



Gestión de Redes

The word "NAGIOS" is displayed in a large, bold, white, sans-serif font. It is centered within a semi-transparent dark grey rectangular box. The background of the slide features a pattern of binary code (0s and 1s) in a light red color, which is visible through the semi-transparent box and across the entire slide.



These materials are licensed under the Creative Commons *Attribution-Noncommercial 3.0 Unported* license
(<http://creativecommons.org/licenses/by-nc/3.0/>)

Introducción

Herramientas de Gestión de Redes

- Disponibilidad
- Fiabilidad
- Desempeño

*Nagios monitoriza activamente la
disponibilidad de nodos y servicios*

Introducción

- Probablemente el software libre de monitorización más utilizado
- Interfaz web para visualizar el estado, revisar la historia de eventos, planificar bajas por mantenimiento
- Envía alarmas por e-mail. Puede configurarse para usar otros mecanismos (ej. SMS)

Ejemplo: Detalle de Servicios

Nagios®

General

- Home
- Documentation

Monitoring

- Tactical Overview
- Service Detail**
- Host Detail
- Hostgroup Overview
- Hostgroup Summary
- Hostgroup Grid
- Servicegroup Overview
- Servicegroup Summary
- Servicegroup Grid
- Status Map
- 3-D Status Map

Service Problems

- Unhandled
- Host Problems
- Unhandled

Network Outages

Show Host:

Comments

- Downtime

Process Info

- Performance Info
- Scheduling Queue

Reporting

- Trends
- Availability
- Alert Histogram
- Alert History
- Alert Summary
- Notifications
- Event Log

Configuration

- View Config

Current Network Status

Last Updated: Thu Sep 3 14:46:07 CDT 2009
Updated every 90 seconds
Nagios® 3.0.2 - www.nagios.org
Logged in as guest

[View History For all hosts](#)
[View Notifications For All Hosts](#)
[View Host Status Detail For All Hosts](#)

Host Status Totals

Up	Down	Unreachable	Pending
41	0	0	0

All Problems	All Types
0	41

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
46	0	0	0	0

All Problems	All Types
0	46

Service Status Details For All Hosts

Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
DNS-ROOT	SSH	OK	2009-09-03 14:43:51	43d 0h 55m 19s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
ISP-DNS	SSH	OK	2009-09-03 14:41:21	16d 3h 57m 24s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
ISP-RTR	SSH	OK	2009-09-03 14:43:57	43d 5h 35m 13s	1/4	SSH OK - Cisco-1.25 (protocol 2.0)
NOC-TLD1	SSH	OK	2009-09-03 14:41:27	1d 0h 1m 59s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NOC-TLD2	SSH	OK	2009-09-03 14:44:04	1d 22h 44m 22s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NOC-TLD3	SSH	OK	2009-09-03 14:41:34	1d 22h 40m 58s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NOC-TLD4	SSH	OK	2009-09-03 14:44:10	1d 22h 44m 16s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NOC-TLD5	SSH	OK	2009-09-03 14:41:40	1d 22h 41m 46s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NOC-TLD6	SSH	OK	2009-09-03 14:44:17	1d 22h 44m 9s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NOC-TLD7	SSH	OK	2009-09-03 14:41:47	1d 22h 41m 39s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NOC-TLD8	SSH	OK	2009-09-03 14:44:23	1d 22h 44m 3s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NS1-TLD1	SSH	OK	2009-09-03 14:41:53	1d 0h 1m 33s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NS1-TLD2	SSH	OK	2009-09-03 14:44:30	1d 22h 43m 56s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NS1-TLD3	SSH	OK	2009-09-03 14:42:00	1d 22h 41m 26s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NS1-TLD4	SSH	OK	2009-09-03 14:44:36	1d 22h 43m 50s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NS1-TLD5	SSH	OK	2009-09-03 14:42:06	1d 22h 41m 20s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)
NS1-TLD6	SSH	OK	2009-09-03 14:44:42	1d 22h 43m 42s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)

Funcionalidades

Utiliza información topológica para determinar las dependencias.

