



Gestion de Redes WALC 2010

NAGIOS



These materials are licensed under the Creative Commons *Attribution-Noncommercial 3.0 Unported* license (<http://creativecommons.org/licenses/by-nc/3.0/>) as part of the ICANN, ISOC and NSRC Registry Operations Curriculum.

Introduccion

- Una herramienta clave de medir en forma activa la disponibilidad de dispositivos y servicio
- Posiblemente el software de fuente abierto para gestion y monitoreo de redes mas usado
- Tiene un interfaz de web
 - Usa CGI's escrito en C para responder mas rapido y apoyar crecimiento
- Apoya hasta miles de dispositivos y servicios.



Instalacion

En Debian/Ubuntu

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

- Archivos estan aqui:

```
/etc/nagios3
```

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

```
/etc/nagios-plugins/conf
```

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

```
/usr/sbin/nagios3
```

```
/usr/sbin/nagios3stats
```

Interfaz de la Web de Nagios esta aqui:

<http://localhost/nagios3/>



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

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 Outages

0 Outages

Network Health

Host Health:
Service Health:

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 All Services Enabled All Hosts Enabled	Enabled All Services Enabled All Hosts Enabled	Enabled All Services Enabled All Hosts Enabled	Enabled All Services Enabled All Hosts Enabled



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
0

All Types
41

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
46	0	0	0	0

All Problems
0

All Types
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 43s	1/4	SSH OK - OpenSSH_5.1p1 Debian-3ubuntu1 (protocol 2.0)

Detalle de Dispositivos

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-RTT	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-RTT	UP	2009-09-03 14:53:51	1d 22h 54m 6s	PING OK - Packet loss = 0%, RTA = 2.22 ms
TLD2-RTT	UP	2009-09-03 14:54:01	1d 22h 53m 46s	PING OK - Packet loss = 0%, RTA = 2.38 ms



Resumen de Servicios por Grupos de Maquinas

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	

Resumen de 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)

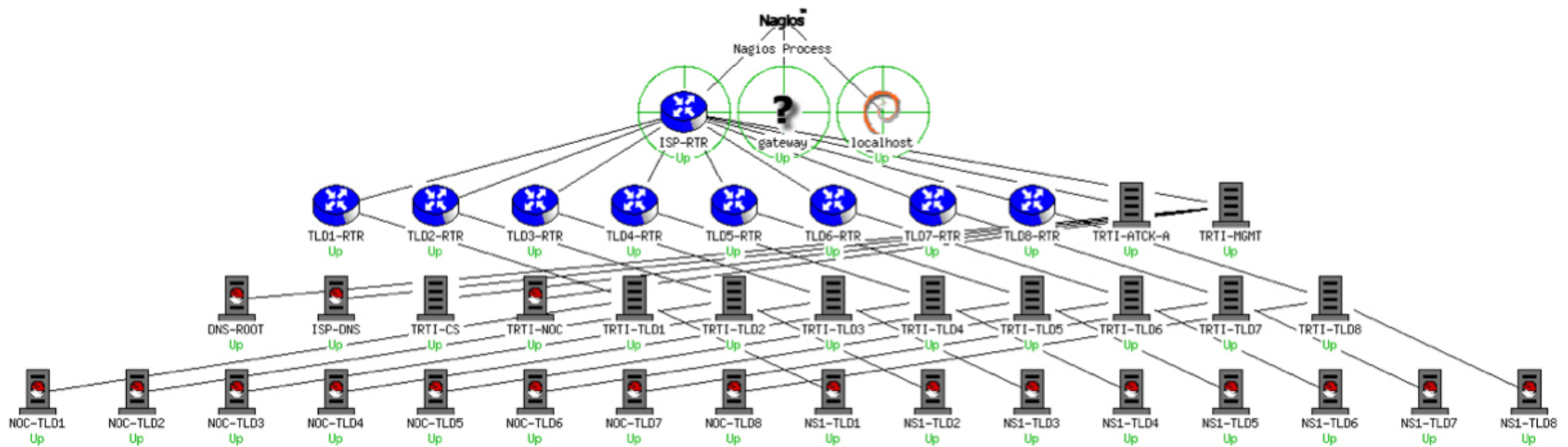
Host	Status	Services	Actions
NS1-TLD1	UP	1 OK	
NS1-TLD2	UP	1 OK	
NS1-TLD3	UP	1 OK	
NS1-TLD4	UP	1 OK	
NS1-TLD5	UP	1 OK	
NS1-TLD6	UP	1 OK	
NS1-TLD7	UP	1 OK	
NS1-TLD8	UP	1 OK	

