NAGIOS

PRESENTADO POR :

RODRIGO AVILA KULJIS

SANTA CRUZ, BOLIVIA
19 DE ABRIL DE 2014

Acerca de Nagios….

http://es.wikipedia.org/wiki/Nagios:

- ***Nagios*** *es un sistema de monitorización de redes de código abierto ampliamente utilizado, que vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado. Entre sus características principales figuran la monitorización de servicios de red (SMTP, POP3, HTTP, SNMP…), la monitorización de los recursos de sistemas hardware (carga del procesador, uso de los discos, memoria, estado de los puertos…), independencia de sistemas operativos, posibilidad de monitorización remota mediante túneles SSL cifrados o SSH, y la posibilidad de programar plugins específicos para nuevos sistemas.*
- *Se trata de un software que proporciona una gran versatilidad para consultar prácticamente cualquier parámetro de interés de un sistema, y genera alertas, que pueden ser recibidas por los responsables correspondientes mediante (entre otros medios) correo electrónico y mensajes SMS, cuando estos parámetros exceden de los márgenes definidos por el administrador de red.*

"Nagios Ain't Gonna Insist On Sainthood"

- Llamado originalmente **Netsaint**, nombre que se debió cambiar por coincidencia con otra marca comercial, fue creado y es actualmente mantenido por **Ethan Galstad**, junto con un grupo de desarrolladores de software que mantienen también varios complementos.
- Nagios fue originalmente diseñado para ser ejecutado en GNU/Linux, pero también se ejecuta bien en variantes de Unix.
- Nagios está licenciado bajo la GNU General Public License Version 2 publicada por la Free Software Fundation.

Initial release	March 14, 1999
Stable release	4.0.4 / March 14, 2014

"The Industry Standard in IT Infrastructure Monitoring"

¿control o monitoreo de infraestructura?

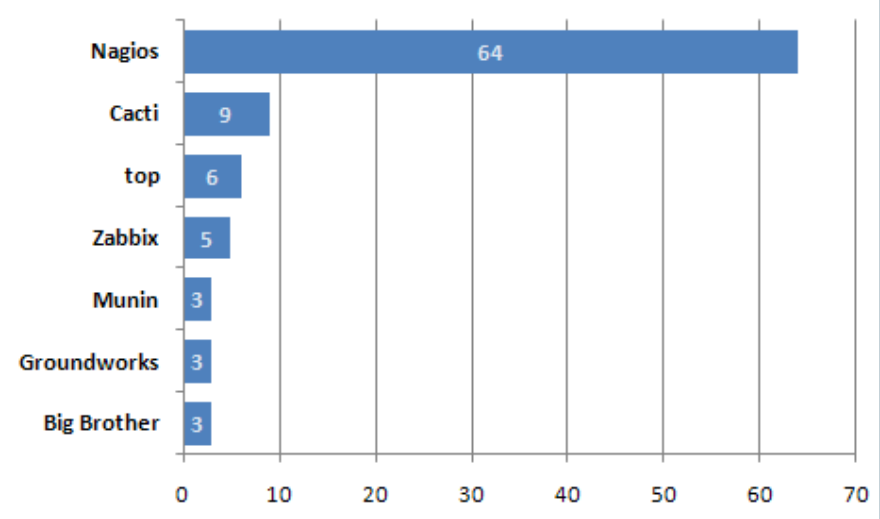
- Este documento NO es otro «*how-to* «

=> Si busca uno ….

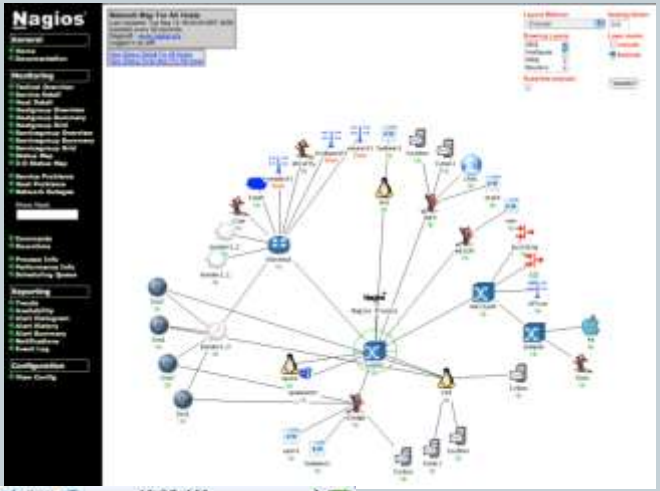
https://nsrc.org/workshops/2010/walc/raw-attachment/wiki/Agenda/nagios.ppt

- Nagios no es la «*quintaescencia*» pero..

