Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Network Monitoring with Nagios

Nagios is a network-monitoring tool that allows administrators the ability to examine computers, routers, printers, and services. Many organizations opt for pricey commercial solutions such as HP-OpenView. Nagios is an excellent solution for those companies looking for a product that is inexpensive (free) and under constant development due to open source availability. Currently there is not a stable release for Nagios, only an alpha version available for download. The reason for the delayed release is not as much appli...

Copyright SANS Institute
Author Retains Full Rights

AD

NETWORK MONITORING WITH NAGIOS

Scott V. Seglie

September 25, 2001

Introduction to Nagios

Nagios is a network-monitoring tool that allows administrators the ability to examine computers, routers, printers, and services. Many organizations opt for pricey commercial solutions such as HP-OpenView. Nagios is an excellent solution for those companies looking for a product that is inexpensive (free) and under constant development due to open source availability. Currently there is not a stable release for Nagios, only an alpha version available for download. The reason for the delayed release is not as much application issues as it is lack of documentation. An Admin Kit with additional documentation, videos, etc will be available for purchase in January 2002.

Some of the many features of Nagios include:

- Monitoring of network services (SMTP, POP3, HTTP, NNTP, PING, etc.)
- Monitoring of host resources (processor load, disk usage, etc.)
- Simple plug-in design that allows users to easily develop their own service checks
- Parallel service checks
- Ability to define network host hierarchy using "parent" hosts, allowing detection of and distinction between hosts that are down and those that are unreachable
- Contact notifications when service or host problems occur and get resolved (via email, pager, or user-defined method)
- Ability to define event handlers to be run during service or host events for proactive problem resolution
- Automatic log file rotation
- Support for implementing redundant monitoring hosts
- Optional web interface for viewing current network status, notification and problem history, log files, etc.

Nagios was developed and is maintained by Ethan Galstad. The original project was known by the name of Netsaint. The last official release of Netsaint was 0.0.7. Due to legal issues, the name “Netsaint” is no longer used. Further development of this project is now known as Nagios.

The major advantage of Nagios is the same as the major disadvantage: extreme flexibility. This is obviously great for administrators that require complete control and flexibility of the application. It also means days of reading, testing, and tweaking. Nagios is not a simple click-and-go installation. There are numerous packages that are required for Nagios to run properly. My advice: Block a few days off on your schedule, join the nagios-users mailing list, read the online documentation, read the man pages, read the install pages, and then read everything again.

Step-By-Step Installation

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Nagios was originally written for the Linux operating system, but ports are now available for many other platforms. This document is intended to detail the Nagios installation process on a default install of Red Hat 7.0 workstation.

Nagios requires many other programs to operate effectively. A major piece of Nagios are the CGIs. CGIs are part of the Nagios installation and are not required for the program to run, although significantly add to the overall functionality of the program. Apache and Thomas Boutell's GD Library must be installed to utilize the CGIs and other features of the application.

Install and Configure Apache
Apache is used as a front-end web interface to Nagios and adds additional security. (note: Apache is recommended, but other web servers will work.)

Install the Apache RPM located on the Red Hat 7.0 CD under /RedHat/RPMS/
Once install is complete, modify the httpd.conf file located at /etc/httpd/conf/httpd.conf by removing the comment "#" before the "ServerName localhost" line
Save the file and exit
Open a shell type: "/etc/rc.d/init.d/httpd restart" to restart the Apache daemon
Test the Apache installation by opening Netscape and typing "localhost" in the address. If the default Apache page comes up, the installation was successful.

Install Thomas Boutell's GD Library (version 1.6.3 or higher is required)
Thomas Boutell's GD Library – this supports the most important *.cgi; the status.cgi, which shows the current status of all hosts and services being monitored.

