ANALELE UNIVERSITĂȚII
"EFTIMIE MURGU" REȘIȚA
ANUL XVII, NR. 2, 2010, ISSN 1453 - 7397

Emanuel Zgârdea, Ladislau Augustinov

Improving IT Infrastructure Management Using Nagios Open Source Package

This paper presents results from adapting Nagios software package to the conditions existing at the University "Eftimie Murgu" Resita, in order to construct an integrated monitoring system of the existing active communication equipment.

***Keywords**: Nagios, management, IT infrastructure*

1. Nagios package presentation

Nagios is an open source software package that comes to help IT infrastructure managers, it provides real-time view of the situation of active equipment and graphical visualization of activity from the previous period [1].

Through its specificity is dedicated to IT infrastructure, this package was used at first for the Linux operating system, then allowing it to be installed on other operating systems [2].

Convenience of Nagios is different and very useful in managing IT infrastructure. These include:

– periodic monitoring of servers by checking their response to ping, monitor different services installed on the monitored servers (NNTP, HTTP, POP3, SMTP);

– defining a hierarchical scheme of connections between IT infrastructure elements;

– to send notifications of various events related to an email address or a pager and can use custom methods to configure notifications;

– web interface can view the status of equipment.

2. Nagios on FreeBSD operating system

Since Nagios package is ported to the FreeBSD operating system, an stable operating system with a high level of security being used on Internet servers and data by a large number of institutions, we considered useful to present some package installation steps of Nagios on FreeBSD systems.

Starting from the idea that the FreeBSD operating system is already installed on the server, we will not go into details about its installation steps.

Since this paper is not subject to a setup guide, I would like to take stock of some options to be taken into account during installation. In the options window for Nagios check EMBEDDED_PERL. At the options for gd 2.0 check only ICONV. In options window for Nagios-plugins check MYSQL and leave the others default. In the compilation process a new user and group named nagios is needed.

For proper functioning of the application may choose to use lines of code in the documentation necessary to configure Apache, these lines are necessary to be inserted in the httpd.conf configuration file (Figure 1).

```
ScriptAlias /nagios/cgi-bin /usr/local/www/nagios/cgi-bin/

<Directory "/usr/local/www/nagios/cgi-bin">
   Options ExecCGI
   AllowOverride None
   Order allow,deny
   Allow from all
   AuthName "Nagios Access"
   AuthType Basic
   AuthUserFile /usr/local/etc/nagios/htpasswd.users
   Require valid-user
</Directory>

Alias /nagios /usr/local/www/nagios
<Directory "/usr/local/www/nagios">
   Options None
   AllowOverride None
   Order allow,deny
   Allow from all
   AuthName "Nagios Access"
   AuthType Basic
   AuthUserFile /usr/local/etc/nagios/htpasswd.users
   Require valid-user
</Directory>
```

Figure 1. Line of code to append in Apache's configuration file

2.1. Arguments about installing Nagios using Apache as Web server

The first and most important argument is the simple way to configure Nagios when using Apache as web server. The simple configuration is given and that the existing documentation for Nagios is built primarily for its installation operating with Apache.

Another argument is that of stability in use Nagios being tested and used in most cases in combination with Apache.

3. Customizing Nagios on FreeBSD Operating System

Nagios can be configured using the standard method, or using a personalized approach. If this configuration is done immediately after a new installation of Nagios, the standard configuration files can be found in the folder /usr/local/etc/nagios. First we check if configuration files are named appropriately because they are the default setting called *.cfg-sample.

The simplest way is to use common file called localhost.cfg that will pass all necessary text lines.

There is necessary to add "cfg_file=/usr/local/etc/nagios/localhost.cfg" and "cfg_file=/usr/local/etc/nagios/commands.cfg" nagios.cfg file located in the folder /usr/local/etc/nagios and any other cfg_file to be commented.

Each host must be defined separately using a few standard options interpreted by Nagios.

First we define the localhost (the server where Nagios is installed).

```
define host{
        use                     freebsd-server
        host_name               localhost
        alias                   localhost
        address                 127.0.0.1
        }
```

Figure 2. Options used to define localhost server

After that there is needed to insert the next server that will be monitored web called, but using the same structure as in the above lines:

```
define host{
  use                   freebsd-server
  host_name             Web
  alias                 Web Server
  address               192.168.0.4
  parents               localhost
  }
define hostextinfo{
```

```
        host_name           Web
        notes               Web Server
        icon_image          web.png
        vrml_image          web.png
        notes_url           http://192.168.0.4
        statusmap_image     web.png
        2d_coords           20,70
        3d_coords           80.0,50.0,75.0
        }
```

Figure 3. Options used to define a web server

For the e-mail server there is needed to user the lines above.

```
define host{
  use                   freebsd-server
  host_name             Email
  alias                 Email Server
  address               192.168.0.5
  parents               localhost
  }
define hostextinfo{
        host_name           Email
        notes               Email Server
        icon_image          email.png
        vrml_image          email.png
        notes_url           http://192.168.0.5
        statusmap_image     email.png
        2d_coords           20,70
        3d_coords           80.0,50.0,75.0
        }
```

Figure 4. Options used to define an e-mail server

There is possible to choose different images for each server, by place the image files in the /usr/local/www/nagios/images/logos/ folder to be accessible on the web.

