Monitorizando con Nagios

- Antonio Mario Molina Saorín
- 13 de Julio de 2011
- Talleres Caldum

Monitorización

- Concocer el estado de los recursos de un PC:
  - CPU, RAM, SWAP, HD, procesos...
- Conocer el estado de servicios:
  - Ssh, http, ftp, bbdd, dns...
- Queremos chequeos:
  - Automáticos (no podemos ir nosotros cada 5 min.)
  - Que se nos avise si pasa algo (mail, sms...)
  - Posibilidad de autocorregir el fallo¿?
- Solución-->Sistema de monitorización

Sistemas de monitorización

- Existen muchos
- La mayoría de pago (de Cisco, Avaya, HP...)
- Pero hay gratuitos. El más conocido: nagios
- Comparación entre todos:
  - `http://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems`
- Nagios permite monitorizar servicios, equipo local, equipos remotos.
- Extensible: plugins, comandos...

Instalación - Prerrequisitos

- Instalamos el servidor www:
  - `# aptitude install apache2`
- Instalamos módulo php5 para apache2
  - `# aptitude install libapache2-mod-php5`

    *(nos pedirá desinstalar apache2-mpm-worker -que es el que permite multiprocesamiento híbrido proceso-hilo- a lo que diremos que **sí**)*
- Instamos software para compilar
  - `# aptitude install build-essential`
- Instalamos librería para crear *X pixmap:*
  - `# aptitude install libgd2-xpm-dev`

Instalación – Usuarios (I)

- Creamos usuario *nagios:*
  - `# useradd -m -s /bin/bash nagios`

    o bien:
  - `# adduser nagios`

- El grupo se habrá creado, si no:
  - `# /user/sbin/groupadd nagios`
  - `# /user/sbin/usermod -G nagios nagios`

Instalación – Usuarios (y II)

- Para permitir ejecución de comandos desde la web → creamos grupo *nagcmd*.
  - `# /usr/sbin/groupadd nagcmd`
- Metemos los usuarios *nagios* y *www-data* (apache2) en dicho grupo.
  - `# /usr/sbin/usermod -a -G nagcmd nagios`
  - `# /usr/sbin/usermod -a -G nagcmd www-data`

Instalación – Nagios-core (I)

- Descargamos de www.nagios.org/download y descomprimimos el fichero *de nagios-core*
  - `cd $HOME/downloads`
  - `# tar zxvf nagios-3.2.3.tar.gz`
- Creamos makefile adecuado a nuestro PC
  - # ./configure –with-command-group=nagcmd
- Compilamos el programa
  - *`# make all`*

Instalación – Nagios-core (II)

- Instalamos los binarios, scripts, ejemplos y fichero de configuración de la web:
  - `# make install`
  - `# make install-init`
  - `# make install-config`
  - `# make install-commandmode`
  - `# make install-webconf`
- Ya tenemos nagios instalado!!...
- … pero aún nos quedan unos pasos para poder dejarlo operativo...

