



Nagios®

Introducción

- Herramienta principalmente de monitorización activa de disponibilidad
- Posiblemente la más utilizada en la categoría de software libre
- Interfaz Web
 - CGI's escritos en C para mayor velocidad
- Soporta miles de nodos/servicios

Instalación

En Debian/Ubuntu:

- `# apt-get install nagios3`
- Archivos estan instalados aquí:
 - `/etc/nagios3`
 - `/etc/nagios3/conf.d`
 - `/etc/nagios-plugins/conf`
 - `/usr/share/nagios3/htdocs/images/logos`
 - `/usr/sbin/nagios3`
 - `/usr/sbin/nagios3stats`
- Acceso al Nagios atravez la Web aquí:
<http://localhost/nagios3/>

Nagios: Vista General

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

Tactical Monitoring Overview

Last Updated: Thu Sep 3 15:37:09 CDT 2009
 Updated every 90 seconds
 Nagios® 3.0.2 - www.nagios.org
 Logged in as guest

Network Outages

0 Outages

Hosts

0 Down	0 Unreachable	41 Up	0 Pending
--------	---------------	-------	-----------

Services

0 Critical	0 Warning	0 Unknown	46 Ok	0 Pending
------------	-----------	-----------	-------	-----------

Monitoring Features

	Flap Detection	Notifications	Event Handlers	Active Checks	Passive Checks
Enabled	All Services Enabled No Services Flapping All Hosts Enabled No Hosts Flapping	Enabled	Enabled	Enabled	Enabled

Monitoring Performance

Service Check Execution Time: 0.01 / 4.07 / 0.115 sec
 Service Check Latency: 0.02 / 0.25 / 0.117 sec
 Host Check Execution Time: 0.01 / 0.13 / 0.018 sec
 Host Check Latency: 0.01 / 0.28 / 0.137 sec
 # Active Host / Service Checks: 41 / 46
 # Passive Host / Service Checks: 0 / 0

Network Health

Host Health:

Service Health:

Nagios: 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 14:41:43	1d 22h 43m 43s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)

Nagios: Detalle de Nodos

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 14:55:18 CDT 2009
 Updated every 90 seconds
 Nagios® 3.0.2 - www.nagios.org
 Logged in as *guest*

- [View Service Status Detail For All Host Groups](#)
- [View Status Overview For All Host Groups](#)
- [View Status Summary For All Host Groups](#)
- [View Status Grid For All Host Groups](#)

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

Host Status Details For All Host Groups

Host ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Status Information
DNS-ROOT	UP	2009-09-03 14:51:41	43d 1h 7m 0s	PING OK - Packet loss = 0%, RTA = 0.33 ms
ISP-DNS	UP	2009-09-03 14:51:41	16d 4h 11m 25s	PING OK - Packet loss = 0%, RTA = 0.29 ms
ISP-RTR	UP	2009-09-03 14:51:51	43d 5h 47m 40s	PING OK - Packet loss = 0%, RTA = 1.24 ms
NOG-TLD1	UP	2009-09-03 14:52:01	1d 0h 10m 56s	PING OK - Packet loss = 0%, RTA = 4.02 ms
NOG-TLD2	UP	2009-09-03 14:52:01	1d 22h 53m 46s	PING OK - Packet loss = 0%, RTA = 2.23 ms
NOG-TLD3	UP	2009-09-03 14:52:11	1d 22h 53m 36s	PING OK - Packet loss = 0%, RTA = 2.62 ms
NOG-TLD4	UP	2009-09-03 14:52:21	1d 22h 53m 36s	PING OK - Packet loss = 0%, RTA = 1.09 ms
NOG-TLD5	UP	2009-09-03 14:52:31	1d 22h 54m 6s	PING OK - Packet loss = 0%, RTA = 5.20 ms
NOG-TLD6	UP	2009-09-03 14:52:31	1d 22h 53m 56s	PING OK - Packet loss = 0%, RTA = 10.49 ms
NOG-TLD7	UP	2009-09-03 14:52:41	1d 22h 53m 56s	PING OK - Packet loss = 0%, RTA = 1.05 ms
NOG-TLD8	UP	2009-09-03 14:52:51	1d 22h 53m 56s	PING OK - Packet loss = 0%, RTA = 1.00 ms
NS1-TLD1	UP	2009-09-03 14:53:01	1d 0h 10m 26s	PING OK - Packet loss = 0%, RTA = 10.19 ms
NS1-TLD2	UP	2009-09-03 14:53:01	1d 22h 53m 56s	PING OK - Packet loss = 0%, RTA = 5.06 ms
NS1-TLD3	UP	2009-09-03 14:53:11	1d 22h 53m 36s	PING OK - Packet loss = 0%, RTA = 1.03 ms
NS1-TLD4	UP	2009-09-03 14:53:21	1d 22h 53m 36s	PING OK - Packet loss = 0%, RTA = 1.15 ms
NS1-TLD5	UP	2009-09-03 14:53:21	1d 22h 54m 6s	PING OK - Packet loss = 0%, RTA = 1.12 ms
NS1-TLD6	UP	2009-09-03 14:53:31	1d 22h 53m 36s	PING OK - Packet loss = 0%, RTA = 1.06 ms
NS1-TLD7	UP	2009-09-03 14:53:41	1d 22h 53m 46s	PING OK - Packet loss = 0%, RTA = 1.11 ms
NS1-TLD8	UP	2009-09-03 14:53:51	1d 22h 53m 36s	PING OK - Packet loss = 0%, RTA = 1.18 ms
TLD1-RTR	UP	2009-09-03 14:53:51	1d 22h 54m 6s	PING OK - Packet loss = 0%, RTA = 2.22 ms
TLD2-RTR	UP	2009-09-03 14:54:01	1d 22h 53m 46s	PING OK - Packet loss = 0%, RTA = 2.38 ms



