

StormTest and Nagios

Monitoring a StormTest Facility using Nagios Monitoring Software

S3 Group Document ID: ST-14010

Revision Date: February 2016

Version: 1.1

Author: Stephen Dolan

Web: <http://www.s3tvtechnology.com>

The contents of this document are owned or controlled by Accenture and are protected under applicable copyright and/or trademark laws. The contents of this document may only be used or copied in accordance with a written contract with Accenture or with the express written permission of Accenture.

Contents

1	Introduction	3
1.1	Nagios Structure.....	3
2	Installation	4
2.1	Architecture	4
2.2	Software Required	4
2.3	Installation	5
2.3.1	Pnp4nagios.....	5
2.3.2	Web Frontend Skins (optional)	5
2.4	Nagios Server Configuration	6
2.4.1	StormTest configuration files.....	6
2.4.2	Edit main configuration files	6
2.4.3	Configure your facility.....	7
2.4.4	Email Notifications	8
2.5	StormTest Server Configuration	8
2.5.1	NSClient++ Configuration.....	8
2.5.2	Additional Tools	10
3	Using Nagios.....	11
3.1	Monitored services	11
3.2	Checking facility status.....	11

1 Introduction

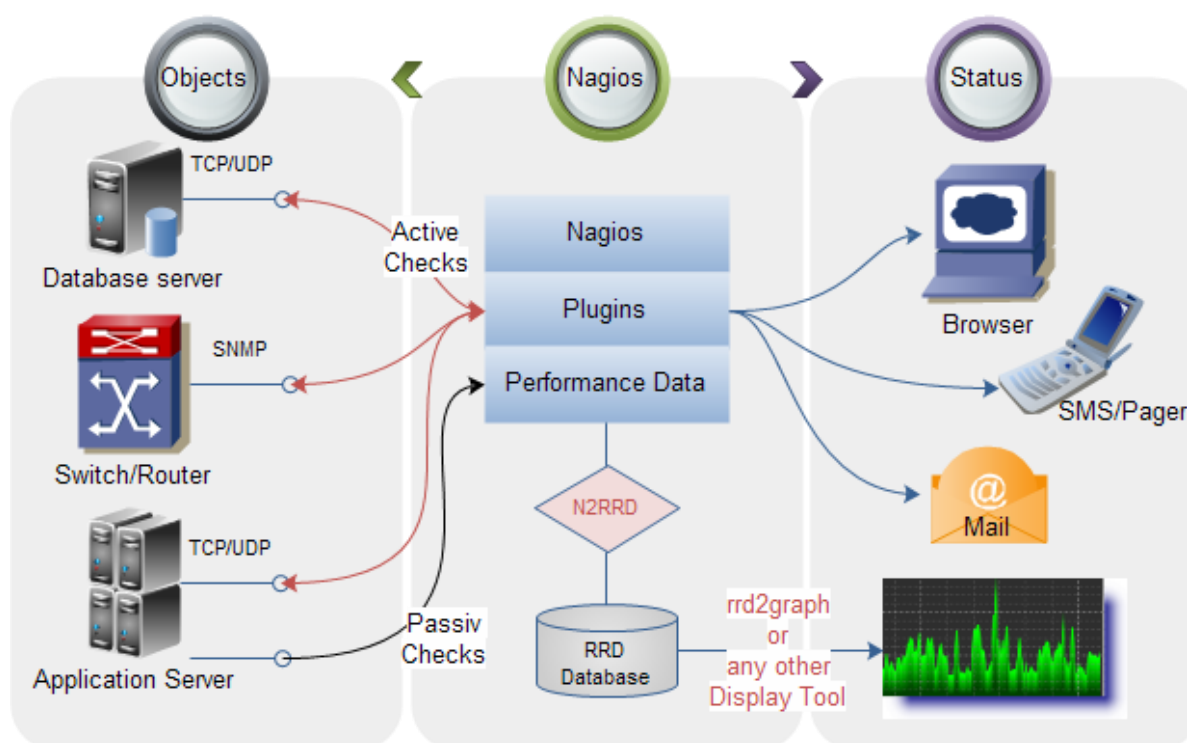
Nagios is an open source computer system monitoring, network monitoring and infrastructure monitoring software application. Nagios offers monitoring and alerting services for servers, switches, applications, and services. It alerts the users when things go wrong and alerts them a second time when the problem has been resolved.