- Diferencia entre lo que está *caído* vs. lo que está *inalcanzable*. Evita hacer comprobaciones y enviar alarmas innecesarias

Permite definir cómo enviar alarmas basado en una combinación de:

- Contactos y listas de contactos
- Dispositivos y sus grupos
- Servicios y sus grupos
- Horarios por personas y grupos.
- El estado de un servicio.

Plugins

Los plugins se usan par verificar servicios y nodos:

- La arquitectura de Nagios hace suficientemente simple el escribir nuevos plugins en el lenguaje de su preferencia.
- Existen ***muchos, muchos*** plugins disponibles (miles).
 - ✓ <http://exchange.nagios.org/>
 - ✓ <http://nagiosplugins.org/>



Plugins pre-instalados en Ubuntu

/usr/lib/nagios/plugins

check_apt	check_file_age	check_jabber	check_nttp	check_procs	check_swap
check_bgstate	check_flexlm	check_ldap	check_nttps	check_radius	check_tcp
check_breeze	check_ftp	check_ldaps	check_nt	check_real	check_time
check_by_ssh	check_host	check_linux_raid	check_ntp	check_rpc	check_udp
check_cload	check_hppjd	check_load	check_ntp_peer	check_rta_multi	check_ups
check_cluster	check_http	check_log	check_ntp_time	check_sensors	check_users
check_dhcp	check_icmp	check_mailq	check_nwstat	check_simap	check_wave
check_dig	check_ide_smart	check_mrtg	check_oracle	check_smtp	negate
check_disk	check_ifoperstatus	check_mrtgtraf	check_overcr	check_snmp	urlize
check_disk_smb	check_ifstatus	check_mysql	check_pgsql	check_spop	utils.pm
check_dns	check_imap	check_mysql_query	check_ping	check_ssh	utils.sh
check_dummy	check_ircd	check_nagios	check_pop	check_ssmtp	

/etc/nagios-plugins/config

apt.cfg	dns.cfg	games.cfg	load.cfg	netware.cfg	ping.cfg	snmp.cfg
breeze.cfg	dummy.cfg	hppjd.cfg	mail.cfg	news.cfg	procs.cfg	ssh.cfg
dhcp.cfg	flexlm.cfg	http.cfg	mailq.cfg	nt.cfg	radius.cfg	tcp_udp.cfg
disk.cfg	fping.cfg	ifstatus.cfg	mrtg.cfg	ntp.cfg	real.cfg	telnet.cfg
disk-smb.cfg	ftp.cfg	ldap.cfg	mysql.cfg	pgsql.cfg	rpc-nfs.cfg	users.cfg

Cómo funcionan los plugins

- Periódicamente Nagios ejecuta un plugin para verificar el estado de cada servicio. Las posibles respuestas son:
 - OK
 - WARNING
 - CRITICAL
 - UNKNOWN
- Si un servicio no está OK, entra en un estado de error “soft”. Después de un número de reintentos (4), entra en un estado de error “hard”. En este momento se envía una alarma.
- Es posible también activar manejadores de eventos (event handlers) externos basándose en transiciones de estados

Cómo funcionan los plugins

Parámetros

- Intervalo de chequeo normal
- Intervalo de reintento (i.e. cuando no es OK)
- Número máximo de reintentos
- Ventana de ejecución de los chequeos
- Ventana para el envío de las alarmas

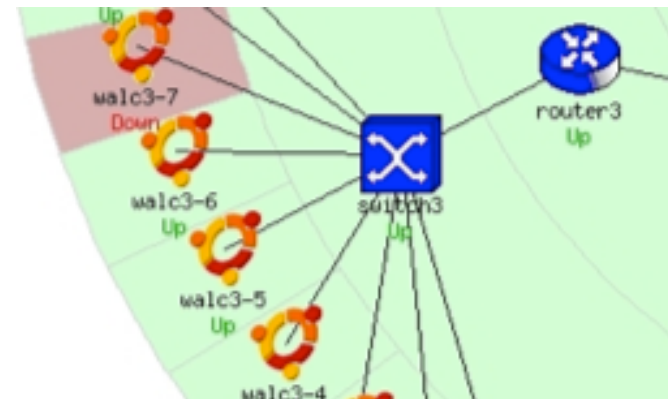
Programación de tareas

- Nagios distribuye sus chequeos a lo largo del intervalo para balancear la carga
- La interfaz web muestra la hora del próximo chequeo

