlin), used for state communication, such as check results.
- All server names must be resolvable by DNS or manually via */etc/hosts*.
- All servers' system clocks must be synchronized, preferably by NTP.
- The host group which the poller will be responsible for must be set up on the master, in advance. At the bare minimum, the host group must contain at least one host, with at least one contact and one service.

Cluster state information

In the op5 Monitor system, a tool called *mon* can be found via the command line (accessed via SSH). To view the current cluster state, run the command like this:

```
mon node status
```

All known nodes, the local one, peers and pollers, should be displayed, including their current state. A properly synchronized and online cluster should display all nodes as *ACTIVE*. Beware of any text colored in red.

More information regarding the mon command can be found here.

The configuration

Setting up the new distributed monitoring solution

This distributed configuration will have one master and one poller node:

- master01
- poller01

The poller will be monitoring a host group named *se-gbg*.

Poller-side configuration

1. Log on to the new poller via SSH, as root.

2. Remove master-only configuration files from the poller:
   ```
   sed -i /^cfg_file=/d /opt/monitor/etc/naemon.cfg
   ```

3. Find out which configuration files are currently active on the poller:
   ```
   mon oconf files
   ```
   This should give you the following list of configuration files, which indicates that the master has not yet pushed any configuration towards the poller.
   ```
   /opt/monitor/etc/synergy/command.cfg
   /opt/monitor/etc/synergy/services.cfg
   /opt/monitor/etc/trapper/command.cfg
   ```
   No configuration files should be seen located directly in */opt/monitor/etc/.*

4. The poller's current configuration files must not be marked as modified in the future, in the point of view of any of the masters. To make sure this isn't the case, reset the file modification timestamps:
   ```
   mon oconf files \| xargs touch -d 01-02-03 --
   ```

Master-side configuration

1. Make sure that the host group which the poller will be responsible for is already configured, saved and can be found in the status pages of the op5 Monitor web interface. Remember, at the bare minimum, the host group must contain at least one host, with at least one contact and one service.

2. In case of running a load balanced setup with peered masters, make sure that all peers are fully connected and synchronized according to mon node status. The following steps (starting from step 3), should be performed on all masters.

3. Log on to the master via SSH, as root.

4. To verify that the host group exists, print its current host members:
   ```
   mon query ls hostgroups -c members name=se-gbg
   ```

5. Add the new poller to the configuration:
   ```
   mon node add poller01 type=poller hostgroup=se-gbg takeover=no
   ```

6. Set up SSH connectivity between the master and the poller:
   ```
   mon sshkey push poller01
   asmonitor mon sshkey push poller01
   ```

7. Add the master to the poller's configuration:
   ```
   mon node ctrl poller01 mon node add master01 type=master connect=no
   ```

Pushing the configuration

In case of peered masters, **perform these steps only on *one* of the masters**.

1. Restart naemon on the master to prepare for configuration push.
   ```
   service naemon restart
   ```

2. Push configuration from the master to the new poller:
   ```
   asmonitor mon oconf push poller01
   ```

3. Restart op5 Monitor on the new poller:
   ```
   mon node ctrl poller01 mon restart
   ```

4. Restart op5 Monitor on all masters:
   ```
   mon node ctrl --self --type=peer mon restart
   ```

Adding a new host group to a poller

A poller can handle several host groups, which is a simple way of increasing a poller's scope.

Master-side configuration

In case of running a load balanced setup with peered masters, make sure that all peers are fully connected and synchronized according to mon node status first. The steps below should be performed on all masters.

1. Log on to the master via SSH, as root.

2. Edit the file */opt/monitor/op5/merlin/merlin.conf* using a text editor:
   ```
   nano /opt/monitor/op5/merlin/merlin.conf
   ```

3. Find the configuration block related to the poller. Within this block, append the new host group onto the *hostgroup* setting's value, prefixed by a comma. In this case a host group called *se-sth* is added.

   In this example, the line originally looked like:
   ```
   hostgroup = se-gbg
   ```

   And then once the new host group had been added:
   ```
   hostgroup = se-gbg,se-sth
   ```

   The setting is comma-separated – not space-separated.

Finish up by pushing the configuration.

Removing a poller

In this instruction we will remove a poller called:

- poller01

The poller will be removed from the master's configuration, and then all distributed configuration on the poller will be removed.

To remove a poller

In case of peered masters, **perform these steps only on *one* of the masters**.

1. Log on to the master via SSH, as root.

2. Remove the poller from the configuration on all masters:
   ```
   mon node ctrl --self --type=peer mon node remove poller01
   ```

3. Restart op5 Monitor on all masters:
   ```
   mon node ctrl --self --type=peer mon restart
   ```

4. Restart op5 Monitor on the poller:
   ```
   mon node ctrl poller01 mon restart
   ```

File synchronization

Information regarding how to synchronize files and/or directories from a master to a poller can be found in the File synchronization chapter.

Notify through master

Depending on the setup of a poller, it might be difficult to send notifications directly from the poller. This could be due to a non-existing or non-accessible SMS/SMTP gateway. In such scenarios it is possible to send notifications through the master instead.