Nagios is highly configurable and widely deployed to monitor IT infrastructure, making it ideal as a tool to monitor StormTest facilities.

1.1 Nagios Structure

A full description of Nagios is beyond the scope of this document, however in brief it consists of:

- Core software that runs on the Nagios server
- Plugins that check both 'hosts' and 'services' to determine their states.
- Plugins that notify users of changes in the states of those hosts and services
- A web frontend that presents the current status and can generate reports and graphs of performance data



The Nagios core server can be run on Linux or Windows, but Linux is the preferred OS.

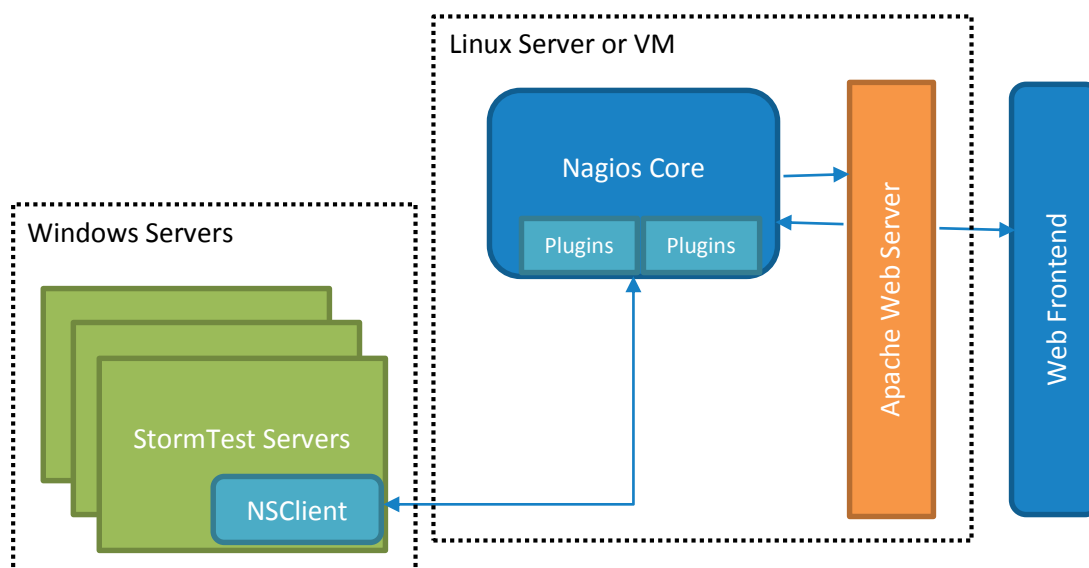
For the purposes of this document, it is assumed that the user either has an existing installation of Nagios core that they are familiar with or is installing a clean installation on a Linux server.

The author was using Nagios-core version 3.5.1. If using a different version, then these instructions may need to be adjusted accordingly.

2 Installation

Note that it's not a requirement for the software packages and versions listed to be used. However, this is the software that was used in S3 Group and other versions and component combinations may give different results.

2.1 Architecture



2.2 Software Required

The following components will be required. Some are installed on the Nagios server and others are installed on each of the StormTest servers. Note that the fact that most of these components are source downloads means there may not be Windows binary distributions available. We strongly recommend that a Linux PC is used to host the Nagios server.

- Software on the Nagios Server:
 - Nagios core (version 3.5.1) : <http://sourceforge.net/projects/nagios/files/nagios-3.x/>
 - Official Nagios plugins (version 1.4.16) : <http://nagios-plugins.org/download/>
 - Nagios Remote Plugin Executor (NRPE) (version 2.15) : <http://sourceforge.net/projects/nagios/files/nrpe-2.x/>
 - PNP4Nagios (version 0.6.24) : <http://sourceforge.net/projects/pnp4nagios/files/PNP-0.6/>
 - RRDTool (version 1.4.8) : <http://oss.oetiker.ch/rrdtool/pub/>
- Software on the StormTest Servers:
 - NSClient++ (version 0.4.3, Windows version. Choose 64 bit or 32 bit installer, depending on the architecture of the Windows OS on your StormTest servers): <http://www.nsclient.org/download/0-4-3/>

2.3 Installation

Follow the appropriate instructions for installing Nagios core and the Nagios plugins on your Linux distribution.

