IPSWITCH
WhatsUpGold

NRPE Devices Monitoring in WhatsUp Gold – Quick Guide
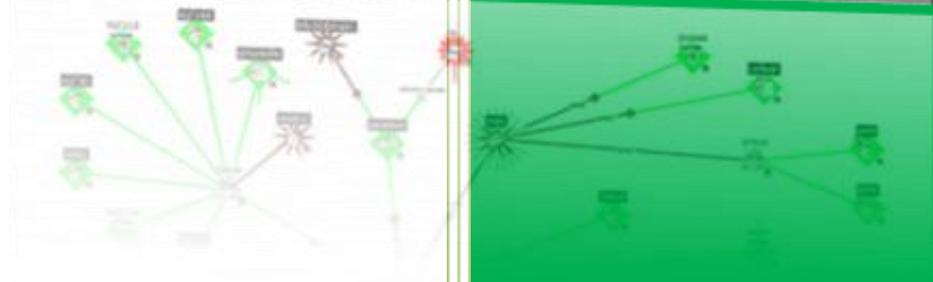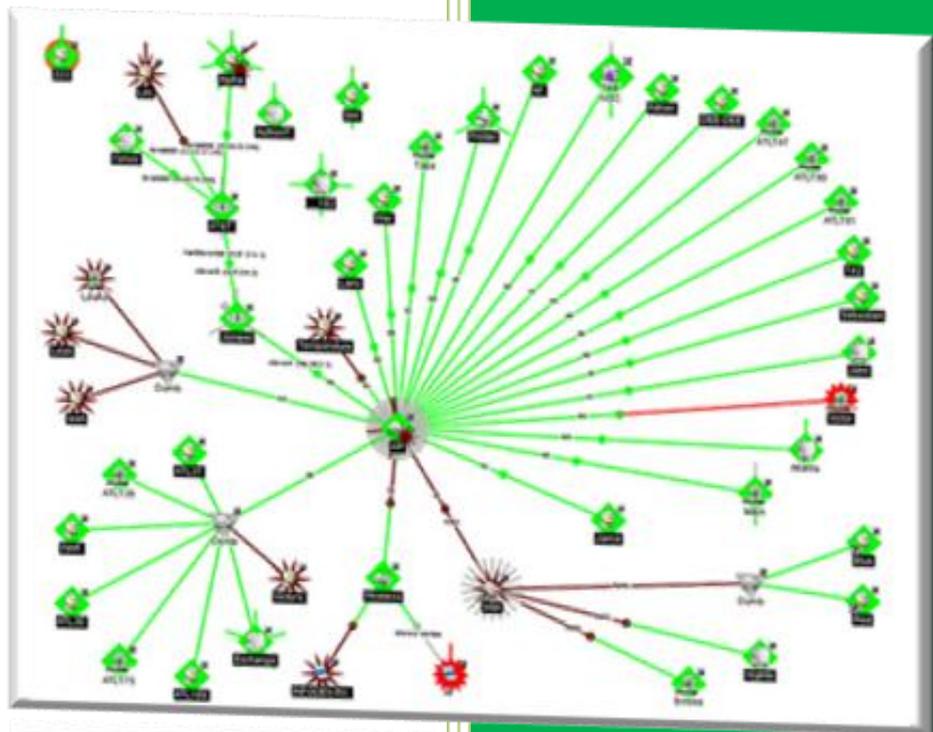
Introduction

NRPE add-on is designed to allow you to execute Nagios plugins on remote Linux/Unix devices. The main reason for doing this is to allow Nagios plugins to monitor local resources (CPU load, Memory usage, Users connected …) on remote Linux/Unix devices and provide these informations to WhatsUp Gold monitoring console. In order to make available these local resources, a NRPE agent must be installed on remote machines.

The main advantages of using NRPE agent are to secure your monitoring transactions through SSL, but also to minimize resource transactions. Indeed, many administrators opt for using the NRPE add-on because of the lower load it imposes.