To define groups of servers or other devices that can be placed in groups according to rules set by the administrator there is an option to define hostgroups.

```
define hostgroup{
        hostgroup_name  test
        alias           Test Servers
        members         localhost
        }
```

Figure 5. Options used to define a standard hostgroup including localhost

This defined hostgroup can be modified to include the other monitorized servers. In this example we will change the group name test, which will become servers, as well as the alias. Then we group this group of servers: localhost, Web, Email.

```
define hostgroup{
        hostgroup_name      Servere
        alias               Servers
        members             localhost,Web,Email
        }
```

Figure 5. Options used to define a custom hostgroup

Above servers is necessary to define which services are monitored individually. We insert the following lines corresponding to localhost, Web server and Email server:

```
define service{
    use                     local-service
    host_name               localhost
    service_description     PING
    check_command           check_ping!100.0,20%!500.0,60%
    }

define service{
        use                     local-service
        host_name               Web
        service_description     PING
        check_command           check_ping!100.0,20%!500.0,60%
        }

define service{
        use                     local-service
        host_name               Email
        service_description     PING
        check_command           check_ping!100.0,20%!500.0,60%
        }
```

Figure 6. Options used to define the monitorized services for each server

Nagios can be secured by using Apache by placing a .htaccess file in the nagios web folder. In this file some options must be defined for the authentification method.

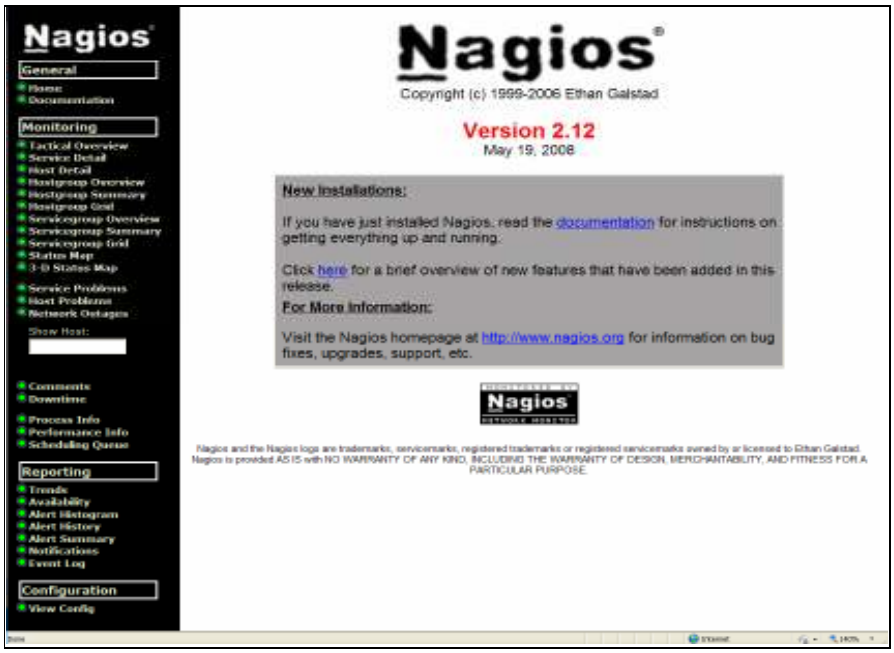

Figure 7. Nagios - Frontpage

To access the web interface, use the IP address of the server that was installed nagios, by example: http://192.168.0.1/nagios/

Type the user and password done above. Window that appears after starting the package Nagios can be seen on Figure 7.

The most important Menu options on Nagios are "Host Details" (Figure 8) and Status Map (Figure 9). The screenshots above are one in production example of Nagios wich is installed and configured by the author of this paper. After a log period of tests and customizations, this system works very well.

In the Host Details window, if the status of the monitorized service on the server is ok, the background of the is green, if the background is red the service has a problem, and in this case Nagios alert the system administrator by sending some email messages.

In the Status Map window, every host and service monitorized can be located in the map. Using the "parent" option on the configuration file, the services and hosts can be grouped in this map. If one service or host has a problem, the background of this will become red.

Nagios can be configured to use some sound files which can be defined according to the status of services, by example if some service not responding, can be defined one sound alert, if everything is ok can be defined one "No problem" sound.