Nagios: Resumen de los Grupos de Nodos

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 14:55:28 CDT 2009
 Updated every 90 seconds
 Nagios® 3.0.2 - www.nagios.org
 Logged in as guest

[View Service Status Detail For All Host Groups](#)
[View Host Status Detail For All Host Groups](#)
[View Status Summary For All Host Groups](#)
[View Status Grid For All Host Groups](#)

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 Overview For All Host Groups

[TRTI TLD1 Servers, Virtual Machines, Routers \(TLD1\)](#)

Host	Status	Services	Actions
NOC-TLD1	UP	1 OK	
NS1-TLD1	UP	1 OK	
TLD1-RTR	UP	1 OK	
TRTI-TLD1	UP	1 OK	

[TRTI TLD2 Servers, Virtual Machines, Routers \(TLD2\)](#)

Host	Status	Services	Actions
NOC-TLD2	UP	1 OK	
NS1-TLD2	UP	1 OK	
TLD2-RTR	UP	1 OK	
TRTI-TLD2	UP	1 OK	

[TRTI TLD3 Servers, Virtual Machines, Routers \(TLD3\)](#)

Host	Status	Services	Actions
NOC-TLD3	UP	1 OK	
NS1-TLD3	UP	1 OK	
TLD3-RTR	UP	1 OK	
TRTI-TLD3	UP	1 OK	

[TRTI TLD4 Servers, Virtual Machines, Routers \(TLD4\)](#)

Host	Status	Services	Actions
NOC-TLD4	UP	1 OK	
NS1-TLD4	UP	1 OK	
TLD4-RTR	UP	1 OK	
TRTI-TLD4	UP	1 OK	

[TRTI TLD5 Servers, Virtual Machines, Routers \(TLD5\)](#)

Host	Status	Services	Actions
NOC-TLD5	UP	1 OK	
NS1-TLD5	UP	1 OK	
TLD5-RTR	UP	1 OK	
TRTI-TLD5	UP	1 OK	

[TRTI TLD6 Servers, Virtual Machines, Routers \(TLD6\)](#)

Host	Status	Services	Actions
NOC-TLD6	UP	1 OK	
NS1-TLD6	UP	1 OK	
TLD6-RTR	UP	1 OK	
TRTI-TLD6	UP	1 OK	

[TRTI TLD7 Servers, Virtual Machines, Routers \(TLD7\)](#)

Host	Status	Services	Actions
NOC-TLD7	UP	1 OK	
NS1-TLD7	UP	1 OK	

[TRTI TLD8 Servers, Virtual Machines, Routers \(TLD8\)](#)

Host	Status	Services	Actions
NOC-TLD8	UP	1 OK	
NS1-TLD8	UP	1 OK	

[TRTI Management Virtual Machines \(VM-mgmt\)](#)

Host	Status	Services	Actions
DNS-ROOT	UP	1 OK	
ISP-DNS	UP	1 OK	

Nagios: Resumen de los Grupos 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: Fri Sep 4 13:29:20 CDT 2009
 Updated every 90 seconds
 Nagios® 3.0.2 - www.nagios.org
 Logged in as guest

- [View Service Status Detail For All Service Groups](#)
- [View Status Summary For All Service Groups](#)
- [View Service Status Grid For All Service Groups](#)

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
53	0	0	1	0
All Problems		All Types		
1		54		