Master-side configuration

The steps below should be performed on all masters, in case of running a load balanced setup with peered masters.

1. Log on to the master via SSH, as root.

2. Edit the file */opt/monitor/op5/merlin/merlin.conf* using a text editor:
   ```
   nano /opt/monitor/op5/merlin/merlin.conf
   ```

3. Find the configuration block related to the poller. Within this block, a new option *notifies* = *no* is inserted, as seen in the example below.

   ```
   poller poller01 {
     address = 192.0.2.50
     port = 15551
     takeover = no
     notifies = no
   }
   ```

4. Restart op5 Monitor:
   ```
   mon restart
   ```

Poller-side configuration

1. Log on to the poller via SSH, as root.

2. Edit the file */opt/monitor/op5/merlin/merlin.conf* using a text editor:
   ```
   nano /opt/monitor/op5/merlin/merlin.conf
   ```

3. Find the *module* configuration block. Within this block, a new option *notifies* = *no* is inserted, as seen in the example below.

   ```
   module {
     log_file = /var/log/op5/merlin/neb.log;
     notifies = no
   }
   ```

4. Restart op5 Monitor:
   `mon restart`

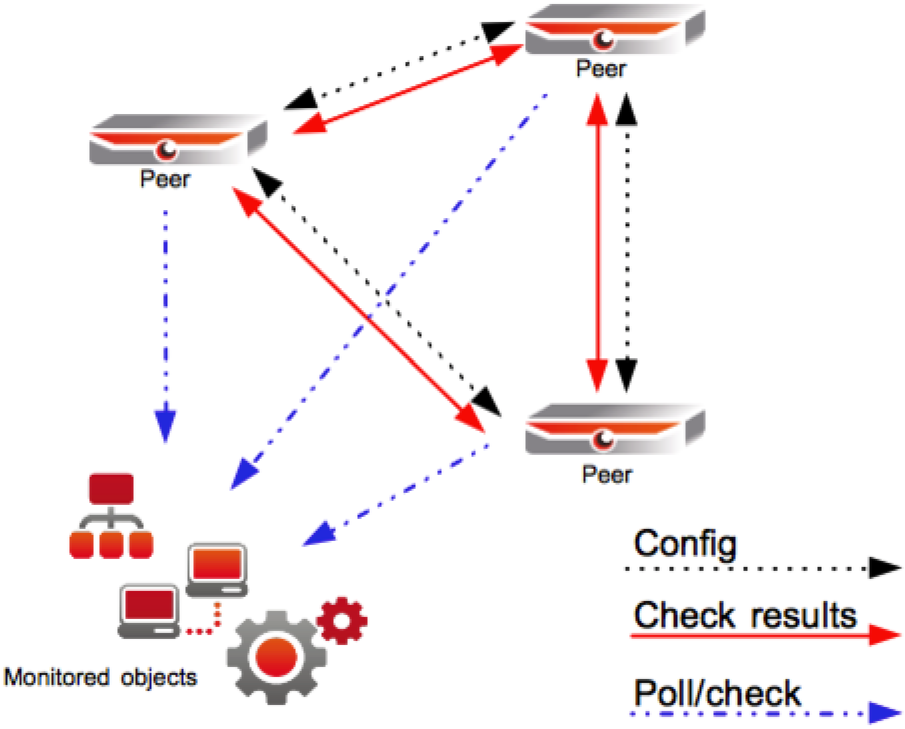
More information

For more information and advanced examples, please have a look at the How-To document found in the merlin project.

Load balanced monitoring

Introduction

The op5 Monitor backend can easily be used as a load balanced monitoring solution. The load balanced model looks like this.



The load balanced solution have two or more peers in the same environment sharing the same tasks (the hosts to monitor). Any new configuration made on any of the peers is distributed to the other peers. The peers divides the load automatically and keep tracks of when one peer go down, the other(s) take over the job.

Table of Content

Before we start

Prerequisites

There are a few things you need to take care of before you can start setting up a load balanced monitoring. You need to make sure you have at least two servers of **the same architecture** (32/64 bit), both running the **same** version of op5 Monitor.

More specifically, make sure that:

- op5 Monitor version >=5.2 is installed and running on all servers.
- The peers will connect to each other on the following TCP ports, that must be opened up for successful communication:
  - 22 (SSH), used for distributing configuration between peers.
  - 15551 (merlin), used for state communication, such as check results.
- All server names must be resolvable by DNS or manually via */etc/hosts*.
- All servers' system clocks must be synchronized, preferably by NTP.

Cluster state information

In the op5 Monitor system, a tool called *mon* can be found via the command line (accessed via SSH). To view the current cluster state, run the command like this:

```
mon node status
```

All known nodes, the local one, peers and pollers, should be displayed, including their current state. A properly synchronized and online cluster should display all nodes as *ACTIVE*. Beware of any text colored in red.

More information regarding the mon command can be found here.

