CIS 410 project report

The experiments of Nagios

Qianyi Feng

Introduction:

Nagios is an open source monitoring system for monitoring the computer systems and networks, and providing the alerts for the abnormal activities. It offers wide range monitoring services, such as system monitoring, protocol monitoring, application monitoring, database monitoring, log monitoring and bandwidth monitoring. From the official website of Nagios, there are more services provided in details with different demands and groups(see https://www.nagios.com/solutions/). In this project, I would focus on the installation and configuration of Nagios first, and explore other functions while Nagios could be run on my VM successfully.

Installation and Configuration:

1. Upgrade the system:
    a) sudo apt update
    b) sudo apt upgrade
    c) sudo apt install build-essential libgd-dev openssl libssl-dev unzip apache2 php

2. Create new users and groups:
    a) sudo useradd nagios
    b) sudo groupadd nagcmd
    c) sudo usermod -a -G nagcmd nagios
3. Download Nagios 4.4.2 and untar it:
    a) sudo wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.4.2.tar.gz
    b) sudo tar xzvf nagios-4.4.2.tar.gz
4. Make install:
    a) cd nagios-4.4.2
    b) sudo ./configure --with-nagios-group=nagios --with-command-group=nagcmd
    c) sudo make all
    d) sudo make install
    e) sudo make install-init
    f) sudo make install-commandmode
    g) sudo make install-config
5. Install the packages for web services and plugins:
    a) sudo /usr/bin/install -c -m 644 sample-config/httpd.conf /etc/apache2/sites-available/nagios.conf

b) sudo usermod -a -G nagcmd www-data

c) cd ..

d) sudo wget http://www.nagios-plugins.org/download/nagios-plugins-2.2.1.tar.gz

e) sudo tar xzvf nagios-plugins-2.2.1.tar.gz

f) cd nagios-plugins-2.2.1

g) sudo ./configure --with-nagios-user=nagios --with-nagios-group=nagcmd --with-openssl

h) sudo make

i) sudo make install

6. Set the user account for the web page

a) sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin

7. Enable apache module:

a) sudo a2enmod rewrite

b) sudo a2enmod cgi

c) sudo ln -s /etc/apache2/sites-available/nagios.conf /etc/apache2/sites-enabled/

8. Create the service file for Nagios:

a) sudo vim /etc/systemd/system/nagios.service

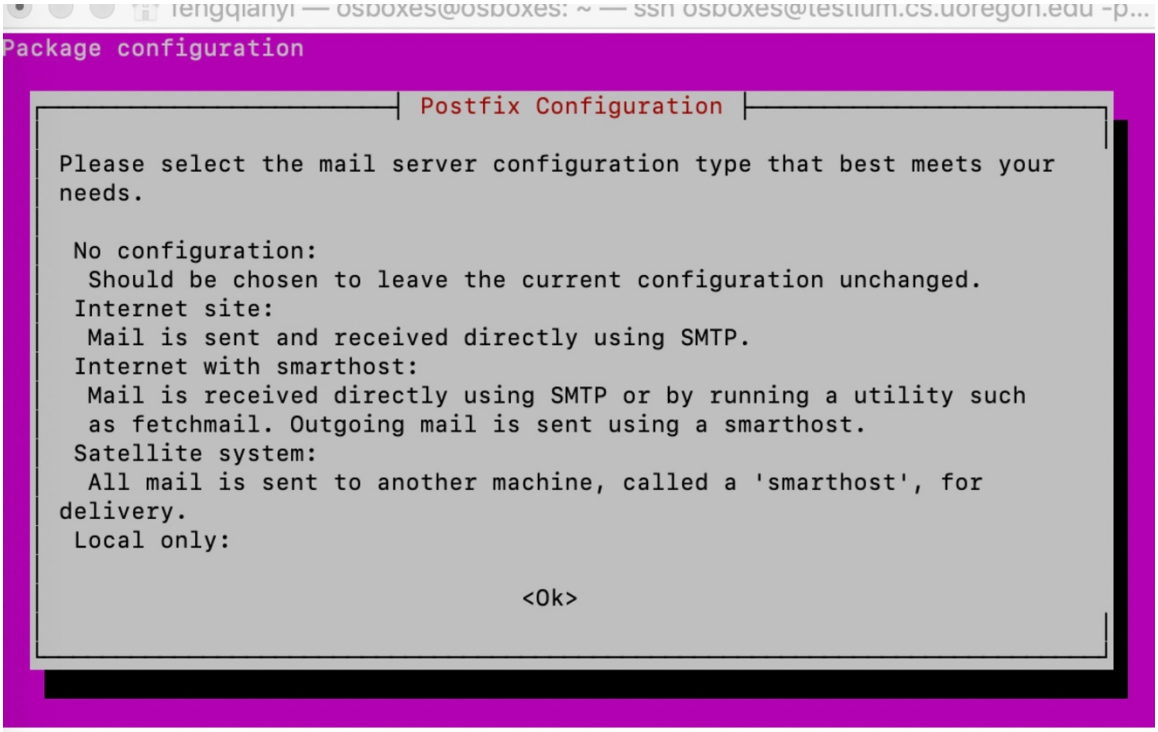
```
##################################################################
    [Unit]
    Description=Nagios
    BindTo=network.target
    [Install]
    WantedBy=multi-user.target
    [Service]
    Type=simple
    User=nagios
    Group=nagcmd
    ExecStart=/usr/local/nagios/bin/nagios /usr/local/nagios/etc/nagios.cfg
```