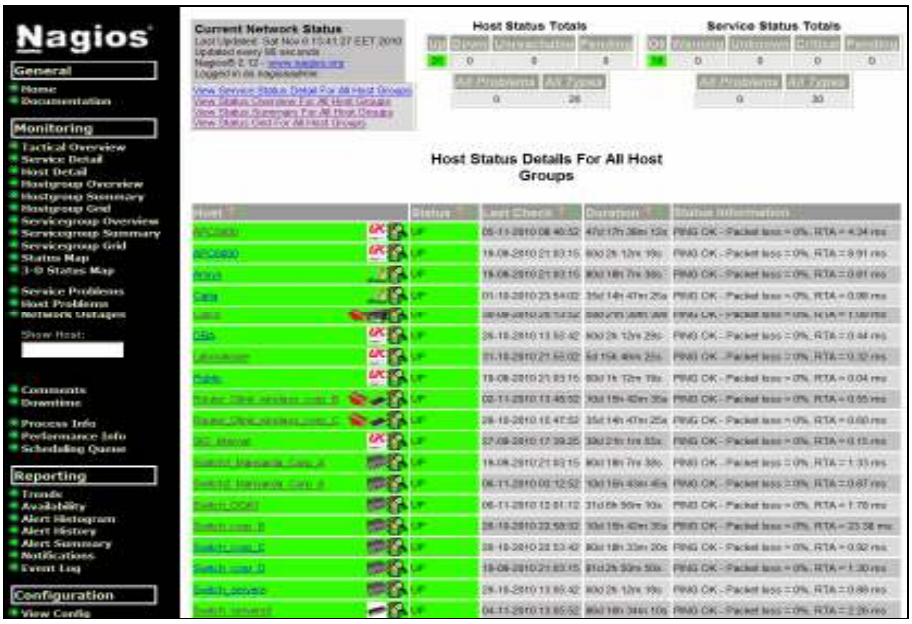

Figure 8. Nagios – Host Detail window

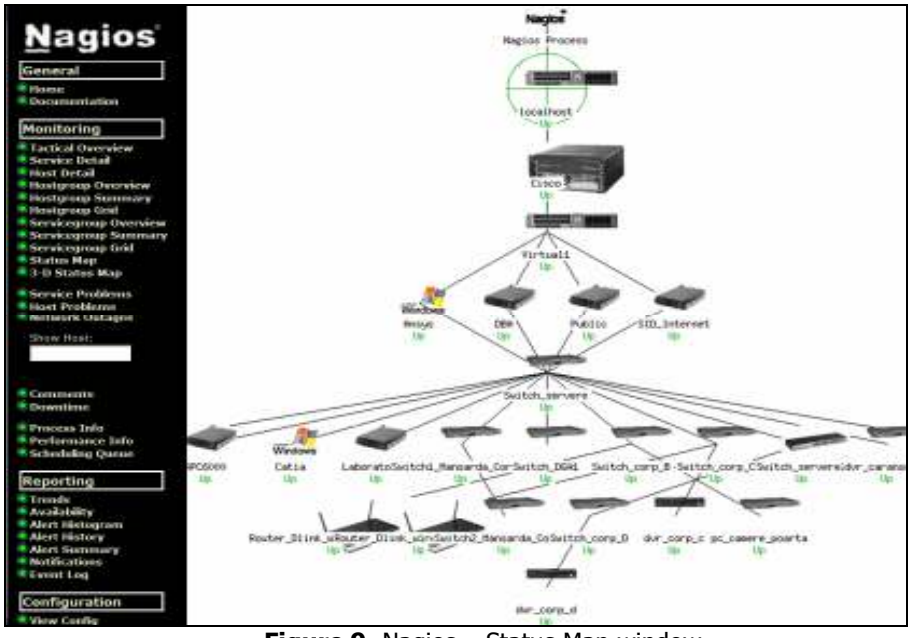

Figure 9. Nagios – Status Map window

4. Conclusion

Nagios package is successfully used for all types of IT infrastructure, proved to be very useful in cases where there is need to quickly diagnose some inevitable failures that occur in most IT infrastructures.

In the University "Eftimie Murgu" Resita Nagios is used successfully. Following the implementation of Nagios adapted to the needs of the university, there was a decrease in operation time restores interrupted services at a time.

Using Nagios the system administrator receive real-time alerts by email or pager about monitorized services. This is very useful in the case of critical services when the downtime is very expensive.

References

[1] http://support.nagios.com/knowledgebase/officialdocs
[2] http://wiki.nagios.org/index.php/Main_Page

Addresses:

- Ec. Inf. Emanuel Zgârdea, "Eftimie Murgu" University of Reşiţa, Traian Vuia Square, No 1-4, 320085, Reşiţa, e.zgardea@uem.ro
- PhD Stud. Eng. Ladislau Augustinov, "Eftimie Murgu" University of Reşiţa, Traian Vuia Square, No 1-4, 320085, Reşiţa, l.augustinov@uem.ro