Service Overview For All Service Groups

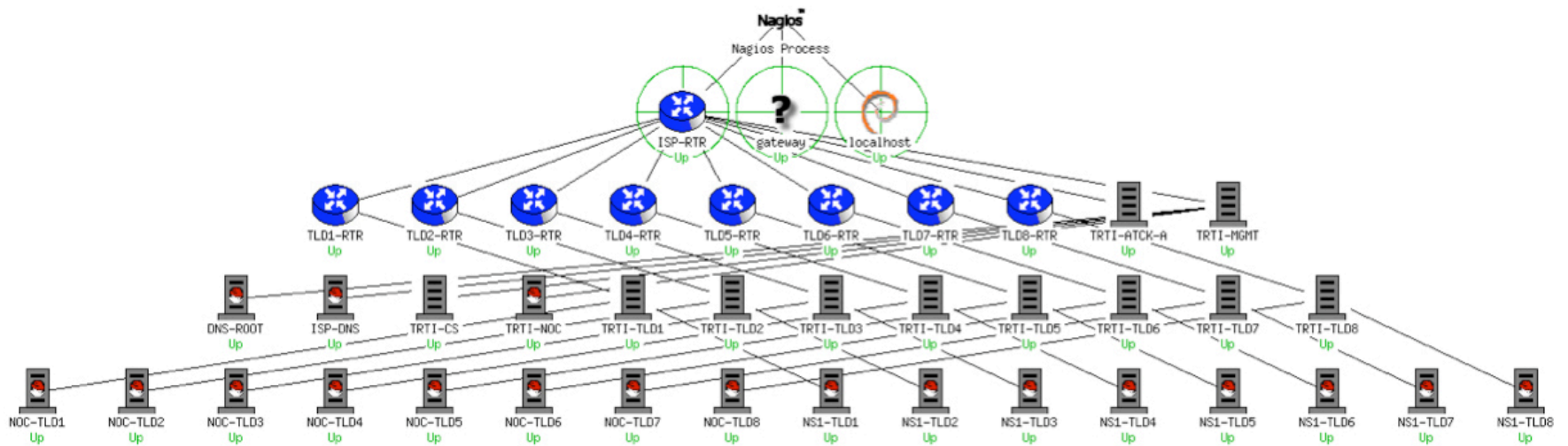
TLD Servers running Nagios (NAGIOS)

Host	Status	Services	Actions
NS1-TLD1	UP	1 OK	[Icons]
NS1-TLD2	UP	1 OK	[Icons]
NS1-TLD3	UP	1 OK	[Icons]
NS1-TLD4	UP	1 OK	[Icons]
NS1-TLD5	UP	1 OK	[Icons]
NS1-TLD6	UP	1 OK	[Icons]
NS1-TLD7	UP	1 OK	[Icons]
NS1-TLD8	UP	1 OK	[Icons]

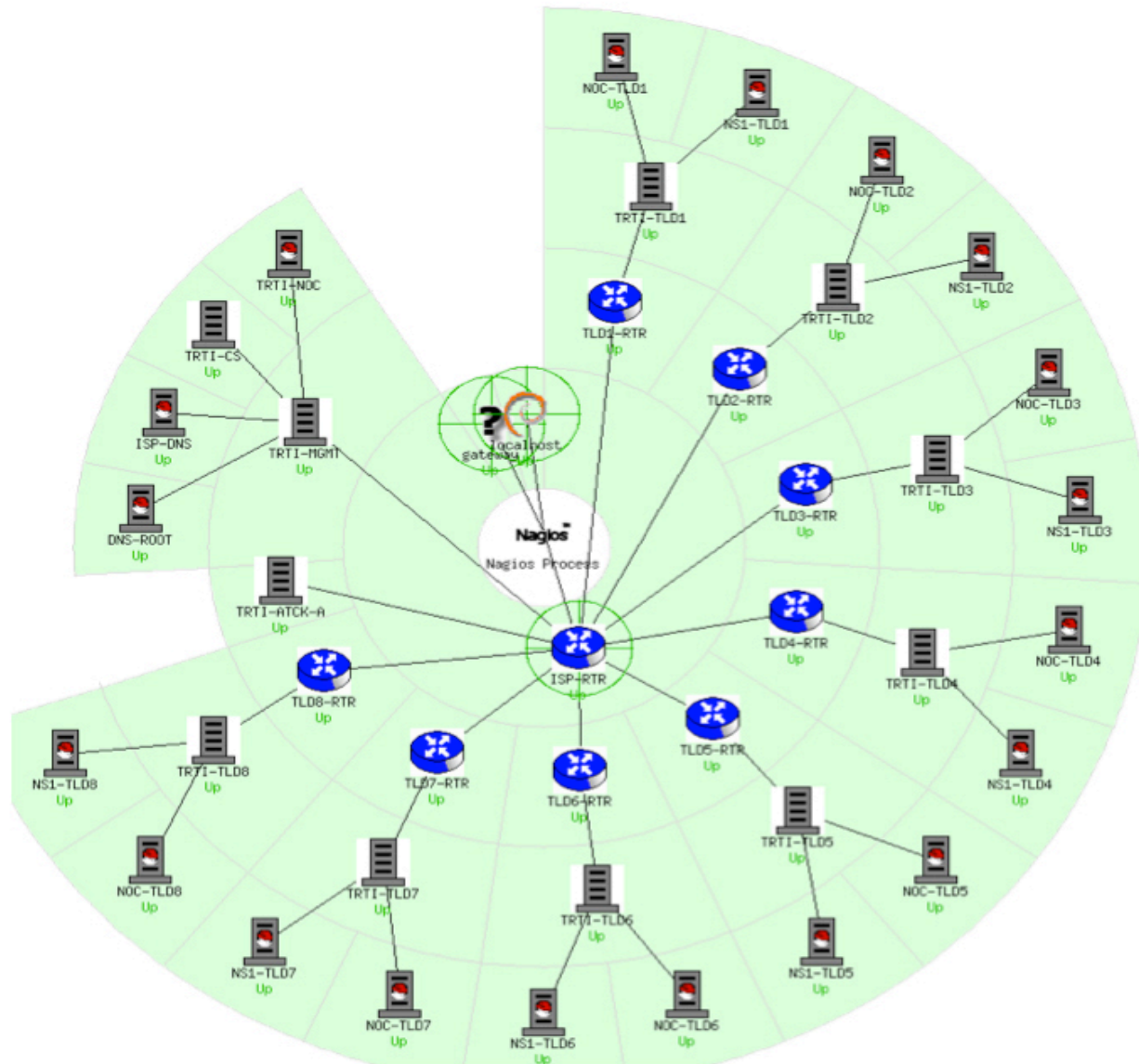
TLD Servers running SSH (SSH)