In this document, we will explain NRPE specifications. We will develop the advantages of using NRPE to monitor your Linux/Unix servers. And, mainly, we will explain how implement NRPE transactions to monitor devices.

NRPE specifications

The NRPE add-on consists of two pieces:

- The check_nrpe plugin on the WhatsUp Gold monitoring console
- The NRPE daemon, which runs on the remote Linux/Unix device
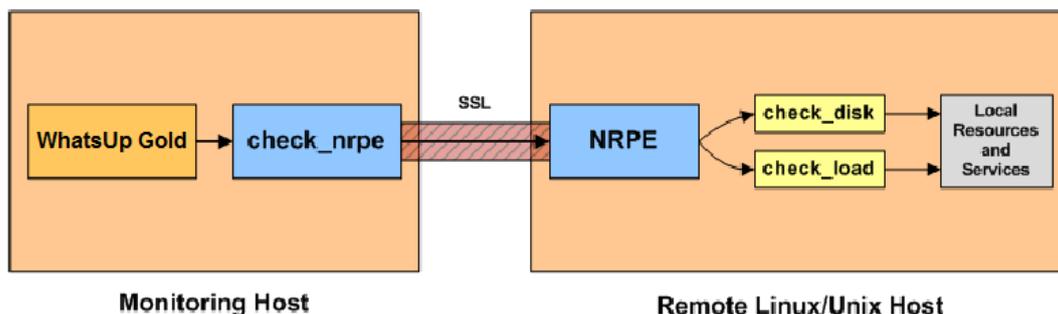
When you need to monitor a Linux/Unix device:

- WhatsUp Gold will execute the check_nrpe and attaches the service needs to be checked (CPU load, memory …)
- Check_nrpe contact NRPE deamon on remote device through SSL-protected connection
- The daemon runs the appropriate plugin to check the asked service.
- The daemon return back the result to the WhatsUp Gold check_nrpe through SSL

In order to implement this monitoring request type, we must install NRPE add-on on your remote devices; this is the subject of the next part.

Installation

In order to use NRPE transactions to monitor your remote server, you must install Nagios plugin and NRPE daemon. The following instructions are based on a remote host running CentOS 5.4.

Before to start the installation, please login to server with root account:

First, you must download Nagios plugins and NRPE daemon. At the time of writing, the latest stable version of the Nagios plugins was 1.4.15. and the last version of NRPE daemon was 2.13.

First of all, Nagios plugins and NRPE daemon installation need xinetd. If it doesn't install on your system, the following command allow installing this:

```
[root@localhost]# yum install xinetd
```

```
 [root@localhost]# cd /tmp/

[root@localhost]# wget
http://sourceforge.net/projects/nagiosplug/files/nagiosplug/1.4.15/n
agios-plugins-1.4.15.tar.gz/download

[root@localhost]# wget
http://sourceforge.net/projects/nagios/files/nrpe-2.x/nrpe-
2.13/nrpe-2.13.tar.gz/download
```

Then, install Nagios plugins. First, you must extract the plugins files.

```
[root@localhost tmp]# tar zxf Nagios-plugins-1.4.15.tar.gz
[root@localhost tmp]# cd nagios-plugins-1.4.15
```

Compil and install the plugin.

```
[root@localhost tmp/nag]# ./configure
[root@localhost tmp/nag]# make
[root@localhost tmp/nag]# make install
```

And, add appropriate permissions on the plugins directory for nagios user

```
[root@localhost]# chown nagios.nagios /usr/local/nagios
[root@localhost]# chown -R nagios.nagios /usr/local/nagios/libexec
```

Now Nagios plugins are installed, you must install the NRPE daemon. So first, extract the tar.gz file

```
[root@localhost]# tar zxf nrpe-2.13.tar.gz
[root@localhost]# cd /nrpe-2.13
```

Then, install and configure the daemon

```
[root@localhost]# ./configure
[root@localhost]# make all
[root@localhost]# make install-plugin
[root@localhost]# make install-daemon
[root@localhost]# make install-daemon-config
[root@localhost]# make install-xinetd
```

The installation is finished, you must now configure xinetd. For this, edit the */etc/xinetd.d/nrpe* file, and add your monitoring server IP address to the *only_from* line.