The configuration

Setting up the load balanced solution

This load balanced configuration will be set up with two peered nodes ("peers"):

- peer-blue
- peer-green

To set up a load balanced monitoring solution

1. Log on to peer-green via SSH, as root.

2. Add peer-blue to peer-green's configuration:
   ```
   mon node add peer-blue type=peer
   ```

3. Set up SSH connectivity towards all of peer-green's configured peers:
   ```
   mon sshkey push --type=peer
   asmonitor mon sshkey push --type=peer
   ```

4. Log on to peer-blue via SSH, as root.

5. Add peer-green to peer-blue's configuration:
   ```
   mon node add peer-green type=peer
   ```
6. Set up SSH connectivity towards all of peer-blue's configured peers:
   ```
   mon sshkey push --type=peer
   asmonitor mon sshkey push --type=peer
   ```

7. Push peer-blue's configuration to peer-green:
   ```
   asmonitor mon oconf push peer-green
   ```

8. Restart op5 Monitor on all nodes:
   ```
   mon node ctrl --self -- mon restart
   ```

9. After a minute or two, make sure that the peers are fully connected and synchronized according to mon node status.

⚠ In case you have been running op5 Monitor for a while already, and you are now about to convert your standalone server to a load balanced setup, you should think of peer-blue as your current op5 Monitor server, and peer-green as the new peer. **This is important to get right, as you may otherwise push the new peer's empty host/service object configuration to the current server,**

effectively overwriting your actual configuration. If in doubt, please consult your technical contact at op5.

Adding another peer

In this instruction we will have the following hosts:

- peer-green
- peer-blue
- peer-red (This is the new one.)

To add a new peer

1. Log on to peer-red via SSH, as root.

2. Add all the previously existing peers to peer-red:
   ```
   mon node add peer-green type=peer
   mon node add peer-blue type=peer
   ```

3. Set up SSH connectivity towards all of peer-red's configured peers:
   ```
   mon sshkey push --type=peer
   asmonitor mon sshkey push --type=peer
   ```

4. Add peer-red to all other nodes:
   ```
   mon node ctrl --type=peer mon node add peer-red type=peer
   ```

5. Log on to all previously existing peers via SSH, as root, and set up SSH connectivity towards all their configured peers (including the new peer-red):
   ```
   mon sshkey push --type=peer
   asmonitor mon sshkey push --type=peer
   ```

6. On any one of the previously existing peers (green or blue in this case), push its configuration to the new peer:
   ```
   asmonitor mon oconf push peer-red
   ```

7. Finally, on any of the peers (old or new), trigger a full restart op5 Monitor on all nodes:
   ```
   mon node ctrl --self -- mon restart
   ```

8. After a minute or two, make sure that the peers are fully connected and synchronized according to mon node status.

Removing a peer

In this instruction we will remove a peer called:

- peer-red

The peer will be removed from all other peers' configuration.

To remove a peer

1. Log on to peer-red via SSH, as root.

2. Remove oneself from all other peers:
   ```
   mon node ctrl --type=peer mon node remove peer-red\; mon restart
   ```

   The backslash (\) in front of the semi-colon (;) is important to get right in this command.

3. Remove all local configuration:
   ```
   mon node remove $(mon node list --type=peer)
   ```

4. Restart op5 Monitor:
   ```
   mon restart
   ```

5. Unless peer-red isn't powered off, the node will be running with the same configuration as its previous peers, but as a standalone server, performing all host/service check on its own.

File and directory synchronization

Information regarding how to synchronize files and/or directories between peers can be found in the File synchronization chapter.

More information

For more information and advanced examples, please have a look at the How-To document found in the merlin project.

File synchronization

Introduction

There is limited support for synchronizing files between peers, and between masters and pollers.

For example, when a new user has been added in op5 Monitor on one of your masters, this function can be used to automatically synchronize the user database files on all other peers and pollers.

Prerequisites

Make sure you have already set up a either a load balanced or distributed monitoring environment (or a combination of which).

Table of Content

The configuration

Although the setup is the same configuration-wise, there are two common but different ways of synchronization:

- Peered masters synchronizing files with one another (two-way).
- Masters synchronizing files to pollers (one-way).

The example and the described procedure below applies to both of these cases. However, it is recommended to repeat the procedure for all peers in case of file synchronization between peers.

Configuring the sync directive

In this example, the master will synchronize files to its poller called *poller01*.

The following files will be synchronized:

- /etc/op5/auth_users.yml
- /etc/op5/auth_groups.yml

The contents of the following directory will also be synchronized.

- /opt/plugins/custom/

Configuration procedure

1. Log on to the source node via SSH (in this case the master), as root.

2. Edit the file */opt/monitor/op5/merlin/merlin.conf* using a text editor:
   `nano /opt/monitor/op5/merlin/merlin.conf`

3. Find the configuration block related to the destination node (in this case poller01). Within this block, a new *sync* sub-block is inserted.

```
poller poller01 {
  hostgroup = se-gbg
  address = 192.0.2.50
  port = 15551
  takeover = no
  sync {
    /etc/op5/auth_users.yml
    /etc/op5/auth_groups.yml
    /opt/plugins/custom/
  }
}
```

> ⚠ The trailing slash at the end of */opt/plugins/custom/* in the example above indicates that the contents of the directory should be synchronized, rather than the directory itself. This is the recommended way of synchronizing directories.