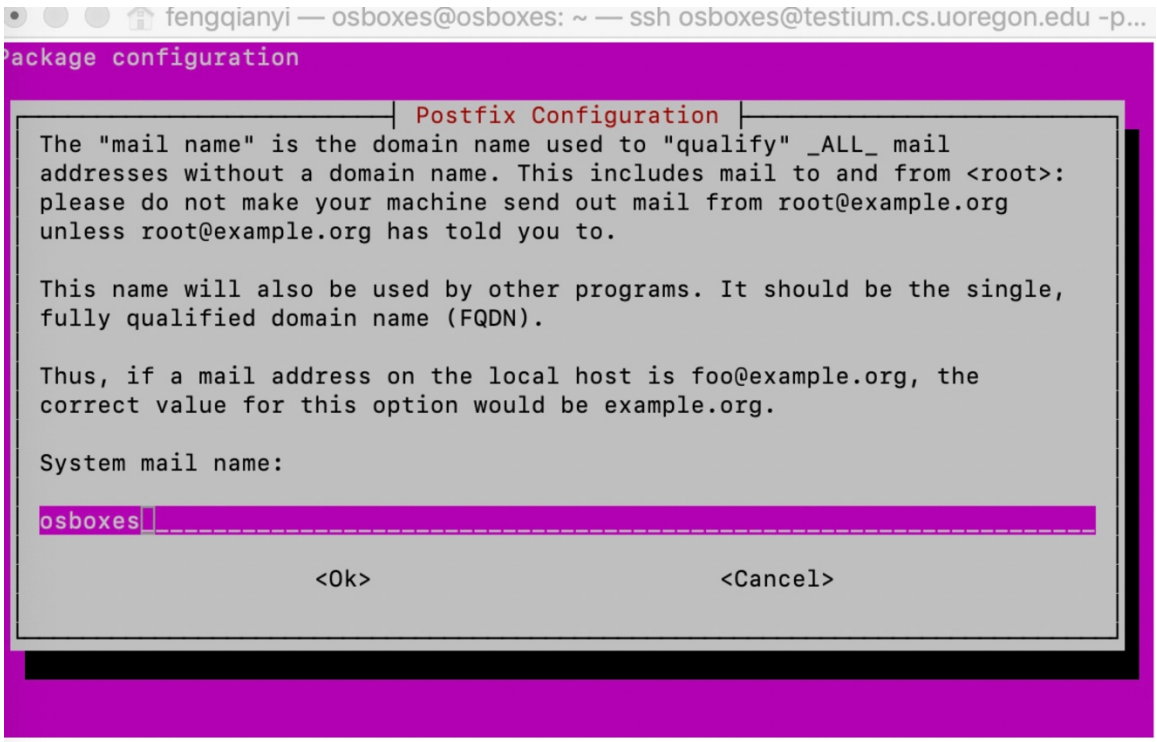
9. Reload apache and Nagios service, check the status of Nagios:
    a) sudo systemctl restart apache2
    b) sudo systemctl enable /etc/systemd/system/nagios.service
    c) sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
    d) sudo systemctl start nagios
    e) sudo systemctl status nagios