Then, modify the /etc/services file, and add a line to precise the NRPE TCP port.

```
nrpe          5666/tcp                    #NRPE
```

You can restart xinetd service:

```
[root@localhost]# service xinetd restart
```

You can verify that NRPE daemon running under xinetd:

```
[root@localhost]# netstat –at | grep nrpe
```

You should obtain this command

```
tcp          0          0*:nrpe          *:*          LISTEN
```

If you haven't this, you should restart from the beginning of the installation.

You can now launch a NRPE request locally.

```
[root@localhost]# /usr/local/nagios/libexec/check_nrpe –H localhost
NRPE v2.13
```

You then get the version of the installed daemon.

Just before to test a remote transaction, you must add appropriate rules in the server firewall for NRPE port.

```
 [root@localhost]# iptables –I RH-Firewall-1-INPUT –p tcp –m tcp –d
5666 –j ACCEPT
[root@localhost]# iptables save
```

Manage your own NRPE commands

You can manage your commands in the NRPE config file (/usr/local/Nagios/etc/nrpe.cfg).
Some commands are pre-configured in the config file:

```
command[check_users]=/usr/local/nagios/libexec/check_users -w 5 -c10
command[check_load]=/usr/local/nagios/libexec/check_load -w 50 -c 80
command[check_disk]=/usr/local/nagios/libexec/check_disk -w 50 -c 80
-p /
command[check_procs]=/usr/local/nagios/libexec/check_procs -w 100 -c
150
```

You can create your own commands, using the different Nagios plugins that we had installed previously.

NRPE Monitoring in WhatsUp Gold

Now that you have configured your remote server to receive NRPE request, you can add your monitors. WhatsUp Gold offers two monitors for NRPE: an Active monitor to alert network administrator in case of counters threshold value excess, and a Performance Monitor to graph and edit report with values return by the NRPE daemon of your remote server.

For example, we will implement check we configured in the previous section. First you can configure an active monitor which checks the number of currently users connected on the server. Threshold values are already configured in the NRPE config file of the remote server, but if you want to fix threshold in the Active Monitor, you must replace the check_users command.

Thresholds fixed in the NRPE config file:

```
command[check_users]=/usr/local/nagios/libexec/check_users -w 5 -c10
```
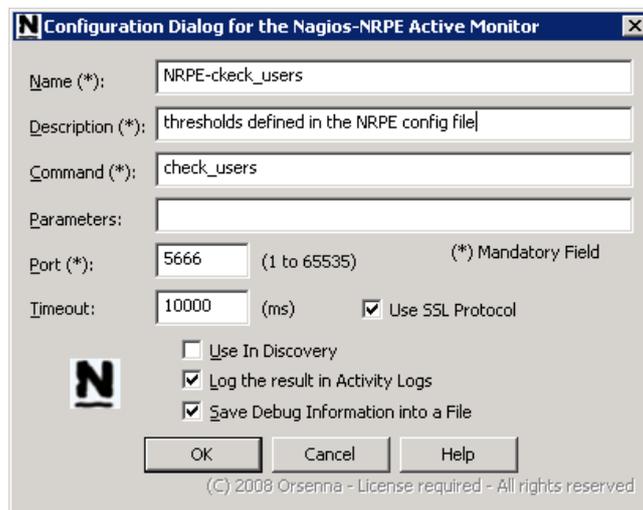
```
command[check_users]=/usr/local/nagios/libexec/check_users -w $ARG1$
-c $ARG2$
```
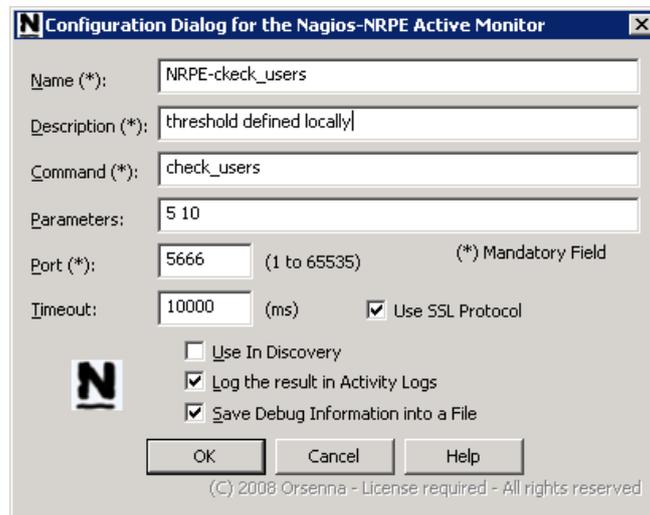