Instalación - Nagios-plugins

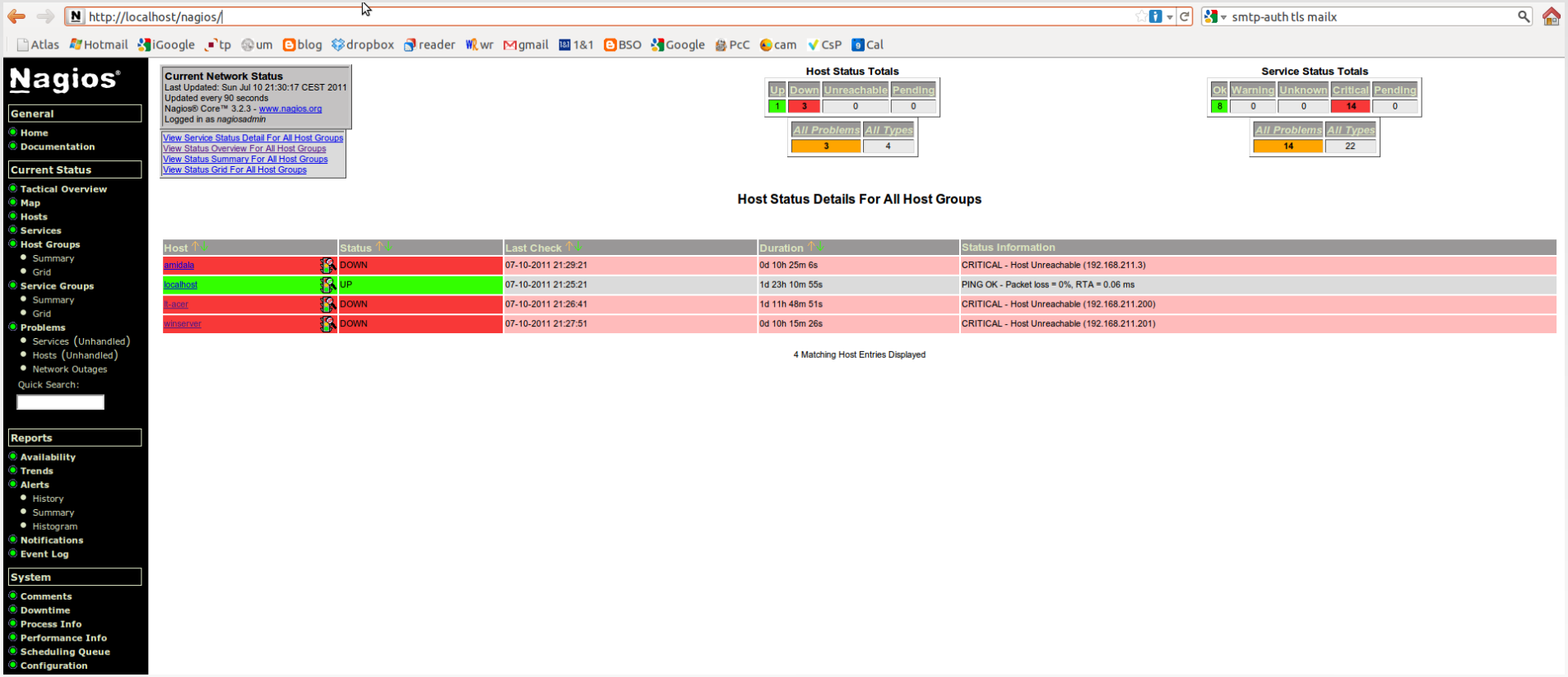
- Descargamos de www.nagios.org/download y descomprimimos los plugins de nagios
  - `cd downloads`
  - `tar zxvf nagios-plugins-1.4.11.tar.gz`
  - `cd nagios-plugins-1.4.11`
- Creamos el makefile
  - `# ./configure –with-nagios-user=nagios`
    `–with-nagios-group=nagios`
- Compilamos e instalamos
  - `# make`
  - `# make install`

Instalación – pasos finales!

- A partir de ahora nos logamos como el usuario *nagios*
- Configuramos nagios para que los mails nos los envíe a nuestra cuenta de e-mail
  - `emacs /usr/local/nagios/etc/objects/contacts.cfg`
- Creamos la cuenta *nagiosadmin* (web nagios)
  - `htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin`
- ”Recargamos” la configuración de nagios
  - `# /etc/init.d/apache2 reload`

Ya tá!

- http://localhost/nagios



Post-instalación

- Para que nagios arranque automáticamente:
  - `# ln -s /etc/init.d/nagios /etc/rcS.d/S99nagios`
- Verificar configuración de nagios
  - `/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg`
- Si no hay errores iniciamos Nagios:
  - `/etc/init.d/nagios restart`
- Ya tenemos nuestro nagios operativo!
- Ahora hay que ”decirle” que monitorice cosas ;-)

Configuración de nagios

- Como casi cualquier servicio Unix/Linux:
  - Se configura mediante ficheros de texto
  - Nagios no iba a ser menos ;-)
- En etc/nagios.cfg tenemos la configuración global de nagios
- Para este taller apenas vamos a modificarlo
- Lo importante:
  - Ficheros de configuración de objetos
- Objetos son todo: hosts, servicios, contactos...

Ficheros de configuración

- Contacts
- ContactGroups
- TimePeriods
- Hosts
- HostGroups
- Services
- ServiceGroups

Monitorización de hosts (I)

- Añadimos un fichero en *etc/objects*.
- Hay que agregar dicho fichero en *nagios.cfg,* o bien agregar un directorio (cfg_dir).
- IMPORTANTE: usamos **plantillas:**
  - Previamente creadas
  - 1 para todos!
  - Nos facilitan el trabajo
  - Sólo tenemos que cambiar nombre e IP ;-)
- Veamos un ejemplo de fichero de host

Monitorización de hosts (II)

