Nagios

Claudia Inostroza
Cinostro@reuna.cl
Albert Astudillo
aastudillo@reuna.cl

Managua 05 y 06 de Diciembre de 2011

Agenda

- Introducción
- Instalación
- Mecánica de chequeos.
- Equipo/dispositivo Padre
- Archivos de configuración

Introducción

- Herramientas de Monitoreo de Redes
  - Disponibilidad
  - Confiabilidad
  - Rendimiento
- Nagios activamente monitorea la disponibilidad de dispositivos y servicios
- Posiblemente sea el software de fuente abierto mas usado para gestión y monitoreo de redes
- Tiene un interfaz de web
  - Usa CGIs escrito en C para responder mas rápido y apoyar crecimiento
- Soporta hasta miles de dispositivos y servicios.

Instalación

- En Debian/Ubuntu

  # apt-get install nagios3

- Directorios importantes
  - /etc/nagios3
  - /etc/nagios3/conf.d
  - /etc/nagios-plugins/conf
  - /usr/lib/nagios/plugins
  - /usr/share/nagios3/htdocs/images/logos

Plugins

- Los Plugins se utilizan para verificar servicios y dispositivos/equipos específicos:
  - La arquitectura de Nagios es bastante simple, lo cual permite que escribir plugins sea relativamente fácil.
  - Se puede realizar en el lenguaje de su elección.

- Hay muchos plugins disponibles
  - http://exchange.nagios.org/
  - http://nagiosplugins.org/

Configuración

- Está hecha en archivos de texto basado en planillas.
- Nagios lee su configuración de un directorio
- Ud. decide cómo dividir los archivos de configuración en ese directorio.
- Usa chequeos en paralelo y bifurcación (forking) por escalabilidad.
- **Utiliza información topológica para determinar dependencias**
- **Diferenciación entre lo que está 'caído' y lo que está 'inalcanzable'**
- **Así no se tratar de hacer chequeos de las máquínas no 'inalcanzable'**

Configuración

- Permite definir políticas de notificación, basadas en combinaciones de:
  - Contactos y listas de contactos
  - Dispositivos y grupos de dispositivos
  - Servicios y grupos de servicios.
  - Horarios definidos por grupos o personas.
  - El estado de los servicios:

Opciones de notificación

- Estado de Servicio:
- Cuando se configura un servicio tiene los siguiente opciones:

  d: DOWN: El servicio esta caído (no disponible)

  u: UNREACHABLE: Dispositivo no esta visible

  r: RECOVERY: (OK) Dispositivo se esta recuperando

  f: FLAPPING: La primera vez con un dispositivo sube, bajo o esta en un estado indeterminado

  n: NONE: No manda ningún notificación

Mecánica de Chequeos

- Un nodo o dispositivo (host) consta de uno o más servicios a chequear (PING, HTTP, MYSQL, SSH, etc)
- Nagios chequea periódicamente cada servicio de cada nodo y determina si ha habido algún cambio de estado:
  - CRITICAL
  - WARNING
  - UNKNOWN
- A cada cambio de estado, se le puede asignar:
  - Opciones de notificación (como vimos antes)
  - Operaciones de manejo de eventos (event handlers)

Mecánica de Chequeos

- Parámetros
  - Intervalo de chequeo normal
  - Intervalo de re-chequeo
  - Número máximo de chequeos
  - Período de chequeo
- Los chequeos de nodo (host) sólo se ejecutan cuando ninguno de los servicios responde
  - Un nodo (host) puede estar:
    - DOWN
    - UNREACHABLE
- Por defecto Nagios hace un chequeo de nodo 3 veces antes de cambiar el estado de un nodo a down.
- El estado de no respuesta va de warning a critical