TLD Servers running SSH (SSH)

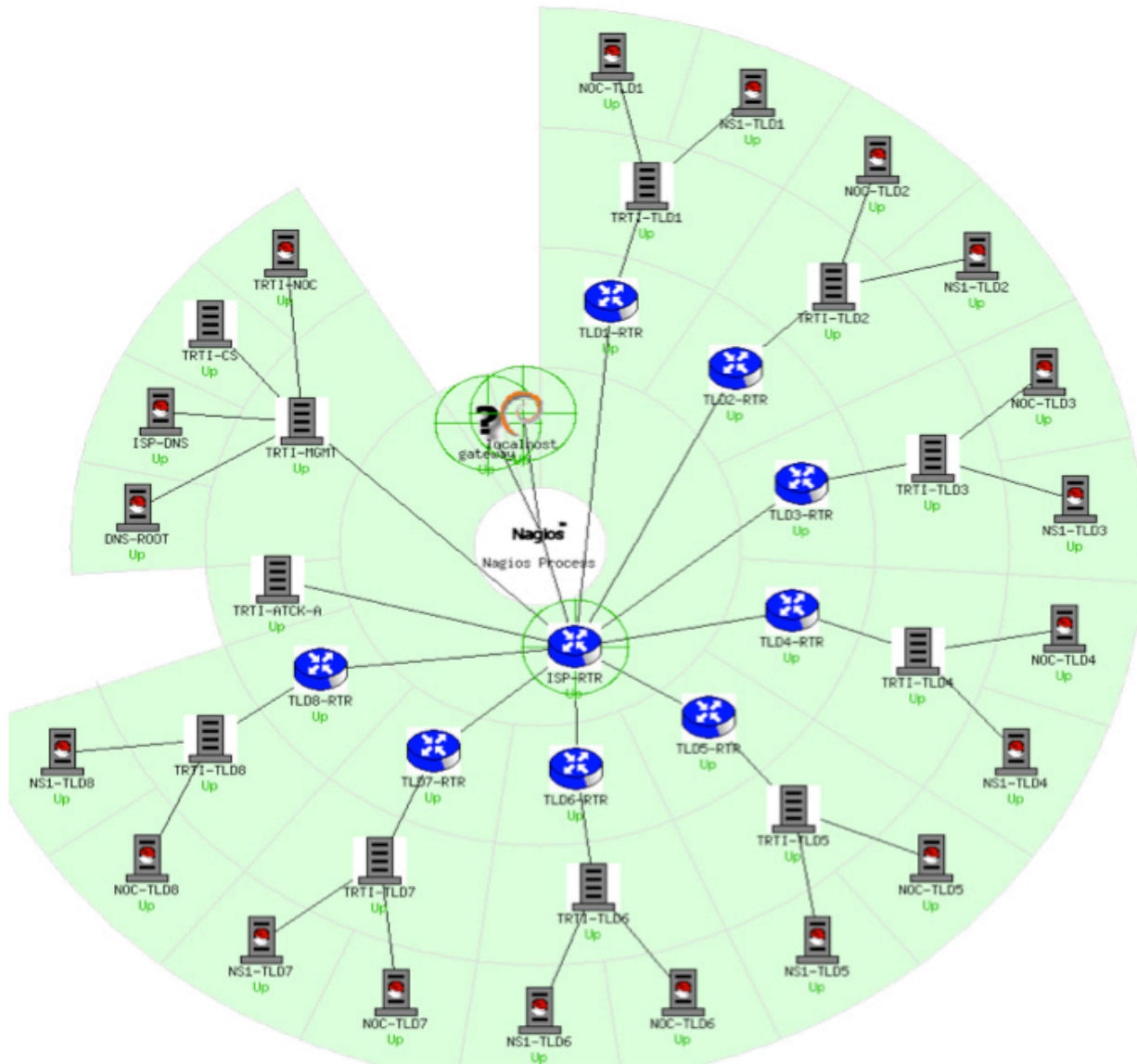
Host	Status	Services	Actions
NS1-TLD1	UP	1 OK	
NS1-TLD2	UP	1 CRITICAL	
NS1-TLD3	UP	1 OK	
NS1-TLD4	UP	1 OK	
NS1-TLD5	UP	1 OK	
NS1-TLD6	UP	1 OK	
NS1-TLD7	UP	1 OK	
NS1-TLD8	UP	1 OK	