This is a good starting point:

http://nagios.sourceforge.net/docs/3_0/quickstart.html

Ensure that you also install the NRPE plugin as well as the core plugins. Also, apache is required to interact with the web frontend for Nagios.

2.3.1 Pnp4nagios

PNP4Nagios is an add-on for Nagios that adds performance graphs generated from RRDTools data. RRD (round robin database) Tool is an industry standard tool for logging and graphing time series data. PNP4Nagios requires the following tools to be installed:

- Perl
- RRDTool
- PHP (with support for GD library – a library for dynamic creation of images)

Follow the instructions included in the pnp4nagios tar file to install the package on the Nagios server.

This will allow performance data to be viewed at

http://nagios_server/pnp4nagios/graph?host=s13074hv04

where *Nagios_server* is the hostname of your Nagios server and the *host* parameter is replaced with one of your host names. However, with the provided StormTest configuration files, the link to the appropriate PNP4Nagios performance chart will be provided in Nagios – the ‘cog’ symbol as seen below will open this chart



Finally, popups of the performance charts can be enabled in Nagios by copying the file **status-header.ssi** from the contrib/ssi/ folder of the PNP package to /usr/share/nagios/htdocs/ssi (in our case – please check your own installation to locate the Nagios web frontend files).

2.3.2 Web Frontend Skins (optional)

The default web frontend skin is quite ugly, but it’s relatively easy to alter it. To view some of the available skins, check out the Nagios exchange:

<http://exchange.nagios.org/directory/Addons/Frontends-%28GUIs-and-CLIs%29/Web-Interfaces/Themes-and-Skins>

As an example to install the Vautour skin, follow these steps:

Get the zip file:

```
wget http://www.be-root.com/downloads/nagios/vautour/vautour_style.zip
```

Unzip it into the Nagios frontend location:

```
unzip vautour_style.zip -d /usr/share/nagios/htdocs/
```

That's it – it's installed.

2.4 Nagios Server Configuration

Nagios is configured using a collection of *cfg* files. For convenience, we have placed all StormTest related changes into their own files and recommend that all those files be located in a single directory.

The location of the configuration files can depend on the particular Linux distribution being used. For the purposes of this guide, we assume all configuration files are in

```
/etc/nagios
```

Other distributions may located the files in

```
/usr/local/nagios/etc
```

2.4.1 StormTest configuration files

A number of configuration files will have been supplied to you by StormTest support in a zip file. Most of the contents of this zip file will be needed on the Nagios server in different locations according to the following table:

Contents of Zip file	Copy to location on Nagios server
stormtest/*	/etc/nagios/objects/stormtest
nagios_server_scripts/*	/var/nagios/home

Ensure that all the files are owned by the 'nagios' user.

2.4.2 Edit main configuration files

2.4.2.1 Nagios.cfg

The /etc/nagios directory contains the main Nagios configuration file (nagios.cfg). You must edit this file and add the following line:

```
cfg_dir=/etc/nagios/objects/stormtest
```

In order to enable the pnp4nagios performance plugin, you must also set process_performance_data to be 1 and set the host and service performance data commands:

```
process_performance_data=1
host_perfdata_command=process-host-perfdata
service_perfdata_command=process-service-perfdata
```

Now save the file and exit.

2.4.2.2 *Commands.cfg*

You must also edit the `commands.cfg` file to define the above process commands. Open the file `/etc/nagios/objects/commands.cfg` and locate the definitions for *process-host-perfdata* and *process-service-perfdata*. Change the command line in both definitions so that they look like the following:

```
# 'process-host-perfdata' command definition
define command{
    command_name    process-host-perfdata
    command_line    /usr/bin/perl /usr/libexec/process_perfdata.pl -d HOSTPERFDATA
}

# 'process-service-perfdata' command definition
define command{
    command_name    process-service-perfdata
    command_line    /usr/bin/perl /usr/libexec/process_perfdata.pl
}
```

Save the file and exit

2.4.2.3 *Cgi.cfg*

The CGI configuration file must be modified to give access to the nagios data from the webserver. As long as the Nagios server is on a secure network, it's safe to just set a default username. Edit `/etc/nagios/cgi.cfg` and set

```
default_user_name=nagiosadmin
```

Then save and exit.