Las relaciones padre-hijo

Los nodos pueden tener “padres”

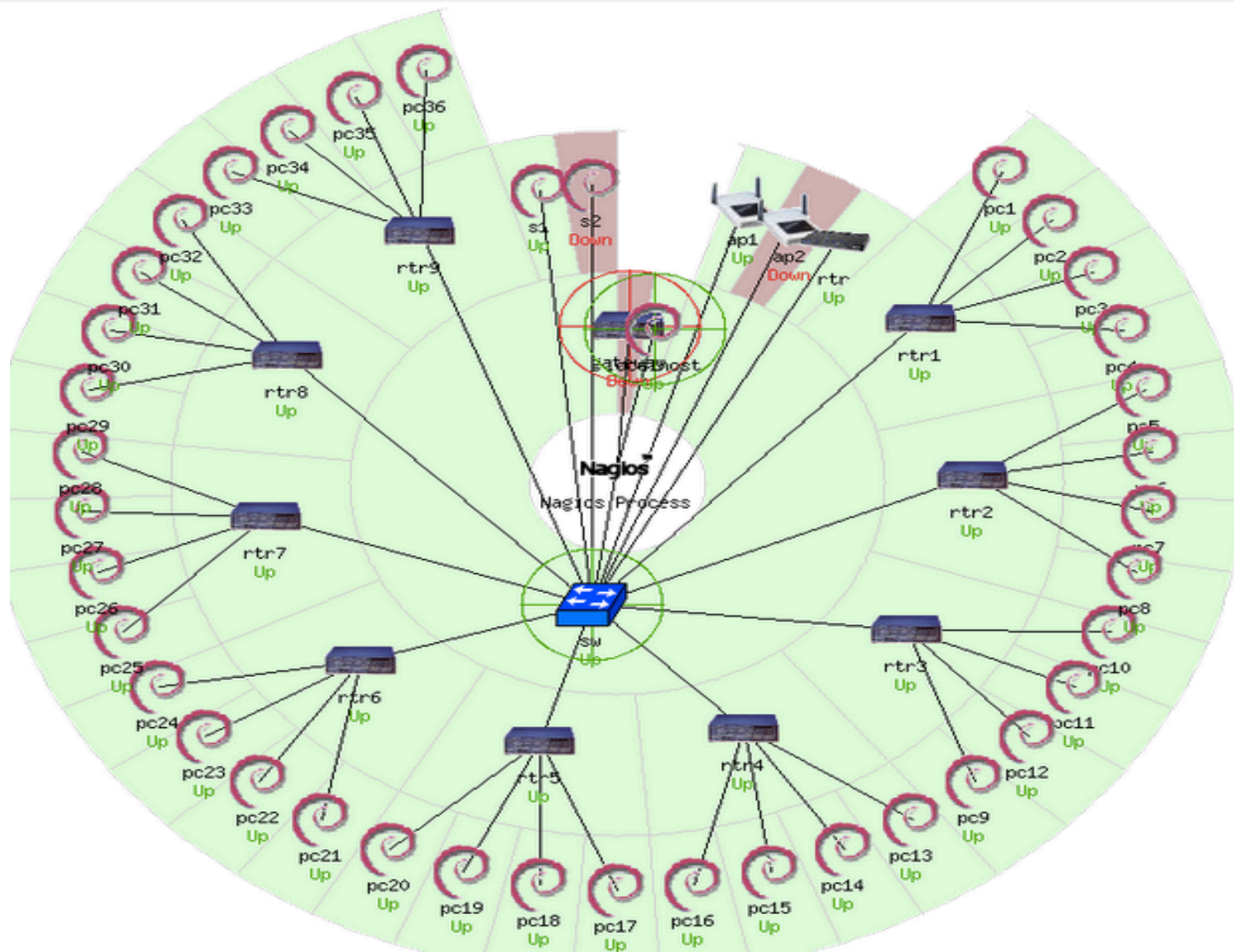
- El padre de un PC conectado a un **switch**, sería el **switch**
- Nos permite especificar las dependencias entre nodos
- Evita enviar alarmas cuando los padres no responden.
- Un nodo puede tener múltiples padres.