- LOCALHOST
-
```
define host{
        use                     linux-server
        host_name               localhost
        alias                   localhost
        address                 127.0.0.1
        }
```
- GRUPO PARA LOS EQUIPOS LINUX
-
```
define hostgroup{
        hostgroup_name  linux-servers
        alias           Linux Servers
        members         localhost
        }
```

Monitorización de servicios (I)

- En un host podemos monitorizar 0, 1 ó varios servicios
- Se definen aparte del host
- Hay comandos para chequear casi muchos tipos de servicios, pero:
- ¡Podemos crear nuestros propios comandos!
- Vamos a monitorizar dos servicios: http y ssh
- En la siguiente vemos fichero de ejemplo

Monitorización de servicios (II)

```
define service{
   use                                local-service
    host_name                         localhost
    service_description               HTTP
   check_command                      check_http
   notifications_enabled              1
   }


define service{
   use                                local-service
   host_name                          localhost
   service_description                SSH
   check_command                      check_ssh
   notifications_enabled              1
    }
```

Notificaciones (I)

- Queremos que nagios nos avise:
  - Si detecta que un servicio cae
  - Si detecta que vuelve a quedar operativo
  - Si detecta un servicio en estado crítico
  - ...
- Puede avisarnos, fundamentalmente,
  - Mediante e-mail
  - Mediante SMS
- Hay otros métodos de aviso (jabber, por ej.).

Notificaciones (II)

- Vamos a configurarlo para aviso por e-mail
- Opciones hay varias. Entre otras:
  - Instalar Postfix para el envío de mails
  - Usar una MTA externa (gmail, por ejemplo)
- La primera es sencilla y útil si:
  - No queremos enviar mails fuera
- Por tanto, nos dará problemas si:
  - Queremos que nos envíe un mail a nuestro gmail
- Solución: usar MTA externo

Notificaciones (III) – Inciso: gmail

- Para enviar mail desde línea de comandos usando gmail:
  - # aptitude install heirloom-mailx
  - ```
    mailx -v -a copiaseguridad.tar.gz
    -S smtp=smtp.gmail.com:587
    -S smtp-auth-starttls
    -S smtp-auth-user=usuario@gmail.com
    -S smtp-auth-password="XXXXXXX"
    -S from=remitente@gmail.com
    destinatario@gmail.com
    ```
- Recibimos en nuestro Android las notificaciones de nagios!!!
    ```

Notificaciones (IV)

- Editamos contacts
- Colocamos nuestra dirección de e-mail:
  - Donde queremos recibir las notifiacciones
- Podemos crear un contactgroup para meter más de una dirección
- Ahora: modificamos *commands.cfg*
- /usr/bin/mailx -s "** $NOTIFICATIONTYPE$ Host Alert: $HOSTNAME$ is $HOSTSTATE$ **" -S smtp=smtp.gmail.com:587 -S smtp-use-starttls -S smtp-auth-user=USER@gmail.com -S smtp-auth-password="PASSWORD" -S smtp-auth=login -S from=USER@GMAIL.com $CONTACTEMAIL$

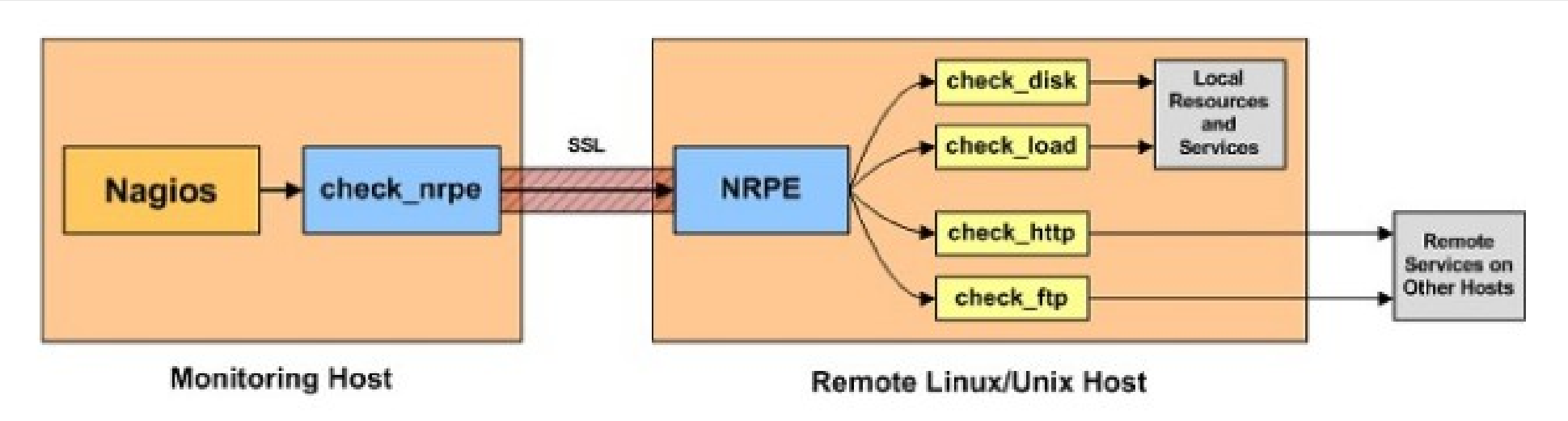
Notificaciones (V) – Ejemplo

- Subject
  - `** PROBLEM Host Alert: winserver is DOWN **`
- Cuerpo del mensaje
-
```
***** Nagios *****
Notification Type: PROBLEM
Host: winserver
State: DOWN
Address: 192.168.1.2
Info: CRITICAL - Host Unreachable
(192.168.1.2)