Permission limitations

The files will be synchronized using the *monitor* system user – not *root*. This means that:

- Files and directories set up for synchronization must be readable and owned by the monitor user. For instance, root-only readable files cannot be synchronized.
- All file paths and their corresponding directories, must be writable by the monitor user on the destination node.

Triggering the synchronization

The file and directory synchronization occurs during a *configuration push*, which is triggered as a new configuration is saved in the web interface. For instance, adding a new host in Monitor and then saving the configuration will trigger this.

Merlin

About

Merlin is the backend engine for a load balanced and/or distributed setup of op5 Monitor.
Merlin, or Module for Effortless Redundancy and Load balancing In Nagios, allows the op5 Monitor processes to exchange information directly as an alternative to the standard nagios way using NSCA.
Merlin functions as backend for Ninja by adding support for storing the status information in a database, fault tolerance and load balancing.
This means that Merlin now is responsible for providing status data and acts as a backend, for the Ninja GUI.

Table of Content

Merlin components

merlin-mod

merlin-mod is responsible for jacking into the NEBCALLBACK_* calls and send them to a socket. If the socket is not available the events are written to a backlog and sent when the socket is available again.

merlind

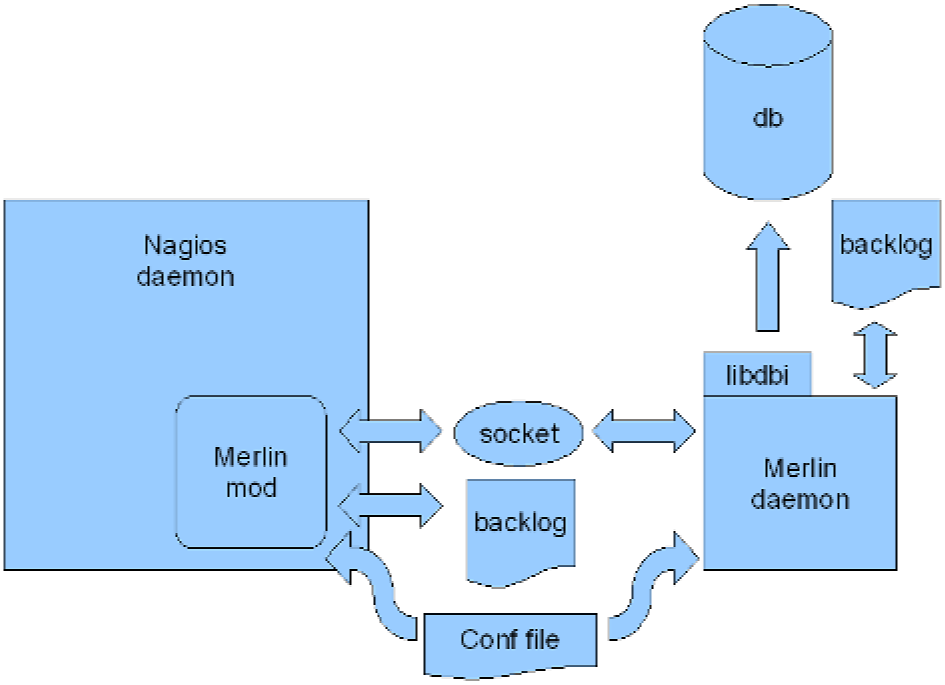
The Merlin deamon listens to the socket that merlin-mod writes to and sends all events received either to a database of your choice (using libdbi) or to another merlin daemon. If the daemon is unsuccessful in this it writes to a backlog and sends the data later.

merlin database

This is a database that includes Nagios object status and status changes. It also contains comments, scheduled downtime etc.

Illustration

This picture illustrates the components described above



The mon command

About

The mon command is a very powerful command. Primarily, this is the command that is used to manually stop and start the monitor system processes, and to set up a distributed or a load balanced environment.

Handle this command with care! It has the power to both create and destroy your whole op5 installation.

Do not use this command unless specifically instructed by op5 Support or the Documentation itself.

Table of Content

The commands

```
# mon
```

Simply running the command without any arguments will present a small syntax help text, and a list of available sub commands. Most sub commands are categorized, meaning that *mon* has to be run with at least two arguments to trigger the sub command. A few sub commands are non-categorized, requiring only a single argument being passed to *mon* to trigger the sub command.

start

```
# mon start
```

This command will start the monitor and merlind system processes.

stop

```
# mon stop
```

This command will stop the monitor and merlind system processes.

restart

```
# mon restart
```

This command will restart the monitor and merlind system processes.

ecmd

search

```
mon ecmd search <regex>
```

Prints 'templates' for all available commands matching <regex>.
The search is case insensitive.

submit

```
mon ecmd submit [options] command <parameters>
```

Submits a command to the monitoring engine using the supplied values.
Available options:

```
--pipe-path=</path/to/nagios.cmd>
```

Example:
An example command to add a new service comment for the service PING on the host foo would look something like this:

```
mon ecmd submit add_svc_comment service='foo;PING' persistent=1 author='John Doe'
comment='the comment'
```

Note how services are written. You can also use positional arguments, in which case the arguments have to be in the correct order for the command's syntactic template. The above example would then look thus:

```
mon ecmd submit add_svc_comment 'foo;PING' 1 'John Doe' 'the comment'
```

log

show

```
# mon log show
```

Runs the showlog helper program. Arguments passed to this command will be sent to the showlog helper.
For more information, a help text can be found by running the command like this:

```
# mon log show --help
```

node

add

```
# mon node add <name> --type=[peer|poller|master] [var1=value] [varN=value]
```

Adds a node with the designated type and variables.

ctrl

```
# mon node ctrl <name1> <name2> [--self] [all|--type=<peer|poller|master>] -- <command>
```

Execute <command> on the remote node(s) named.