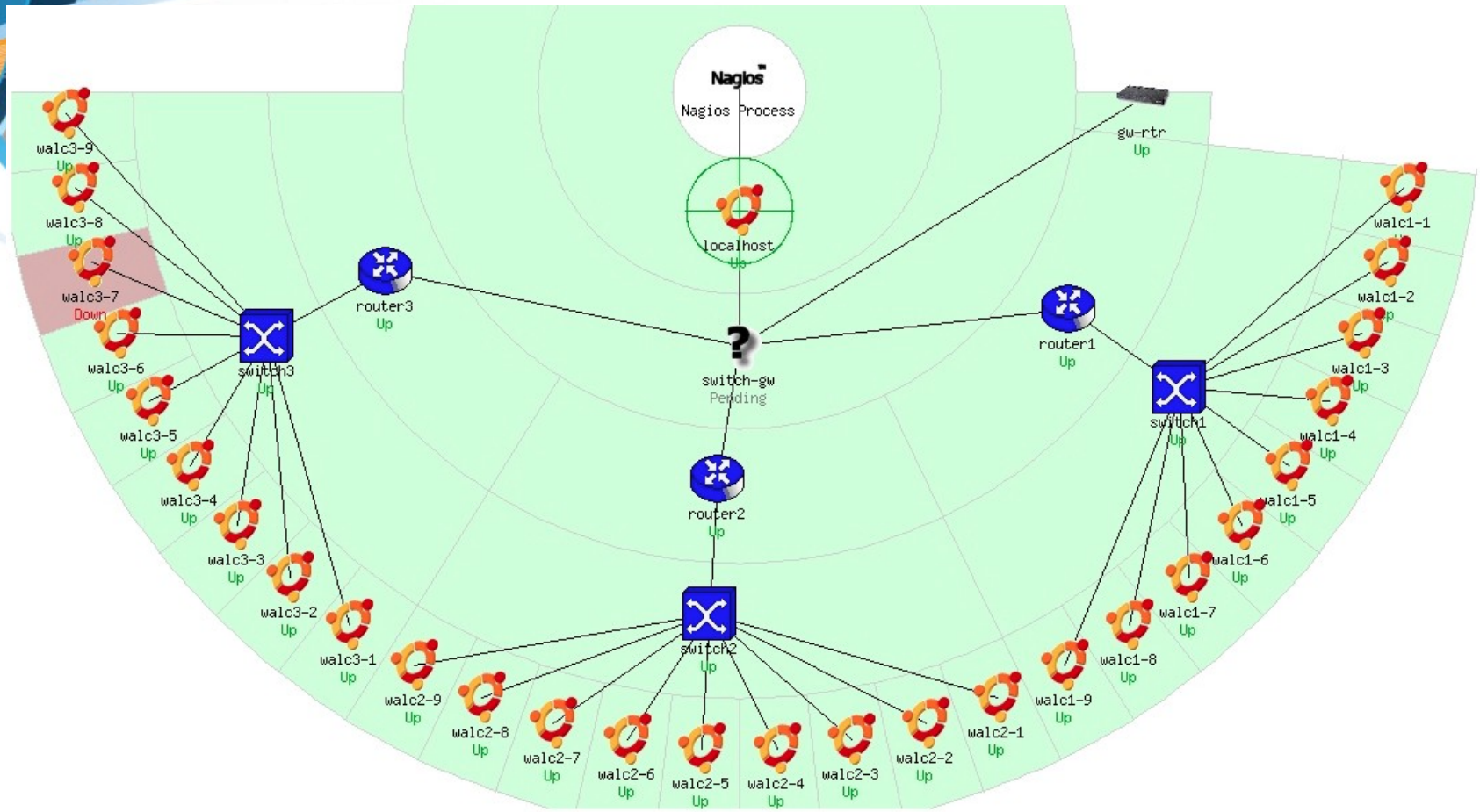
Concepto de “padre”

- El padre de un PC conectado a un switch seria el switch.
- Nos permite especificar las dependencias entre dispositivos (PCs, switches, enrutadores)
- Evita mandar múltiples alarmas cuando el padre no responde.
- Es un sistema jerárquico.
- Un nodo puede tener múltiple padres (dual homes).

Punto de vista de la red

- Donde pones Nagios va a determinar su punto de vista de la red.
- El servidor de Nagios se pone como el “raíz” de su árbol de dependencias.

Punto de vista de la red



Demostración

- Archivos de Configuración
  - Muchos! Parece complejo al principio
- Orientada a objetos.
- Objetos (dispositivos o servicios) heredan los atributos.
- Permite aplicar funcionalidad a grupos de dispositivos o servicios.
- No aplica funcionalidad a objetos individuales.
- No se escala!
- Después que entiende los archivos de configuración de Nagios el resto es fácil.