Thomas Boutell's GD Library requires the following packages:
-libpng (already installed in default Red Hat 7.0)
-zlib (already installed in default Red Hat 7.0)
-jpeg-6b or later (this package can be found at http://rpmfind.net)

Download the GD library package at: http://www.boutell.com/gd/
gunzip [gd_library_package_name].tar.gz
tar -xf [gd_library_package_name].tar
cd [gd_library_package_name]
make
make install
note: if the error: "/usr/local/include/dg.h: No such file or directory" occurs, simply type the command "mkdir /usr/local/include" in a shell, then re-do the "make install"

Install Nagios

Download Nagios from https://www.nagios.org (the alpha version is available at: http://www.nagios.org/download/)

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

```
gunzip [nagios_package].tar.gz
tar -xf [nagios_package].tar
mkdir /usr/local/nagios
adduser nagios
passwd nagios
./configure
make all
make install
make install-init
make install-config
cd /usr/local/nagios
mkdir etc
mkdir libexec
```

Of note, Nagios runs as a specific user, “nagios,” which adds to the overall security of the application and is a basic security precaution. Everything, including your Nagios configuration files should be treated on a 'need to know' only basis.

Install the Plug-ins

Nagios uses plug-ins to perform actual service checks on the computers, routers, printers, and services. This is a very flexible approach that allows new plug-ins to be created by the user for more granular checks. Since this project is open source, many of the personalized plug-ins are available to the public.

These plug-ins use additional tools that should also be installed. The additional files are: snmpget, qstat, and fping. Make sure to install these before you go on to the Nagios plug-ins install. Searches at https://rpmfind.net will allow for download. Documentation below describes the plug-in install steps.

Download the *Netsaint* plug-ins.tar.gz from http://netsaintplug.sourceforge.net. The Netsaint plug-ins are compatible with Nagios, but continue to check the Nagios website for the first release of plug-ins for the new project.

```
gunzip [netsaint-plug-ins].tar.gz
tar –xf [netsaint-plug-ins].tar
cd [netsaint-plug-ins]
#autoconf
#autoheader
#automake
./configure --prefix=/usr/local/nagios --with-netsaint-user=nagios --with-netsaint-
group=nagios --with-cgiurl=/cgi-bin/nagios
make all
make install
```

note: make sure hosts.cfg contains the correct paths to the new plug-ins

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Setting Up and Configuring the Web Server

Go to the /etc/httpd/conf directory and open the httpd.conf file. There are two modifications necessary in this file.
Before the “Alias” that is already there, type:
Alias /nagios/ "/usr/local/nagios/share/"
(note: the “quote” marks should be included)
Before the ScriptAlias type:
ScriptAlias /cgi-bin/nagios/ /usr/local/nagios/sbin/

Important! The ScriptAlias entry for the CGIs must precede the standard 'ScriptAlias directive already present in the configuration file. If this configuration is not followed, use of the CGIs may not be available.

Once you've finished editing the Apache configuration file, you'll need to restart the web server with a the following command:
/etc/rc.d/init.d/httpd restart

Verify the Changes

It is important to make sure the changes to Apache work correctly. If http://yourmachine/nagios/ brings up the web interface, then the changes thus far are complete. None of the links will work at this step since Nagios is not running. Also, the functionality of the CGIs and other features have not yet been configured.

Configuring the Web Server for Authentication

The first step to configuring the web server for authentication is to make sure the access.conf file located at /etc/httpd/conf contains an “AuthOverride AuthConfig” statement in it for the Nagios cgi-bin directory. By default, the statement does not exist and it is necessary to add the following text to the access.conf file.

```
<Directory /usr/local/nagios/sbin>
AllowOverride AuthConfig
order allow,deny
allow from all
Options ExecCGI
</Directory>
```

It is not required to authorize a user to the HTML pages, but the option is available. To do this, add the statement bellow to the access.conf file as well.

```
AllowOverride AuthConfig
order allow,deny
allow from all
```

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The second step is to create a file named .htaccess in the root your CGI directory (and optionally also you HTML directory) for Nagios. This file(s) should be located in the /usr/local/nagios/sbin directory and the /usr/local/nagios/share directory, respectively. The file(s) should have contain the following text

```
AuthName "Nagios Access"
AuthType Basic
AuthUserFile /usr/local/nagios/etc/htpasswd.users
require valid-user
```

It is necessary to create the AuthUserFile and create the Nagiosadmin account by entering the following command:

```
htpasswd -c /usr/local/nagios/etc/htpasswd.users Nagiosadmin
```

Next, make sure that the CGIs are configured to use the authentication and authorization functionality in determining what information and/or commands users have access to. This is done be setting the use_authentication variable in the CGI configuration file (cgi.cfg in the /etc directory of the Nagios installation) to a non-zero value. The use_authentication variable should be set to equal 1. (use_authentication=1)