Optional arguments:

--self	Run the command on the local system also.
--all	Run the command on all configured nodes.
--type	Run the command on configured nodes of the given type(s).
--	Stop argument scanning. Everything beyond will be treated as the command to run.

The first unrecognized argument marks the start of the command to be executed, but using double dashes is recommended. Use single-quotes to execute commands with shell variables, output redirection or scriptlets, like so:

```
# mon node ctrl -- '(for x in 1 2 3; do echo $x; done) > /tmp/foo'
```

```
# mon node ctrl -- cat /tmp/foo
```

list

```
# mon node list [--type=poller,peer,master]
```

Lists all nodes of the (optionally) specified type

remove

```
# mon node remove <name1> [name2] [nameN]
```

Removes one or more nodes from the merlin configuration.

show

```
# mon node show [--type=poller,peer,master]
```

Display all variables for all nodes, or for one node in a fashion suitable for being used as eval $(mon node show nodename) from shell scripts and scriptlets.

status

```
# mon node status
```

Show status of all nodes configured in the running Merlin daemon.
Red text points to problem areas, such as high latency or the node being inactive, not handling any checks, or not sending regular enough program_status updates.

oconf

changed

```
# mon oconf changed
```

Print the last modification time among all object configuration files.

files

```
# mon oconf files
```

Print a list of the nagios object configuration files in alphabetical order.

hash

```
# mon oconf hash
```

Print an sha1 hash of the running configuration.

hglist

```
# mon oconf hglist
```

Print a sorted list of all configured hostgroups.

nodesplit

```
# mon oconf nodesplit
```

Same as 'split', but use merlin's config to split config into configuration files suitable for poller consumption

push

```
# mon oconf push
```

Splits configuration based on merlin's peer and poller configuration and send object configuration to all peers and pollers, restarting those that receive a configuration update. ssh keys need to be set up for this to be usable without admin supervision. This command uses 'nodesplit' as its backend.

split

```
# mon oconf split <outfile:hostgroup1,hostgroup2,hostgroupN>
```

Write config for hostgroup1,hostgroup2 and hostgroupN into outfile.

sshkey

fetch

```
# mon sshkey fetch
```

Fetches all the SSH keys from peers and pollers.

> ⚠ The fetch command is not recommended – run the push command instead.

push

```
# mon sshkey push
```

Pushes the local SSH keys to all peers and pollers.

sysconf

ramdisk

```
# mon sysconf ramdisk
```

To enable the ramdisk setup:

```
# mon sysconf ramdisk enable
```

A ramdisk can be enabled for storing spools for performance data and checkresults.

~~By storing these spools on a ramdisk we can lower the disk I/O significantly.~~

> ⚠ As of Monitor 6, enabling the ramdisk is no longer recommended. To disable the ramdisk if already enabled, see the separate article Reverting a ramdisk enabled setup back to the default non-ramdisk layout.

rrdmultiple

```
# mon sysconf rrdmultiple
```

This will convert RRD graphing files from being stored in *single* mode, into being stored in *multiple* mode instead. This is not needed for new installations as of op5 Monitor version 6.3.

check

spool

```
$ mon check spool [--maxage=<seconds>] [--warning=X] [--critical=X] <path> [--delete]
```

Checks a certain spool directory for files (and files only) that are older than 'maxage'. It's intended to prevent buildup of checkresult files and unprocessed performance-data files in the various spool directories used by op5 Monitor.

--delete	Remove files that are too old.
--maxage	Is given in seconds and defaults to 300 (5 minutes).
<path>	May be 'perfdata' or 'checks', in which case directory names will be taken from op5 defaults
--warning and --critical	Have no effect if '--delete' is given and will otherwise specify threshold values.

> Only one directory at a time may be checked.

cores

```
$ mon check cores --warning=X --critical=X [--dir=]
```

Checks for memory dumps resulting from segmentation violation from core parts of op5 Monitor. Detected core-files are moved to /tmp/mon-cores in order to keep working directories clean.

--warning	Default is 0
--critical	Default is 1 (any corefile results in a critical alert)
--dir	Lets you specify more paths to search for corefiles. This option can be given multiple times.
--delete	Deletes corefiles not coming from 'merlind' or 'monitor'.

distribution

```
$ mon check distribution [--no-perfdata]
```

Checks to make sure distribution works ok.