If your Nagios server will be accessible external to your LAN, then you will need user authentication. This subject is outside the scope of this document.

2.4.3 *Configure your facility*

Open the file `/etc/nagios/objects/stormtest/stormtest_hosts.cfg`

This file is where you define all the StormTest servers in your facility.

At the top of the file, define a host for each server in your facility. Use the existing entries as templates. The 'address' field can either be a DNS hostname or an IP address.

Once all hosts are defined, you need to put them into the appropriate groups.

All hosts are in the *stormtest-servers* group by default.

For the server or servers that act as config servers, then add the host to the *st-config-servers* host group. Just add the host to the *members* line in the hostgroup.

For servers that are HD, add the hosts to the *stormtest-hd-servers* hostgroup and the SD StormTest servers are added to the *stormtest-sd-servers* hostgroup.

Adding the hosts to the appropriate hostgroups means that all the appropriate services will be automatically monitored.

2.4.4 Email Notifications

All configured StormTest services are setup to send notifications to the *stormtest-admins* contact group.

All users that need to get notifications need to be added to this group. To do this, edit the file `/etc/nagios/objects/stormtest/stormtest_contacts.cfg`

For each user that needs to receive notifications, create a *contact* and then add that contact as a member of the *stormtest-admins* contact group.

Note that Nagios assumes that email delivery is configured correctly on your server and that the standard 'mail' program can be used to send email. If email is not configured on your server then you will not receive notifications

If a different mail program is used than `/usr/bin/mail`, then the

```
notify-host-by-email
```

and

```
notify-service-by-email
```

commands in `/etc/Nagios/objects/commands.cfg` will need to be updated to add the appropriate command.

2.5 StormTest Server Configuration

2.5.1 NSClient++ Configuration

NSClient++ must be installed on each StormTest Server and Config Server. There is a 64 bit and a 32 bit version of the installer so choose the appropriate one for each server.

To install, user the wizard

- choose the 'typical' option
- choose next
- enter the nagios server address in the 'allowed hosts' box and click next

Once the installation is complete, go to `C:\Program Files\NSClient++` and open `nsclient.ini`

Edit the file so the following options are present:

```
[/modules]
CheckSystem = 1
CheckDisk = 1
NSClientServer = 1
NRPEServer = 1
CheckExternalScripts = 1
```



```
[/settings/external scripts]
allow arguments=true
```

```
[/settings/default]
; This should match your Nagios Server's IP address or IP range
; e.g. allowed hosts = 192.168.7.0/24 to allow any host in the
; 192.168.7.x network access the information
allowed hosts = 192.168.7.154
```

```
[/settings/NRPE/server]
allow arguments = true
insecure=1
```

Then restart the Nagios Windows service.

2.5.1.1 Specific SD server configuration

Add the line, `check_rst=python scripts\check RAID.py` to the tag `[/settings/external scripts]`, once the Nagios server has been configured to call this script, RAID information on the server will be reported back the Nagios server.

2.5.1.2 Additional configuration for HD servers

If installing NSClient++ on an HD server, you must also add the following options to the `/modules` section in the `nsclient.ini` file:

```
[/modules]

[/settings/external scripts/scripts]
check_vs=python scripts\check_vs.py $ARG1$
check_hdd=python scripts\hddSpace.py $ARG1$
```

This enables a custom python script to be executed, which is used to monitor the StormTest HD video servers.

These python scripts need to be copied into the `C:\Program Files\NSClient++\scripts` directory from the S3 supplied zip file (they can be found in the **nsclient_script** directory – everything in this directory should be copied over).

To enable checking of the Dell hardware on HD systems add the following line under the `[/settings/external scripts/scripts]` tag.

```
check_dell=scripts\check_openmanage.exe
```

You will also need to install the necessary executable on the StormTest server (see next section).

It may be necessary to black list some devices for monitoring, this is done by using the “black-listed”, -b switch, e.g. -b volt=18,19 This will mean that all errors from the black listed device will be ignored.

2.5.2 Additional Tools

The following tools can be downloaded and installed with NSClient++ to enable further monitoring of the server

2.5.2.1 *check_openmanage.exe*

check_openmanage.exe is a Nagios Plugin which checks the hardware health of Dell servers running Open Manage Server Administrator. The plugin checks the health of the storage sub system, RAID integrity, power supplies, memory modules, temperature probe etc and will provide an alert if any of the components are faulty or are running outside normal parameters, more details can be found here https://exchange.nagios.org/directory/Plugins/Hardware/Server-Hardware/Dell/check_openmanage/details and the plugin can be downloaded from here http://folk.uio.no/trondham/software/check_openmanage.html#download

To use the plugin copy, check_openmanage.exe to the c:\Program Files\NSClient++\scripts directory on the StormTest HD server you wish to monitor. Ensure you add the line in section 2.5.1.2 to the nsclient.ini file to enable this.

2.5.2.2 *rstCli4.exe*

rstCli64.exe can be downloaded from <https://downloadcenter.intel.com/download/23932/Intel-Rapid-Storage-Technology-Command-Line-Interface-RST-CLI-> . This tool enables users to provision systems with Intel Smart Response Technology and other features of Intel Rapid Storage Technology thereby allowing Nagios to monitor the health of the Intel RAID on the StormTest SD server.

To use this plugin copy rstcli64.exe to the c:\Program Files\NSClient++\scripts directory on the StormTest SD server you wish to monitor. The python file check_raid.py should also be present in this directory.

3 Using Nagios

To access the Nagios portal, navigate to the following URL on your Nagios server:

http://nagios_server/nagios

This will give you access to all the monitored hosts and services.

3.1 Monitored services

All the StormTest services monitored are defined in the file:

`/etc/nagios/objects/stormtest/stormtest_services.cfg`

At time of writing, the following services are monitored. Note that some items are looking at the general health of the server in addition to the health of StormTest services. The services highlighted in blue track performance data also.

	StormTest SD Server	StormTest HD Server	StormTest Config Server
Admin Console			✓
Dashboard			✓
Config Server			✓
FTP	✓	✓	✓
Uptime	✓	✓	✓
CPU Load	✓	✓	✓
Memory Usage	✓	✓	✓
D:\ Drive Space	✓	✓	✓
Host Service	✓	✓	✓
IRNetBox Availability	✓	✓	✓
StormTest Server	✓	✓	✓
Client Daemon	✓	✓	✓
OCR Server	✓	✓	✓
HD Video Server One		✓	
HD Video Server Two		✓	
HD Video Server Three		✓	
HD Video Server Four		✓	
VideoServerOneHDD		✓	
VideoServerTwoHDD		✓	
VideoServerThreeHDD		✓	
VideoServerFourHDD		✓	
Dell Server Health Check		✓	
Server RAID	✓		

3.2 Checking facility status

To check on the overall status of your facility, click on *tactical overview*. This will show a page such as this:

Tactical Monitoring Overview

Last Updated: Thu Jun 19 16:16:44 IST 2014
Updated every 90 seconds
Nagios® Core™ 3.3.1 - www.nagios.org
Logged in as nagiosadmin


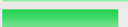
Monitoring Performance

Service Check Execution Time: 0.04 / 0.38 / 0.114 sec
Service Check Latency: 0.01 / 0.58 / 0.191 sec
Host Check Execution Time: 4.08 / 4.13 / 4.091 sec
Host Check Latency: 0.18 / 0.51 / 0.314 sec
Active Host / Service Checks: 4 / 50
Passive Host / Service Checks: 0 / 0

Network Outages

0 Outages

Network Health

Host Health: 
Service Health: 

Hosts

0 Down 0 Unreachable 4 Up 0 Pending

Services

4 Critical 1 Warning 0 Unknown 45 Ok 0 Pending

3 Unhandled Problems 1 Unhandled Problems
1 Disabled

Monitoring Features

Flap Detection	Notifications	Event Handlers	Active Checks	Passive Checks
ENABLED All Services Enabled No Services Flapping All Hosts Enabled No Hosts Flapping	ENABLED All Services Enabled All Hosts Enabled	ENABLED All Services Enabled All Hosts Enabled	ENABLED 1 Service Disabled All Hosts Enabled	ENABLED All Services Enabled All Hosts Enabled