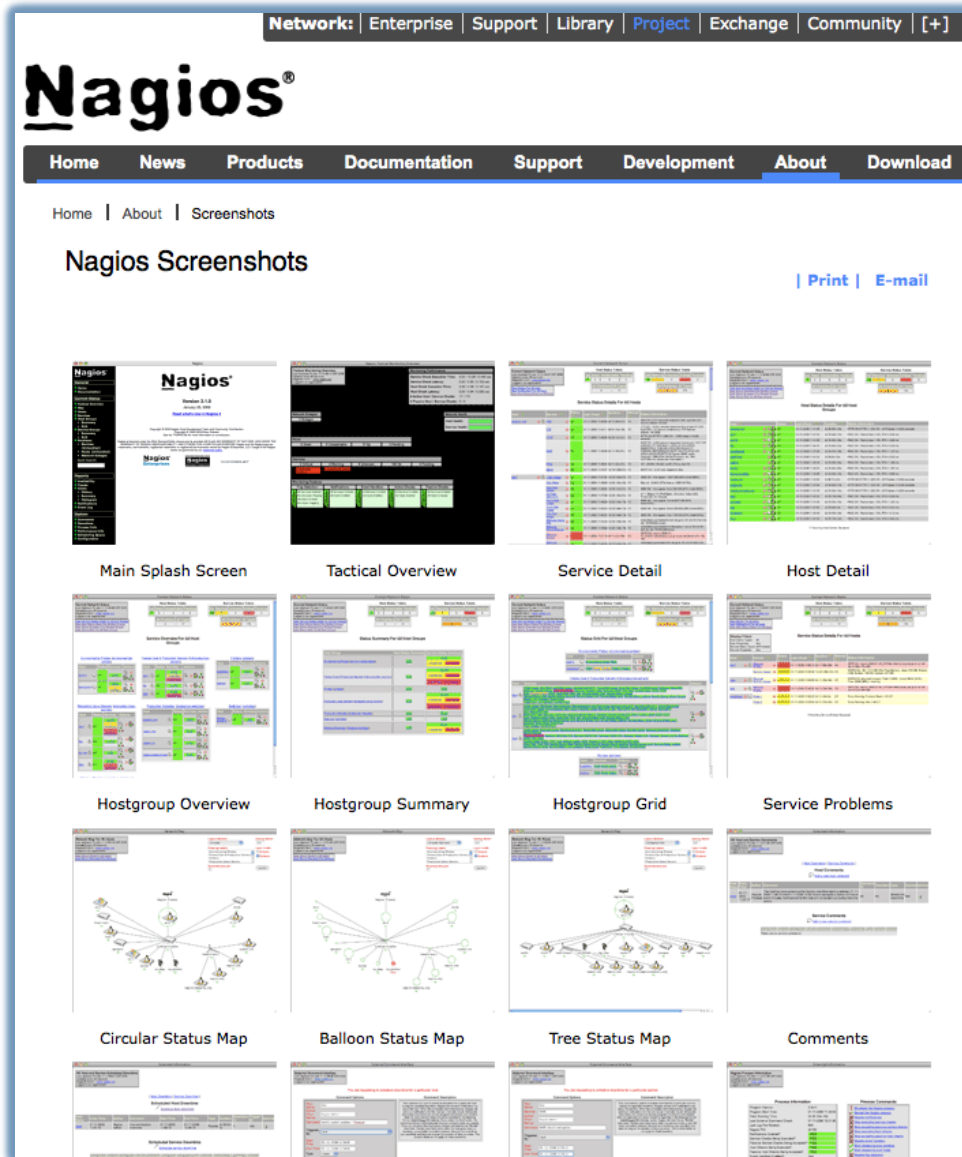
Mapa de estatus de arbol colapsado



Mapa de estatus circular y con comentario



Mas muestras de menus de Nagios



Mucho mas muestras de pantallas de Nagios estan disponible aqui:

<http://www.nagios.org/about/screenshots>



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:



Y, aun mas...

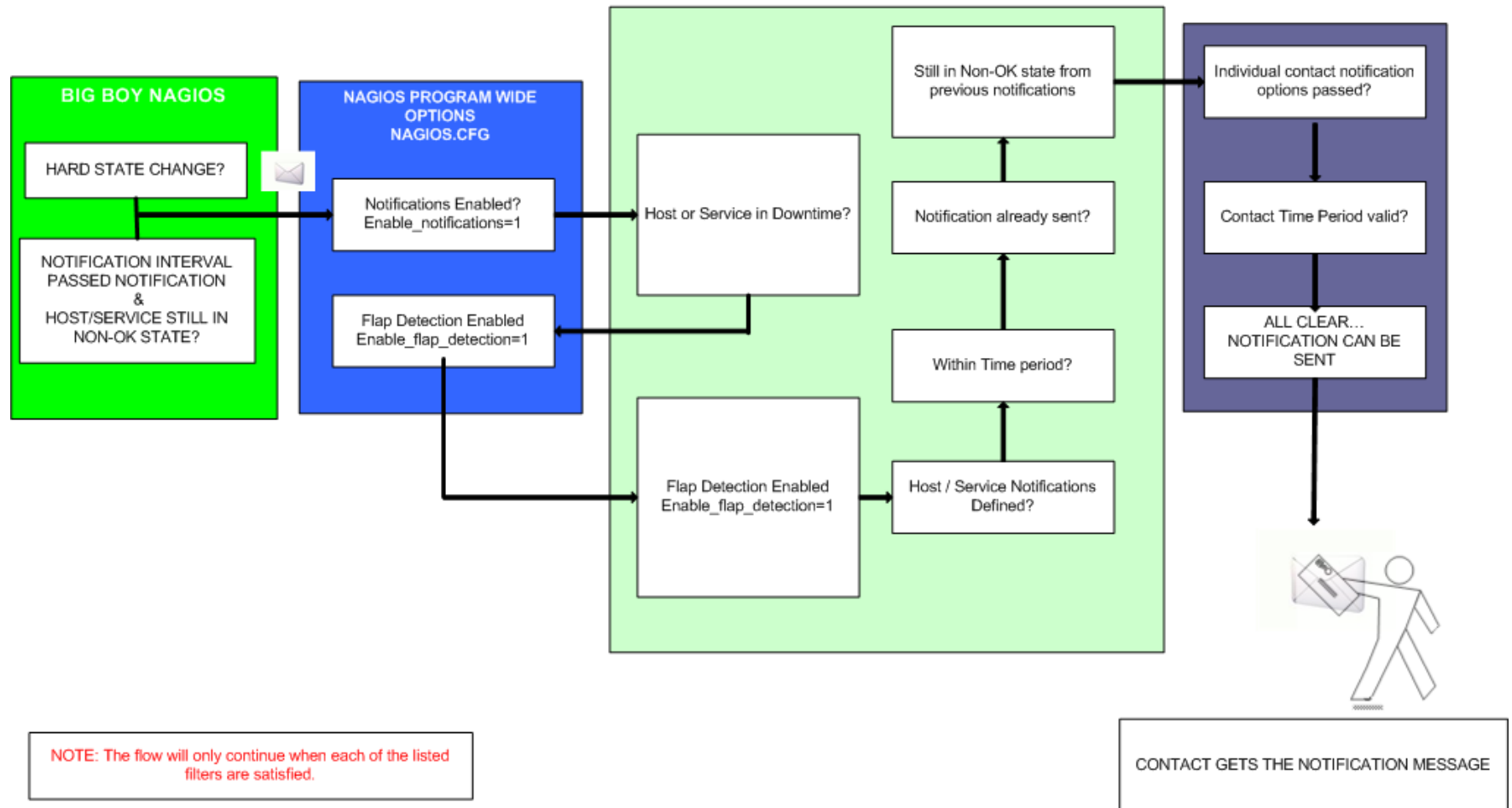
Estado de Servicio:

Cuando uno configura un servicio tiene las siguientes opciones:

- **d:** DOWN: El servicio está caído (no disponible)
- **u:** UNREACHABLE: Dispositivo no está visible
- **r:** RECOVERY: (OK) Dispositivo recuperando
- **f:** FLAPPING: La primera vez con un dispositivo sube, baja o está en un estado indeterminado
- **n:** NONE: No manda ninguna notificación



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 cont.

- 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 cont.

- 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 hayan 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.

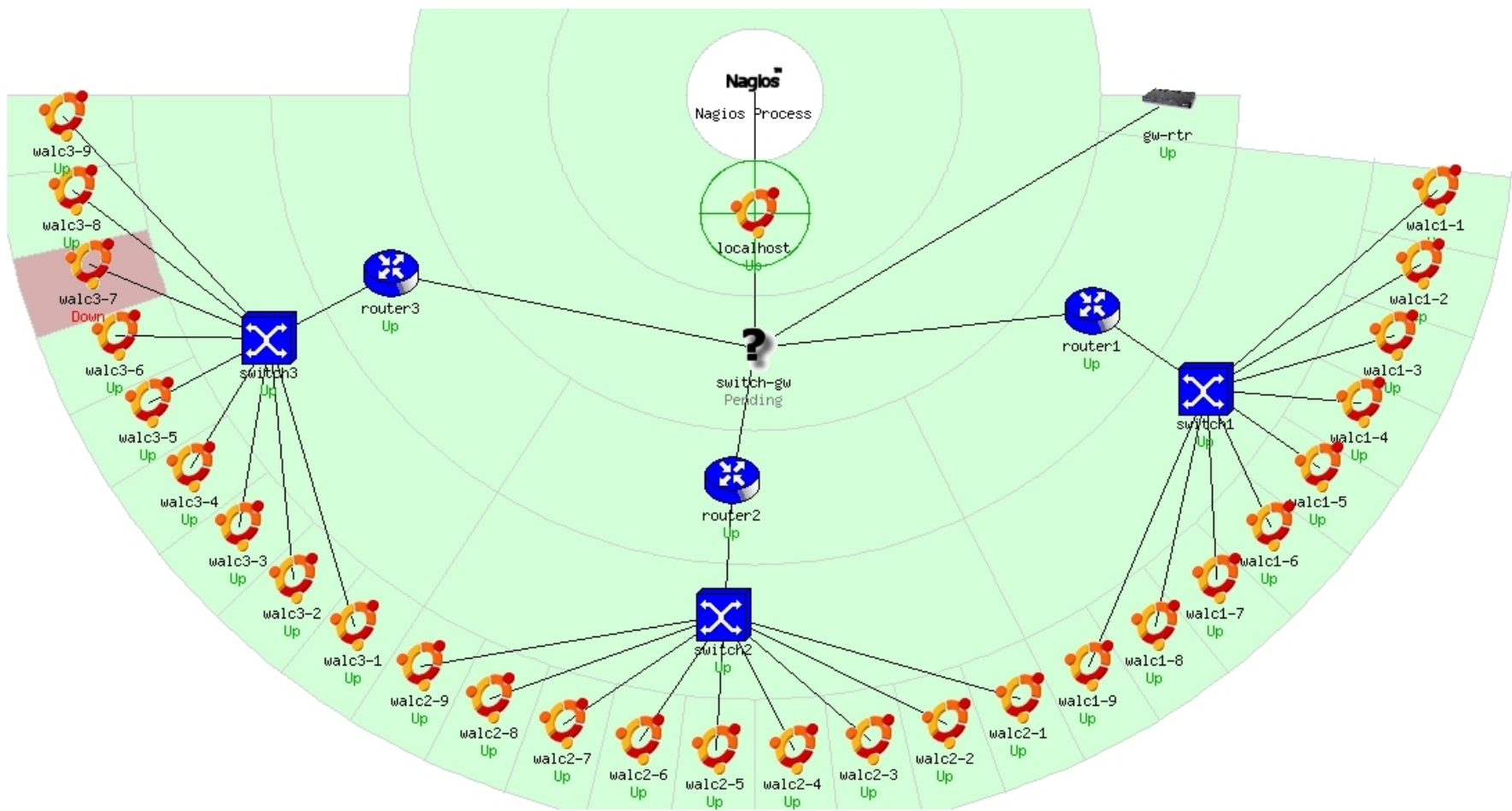


Concepto de Punto de Vista

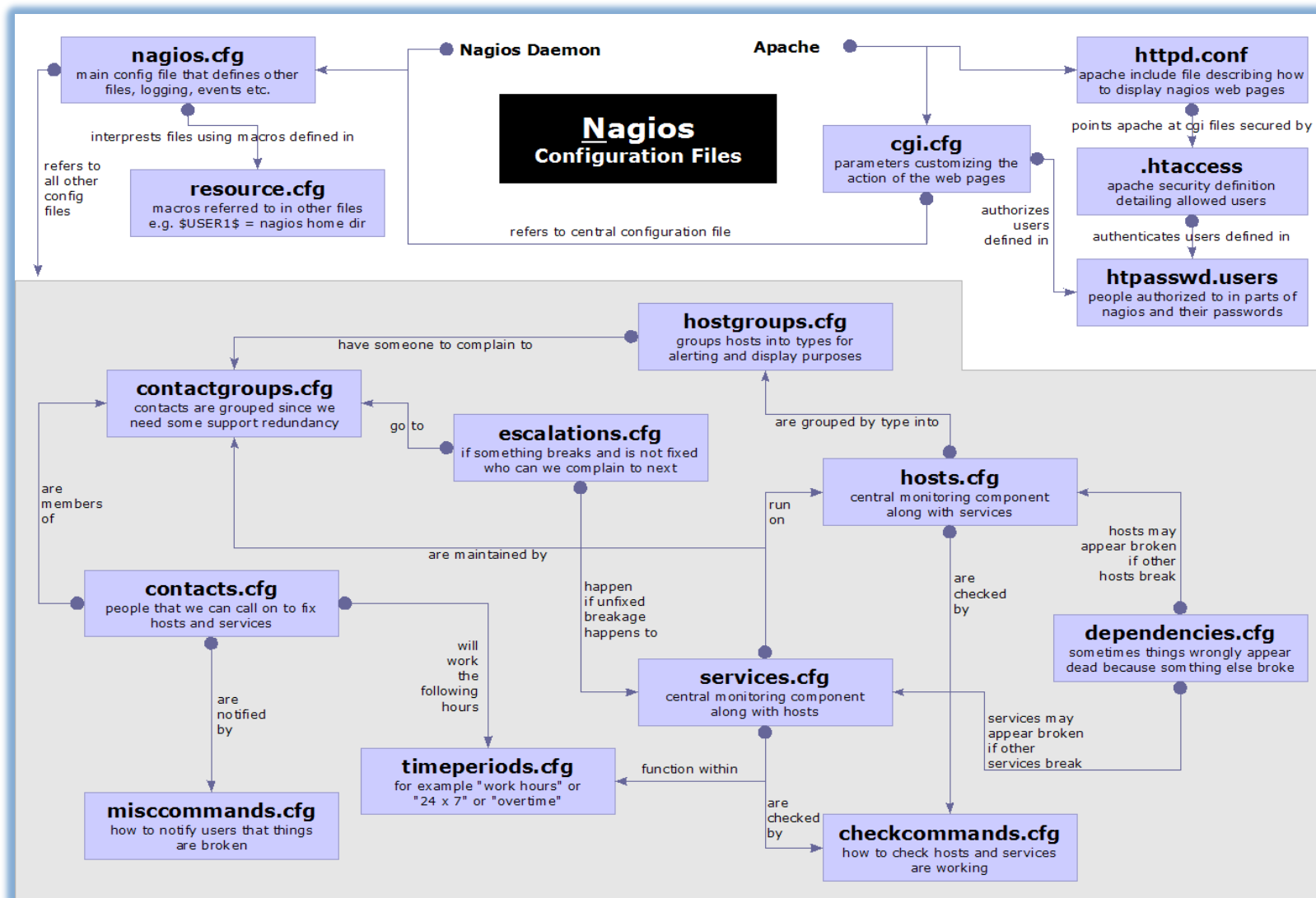
- Donde queda tu servidor de Nagios en la red va a cambiar como vea y monitorea nodos y servicios.
- Nagios apoya el concepto de servidores en paralelo que corren en otras partes de tu red.
- Así, probablemente mejor que el servidor corre cerca del borde de tu red y no adentro.