> Note that it's not expected to work properly the first couple of minutes after a new machine has been brought online or taken offline

exectime

```
$ mon check exectime [host|service] --warning=<min,max,avg> --critical=<min,max,avg>
```

Checks execution time of active checks.

[host|service]	Select host or service execution time.
--warning	Set the warning threshold for min,max and average execution time, in seconds
--critical	Set the critical threshold for min,max and average execution time, in seconds

latency

```
$ mon check latency [host|service] --warning=<min,max,avg> --critical=<min,max,avg>
```

Checks latency time of active checks.

[host|service]	Select host or service latency time.
--warning	Set the warning threshold for min,max and average execution time, in seconds
--critical	Set the critical threshold for min,max and average execution time, in seconds

orphans

```
#mon check orphans
```

Checks for checks that haven't been run in too long a time.

VRRP

About

VRRP can be used in this setup to have one DNS-name and one IP address that is primary linked to one of the master servers and if the primary master for some reason is unavailable VRRP will automatically detect this and send you to the secondary master.

Table of Content

Setup

To enable VRRP on you master servers follow the steps below.
In this example we have two masters that we want to use VRRP with.
The VRRP IP will be 192.168.1.3 and we will bind that IP to the network interface eth0.
The IP and interface will have to change to match your network configuration.

⚠ If you already use VRRP in your network, make sure that you use the correct virtual_router_id.

Edit the file */etc/keepalived/keepalived.conf*

On the "primary" master

```
vrrp_instance VI_1 {
state MASTER
interface eth0
virtual_router_id 51
priority 200
advert_int 1
virtual_ipaddress {
192.168.1.3 dev eth0
}
}
```

On the "secondary" master

```
vrrp_instance VI_1 {
state BACKUP
interface eth0
virtual_router_id 51
priority 100
advert_int 1
virtual_ipaddress {
192.168.1.3 dev eth0
}
}
```

Activate VRRP

To activate vrrp run the following command:

```
# chkconfig keepalived on
```

Third Party Configuration Import

Introduction

op5 Monitor has the capability to import the configuration from any nagios installation.
To do follow this manual basic knowledge in linux and nagios is necessary.

Table of Content

Pre-requirements

A running nagios 3.x installation and op5 Monitor.

Limitations

There are some of limitations of the import script.
The import-script does not work with a nagios 1 or 2 installation.
Host and service history can not be imported, but can be copied manually.
Graph history can not be imported.

Import configuration

About

To import a nagios 3 configuration we need to prepare the nagios configuration files first, after that we can use the import script to import the files into op5 Monitor.

Table of Content

Preparing nagios configuration

Log in to the nagios server via ssh or locally.
Create a new file called templates.cfg in which you manually add both your host-templates and your service-templates. These are usually

located in `hosts.cfg` and `services.cfg`.
Create a nagios pre-cache file by stopping nagios and start it with the -p option. this is done from you nagios binary directory, usually "`/usr/local/nagios/bin/`".

```
# service nagios stop
# ./nagios -pv <path to your nagios.cfg>
```

This will create a file called objects.precache in your “`var`” directory under your nagios installation.

Import nagios configuration

Make sure op5 monitor is stopped

```
# mon stop
```

Copy the files to the correct directory on your op5 Monitor server.

File	To folder
objects.precache	/opt/monitor
templates.cfg	/opt/monitor
nagios.log	/opt/monitor/var/
log archive	/opt/monitor/var/archives

Run the import script

```
# php /opt/monitor/op5/nacoma/import-reduce.php --cfg-file=/opt/monitor/templates.cfg
--object-cache=/opt/monitor/objects.precache
```

Do a config-test on the imported configuration # service

```
# service monitor configtest
```

If you have any errors these needs to be resolved before we can continue with starting the op5 monitor service. When there are no issues left start the monitor service

```
# mon start
```

Troubleshooting

About

In this chapter we will cover what you should do if you need to troubleshoot a problem related to op5 Monitor.

Preface

A logfile is a file that records either events that occur in an operating system or other software runs, or messages between different users of a communication software. This information is very useful when you need to troubleshoot but it might generate a lot of data depending on the configured log level. This text will also cover what logfile that contains what type of information.

Standard CentOS 6 installation is assumed.

Logfiles

The table shows the available modules and their logfiles:

	Module	Log configuration file	Default logfile path	Default debug level	Default reference*	Content
Authentication & Authorization	Auth	/etc/op5/log.yml	/var/log/op5/auth.log	Error	True	PHP errors.
Business service	Synergy	/etc/op5/log.yml	/var/log/op5/synergy.log	Error	True	PHP errors.
Business service	Synergy	/opt/synergy/etc/config.lua	See Syslog.	See Syslog.	See Syslog.	Only on/off configuration available, everything else managed by syslog-ng.
Configuration	Nacoma	/etc/op5/log.yml	/var/log/op5/nacoma.log	Error	True	PHP errors.
GUI	Ninja	/etc/op5/log.yml	/var/log/op5/ninja.log	Error	True	PHP errors.
HTTP API	HTTP API	/etc/op5/log.yml	/var/log/op5/http_api.log	Error	True	PHP errors.
MayI	MayI	/etc/op5/log.yml	/var/log/op5/mayi.log	Error	False	PHP errors.
SMS	-	/etc/smsd.conf	/var/log/smsd/smsd.log	Notice	-	
SMS	-	/etc/smsd.conf	/var/log/smsd/smsd_trouble.log	Notice	-	Only available if smart_logging is enabled. Smart_logging creates a separate log file for errors in order to clearly
Syslog		/etc/syslog-ng/syslog-ng.conf	/dev/console /var/log/messages /var/log/secure /var/log/maillog /var/log/spooler /var/log/boot.log /var/log/cron /var/log/kern			

*If reference is enabled a reference to the concerned file will be included in the log message; please be aware that this is a costly operation.