Host	Status	Services	Actions
NS1-TLD1	UP	1 OK	[Icons]
NS1-TLD2	UP	1 CRITICAL	[Icons]
NS1-TLD3	UP	1 OK	[Icons]
NS1-TLD4	UP	1 OK	[Icons]
NS1-TLD5	UP	1 OK	[Icons]
NS1-TLD6	UP	1 OK	[Icons]
NS1-TLD7	UP	1 OK	[Icons]
NS1-TLD8	UP	1 OK	[Icons]

Nagios: Mapa de Estatus: Arbol Colapsado



Nagios: Mapa de Estatus: Circular (Marcado)



Características

- La verificación de disponibilidad se delega en *plugins*
 - La arquitectura es muy simple, por lo que es fácil escribir plugins (en cualquier lenguaje)
 - Existen docenas de plugins, muchos contribuidos por terceros
- *Chequeos en paralelo (usando forking)*
 - *Version 3 se lo hace ya mejor chequeos en paralelo.*

Características cont.

- Programación de chequeos inteligente. Busca una distribución equitativa de la carga de la máquina que ejecuta Nagios, y la máquina siendo chequeada
- Configuraciones (en archivos de texto) muy detalladas y basadas en plantillas
- *Lea su configuración al nivel de directorio. Tu decides como definir los archivos.*

Y mas Características...

- 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 los máquinas no 'inalcanzable'
- 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 servicio:

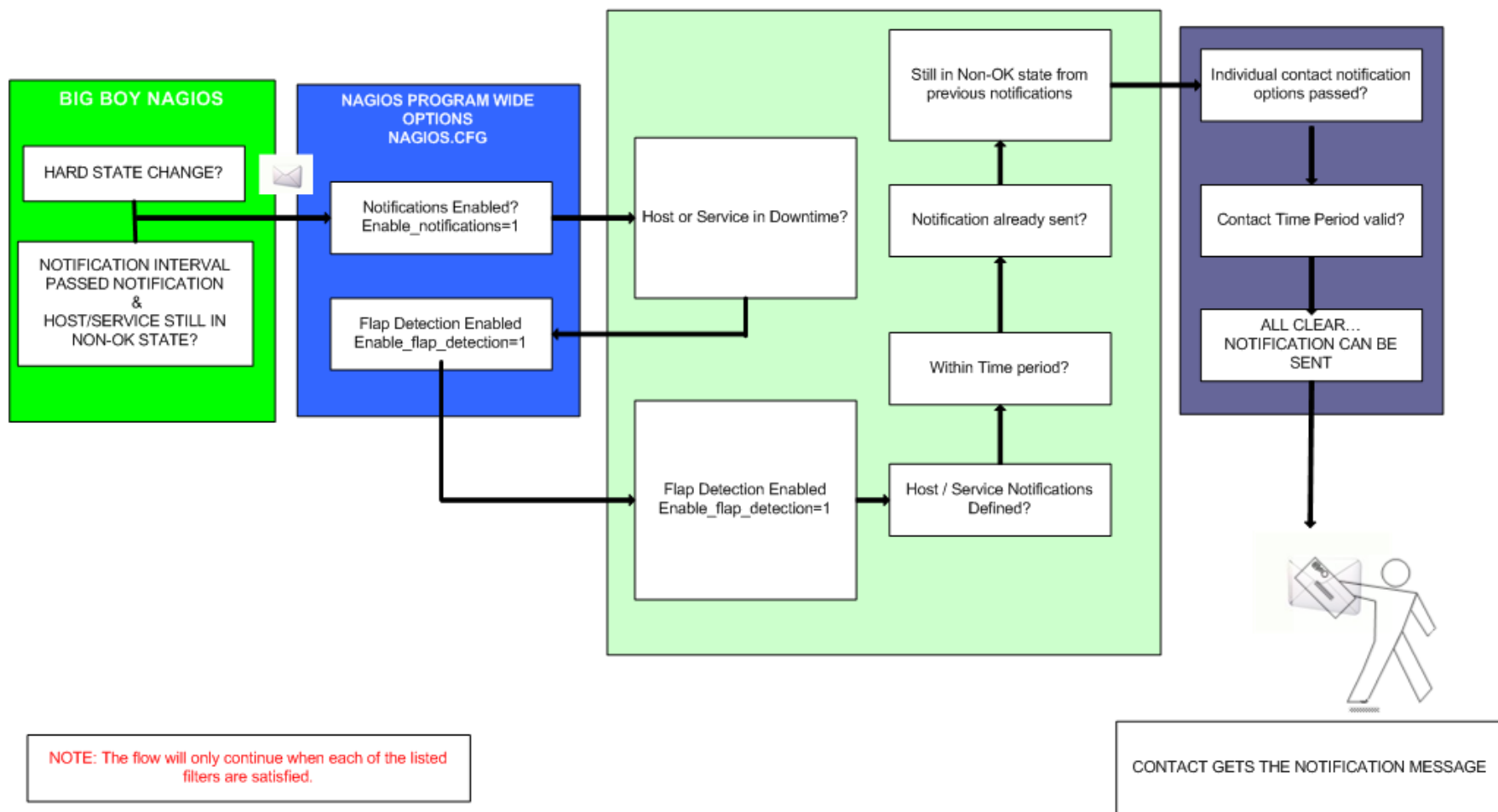
And, even more...

Service state:

When configuration a service you have the following notification options:

- **d: DOWN:** The service is down (not available)
- **u: UNREACHABLE:** When the host is not visible
- **r: RECOVERY:** (OK) Host is coming back up
- **f: FLAPPING:** When a host first starts or stops or it's state is undetermined.
- **n: NONE:** Don't send any notifications

NAGIOS - NOTIFICATION FLOW DIAGRAM



Características y mas Características...

- Permite acusar recibo de eventos (acknowledge)
 - El usuario puede agregar comentarios
- Permite definir períodos de mantenimiento
 - Por dispositivo o grupo de dispositivos
- Mantiene estadísticas de disponibilidad
- Detecta flappings y suprime las notificaciones
- Permite múltiples métodos de notificación via comandos
 - e-mail, pager, SMS, winpopup, audio, etc...
- Permite definir niveles de escalamiento de notificaciones

Mecánica de chequeos

- Uno 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
 - Uno nodo (host) puede estar:
 - DOWN
 - UNREACHABLE

Mecánica de chequeos

- Así se puede demorar hasta que un host cambia su estado a “down” (no disponible o alcanzable) por el hecho de que Nagios hace un chequeo de servicios primero, después se hace el chequeo de nodo
- Por defecto Nagios se lo hace un chequeo de nodo 3 veces antes que se cambia el estado de un nodo.
- Naturalmente, puedes cambiar todo esto.

Concepto de “Parents”