Date/Time: Tue Jul 12 14:34:26 CEST 2011
```

Chequeo de equipos GNU/Linux

- Usaremos NRPE
- Funcionamiento:



NRPE – Instalación cliente (I)

- Instalamos nagios-plugins
  - `tar zxvf nagios-plugins-1.4.15.tar.gz`
  - `./configure ; make ; make install`
  - `chown nagios.nagios /usr/local/nagios`
  - `chown -R nagios.nagios /usr/local/nagios/libexec`
- Instalamos tcp wrapper: xinetd
  - `# aptitude install xinetd`
- Instalamos nrpe:
  - `# aptitude install libssl-dev`
  - `tar zxvf nrpe-2.12.tar.gz`
  - `./configure ; make all ; make install-plugin ;  make install-daemon; make install-daemon-config; make install-xinetd`

NRPE – Instalación cliente (II)

- Ahora añadimos la IP del servidor nagios:
  - `only-from = 127.0.0.1 192.168.1.15`
- Reiniciamos xinetd:
  - `service xinetd restart`
- Chequeo de que está ok:
  - `netstat -at | grep nrpe`
  - `/usr/local/nagios/libexec/check_nrpe -H localhost`
- Si tuviéramos firewall:
  - `iptables -I INPUT -p tcp -m tcp –dport 5666 -j ACCEPT`

NRPE – Comandos

- Nrpe viene con ciertos comandos instalados por defecto, pero podemos añadir más
- Basta editar /usr/local/nagios/etc/nrpe.cfg

- Ahora veremos la instalación en el servidor, es decir, en el PC donde tenemos nagios

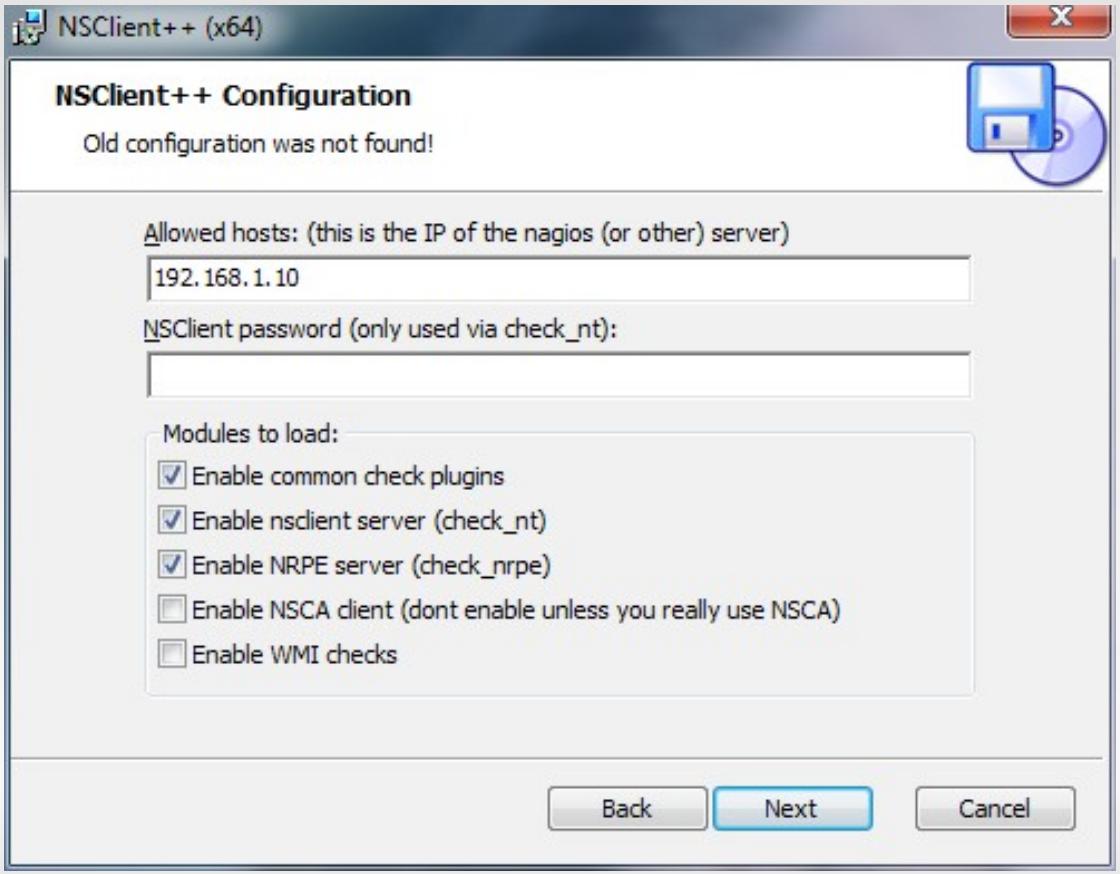
NRPE – Instalación servidor

- Instalación de nrpe:
  - `# aptitude install libssl-dev`
  - `tar zxvf  nrpe-2.12.tar.gz`
  - `./configure ; make install ; make install-plugin`
- No hay que instalar el demonio (lógico ;-))
- Chequeo de si llegamos al pc a monitorizar:
  - `/usr/local/nagios/libexec/check_nrpe -H IP`
- Creamos el comando (en commands.cfg):