Log levels

All less granular levels will be included automatically; i.e. if the debug level is set to "Warning" both "Warning", "Error" and "Critical" (when it exists) will be logged.

log.yml

The following debug levels are available:

Level	Corresponding integer	Description
Error	1	Errors that have already occurred.
Warning	2	Potentially harmful situations.
Notice	3	Informational message.
Debug	4	Fine-grained informational events.

smsd.log

Level	Corresponding integer	Description
Debug	7	All AT commands and modem answers and other detailed informations useful for debugging
Info	6	Information regarding current occurrences. Not detailed enough for debugging but maybe interesting.
Notice	5	Information regarding when a message was received or sent and when something not normal happens but program still works fine (for example wrong destination number in SMS file).
Warning	4	Warning message when the program has a problem sending a single short message.
Error	3	Error message when the program has temporary problem (for example modem answered with ERROR during initialization or a file can not be accessed).
Critical	2	Error message when the program has a permanent problem (for example sending failed on multiple occurences or wrong permissions to a queue).

syslog-ng

Level	Corresponding integer	Description
emerg	0	System is unusable.
alert	1	Action must be taken immediately.
crit	2	Critical conditions.
err	3	Error conditions.
warning	4	Warning conditions.
notice	5	Normal but significant condition.
info	6	Informational.
debug	7	Debug-level messages.

Examples

Business Services

There are (mainly) two configuration files that manage logging for business services: /etc/op5/log.yml and /opt/synergy/etc/config.lua. The default configuration for /etc/op5/log.yml:

```
...
synergy:
  file: /var/log/op5/synergy.log
  level: error
  reference: true
...
```

Open /etc/op5/log.yml in any editor and change the settings to:

```
...
synergy:
  file: /var/log/op5/synergy.log
  level: debug
  reference: true
...
```

Default configuration for /opt/synergy/etc/config.lua:

```
...
  -- If true logs debugging to syslog
    debug = false,
...
```

Open /opt/synergy/etc/config.lua in any editor and change the settings to:

```
...
  -- If true logs debugging to syslog
    debug = true,
...
```

If you would like to change the default syslog-ng log levels the change is done in /etc/syslog-ng/syslog-ng.conf. This does however require a deeper understanding of syslog-ng's filters than this documentation can cover.

Restart synergy and syslog-ng:

> *service synergy restart*
>
> *service syslog-ng restart*

Remember to restore the original settings and restart the services when you no longer need to troubleshoot.

Table of Content

Upgrading

Introduction

op5 Monitor is upgraded in the same way as the other op5 products. If you have an op5 Appliance system you can read about the upgrade procedure in the op5 Appliance system manual.
This chapter will only cover how to upgrade an op5 Monitor.
We will learn how to upgrade with the

- Linux command yum
- tar.gz files you may download from our support site.

If you are upgrading from one main version to an other (eg. from version 4 to 5) you need to use the tar.gz files found at our support site.
When upgrading over more than one main version (eg. from version 3 to 5) you shall follow the Upgrade guide found at our support site:
https://kb.op5.com/display/HOWTOs/Upgrade+paths+for+op5+products

Upgrading with tar.gz files

About

Before you start with the upgrade you need to make sure you have the login to the download sections at www.op5.com. Otherwise you will not be able to download the `tar.gz` files.
To create an account please go to http://www.op5.com/sign-in/

Table of Content

To upgrade with tar.gz files

1. Download the `tar.gz` file from http://www.op5.com/download-op5-monitor/archive/. Find the `tar.gz` file you need. You might need to open up the Archived files at the bottom of the page.
2. Upload the `tar.gz` file to the op5 Monitor server.
3. Login to the op5 Monitor server via ssh as the `root` user.
4. Untar the `tar.gz` file in the `root/` folder.
5. Go to the folder that was extracted from the `tar.gz` file.
6. Now start the upgrade by executing the following script: `./install.sh`

Upgrading with yum

About

`yum` is the package manager for CentOS and op5 appliance system operating systems.

Table of Content

To upgrade with yum

1. Login to the op5 Monitor server via ssh as the `root` user.
2. Check what packages that is pending for upgrade by execute: `yum check-update`
3. If you want to apply the upgraded packages execute: `yum update`

User Menus

User menus

Customize user menus

About

It is possible for an administrator to customize users menu.