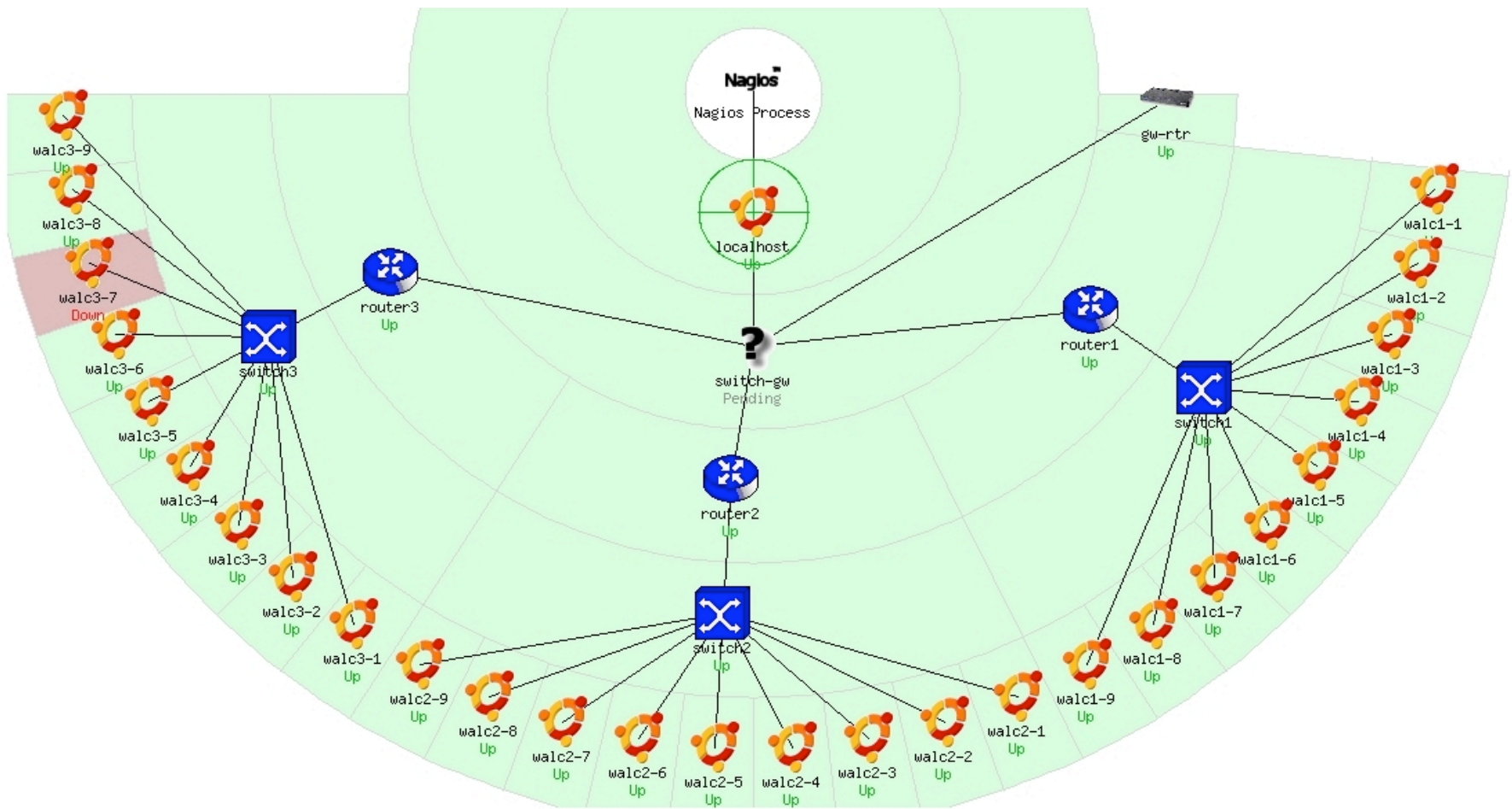
- Nodos pueden tener “parents”
 - Por ejemplo, el parent de un pc conectado a un switch seria el switch.
 - Nos permite especificar las dependencias que haya en la red entre maquinas, switches, routers, etc.
 - Evita que Nagios mande alarmas si un parent ya no responde.
 - Un nodo puede tener multiple parents.



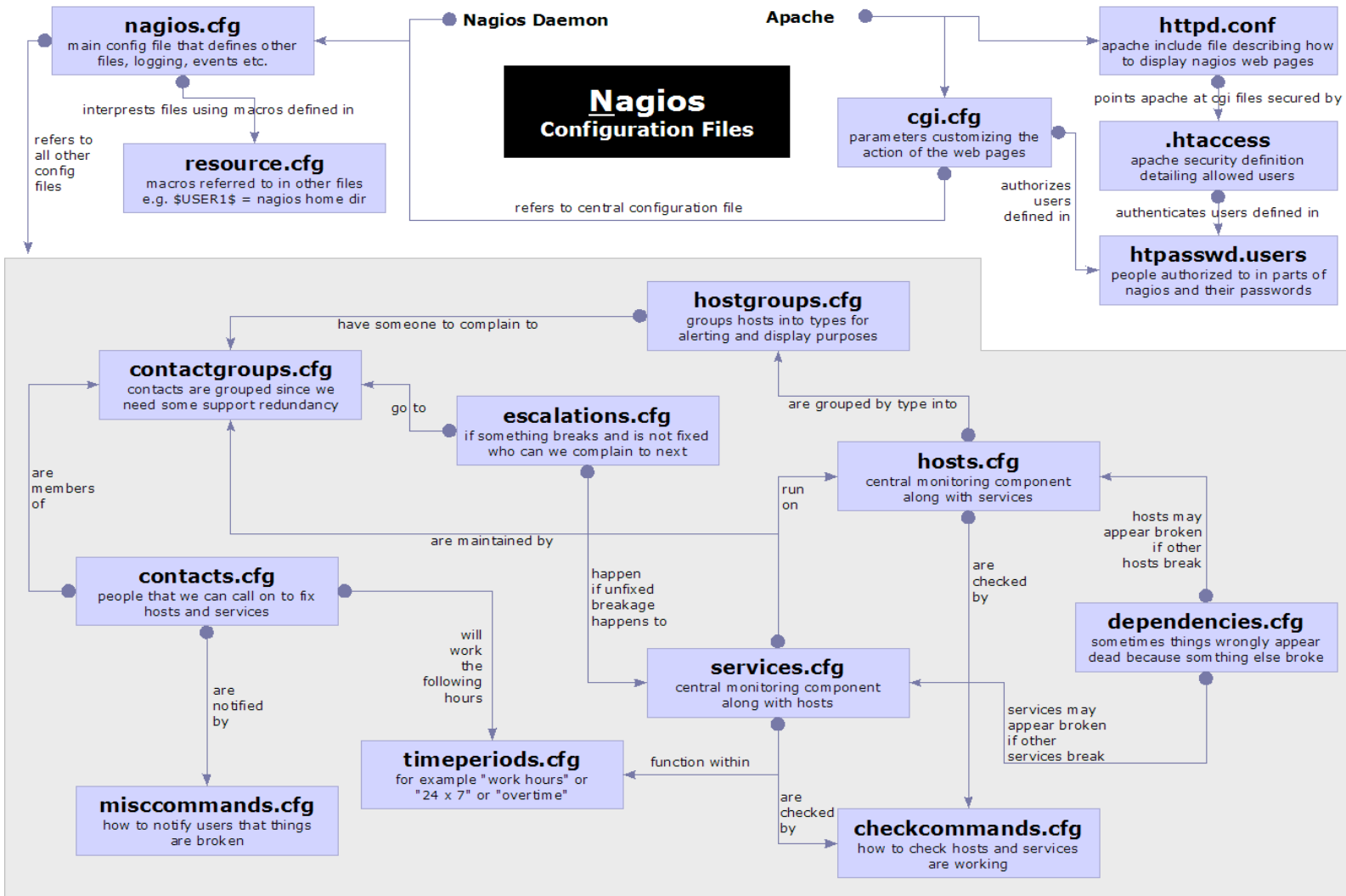
Concepto de Punto de Vista

- Donde queda tu servidor de Nagios en la red va a cambiar como vea y monitorea nodos y servicios.
- Nagios apoya el concepto de servidores en paralelo que corren en otras partes de tu red.
- Así, probablemente mejor que el servidor corre cerca del borde de tu red y no adentro.

Concepto de Punto de Vista



Archivos de Configuración



Archivos de Configuración

- Ubicado in `/etc/nagios3/`
- Archivos importantes:
 - `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 configuracion
 - `conf.d/*` El resto de los archivos de configuracion por servicios, grupos, nodos, etc.

Archivos de Configuración

Bajo conf.d/* *(solo muestra)*

- [contacts_nagios2.cfg](#) usuarios y grupos
- [generic-host_nagios2.cfg](#) plantilla host (defecto)
- [generic-service_nagios2.cfg](#) plantilla servicio (defecto)
- [hostgroups_nagios2.cfg](#) definiciones de grupos de hosts
- [services_nagios2.cfg](#) que servicios chequear
- [timeperiods_nagios2.cfg](#) cuando chequear y como y quien a notificar

Archivos de Configuración

Bajo conf.d otros archivos opcionales:

- [host-gateway_nagios3.cfg](#) definición de ruta por defecto
- [extinfo.cfg](#) informacion extra por nodos
- [servicegroups.cfg](#) grupos de máquinas y servicios
- [localhost.cfg](#) definicion de monitoreo por el servidor de Nagios (localhost)
- [pcs .cfg](#) definicion de un grupos de nodos
- [switches.cfg](#) definicion de un grupo de switches
- [routers.cfg](#) definicion de un grupo de routers

Configuración de Plugins

El paquete de nagios-plugins ya esta instalado en Ubuntu y contiene:

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

Configuración Principal

- Parámetros que afectan al programa globalmente
- Archivo: `/etc/nagios3/nagios.cfg`
 - Indicar la ubicación de los demás archivos de configuración
 - Comportamiento de Nagios en general
 - Importante ajustar para asegurar un buen desempeño en instalaciones con cientos de servicios monitorizados
 - Ver: *Tunning Nagios for Maximum Performance*
http://nagios.sourceforge.net/docs/2_0/tuning.html

