Nagios and Request Tracker Ticket Creation

Notes:
------
* Commands preceded with "$" imply that you should execute the command as
  a general user - not as root.
* Commands preceded with "#" imply that you should be working as root.
* Commands with more specific command lines (e.g. "RTR-GW>" or "mysql>")
  imply that you are executing commands on remote equipment, or within
  another program.

Exercises

To configure RT and Nagios so that alerts from Nagios automatically
create tickets requires a few steps:

* Create a proper contact entry for Nagios in
  /etc/nagios3/conf.d/contacts_nagios2.cfg

* Create the proper command in Nagios to use the rt-mailgate
  interface. The command is defined in /etc/nagios3/commands.cfg

These next two items should already be done in RT if you have
finished the RT exercises.

* Install the rt-mailgate software and configure it properly
  in your /etc/aliases file for your MTA in use.

* Configure the appropriate queues in RT to receive emails
  passed to it from Nagios via the rt-mailgate software.

Exercises
----

0. Log in to your PC or open a terminal window as the sysadmin user.

1.) Configure a Contact in Nagios

   - Edit the file /etc/nagios3/conf.d/contacts_nagios2.cfg

   # vi /etc/nagios3/conf.d/contacts_nagios2.cfg

   - In this file we will first add a new contact name under
     the default root contact entry. The new contact should
     look like this:

```
define contact{
        contact_name                    net
        alias                           RT Alert Queue
        service_notification_period     24x7
        host_notification_period        24x7
        service_notification_options    c
        host_notification_options       d
        service_notification_commands   notify-service-ticket-by-email
        host_notification_commands      notify-host-ticket-by-email
        email                           net@localhost
        }
```

   - the service_notification_option of "c" means only notify once a
     service is considered "critical" by Nagios (i.e. down). The
     host_notification_option of "d" means down. By specify only "c"
     and "d" this means that notifications will not be sent for other
     states.

   - Note the email address in use "net@localhost" - this is important
     as this was previously defined for RT.

   - Now we must create a Contact Group that contains this contact.
     We will call this group "tickets." Do this at the end of the file:

```
define contactgroup{
        contactgroup_name       tickets
        alias                   email to ticket system for RT
        members                 net,root
        }
```

   - You could leave off "root" as a member, but we've left this on to
     have another user that receives email to help us troubleshoot if
     there are issues.

   - Now that your contact has been created you need to create the commands
     that were referenced in the initial contact creation above, these are
     "notify-service-ticket-by-email" and "notify-host-ticket-by-email"

2.) Update Nagios Commands

   - To create the notify-service-ticket-by-email and notify-host-ticket-by-email
     commands we need to edit the file /etc/nagios3/commands.cfg.

   # vi /etc/nagios3/commands.cfg

  - In this file you already have two command definitions that we are using. These are
    called notify-host-by-email and notify-service-by-email. We are going to add two
    new commands.

  - We _strongly_ suggest that you COPY and PASTE the text below. It is almost impossible
    to type it without errors.

  - Put these two new entries below the current notify-host-by-email and notify-service-by-email
    command entries. Do not remove the old one.

  - NOTE: The "commands below do not contain breaks. They are a single line. Be aware of this as
    COPY and PASTE between some editors and environments may insert line breaks.

```
################################################################
# Additional commands created for network management workshop #
################################################################

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

# 'notify-service-ticket-by-email' command definition
define command{
        command_name    notify-service-ticket-by-email
        command_line    /usr/bin/printf "%b" "***** Nagios *****\n\nNotification Type: $NOTIFICATIONTYPE$\n\nService:
$SERVICEDESC$\nHost: $HOSTALIAS$\nAddress: $HOSTADDRESS$\nState: $SERVICESTATE$\n\nDate/Time: $LONGDATETIME$\n
\nAdditional Info:\n\n$SERVICEOUTPUT$" | /usr/bin/mail -s "** $NOTIFICATIONTYPE$ Service Alert: $HOSTALIAS$/$SERVICEDESC
$ is $SERVICESTATE$ **" $CONTACTEMAIL$
        }
```

3.) Choose a Service to Monitor with RT Tickets

   - The final step is to tell Nagios that you wish to notify the contact "tickets" for a
     particular service. If you look in /etc/nagios3/conf.d/generic-service_nagios2.cfg the
     default contact_groups is "admins". To override this for a service edit the file
     /etc/nagios3/conf.d/services_nagios2.cfg and a contact_groups entry for one of the
     service definitions.

    - To send email to generate tickets in RT if SSH goes down on a box you would edit the
      SSH service check so that it looks like this:

```
define service {
        hostgroup_name                  ssh-servers
        service_description             SSH
        check_command                   check_ssh
        use                             generic-service
        notification_interval           0 ; set > 0 if you want to be renotified
        contact_groups                  tickets
}
```

Note the additional item that we now have, "contact_groups." You can do this for other entries as well if you wish.

- When you are done, save the file and exit.

- Now restart Nagios to verify your changes are correct.

```
# /etc/init.d/nagios3 stop
# /etc/init.d/nagios3 start
```

4.) Generate RT Tickets for Hosts

- To do this you must either specify "contact_groups tickets" for individual host definitions, or you must update the template file for all hosts and change the default contact_groups entry to tickets. This file is generic-host_nagios2.cfg.

- If you wish to do this go ahead. Tickets will be generated if a host goes down and you have specified the contact_groups for that host as being "tickets"

5. See Nagios Tickets in RT

- To verify your changes have worked you will need to stop the ssh service on your machine or another machine.

```
# /etc/init.d/ssh stop
```

- It will take a while (up to 10 minutes) for Nagios to report that SSH is "critical", but once that happens a new ticket should appear in your RT instance in the net queue generated by Nagios.

- Remember to see this go to http://MyMAchine/rt/ and log in as Username "sysadmin" with the password you chose when you created the RT sysadmin account. The new ticket should appear in the "10 newest unowned tickets" box in the main log in page in RT.