Modify configuration files:

1. Check if the mail service could work on VM:

   a) sudo apt install mailutils





echo “Testing” | mail -s “Testing” qfeng0710@gmail.com

2. cd /usr/local/nagios/etc/, modify nagios.cfg file, make sure the configuration includes the four later files.

3. cd /usr/local/nagios/etc/objects, modify localhost.cfg file (to create self-defined services)

```
define service {
    use                             local-service
    host_name                       localhost
    service_description             Check Current Uses
    check_command                   check_current_users!2
    notifications_enabled           1
-- INSERT --
```

contacts.cfg(add the admin mail address for sending the notification email)

```
#
# CONTACTS
#
###############################################################################

# Just one contact defined by default - the Nagios admin (that's you)
# This contact definition inherits a lot of default values from the
# 'generic-contact' template which is defined elsewhere.

define contact {

    contact_name            nagiosadmin             ; Short name of user
    use                     generic-contact         ; Inherit default values from gen
ined above)
    alias                   Nagios Admin            ; Full name of user
    email                   qfeng1021@gmail.com ; <<***** CHANGE THIS TO YOUR EMAIL A
}



###############################################################################
#
# CONTACT GROUPS
#
###############################################################################

# We only have one contact in this simple configuration file, so there is
# no need to create more than one contact group.

define contactgroup {

    contactgroup_name       admins
    alias                   Nagios Administrators
    members                 nagiosadmin
}
~
-- INSERT --
```

commands.cfg(check if the directory of mail notification is correct and tell Nagios how to execute new user-defined function)

```
################################################################################

define command {

    command_name    notify-host-by-email
    command_line    /usr/bin/printf "%b" "***** Nagios *****\n\nNotification Type: $NOTIFICATIONTYPE$\nHost: $H
OSTNAME$\nState: $HOSTSTATE$\nAddress: $HOSTADDRESS$\nInfo: $HOSTOUTPUT$\n\nDate/Time: $LONGDATETIME$\n" | /bin
/mail -s "** $NOTIFICATIONTYPE$ Host Alert: $HOSTNAME$ is $HOSTSTATE$ **" $CONTACTEMAIL$
}



define command {

    command_name    notify-service-by-email
    command_line    /usr/bin/printf "%b" "***** Nagios *****\n\nNotification Type: $NOTIFICATIONTYPE$\n\nServic
e: $SERVICEDESC$\nHost: $HOSTALIAS$\nAddress: $HOSTADDRESS$\nState: $SERVICESTATE$\n\nDate/Time: $LONGDATETIME$
\n\nAdditional Info:\n\n$SERVICEOUTPUT$\n" | /bin/mail -s "** $NOTIFICATIONTYPE$ Service Alert: $HOSTALIAS$/$SE
RVICEDESC$ is $SERVICESTATE$ **" $CONTACTEMAIL$
}
```

-

```
define command {
    command_name    check_current_users
    command_line    $USER1$/check_current_users -H $HOSTADDRESS$ -c $ARG1$
-- INSERT --
```

templates.cfg

```
# Local service definition template
# This is NOT a real service, just a template!

define service {

    name                            local-service           ; The name of this service templ
    use                             generic-service         ; Inherit default values from th
efinition
    max_check_attempts              4                       ; Re-check the service up to 4 t
termine its final (hard) state
    check_interval                  5                       ; Check the service every 5 minu
nditions
    retry_interval                  1                       ; Re-check the service every min
ate can be determined
    register                        0                       ; DONT REGISTER THIS DEFINITION
RVICE, JUST A TEMPLATE!
    notifications_enabled           1
    notification_period             24x7
    notification_interval           6
    notification_options            c,u,r
    contact_groups                  admins
}
-- INSERT --
```