Punto de referencia

- La ubicación del servidor de Nagios determina el punto de referencia de la red.
- El servidor Nagios se convierte en el nodo “raíz” de su estructura de árbol jerárquico

Punto de referencia



Demostración de Nagios

Instalación

En Debian/Ubuntu

```
# apt-get install nagios3
```

Directorios clave

```
/etc/nagios3
```

```
/etc/nagios3/conf.d
```

```
/etc/nagios-plugins/config
```

```
/usr/lib/nagios/plugins
```

```
/usr/share/nagios3/htdocs/images/logos
```

La interfaz web de Nagios está en:

<http://pcN.ws.nsrc.org/nagios3/>

Configuración

- Se define en archivos de texto
 - `/etc/nagios3/conf.d/*.cfg`
 - Detalles en http://nagios.sourceforge.net/docs/3_0/objectdefinitions.html
- La configuración por defecto se distribuye entre varios archivos por tipo de objeto, pero en realidad se pueden organizar a su gusto
- Siempre verifique antes de reiniciar Nagios, de lo contrario su sistema se caerá!
 - `nagios3 -v /etc/nagios3/nagios.cfg`

Configuración de nodos y servicios

Basado en plantillas

- Esto ahorra mucho tiempo ya que evita la repetición

Hay plantillas por defecto con parámetros por defecto para:

- *Nodo genérico* (generic-host_nagios2.cfg)
- *Servicio genérico* (generic-service_nagios2.cfg)
- Los parámetros individuales se pueden sobreponer
- Los valores por defecto son razonables

Monitorizar un nodo

pcs.cfg

```
define host {  
    host_name pc1  
    alias      pc1 in group 1  
    address    pc1.ws.nsrc.org  
    use        generic-host  
}
```

Heredar parámetros de esta plantilla

- Ésta es una configuración mínima
 - Simplemente está haciendo ping al nodo; Nagios le advertirá que no está monitorizando ningún servicio
- El archivo puede nombrarse cualquier cosa terminando en **.cfg** (nagios.cfg)
- Organice sus nodos como le convenga, por ejemplo, nodos relacionados en el mismo archivo

Plantilla genérica de nodo

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 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 ; DON'T REGISTER THIS DEFINITION —
                           ; IT'S NOT A REAL HOST, JUST A TEMPLATE!
}
```

Sobreponiendo valores por defecto

Los valores heredados se pueden sobreponer en el nodo

pcs.cfg

```
define host {  
    host_name          pc1  
    alias              pc1 in group 1  
    address            pc1.ws.nsrc.org  
    use                generic-host  
    notification_interval 120  
    contact_groups      admins,managers  
}
```

Definición de servicios (modo directo)

pcs.cfg

```
define host {
    host_name      pc1
    alias          pc1 in group 1
    address        pc1.ws.nsrc.org
    use            generic-host
}

define service {
    host_name      pc1
    service_description HTTP
    check_command  check_http
    use            generic-service
}

define service {
    host_name      pc1
    service_description SSH
    check_command  check_ssh
    use            generic-service
}
```

service "pc1,HTTP"

plugin

Plantilla de
servicio

Comprobaciones de servicio

- La combinación de nodo+servicio es un identificador único para el chequeo, ej:
 - “pc1,HTTP”
 - “pc1,SSH”
 - “pc2,HTTP”
 - “pc2,SSH”
- *check_command* hace referencia al plugin
- *service template* causa que se hereden los parámetros acerca de qué tan frecuentemente comprobar, y a quién y cuándo enviar las alarmas

Plantilla genérica de servicio

generic-service_nagios2.cfg*