Then, you can test the Active monitor.
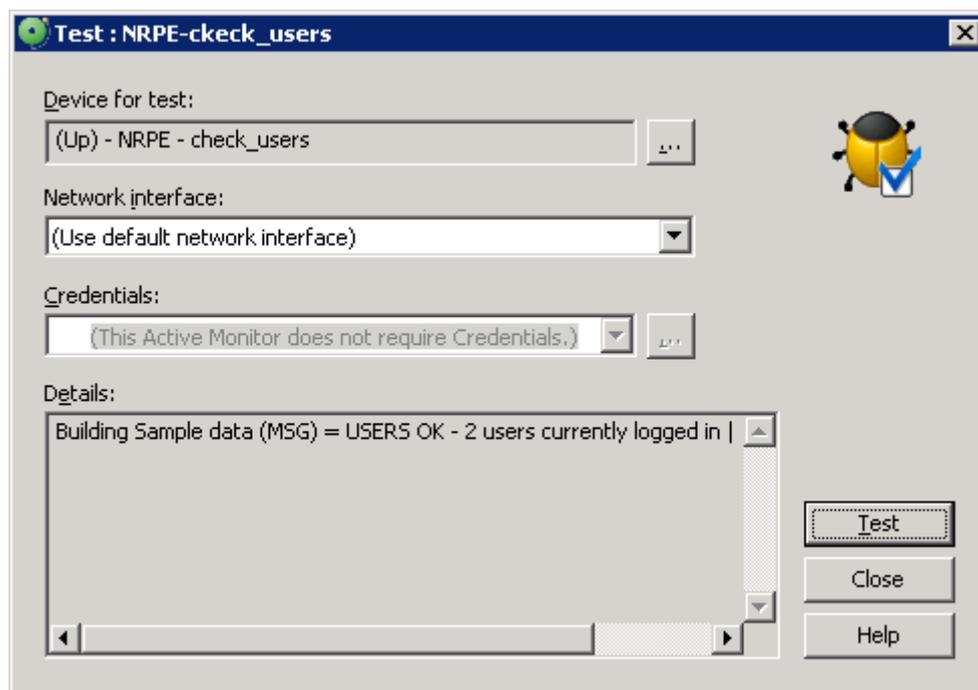
In the present case, the Active Monitor returns Code 0, because two users are currently logged and the threshold is fixed on 5 users.