There are many options in the cgi.conf file that allow more privileges. To gain additional access, remove the comments ("#") from the following variables:

```
authorized_for_system_information
authorized_for_system_commands
authorized_for_configuration_information
authorized_for_all_hosts
authorized_for_all_host_commands
authorized_for_all_services
authorized_for_all_service_commands
```

Modifying the .cfg Files

There are several configuration files that Nagios utilizes when monitoring the network. Nagios configuration files are located in the /usr/local/etc/nagios directory. Fortunately, these files are highly configurable. Unfortunately, each administrator will require different services, computers, and processes be monitored on the network. The individual configuration of each of these files is not in scope of this document. Information on these files is provided below. Further information on the configuration of these files may be found on the Nagios website and in the manual pages.

Main Configuration File

The default installation places the main configuration file in the /usr/local/nagios/etc directory. The Nagios processes and the CGIs both read the nagios.cfg file. A sample main configuration file is automatically generated when the *make install-config* script is run during install.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Resource Files

Resource files are used to store user-defined settings. These files also contain other information such as database connection settings depending on how Nagios was configured. The main purpose of the resource files is to store sensitive configuration information.

Object Configuration Files

Object configuration files are used to define the hosts, services, hostgroups, contacts, contactgroups, commants, etc. relative to the network Nagios is monitoring. These files define what is to be monitored and how to monitor them.

CGI Configuration File

The CGI configuration file contains directives that affect the operation of the CGIs. A sample configuration file is generated when the *make install-config* script is run.

Extended Information Configuration Files

These files are used to define additional information for hosts and services that should be used by the CGIs. The extended information files allow the user to define icons and information to draw coordinates.

Verifying the Configuration

With all of the necessary modifications, it is necessary to run a test to verify the existing setup. This step is extremely helpful when troubleshooting Nagios because this check will produce error messages with additional information on where the error occoured.

Nagios automatically runs a "pre-check" before monitoring begins, but the check can also be initiated manually by using the following command:

usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

Starting Nagios

There are four ways to initiate Nagios:

Manually, as a foreground process (useful for initial testing and debugging)
Nagios has the option to enable debugging during the initial configure script. Running Nagios as a foreground process in a shell prompt will allow simplified monitoring and notification processes.

/usr/local/nagios/bin/nagios /usr/local/nagios/etc/nagios.cfg

Manually, as a background process
To run Nagios as a background process, invoke it with an ampersand.

/usr/local/nagios/bin/nagios /usr/local/nagios/etc/nagios.cfg &

Manually, as a daemon

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The –d switch is required to run Nagios in daemon mode.

```
/usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
```

Automatically at system boot

After Nagios has been tested and seems reasonable stable, enable Nagios to start automatically during boot. A startup script will need to be placed in the /etc/rc.d/init.d/ directory. A link to the script will also be required in the runlevel that Nagios should start in. A sample script is created (daemon-init) during the make install-init command.

Nagios is still in the alpha release stages, but has been in open source development under the previous name "Netsaint" for some time. Nagios is an excellent solution for any company requiring a comprehensive network monitoring utility. Prerequisites: time and patience.

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Sources

[1] Galstad, Ethan. "Nagios." 1999-2001. URL:
http://www.nagios.org

[2] Galstad, Ethan. 1999-2001. Program manual pages.

[3] Galstad, Ethan. "Netsaint." 1999-2001. URL:
http://www.netsaint.org

[4] Bar, Moshe. " How to Monitor Networks with Linux." July 28, 1999. URL:
http://www.byte.com/documents/s=94/byt19990728s0008/index.htm

[5] Unknown author. "Netsaint-a network monitor." September 10, 2001. URL:
http://www.freebsddiary.org/netsaint.php

[6] Geocrawler. "Netsaint-users – 2001." URL:
http://www.geocrawler.com/archives/3/1108/2001/

Additional Sources

The Apache Project URL: http://httpd.apache.org/

GD Graphics Library URL: http://www.boutell.com/gd/

Freshmeat URL: http://freshmeat.net/projects/netsaint/

SourceForge URL: http://sourceforge.net/projects/nagios/

RPM repository for Rpmfind.net URL: http://rpmfind.net/

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 4th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced