Using Nagios to Monitor Networks

Posted by philcore on Mon 28 Nov 2005 at 12:23

Nagios is a powerful, modular network monitoring system that can be used to monitor many network services like smtp, http and dns on remote hosts. It also has support for snmp to allow you to check things like processor loads on routers and servers. I couldn't begin to cover all of the things that nagios can do in this article, so I'll just cover the basics to get you up and running.

```
apt-get install nagios-text
```

First we need to define people that will be notified, and define how they should be notified. In the example below, I define two users, joe and paul. Joe is the network guru and cares about routers and switches. Paul is the systems guy, and he cares about servers. Both will be notified via email and by pager. Note that if you are going to monitor your email server, you will want to use another notification method besides email. If your email server is down, you can't send anybody an email to notify them! :) In that case you will want to use a pager server to send a text message to a phone or pager, or set up a second nagios monitor that uses a different mail server to send email.

Edit /etc/nagios/contacts.cfg and add the following users:

```
define contact{
    contact_name                    joe
    alias                           Joe Blow
    service_notification_period     24x7
    host_notification_period        24x7
    service_notification_options    w,u,c,r
    host_notification_options       d,u,r
    service_notification_commands   notify-by-email,notify-by-pager
    host_notification_commands      host-notify-by-email,host-notify-by-epager
    email                           joe@yourdomain.com
    pager                           5555555@pager.yourdomain.com
    }

define contact{
    contact_name                    paul
    alias                           Paul Shiznit
    service_notification_period     24x7
    host_notification_period        24x7
    service_notification_options    w,u,c,r
    host_notification_options       d,u,r
    service_notification_commands   notify-by-email,notify-by-epager
    host_notification_commands      host-notify-by-email,host-notify-by-epager
    email                           paul@yourdomain.com
    pager                           5556666@pager.yourdomain.com
    }
```

Now add the users to groups.
In /etc/nagios/contactgroups.cfg add the following:

```
define contactgroup{
    contactgroup_name   router_admin
    alias               Network Administrators
    members             joe
}

define contactgroup{
    contactgroup_name   server_admin
    alias               Systems Administrators
```

```
    members             paul
}
```

You can add multiple members to a contact group by listing comma separated users.

Now to define some hosts to monitor. For my example, I define two machines, a mail server and a router.

Edit /etc/nagios/hosts.cfg and add:

```
define host{
    use                     generic-host
    host_name               gw1.yourdomain.com
    alias                   Gateway Router
    address                 10.0.0.1
    check_command           check-host-alive
    max_check_attempts      20
    notification_interval   240
    notification_period     24x7
    notification_options    d,u,r
    }

define host{
    use                     generic-host
    host_name               mail.yourdomain.com
    alias                   Mail Server
    address                 10.0.0.100
    check_command           check-host-alive
    max_check_attempts      20
    notification_interval   240
    notification_period     24x7
    notification_options    d,u,r
    }
```

Now we add the hosts to groups. I define groups called 'routers' and 'servers' and add the router and mail server respectively.

Edit /etc/nagios/hostgroups.cfg

```
define hostgroup{
    hostgroup_name  routers
    alias           Routers
    contact_groups  router_admin
    members         gw1.yourdomain.com
    }

define hostgroup{
    hostgroup_name  servers
    alias           Servers
    contact_groups  server_admin
    members         mail.yourdomain.com
    }
```

Again, for multiple members, just use a comma separated list of hosts.

Next define services to monitor on each of the hosts. Nagios has many built-in plugins for monitoring. On a debian sarge system, they are stored in /usr/lib/nagios/plugins. Here we want to monitor the smtp service on the mail server, and do ping checks on the router.

Edit /etc/nagios/services.cfg

```
define service{
```

```
    use                     generic-service
    host_name               mail.yourdomain.com
    service_description     SMTP
    is_volatile             0
    check_period            24x7
    max_check_attempts      3
    normal_check_interval   5
    retry_check_interval    1
    contact_groups          server_admin
    notification_interval   240
    notification_period     24x7
    notification_options    w,u,c,r
    check_command           check_smtp
    }

define service{
    use                     generic-service
    host_name               gw1.yourdomain.com
    service_description     PING
    is_volatile             0
    check_period            24x7
    max_check_attempts      3
    normal_check_interval   5
    retry_check_interval    1
    contact_groups          router_admin
    notification_interval   240
    notification_period     24x7
    notification_options    w,u,c,r
    check_command           check_ping!100.0,20%!500.0,60%
    }
```

And that's it. To test your configurations, you can run

```
nagios -v /etc/nagios/nagios.cfg
```

If all is well we can restart nagios and move on to the apache side to get a visual view of the monitor.

```
/etc/init.d/nagios restart
```

Assuming you have a working apache install, you can add the apache.conf file included in the nagios package to set up the nagios cgi administration interface. The web interface is not required to run nagios, but it is definitely worth setting it up. The simplest way to get it up and running is to copy the supplied conf file over to our apache installation. On my system, I'm running apache2. Systems running apache 1.3.xx will have slightly different setups.

```
cp /etc/nagios/apache.conf /etc/apache2/sites-enabled/nagios
```

Of course you may want to set it up as a virtual server, but I leave that as an exercise for the reader. Now you will want to set up an allowed user to view the cgi interface. By default, nagios issues full administrative access to the nagiosadmin user. Nagios uses apache htpasswd style authentication. So here we add a user and password to the default nagios htpasswd file. Here we add the user nagiosadmin with password mypassword to the nagios htpasswd file.

```
htpasswd2 -nb nagiosadmin mypassword >> /etc/nagios/htpasswd.users
```

You should now be able to restart apache and logon to

http://your.nagios.server/nagios

Nagios is a very powerful tool for monitoring networks. I've only touched on the basics here, but it should be enough to get you up and running. Hopefully, once you do, you'll start experimenting with all the cool features and plugins that are available. The documentation included in the cgi

interface is very detailed and helpful.

This article can be found online at the **Debian Administration** website at the following bookmarkable URL:

- http://www.debian-administration.org/articles/299

At the time this print version was generated, the online version had 20 comments posted in reply to it.

This article is copyrighted, please check the online version for details.