You can now implement a performance monitor. For this click, in WhatsUp administrator console, Configure / Performance Monitor…/New/NRPE Performance Monitor. The window is almost the same as for the Active Monitor. There is just a difference, for result processing:

Server response after a check_load request:

```
Check NRPE: Return code = 0 in 46 ms – Message : OK – load average:
0.52,0.58,0.51|load1=0.520;15.000;30.000;0;
load5=0.580;10.000;25.000;0; load15=0.510;5.000;20.000;0;
```

We can note that values always follows a string 'load1=', 'load5=' or 'load10='. So to extract these values, you must use this syntaxe: **(?<=load1=)\d+** or **(?<=load5=)\d+**
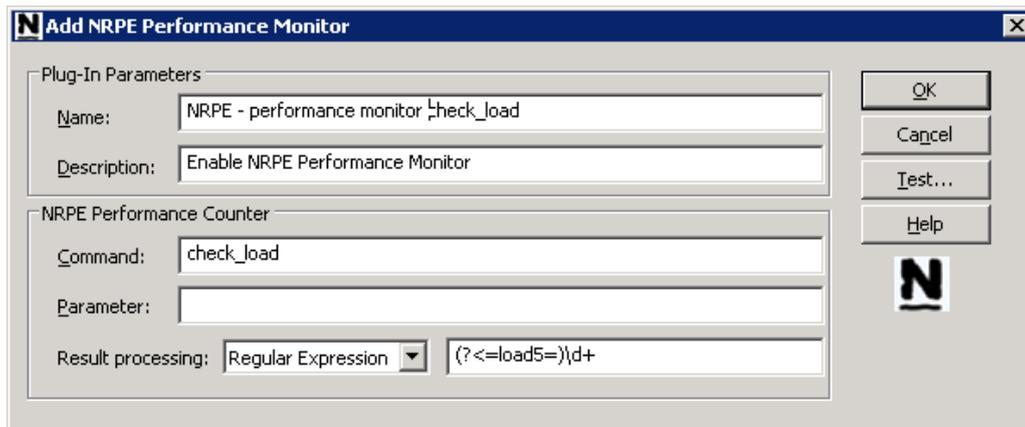
Then, you can test your performance monitor,
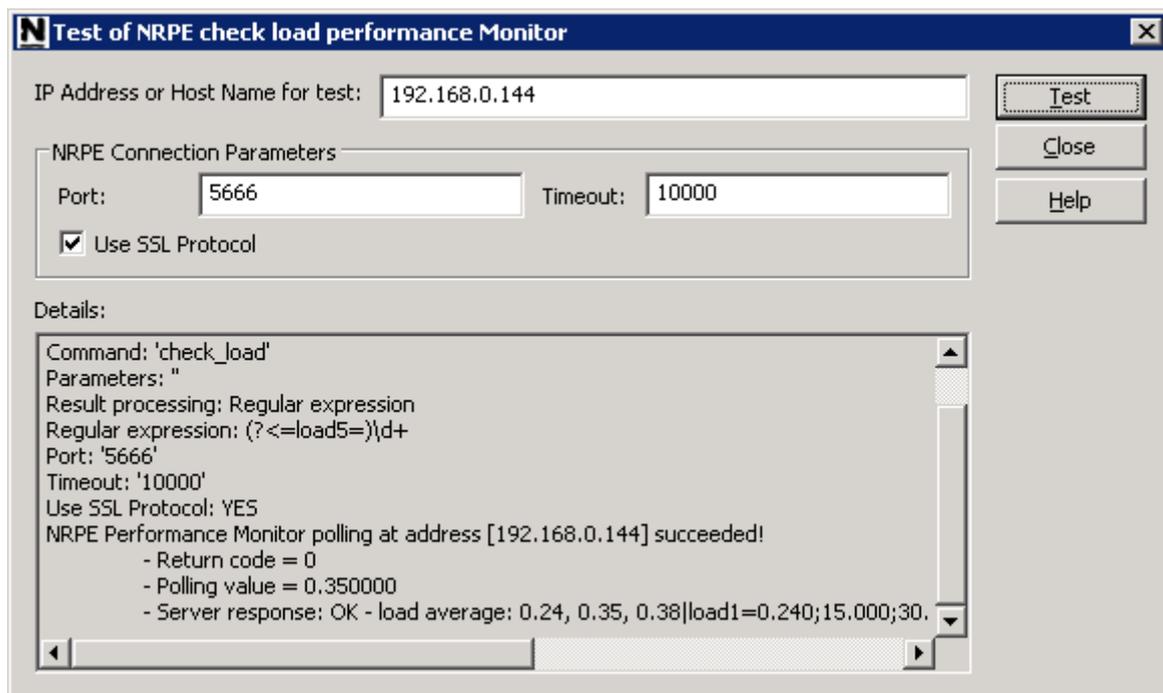
To finish, you can apply your performance monitor to your remote server.
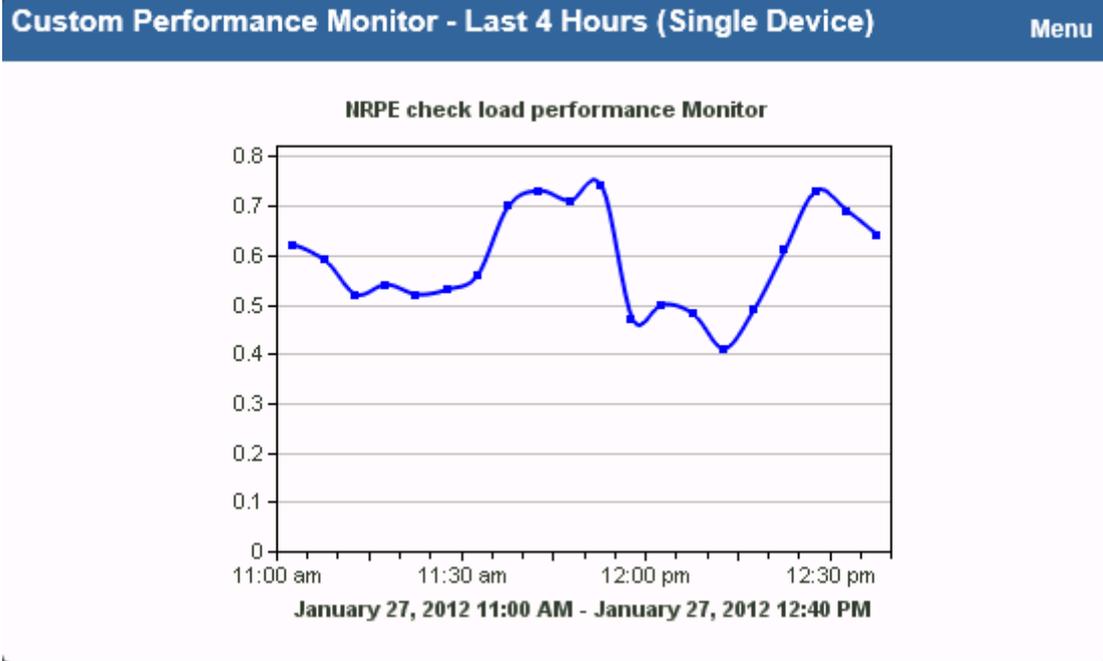
Windows Server Monitoring with NRPE

NRPE offers some advantages as secure transactions through SSL or minimize resources. So, why not use NRPE to monitor Windows Server. NRPE use approximately ten times less resources than WMI, so it can sometimes be a solution of WMI replace, for example to monitor NT services. Indeed, if you want monitoring multiple NT services, you will need as far monitors as services with WMI. However, you just need one monitor with NRPE. If you want to have more information on Windows server monitoring with NRPE, you can refer to the following document:

http://www.orsenna.org/ftp/companion/Forums/Improve_WUG_perf_with_NRPE.pdf

Nagios NRPE Active and Performance Monitors are WhatsUp Companion components, if you want more information, you can refer to this video tutorial or download a trial version.

http://www.youtube.com/watch?v=jdnYBjqudkw

http://whatsupcompanion.orsenna.com/download/download-presentation.html