```
define command{
        command_name check_nrpe
        command_line $USER1$/check_nrpe -H
                     $HOSTADDRESS$ -c $ARG1$
        }
```

Monitorizando Pcs con windows

- Para este cometido usaremos NSClient++
- La instalación es sencilla. A tener en cuén:



Monitorizando Pcs con windows

- Sólo falta configurar comandos para chequear los equipos windows en nagios
- Ventaja: vienen ya por defecto
- Por tanto, sólo tenemos que cambiar IP del equipo *winserver*
- Si queremos añadir más equipos ya sabemos cómo hacerlo.
- El comando a usar es *check_nt*

Nagios - Tips

- Usar plantillas!!
- Usar hostgroups y servicegroups
- Ej.

```
define service{
hostgroup_name          HOSTGROUP1,HOSTGROUP2,...
service_description     SOMESERVICE
other service directives …
}
```

- Mirar la documenatción de nagios:
  - `http://nagios.sourceforge.net/docs/nagioscore/3/en/`

Más allá: Event Handler (I)

- Ejecucion de acciones con nagios
- Nagios permite que ejecutar acciones ante alarmas
- -> Solucionamos automáticamente el problema
- Event handler:
  - se ejecuta cuando host/servicio
  - cambia de stado
- Ej.: Detectamos servicio cae
- -> Event handler puede dejarlo operativo

Event Handler (II)

- Se ejecuta cuando un host / servicio:
  - Está en estado SOFT
  - Está en estado HARD
  - Se recupera de un estado SOFT o HARD
- Es un simple script (bash, python...)
- Tiene que tener unos parámetros:
  - $SERVICESTATE$, $STATETYPE$, $SERVICETTEMPT$
  - $HOSTSTATE$, $STATETYPE$, $HOSTATTEMPT$
- Más info:
  - Http://infodocs.net/articulo/nagios/event-handlers-en-nagios

Otras posibilidades

- Icinga.
  - Fork de nagios
  - OpenSource
  - Totalmente compatible con los archivos de configuración de nagios
  - Más completo (nagios avanza muy lentamente)
  - Interfaz web más estético
- OpenNMS.
  - Sistema de monitorización de nivel empresarial
  - OpenSource
  - http://www.rootdev.com/tech/opennms-vs-nagios

Antes de finalizar

- Licenciado bajo Creative Commons
- Reconocimiento - No Comercial - Compartir igual
- Puedes:
  - Copiar, reproducir, mostrar públicamente y modificarlo, siempre y cuando cites al autor (o sea, yo),
  - no lo uses para fines comerciales,
  - y las obras derivadas se mantengan bajo esta misma licencia.

Preguntas

Gracias por vuestra atención