4. cd /usr/local/nagios/libexec
    a) touch check_current_users
    b) vim check_current_user
    c) chmod +x /usr/local/nagios/libexec/check_current_users

Test if Nagios could work:

1.

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

sudo systemctl restart nagios

sudo systemctl status nagios

2. Create new testuser account.
3. cat /usr/local/nagios/var/nagios.log to check the log of Nagios
4. Check if the mail notification works:
    a) iptables -A INPUT -p icmp -j DROP: drop all the packages include ping.

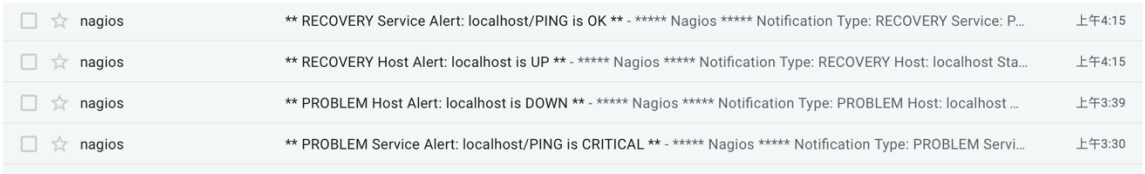
When the host found that the PING service does not work, it would send the notification email to the admin. The host would check the service of the server. If it found that the PING service still could not work, it would send the email to the admin again and reports the DOWN state.

b) iptables -F

c) iptables -X

d) iptables -Z

After the recovery of iptables, the host would send the notification email to the admin.



5. For the monitoring the service, event log, notifications on web page of Nagios:

   Because there is no UI for the VM, I use w3m for viewing the web page in the terminal:

   sudo apt-get install w3m w3m-img -y

   w3m 192.168.73.10/nagios

   user account: nagiosadmin

   user password: qfeng1021

Then the website would be loaded:

Go to the side link:

From the service links the admins could check the status of the server.