```
define service{
    name                                generic-service
    active_checks_enabled               1
    passive_checks_enabled              1
    parallelize_check                   1
    obsess_over_service                 1
    check_freshness                     0
    notifications_enabled               1
    event_handler_enabled               1
    flap_detection_enabled              1
    failure_prediction_enabled          1
    process_perf_data                  1
    retain_status_information            1
    retain_nonstatus_information        1
    notification_interval               0
    is_volatile                         0
    check_period                        24x7
    normal_check_interval               5
    retry_check_interval                1
    max_check_attempts                  4
    notification_period                 24x7
    notification_options                w,u,c,r
    contact_groups                      admins
    register                            0    ; DONT REGISTER THIS DEFINITION
}
```

* Comentarios eliminados

Sobreponiendo valores por defecto

De nuevo, los valores por defecto se pueden sobreponer

services_nagios2.cfg

```
define service {  
    host_name                pc1  
    service_description      HTTP  
    check_command             check_http  
    use                       generic-service  
    contact_groups           admins,managers  
    max_check_attempts      3  
}
```

Chequeos de servicio repetidos

- Frecuentemente monitorizamos el mismo servicio en múltiples nodos
- Para evitar la duplicación, es más conveniente definir un *service check* para todos los nodos en un *hostgroup*

Crear grupos de nodos (hostgroups)

hostgroups_nagios2.cfg

```
define hostgroup {  
    hostgroup_name    http-servers  
    alias             HTTP servers  
    members          pc1,pc2  
}  
  
define hostgroup {  
    hostgroup_name    ssh-servers  
    alias             SSH servers  
    members          pc1,pc2  
}
```

Monitorizando servicios en hostgroups

services_nagios2.cfg

```
define service {
    hostgroup_name      http-servers
    service_description  HTTP
    check_command        check_http
    use                  generic-service
}

define service {
    hostgroup_name      ssh-servers
    service_description  SSH
    check_command        check_ssh
    use                  generic-service
}
```

Ej. si el hostgroup “http-servers” contiene a pc1 y pc2 entonces Nagios crea chequeos de HTTP para cada nodo. Los chequeos de servicio se llaman “pc1,HTTP” y “pc2,HTTP”

Vista alternativa

- En lugar de decir “este *hostgroup* contiene a estas PCs” puede decir “esta PC pertenece a estos *hostgroups*”
- No es necesaria la sección “members” en el archivo de hostgroups

Membresía de grupo alternativa

pcs.cfg

```
define host {
    host_name      pc1
    alias          pc1 in group 1
    address        pc1.ws.nsrc.org
    use            generic-host
    hostgroups    ssh-servers,http-servers
}

define host {
    host_name      pc2
    alias          pc2 in group 1
    address        pc2.ws.nsrc.org
    use            generic-host
    hostgroups    ssh-servers,http-servers
}
```

Nodos y servicios definidos en el mismo sitio (más conveniente)

Otros usos de los hostgroups

Elegir iconos para el mapa de estado

pcs.cfg

```
define host {
    host_name      pc1
    alias          pc1 in group 1
    address        pc1.ws.nsrc.org
    use            generic-host
    hostgroups     ssh-servers,http-servers,debian-servers
}
```

extinfo_nagios2.cfg

```
define hostextinfo {
    hostgroup_name    debian-servers
    notes            Debian GNU/Linux servers
    icon_image       base/debian.png
    statusmap_image  base/debian.gd2
}
```

Opcional: servicegroups

- También puede agrupar los servicios usando un “servicegroup”
- De manera que los servicios relacionados o dependientes se puedan ver juntos en la interfaz web
- Los servicios deben estar definidos

servicegroups.cfg

