

Nagios and Request Tracker Integration Creating Tickets

Notas:

- * Los comandos precedidos por "\$" implican que debe ejecutar el comando como usuario genérico - no como root
- * Los comandos precedidos por "#" implican que debería estar trabajando como usuario root.
- * Los comandos con inicios de línea más específicos como "rtrX>" o "mysql>" indican que debe ejecutar los comandos en un equipo remoto, o dentro otro programa
another program.

En resumen:

Para configurar RT y Nagios de manera que las alarmas de Nagios automáticamente creen tickets (incidencias) en RT, es necesario seguir los siguientes pasos:

- * Crear un contacto en Nagios
- * Actualizar la configuración de servicios o la de un nodo en particular para usar el nuevo grupo de contactos.
- *

Los siguientes dos pasos ya deberían estar hechos si ha terminado los ejercicios de RT.

- * Instalar el programa rt-mailgate y configurarlo apropiadamente en su archivo de alias para que su programa de correo lo pueda usar.
- * Configurar las colas (queues) en RT de manera correspondiente para recibir e-mails que lleguen de Nagios a través de rt-mailgate.

Ejercicios

0. Ingrese en su máquina virtual con ssh, como usuario sysadm

1.) Configurar el contacto en Nagios

Conviértase en root:

```
$ sudo -s
```

Edite el archivo de contactos

```
# editor /etc/nagios3/conf.d/contacts_nagios2.cfg
```

En este archivo, primero agregaremos un nuevo contacto debajo del usuario root por defecto.

ATENCIÓN: No elimine el contacto de root!

El nuevo contacto debería verse similar a (DEBAJO DEL CONTACTO root):

```

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-by-email
    host_notification_commands notify-host-by-email
    email                 net@localhost
}

```

Ahora, al final del archivo, agregue también:

(Nota: No borre o edite ninguna otra definición existente.)

```

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

```

Grabe y salga

Notas

- La opción "c" de service_notification significa que sólo se ha de enviar una alarma cuando el servicio esté en estado "crítico" en Nagios (ej. down). La opción "d" significa "down". Si se seleccionan sólo "c" y "d", no se enviarán alarmas para otros estados.

- Fíjese en la dirección de correo usada "net@localhost" - esto es importante ya que esta cuenta se definió anteriormente en los ejercicios de RT.

- Podría no incluir a "root" como miembro, pero lo hemos dejado para que haya otro usuario recibiendo correo, y así podríamos resolver problemas.

3.) Elija un servicio a monitorear que pueda crear tickets en RT

Para que se generen tickets en RT si se cae el servicio SSH en una máquina, debemos editar el chequeo de servicio de SSH:

```
# editor /etc/nagios3/conf.d/services_nagios2.cfg
```

Busque el servicio con el hostgroup_name de "ssh-servers" y agregue la línea "contact_groups". Cuando termine de editar la definición del servicio, será algo como lo siguiente:

```

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,admins
}
```

Grabe y salga del editor.

Notas

- Fíjese en el elemento adicional que tenemos ahora, "contact_groups". Podría hacer esto con otras definiciones si así lo desea.
- También notará que incluimos el grupo de contacto por defecto "admins". Podría no incluirlo si quiere.

Reinicie Nagios para verificar que sus cambios son correctos:

```
# service nagios3 restart
```

Si se cae el servicio SSH en cualquiera de los nodos que estamos monitoreando, Nagios debería generar un nuevo ticket en RT. Vamos a bajar el servicio SSH en el servidor NOC del taller. Si no está monitoreando esta máquina, tendrá que agregar configuración en Nagios (hostgroups_nagios2.cfg)

5. Ver los tickets de nagios en RT

- Nagios tardará un rato (hasta 5 minutos) para reportar que el servicio SSH está crítico. Luego ha de esperar un total de 4 chequeos para que el servicio se considere como "down hard". En este momento, Nagios enviará una notificación al e-mail net@localhost y se creará un ticket en RT.
- Recuerde ir a <http://pcX.ws.nsrc.org/rt/> y entrar como "sysadm". El nuevo ticket debería aparecer en la lista "10 newest unowned tickets" de la página principal de RT.