6. Check if the user login activities could be monitored:

   a) Check if the “check_current_users” could work on bash

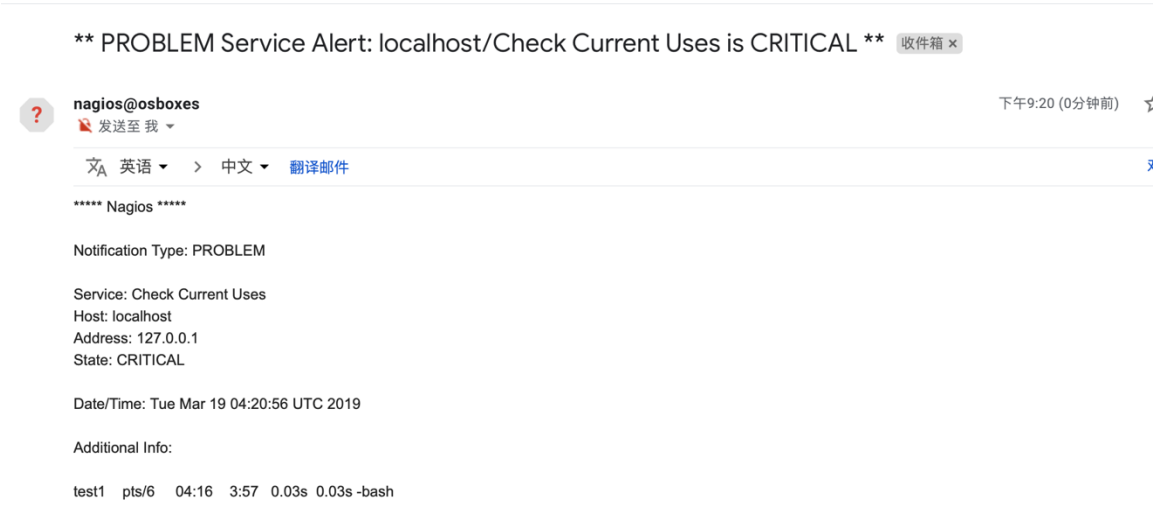
   b) Login the VM with the new user

   c) Go to the webpage -> Alerts:

```
March 19, 2019 04:00

Service Critical[03-19-2019 04:20:56] SERVICE ALERT: localhost;Check Current Uses;CRITICAL;HARD;4;test1 pts/6 04:16 3:57
0.03s 0.03s -bash
Service Critical[03-19-2019 04:19:56] SERVICE ALERT: localhost;Check Current Uses;CRITICAL;SOFT;3;test1 pts/6 04:16 2:57
0.03s 0.03s -bash
Service Critical[03-19-2019 04:18:56] SERVICE ALERT: localhost;Check Current Uses;CRITICAL;SOFT;2;test1 pts/6 04:16 1:57
0.03s 0.03s -bash
Service Critical[03-19-2019 04:17:56] SERVICE ALERT: localhost;Check Current Uses;CRITICAL;SOFT;1;test1 pts/6 04:16
57.00s 0.03s 0.03s -bash
Program Start[03-19-2019 04:16:51] Nagios 4.4.2 starting... (PID=6198)
Program End[03-19-2019 04:16:51] Caught SIGTERM, shutting down...
Program End[03-19-2019 04:16:51] Caught SIGTERM, shutting down...
```

Also, there would be an email sent to the admin's address:
The addition info is the same with the result of execute "check_current_users" in the terminal:




```
osboxes@osboxes:/usr/local/nagios/libexec$ sudo bash ./check_current_users
osboxes  pts/5     03:46    9:00   0.74s  0.71s w3m 192.168.73.10/nagios
osboxes@osboxes:/usr/local/nagios/libexec$ sudo bash ./check_current_users
test1    pts/6     04:15    3.00s  0.03s  0.03s -bash
osboxes@osboxes:/usr/local/nagios/libexec$ sudo bash ./check_current_users
test1    pts/6     04:15    5.00s  0.03s  0.03s -bash
```

7. Check if the check_load works:
   a) Run the forkbomb.sh on test1 user account:

```
Current Status:             OK
                           (for 8d 21h 34m 31s)
Status Information:        OK - load average: 0.03, 0.03, 0.00
Performance Data:          load1=0.030;5.000;10.000;0; load5=0.030;4.000;6.000;0; load15=0.000;
                           3.000;4.000;0;
Current Attempt:           1/4  (HARD state)
Last Check Time:           03-19-2019 05:38:26
Check Type:                ACTIVE
Check Latency / Duration: 0.001 / 0.005 seconds
Next Scheduled Check:      03-19-2019 05:43:26
Last State Change:         03-10-2019 08:07:24
Last Notification:         N/A (notification 0)
Is This Service Flapping?   NO
                           (0.00% state change)
In Scheduled Downtime?      NO
Last Update:               03-19-2019 05:41:50  ( 0d 0h 0m 5s ago)
```

The initial load average was 0.0, 0.0, 0.0. After the forkbomb.sh has been launched for half an hour, the load average has increased.

References:

https://www.cnblogs.com/kaituorensheng/p/4682565.html

https://blog.csdn.net/qq_35346390/article/details/76066326

https://www.cnblogs.com/hanxiaomeng/p/5423028.html

https://geekpeek.net/nagios-configuration/

https://serverfault.com/questions/774498/failed-to-start-nagios-service-unit-nagios-service-failed-to-load-no-such-file