```
define servicegroup {  
    servicegroup_name    mail-services  
    alias                Services comprising the mail platform  
    members              web1,HTTP,web2,HTTP,mail1,IMAP,db1,MYSQL  
}
```

Configurar la topología

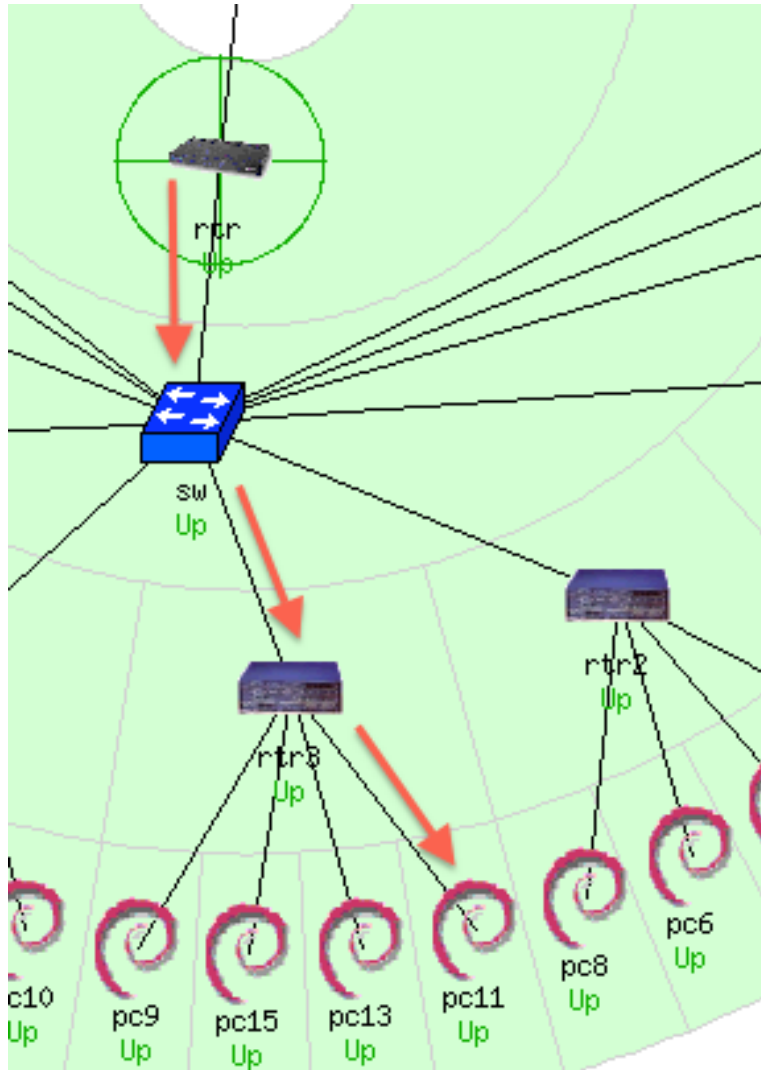
pcs.cfg

```
define host {  
    host_name      pc1  
    alias          pc1 in group 1  
    address        pc1.ws.nsrc.org  
    use            generic-host  
    parents       rtr1 ←  
}
```

Nodo padre

- Esto significa “pc1 está del otro lado de rtr1”
- Si rtr1 cae, pc1 se marca como “unreachable” en lugar de “down”
- Evita una cascada de alarmas si cae rtr1
- También permite a Nagios dibujar el mapa

Otra vista de la configuración



RTR

```
define host {  
  use  
  host_name  
  alias  
  address
```

```
generic-host  
rtr  
Gateway Router  
10.10.0.254 }
```

SW

```
define host {  
  use  
  host_name  
  alias  
  address  
  parents
```

```
generic-host  
sw  
Backbone Switch  
10.10.0.253  
rtr }
```

RTR3

```
define host {  
  use  
  host_name  
  alias  
  address  
  parents
```

```
generic-host  
rtr3  
router 3  
10.10.3.254  
sw }
```

PC11...

Notificaciones fuera de línea (out of band)

Una cosa crítica que recordar: un sistema de mensaje que no dependa de su red

- Puede usar un teléfono celular conectado al servidor Nagios, o un dispositivo USB con tarjeta SIM

- Puede usar herramientas como:

gammu: <http://wammu.eu/>

gnokii: <http://www.gnokii.org/>

sms-tools: <http://smstools3.kekekasvi.com/>

Referencias

- **Sitio web de Nagios**
<http://www.nagios.org/>
- **Plugins**
<http://www.nagiosplugins.org/>
- *Nagios System and Network Monitoring*, por Wolfgang Barth. Muy bueno.
- **Sitio web de plugins (no-oficial)**
<http://nagios.exchange.org/>
- **Un tutorial de Nagios por Debian**
<http://www.debianhelp.co.uk/nagios.htm>
- **Consultoría de Nagios comercial**
<http://www.nagios.com/>

Preguntas?

?