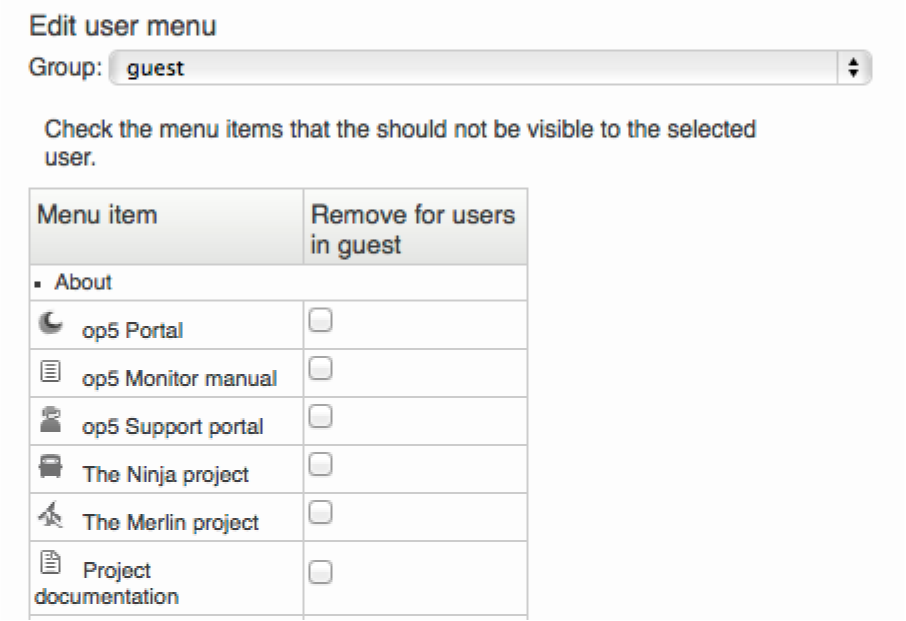
This can be uses to limit the menu options for users that are not allowed to use certain parts of op5 Monitor.

Table of Content

Customizing

The customizing is done per usergroup and not on individual users
Only user with full access can edit usergroup menus.

To change a specific usergroup menu, go to **My Account** in the menu and click on **Edit user menu**. Select the group you want to change the menu for.
You can now hide the options in the menu that you don't want to be visible for that members in that group. In the example below we have removed **op5 Support portal**, **View Config** and **Configure** options.



Edit user menu

Group: guest

Check the menu items that the should not be visible to the selected user.

Menu item	Remove for users in guest
▪ About	
op5 Portal	☐
op5 Monitor manual	☐
op5 Support portal	☐
The Ninja project	☐
The Merlin project	☐
Project documentation	☐

When you are done, click on **save**.

Wiki

Introduction

A wiki is included in op5 Monitor which can be used for documenting hosts and services.
Wiki pages can be created for both hosts and services.
The wiki has a built in version revisioning, that can be used to track changes in wiki pages and restore an older version. It is also possible to view changes between versions.
The wiki can be used for documenting hardware information, serial numbers and other information regarding a host or service. It can also be used to document workflows and how to act when there is a problem with a host or service.
The official docuwiki manual can be found here: http://www.dokuwiki.org/manual

Managing wiki pages

Introduction

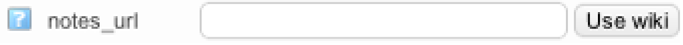
A wiki is included in op5 Monitor which can be used for documenting hosts and services.
Wiki pages can be created for both hosts and services.
The wiki has a built in version revisioning, that can be used to track changes in wiki pages and restore an older version. It is also possible to view changes between versions.
The wiki can be used for documenting hardware information, serial numbers and other information regarding a host or service. It can also be used to document workflows and how to act when there is a problem with a host or service.
The official docuwiki manual can be found here: http://www.dokuwiki.org/manual

Table of Content

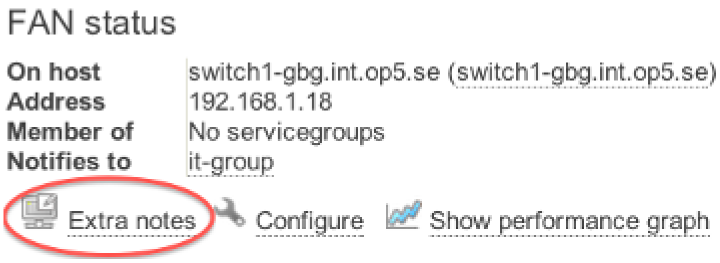
Create a wiki page

To create a wiki page for a host or service

1. Go to **Configuration**
2. Go to the host or service you want to create a page for.
3. Click on **Advanced**
4. Scroll down to 'notes_url' and click **Use wiki**. This will add a notes url to a wiki page.



5. Click **Submit** and save your configuration.
6. Go to the host in op5 Monitor and click on **Extra notes**


FAN status

On host switch1-gbg.int.op5.se (switch1-gbg.int.op5.se)
Address 192.168.1.18
Member of No servicegroups
Notifies to it-group

7. Click on **Create page**.
8. Edit the information and click on **Save**

Deleting a wiki page

If you edit a page and remove all its content then DokuWiki will delete the page, and the associated page name.
For more information about the docuwiki
http://www.dokuwiki.org/manual