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 cont

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 cont.

Bajo conf.d otros archivos opcionales:

- `host-gateway_nagios3.cfg` definicion 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



Plugins instalado en Ubuntu

check_bgpstate	check_hpjd	check_mailq	check_overcr
check_ssmtp	check_breeze	check_http	check_mrtg
check_pgsql	check_swap	check_by_ssh	check_icmp
check_mrtgtraf	check_ping	check_tcp	check_clamd
check_ide_smart	check_mysql	check_pop	check_time
check_cluster	check_ifoperstatus	check_mysql_query	
check_procs	check_udp	check_dhcp	check_ifstatus
check_nagios	check_radius	check_ups	check_dig
check_imap	check_nntp	check_real	check_users
check_disk	check_ircd	check_nntps	check_rpc
check_wave	check_disk_smb	check_jabber	check_nt
check_sensors	check_dns	check_ldap	check_ntp
check_simap	check_dummy	check_ldap	check_ntp_peer
check_smtp	check_file_age	check_linux RAID	check_ntp_time
check_snmp	check_flexlm	check_load	check_nwstat



Configuración Principal

Parámetros que afectan al programa globalmente

File: `/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

`/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

Definicion de “host alive”

```
# '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
- Nagios se lo refiere a estos chequeos de “service” y/o “host” como “commands”



Comandos de notificación

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

```
# '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: router_group@localdomain
Subject: Host DOWN alert for TLD1-RTR!
Date: Thu, 29 Jun 2006 15:13:30 -0700
```

```
Host: TLD1-RTR
In: Core_Routers
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          gw-rtr
    alias              Rutador principal de Taller
    address            10.10.10.1
    contact_groups     router_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          gw-rtr  
    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      router_group  
}
```



Configuracion de Grupo de Servicio

```
# 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
}
```

La descripcion de servicio es importante si planea de crear Grupos de Servicios. Ahi una muestra de un Definicion de Grupo de Servicio:

```
define servicegroup{
    servicegroup_name  Webmail
    alias               web-mta-storage-auth
    members             svr1,HTTP,svr1,SMTP,svr1,POP,svr1,IMAP,
                       svr1,RAID,svr1,LDAP, svr2,HTTP,svr2,SMTP,
                       svr2,POP,svr2,IMAP,svr2,RAID,svr2,LDAP
}
```



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

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