Archivos de Configuración

- Ubicados en /etc/nagios3/
- Archivos importantes incluyen:
- cgi.cfg — Controla el interfaz de Web y los opciones de seguridad.
- commands.cfg — Los comandos que usa Nagios para notificaciones.
- nagios.cfg — El archive principal de configuración
- conf.d/* — El resto de los archivos de configuración por servicios, grupos, nodos, etc.

Archivo de Configuración

- Bajo conf.d/*
- contacts_nagios2.cfg Usuarios y grupos
- extinfo_nagios2.cfg Mejora la UI
- generic-host_nagios2.cfg Plantilla de host por defecto
- generic-service_nagios2.cfg Plantilla de servicio p/defecto
- host-gateway_nagios3.cfg Definición enlace de puerto
- hostgroups_nagios2.cfg Agrupacion de nodos
- localhost_nagios2.cfg Definición de localhost
- services_nagios2.cfg Que servicios a chequear
- timeperiods_nagios2.cfg Cuando hacer chequeo

Quien a notificar

Archivo de Configuración

- Bajo /etc/nagios3/conf.d puede hacer (por ejemplo):

- servicegroups.cfg Agrupación de servicios y nodos
- pcs.cfg Definición de los PCs en su red
- switches.cfg Definición de los switches
- routers.cfg Definición de los enrutadores

- PCs, switches y enrutadores son (hosts). Se defina servicios a monitorear por los hosts (si quieres).

Basado en Plantillas

•Ahorra tiempo evitando repetición

•Nagios viene con una plantilla por defecto con parámetros por un:

- Nodo genérico (generic-host_nagios2.cfg)
- Servicio genérico (generic-service_nagios2.cfg)
- Contacto genérico (contacts_nagios2.cfg)

Plantilla de nodo genérico

generic-host_nagios2.cfg

```
define host{
        name                            generic-host    ; The name of this host template
        notifications_enabled           1               ; Host notifications are enabled
        event_handler_enabled           1               ; Host event handler is enabled
        flap_detection_enabled          1               ; Flap detection is enabled
        failure_prediction_enabled      1               ; Failure prediction is enabled
        process_perf_data               1               ; Process performance data
        retain_status_information       1               ; Retain status information across program restarts
        retain_nonstatus_information    1               ; Retain non-status information across program restarts
                check_command                   check-host-alive
                max_check_attempts              10
                notification_interval           0
                notification_period             24x7
                notification_options            d,u,r
                contact_groups                  admins
        register                        0       ; DONT REGISTER THIS DEFINITION - ITS NOT A REAL HOST, JUST A TEMPLATE!
        }
```

Configuración de un nodo individual

```
define host{
        use                     generic-host
        host_name               gw-rtr
        alias                   Enrutador principal de taller
        address                 10.10.0.254
        contact_groups          router_group
}
```

Plantilla de servicio generico

generic-service_nagios2.cfg

```
define service{
        name                            generic-service
        active_checks_enabled           1
        passive_checks_enabled          1
        parallelize_check               1
        obsess_over_service             0
        check_freshness                 1
        notifications_enabled           1
        event_handler_enabled           1
        flap_detection_enabled          1
        process_perf_data               1
        retain_status_information       1
        retain_nonstatus_information    1
        is_volatile                     0
        check_period                    24x7
        max_check_attempts              5
        normal_check_interval           5
        retry_check_interval            1
        notification_interval           60
        notification_period             24x7
        notification_options            c,r
        register                        0
        }
```

Configuración de un servicio individual

```
define service{
        hostgroup_name                  servers
        service_description             PING
        check_command                   check-host-alive
        use                             generic-service
        max_check_attempts              5
        normal_check_interval           5
        notification_options            c,r,f
        notification_interval           0 ; set > 0 if you want to be renotified
}
```

c: Critico
r: Recuperando
f: Aleteo (Flapping)