We can quickly see that a number of services are in the *critical* state. Clicking on the link **3 Unhandled Problems** will bring us directly to the problem services:

Current Network Status

Last Updated: Thu Jun 19 16:18:25 IST 2014
Updated every 90 seconds
Nagios® Core™ 3.3.1 - www.nagios.org
Logged in as nagiosadmin

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

Host Status Totals

Up	Down	Unreachable	Pending
4	0	0	0
All Problems		All Types	
0		4	

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
45	1	0	4	0
All Problems			All Types	
5			50	

Display Filters:

Host Status: Pending | Up

Types:

Host: Any

Properties:

Service: Critical

Status:

Types:

Service: Not In Scheduled Downtime & Has Not Been

Properties: Acknowledged & Active Checks Enabled

Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
stormtest33	IRNetBox Availability	CRITICAL	06-19-2014 16:16:33	1d 6h 33m 52s	3/3	<class 'socket.error'>, error(111, 'Connection refused'), <traceback object at 0x962710>
	StormTest OCR Server	CRITICAL	06-19-2014 16:16:22	1d 6h 34m 3s	3/3	StormTest Server stormtest33 is not running. Cannot retrieve available OCR characters
	StormTest Server Process	CRITICAL	06-19-2014 16:17:12	1d 6h 33m 13s	3/3	StormTest Server stormtest33 is not running

In this case, we can see that the StormTest server process and the OCR server process on the stormtest33 server are not running and have been down for 1 day, 6.5 hours. At this point, you can go directly to the problematic server and find and fix the issue.

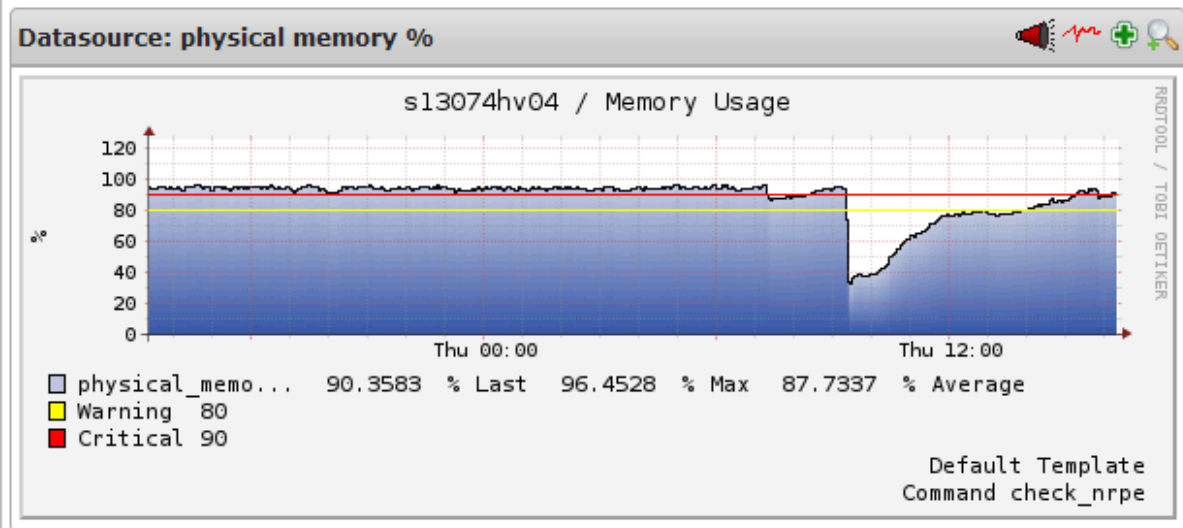
For some services, the state will be *critical* or *warning* due to the performance data. For instance, the OCR service monitor will raise a warning if the number of characters falls below 800,000. It moves to critical if the available characters falls below 1,000.

Similar notifications will occur for high CPU usage and memory usage.

In the case below, we can see from the performance data that this server has a problem with memory usage as it is consistently above the warning and critical limits:

Host: s13074hv04 **Service:** Memory Usage

25 Hours 18.06.14 14:20 - 19.06.14 15:20



Data such as this can be very useful in debugging other problems in the system, as constrained resources will certainly have a knock on effect on other activities on the server.