Configuración de CGI

- Archivo: `/etc/nagios3/cgi.cfg`
 - Configurar directorio de CGIs
 - Autenticación y Autorización
 - Activar autenticación en Apache vía `.htpasswd` (o Radius/Ldap)
 - Listar los nombres de usuario en las variables de autorización:
 - `authorized_for_system_information`
 - `authorized_for_configuration_information`
 - `authorized_for_system_commands`
 - `authorized_for_all_services`
 - `authorized_for_all_hosts`
 - `authorized_for_all_service_commands`
 - `authorized_for_all_host_commands`

Configuración de Períodos

- Definir períodos básicos que controlarán los chequeos, notificaciones, etc.
 - 24 horas, 7 días a la semana
 - Horario de trabajo
 - Horario fuera de trabajo

```
# '24x7'  
define timeperiod{  
    timeperiod_name 24x7  
    alias           24 Hours A Day, 7 Days A Week  
    sunday          00:00-24:00  
    monday          00:00-24:00  
    tuesday         00:00-24:00  
    wednesday       00:00-24:00  
    thursday        00:00-24:00  
    friday          00:00-24:00  
    saturday        00:00-24:00  
}
```

Configurando chequeo de Servicios/Hosts

- Definir cómo se van a probar los servicios:

```
# 'check-host-alive' command definition
define command{
    command_name    check-host-alive
    command_line    $USER1$/check_ping -H $HOSTADDRESS$ -w 2000.0,60% -c
5000.0,100% -p 1 -t 5
}
```

Ubicado en /etc/nagios-plugins/config, despues ajuste en /etc/nagios3/conf.d/services_nagios2.cfg

Comandos de notificación

Permite utilizar cualquier comando que quieras. Puedes usar esto para generar tickets en RT

```
# 'notify-by-email' command definition
define command{
    command_name      notify-by-email
    command_line      /usr/bin/printf "%b" "Service: $SERVICEDESC$\nHost:
$HOSTNAME$\nIn: $HOSTALIAS$\nAddress: $HOSTADDRESS$\nState: $SERVICESTATE$
\nInfo: $SERVICEOUTPUT$\nDate: $SHORTDATETIME$" | /bin/mail -s
'$NOTIFICATIONTYPE$: $HOSTNAME$/$SERVICEDESC$ is $SERVICESTATE$'
$CONTACTEMAIL$
}
```

```
From: nagios@nms.localdomain
To: grupo-redes@localdomain
Subject: Host DOWN alert for switch1!
Date: Thu, 29 Jun 2006 15:13:30 -0700
```

```
Host: switch1
In: Core_Switches
State: DOWN
Address: 111.222.333.444
Date/Time: 06-29-2006 15:13:30
Info: CRITICAL - Plugin timed out after 6 seconds
```

Configuración de nodos y servicios

- Método basado en plantillas (templates)
 - Ahorra mucho trabajo repetitivo
 - Similar a programación OO
- Crear plantillas con todos los parámetros por defecto
 - nodo genérico
 - servicio genérico
 - contacto genérico

Configuración de nodo genérico - plantilla

```
define host{
    name                generic-host
    notifications_enabled 1
    event_handler_enabled 1
    flap_detection_enabled 1
    process_perf_data    1
    retain_status_information 1
    retain_nonstatus_information 1
    check_command        check-host-alive
    max_check_attempts  5
    notification_interval 60
    notification_period 24x7
    notification_options d,r
    contact_groups       nobody
    register              0
}
```

Configuración de nodo individual

```
define host{
    use                generic-host
    host_name          switch1
    alias              Core_switches
    address            192.168.1.2
    parents            router1
    contact_groups     switch_group
}
```

Configuración de Servicio (genérico)

```
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
    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 Servicio

```
define service{
    host_name          switch1
    use                generic-service
    service_description PING
    check_command      check-host-alive
    max_check_attempts 5
    normal_check_interval 5
    notification_options c,r,f
    contact_groups     switch-group
}
```

Mensajes a Beepers/SMS

- Importante integrar Nagios con un sistema de mensajes a beepers
 - Los problemas también ocurren fuera del horario de trabajo
- El sistema de envío a beepers debe ser independiente de la red
 - Utilizar un módem y una línea telefónica
 - Pueden utilizarse paquetes como *sendpage* o *qpage*

Referencias

- <http://www.nagios.org>: Nagios web site
- <http://sourceforge.net/projects/nagiosplug>: Nagios plugins site
- *Nagios. System and Network Monitoring* by Wolfgang Barth. Good book on Nagios
- <http://www.nagiosexchange.org>: Unofficial Nagios plugin site
- <http://www.debianhelp.co.uk/nagios.htm>: A Debian tutorial on Nagios
- <http://www.nagios.com/>: Commercial Nagios support