Flujo de configuración

RTR

```
define host {
   use                  generic-host
   host_name            rtr
   alias                Enrutador GW
   address              10.10.0.254 }
```

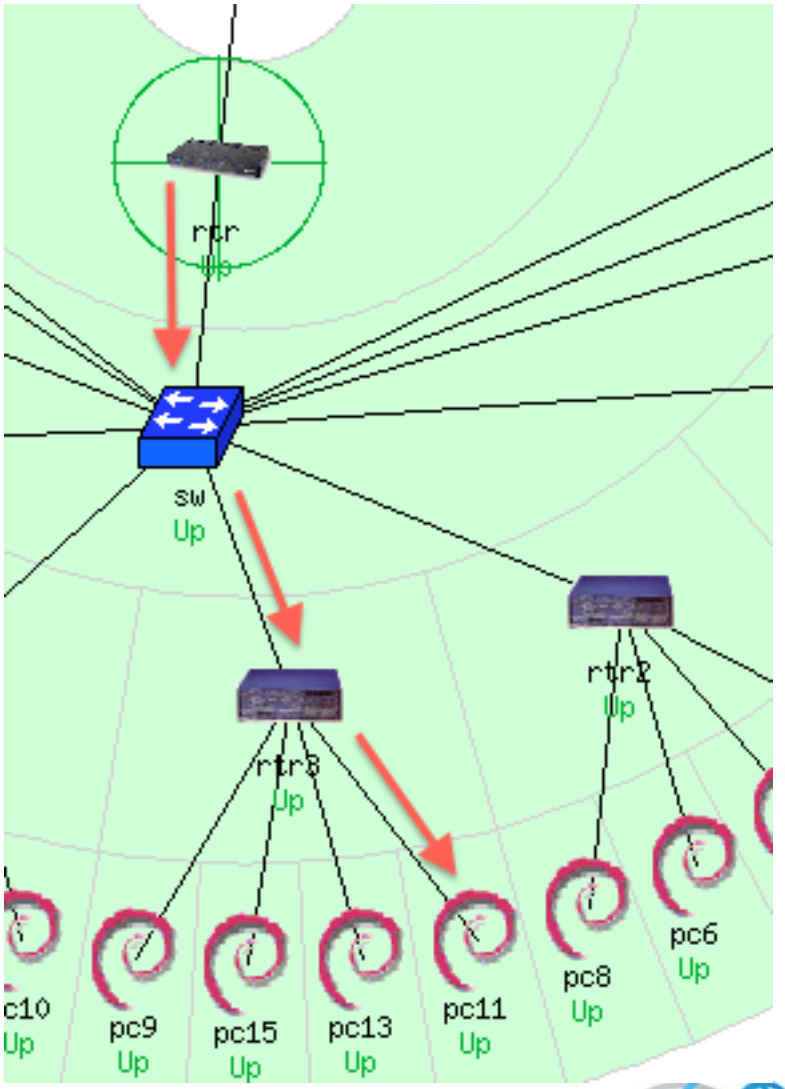
SW

```
define host {
   use                  generic-host
   host_name            sw
   alias                Switch Dorsal
   address              10.10.0.253
   parents              rtr }
```

RTR3

```
define host {
   use                  generic-host
   host_name            rtr3
   alias                router 3
   address              10.10.3.254
   parents              sw }
```

PC11…



Notificaciones vía SMS

- Es importante recordar un sistema de mensaje de texto o mensajes que sea independiente de su red.
- Puede utilizar un celular conectado a su servidor de Nagios
- Puede usar software como:
  - Gnokii: http://www.gnokii.org/
  - Qpage: http://www.qpage.org/
  - Sendpage:http://www.sendpage.org/

Referencias

- Sitio de web Nagios
  http://www.nagios.org/
- Sitio de web de Plugins por Nagios
  http://www.nagiosplugins.org/
- Nagios System and Network Monitoring, por Wolfgang Barth. Un buen libro sobre Nagios.
- Sitio no oficial de Plugins por Nagios
  http://nagios.exchange.org/
- Una enseñanza de Debian sobre Nagios
  http://www.debianhelp.co.uk/nagios.htm
- Aporte Comercial por Nagios
  http://www.nagios.com/

Consultas?