

Notas:

- * Comandos que empiezan con un "\$" implica que deberia ejecutar el comando como un usuario general - no como root.
- * Comandos que empiezan con un "#" implica que deberia trabajar como el usuario root.
- * Comandos con lineas mas especificas (como "GW-RTR>" o "mysql>") implica que esta ejecutando el comando en un equipo remoto o dentro otro programa.
- * Si una linea termina con un "\" esto indica que el comando sigue en la proxima linea y Ud. deberia tratar el comando si como fuera en una sola linea.

Exercicios Parte I

Para configurar RT y Nagios para que las alertas de Nagios pueden generar un pedido en RT en forma automatica se requiere algunos pasos de configuracion:

- * Crear una entrada de contacto en Nagios en /etc/nagios3/conf.d/contacts_nagios2.cfg
- * Crear un comando nuevo de Nagios para usar la facilidad de rt-mailgate. El comando se lo define en /etc/nagios3/commands.cfg
- * Si termino de configurar RT el software de rt-mailgate ya esta instalado y configurado con una cola de "net" para recibir correo y cambiarlo en un pedido.

Exercises

0. Haz un log in en su PC.

1.) Configurar un contacto en Nagios

- Abre el archivo /etc/nagios3/conf.d/contacts_nagios2.cfg

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

- Agregamos un nombre nuevo debajo la entrada por root. La entrada nueva se vea asi:

```
define contact{
    contact_name      net
    alias             Cola de Alerta RT
    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
}
```

- La opcion de service_notification_option de "c" significa que Nagios notifica despues que un servicio llega al estado de "critico" (caido). La opcion de host_notification_option de "d" es para "down" (caido). Asi, usando solo estos Nagios solo manda una notificacion cuando algo deja de responder o funcionar.

- El correo net@localhost es la clave. Esto es que corresponde a la cola de "net" en RT usando el software to rt-mailgate y la definicion en el archivo /etc/aliases.

- Ahora necesitamos un Grupo de Contactos que contiene el nuevo contact. Vamos a llamar este grupo "tickets". Agrega esta entrada al fin del archivo:

```
define contactgroup{
    contactgroup_name tickets
    alias             sistema de correo a pedido con RT
    members          net,root
}
```

- "root" no es necesario pero es bueno durante el proceso de verificacion para ayudar si hay problemas en la configuracion.

- Ya tenemos los contactos. Ahora necesitamos crear los comandos que usamos en caso de que queremos que Nagios manda un correo a net@localhost.

2.) Actualizar Comandos de Nagios

- Para crear los dos comandos nuevos que vamos a llamar notify-service-ticket-by-email y notify-host-ticket-by-email tenemos que editar el archivo /etc/nagios3/commands.cfg.

```
# vi /etc/nagios3/commands.cfg
```

- En este archivo ya tenemos dos definiciones de comandos que usamos. Estos se llaman notify-host-by-email y notify-service-by-email. Vamos a agregar los comandos nuevos.

- Sugiero que haz un COPY y PASTE del texto abajo. Es casi imposible tipearlo sin tener errores.
- Ponga estos dos entradas debajo las entradas de notify-host-by-email y notify-service-by-email.
- NOTA! El "command_line" es una sola linea.

```
#####
# Comandos adicionales hecho por el taller gestion de redes #
#####

# 'notify-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: $HOSTSTATES$\nAddress:
$HOSTADDRESS$\nInfo: $HOSTOUTPUT$\n\nDate/Time: $LONGDATETIME$\n" | /usr/bin/mail -s "*** $NOTIFICATIONTYPE$ Host Alert: $HOSTNAME$ is $HOSTSTATES ***
$CONTACTEMAIL$
    }

# '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: $SERVICESTATES$\n\nDate/Time: $LONGDATETIME$\n\nAdditional Info:\n\n$SERVICEOUTPUT$" | /usr/bin/mail -s "***
$NOTIFICATIONTYPE$ Service Alert: $HOSTALIAS/$SERVICEDESC$ is $SERVICESTATES ***" $CONTACTEMAIL$
    }

```

3.) Elige un Servicio para Monitorear y Generar Tickets en RT

- Esto es el ultimo paso. Tiene que indicar a Nagios que quiere notificar el contact "tickets" por un servicio en particular. Vea en /etc/nagios3/conf.d/generic-service_nagios2.cfg que grupo de contacto por defecto es "admins" - Para cambiar este por un servicio tiene que editar el archivo /etc/nagios3/conf.d/services_nagios2.cfg y agregar una entrada de contact_groups por uno de las entradas de definicion de servicio.
- Para mandar un correo que genera un ticket si el servicio de SSH se caya tiene que editar el chequeo del service SSH para que se vea asi:

```
# check that ssh services are running
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
}

```

Nota que agregamos el parametro "contact_groups" - Puede hacer esto por otras entradas si quiere.

- Ahora graba el archivo y sale.
- Recargar Nagios para verificar que todo esta bien.

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

```

4.) Generar Pedidos en RT por Hosts

- Para hacer esto tiene que especificar el parametro "contact_groups tickets" por una definicion de cada host (por ejemplo un pc en pcs.cfg), o tiene que actualizar la plantilla por todo los "hosts" y cambiar la entrada de contact_groups para usar "tickets". Esto es el archivo /etc/nagios3/conf.d/generic-host_nagios2.cfg.
- 0, se puede agregar contact_groups a ping_servers en services_nagios2.cfg y, despues en hostgroups_nagios2.cfg puede agregar mas miembros al hostgroup "ping_servers". Por defecto solo tiene una entrada (gateway).
- Si lo hace esto Nagios se va a generar un pedido nuevo en RT cada vez que se caya una maquina.

5. Ver los Pedidos de Nagios en RT

- Para verificar que todo esta funcionando tiene que parar el servicio ssh en su maquina o en otra maquina:

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

```

- Si quiere hemos habilitado la maquina pc100 en grupo 3. Su direccion es 10.10.3.100. Puede agregar pc100.ws.nsrc.org (10.10.3.100) a su configuracion de Nagios y vigilar ssh por esta maquina. Si lo hace, dile al instructor para que el o ella baja ssh en la maquina - Ud. puede tambien porque tiene la misma contrasena y usuario (sysadm) que lo demas maquinas virtuales.

- Puede demorar hasta 10 minutos para que Nagios reporta que el servicio de SSH es critico. Pero, despues que se lo hace deberia aparecer un pedido nuevo en la cola

de "net" en RT.

- Para ver esto vaya a <http://pcN.ws.nsrc.org/rt/> y haz un login como "sysadm". El pedido nuevo debería aparecer en la página en la caja llamada "10 newest unowned tickets".
- El problema ahora es que no puede conectar a su máquina a través de ssh. Si cree que no está funcionando avise a su instructor y él/ella puede reinicializar ssh en su máquina virtual.