GeekSutff.com : *Survey Says: 7 Out of 10 Geeks Prefer Nagios* (2009)



¿A dónde queremos llegar?



*Toda la red

* Notificación adecuada

* Representación gráfica

Por si existen reclamos….

Gartner …..

http://blogs.gartner.com/jonah-kowall/2013/02/22/got-nagios-get-rid-of-it/

*"**The problem** with all of these approaches is that they **don't auto-configure** themselves, they don't detect application instances properly or consistently, and configuration of checks is painful."*

Hay otras alternativas

- OMD
- MK Check Moniotring System
- Icinga
- op5 Monitor
- NAGIOS IX
- Hp Openview
- IBM Tivoli
- Zabbix
- Zenoss
- Pandorafms
- Munin,
- Gangl
- Cacti
- *www.fully**automatednagios**.org/*

etc, etc, etc

Quickstart

How To Install Nagios 3.2.2 On Ubuntu (Under 5 Minutes ...
https://www.youtube.com/watch?v=kbel-rBjAC8

http://blog.infizeal.com/2011/11/install-nagios-on-centos-in-20-minutes.html

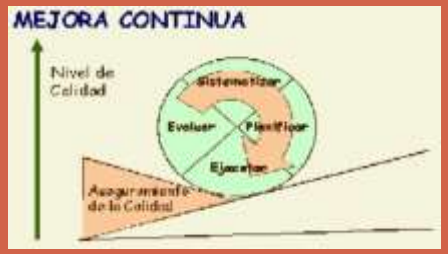
http://www.susegeek.com/monitoring/install-configure-nagios-in-less-than-5-minutes/

Install Nagios in openSUSE

Based on your version of openSUSE, click the following 1-click installs to install Nagios Core application, Nagios Plugins and Nagios Plugins extras (install in the same order)

	Nagios	Nagios Plugins	Nagios Addons Extras
	Install software via 1-click	Install software via 1-click	Install software via 1-click

VARIOS MESES DESPUES…



- Tipos de monitoreo..
- Grupos de hosts…
- Servicios por cada host…
- Valores «*Warning*» y «*Critical*»…
- Performance Data…
- Horarios…
- Notificaciones…
- Destinatarios de notificaciones
- Reportes…
- Probar, Validar, Corregir

REPETIR REPETIR REPETIR

¿Qué puedo revisar?

- Ping
- Disco, memoria, CPU, etc.
- Ancho de banda, Estatus de enlaces, etc.
- Voltaje, % de carga, temperatura, humedad ambiental…
- Procesos, motor db , estados, etc
- CUSTOM (otros)

ADICIONALMENTE:

- Estadísticas
- Planificación de Continuidad
- Planificación de Crecimiento
- Reportes
- Registro y Seguimiento de Eventos

Mucho mas….

«Under the hood»

EMPECEMOS A CONFIGURAR.. (lo más básico..)

1.-Tengo un servidor…

=> Creo el archivo ej. servidor01.cfg

2.-Este servidor tiene un servicio..

=> Agrego este servicio en el mismo archivo…

3.-Este servicio se revisa con un comando…

=> Defino esta revisión en el archivo de comandos

4.-Pruebo la definición

5.- Recargo la configuración de Nagios

1.-Tengo un servidor...
=> Creo el archivo ej. servidor01.cfg

```
define host{
        use             critical-server          ; Name of host template to use
                                                 ; This host definition will inherit all variables that are defined
                                                 ; in (or inherited by) the linux-server host template definition.
        host_name               nombre_servidor
        alias                   Una descripcion breve, por ejemplo: Controlador de dominio
        address                   la IP del servidor
        }
```

2.-Este servidor tiene un servicio..
=> Agrego este servicio en el mismo archivo...

```
define host{
        use             critical-server            ; Name of host template to use
                                                 ; This host definition will inherit
all variables that are defined
                                                 ; in (or inherited by) the linux-
server host template definition.
        host_name               nombre_servidor
        alias                   Una descripcion breve, por ejemplo: Controlador de
dominio
        address                 la IP del servidor
        }

define service {
        use                       template a usar
        service_description Espacio_Disco_E
        check_command check_snmp_winstorage!comunidad!E!pl!50!35
        host_name nombre_servidor
}
```

3.-Este servicio se revisa con un comando…
=> Defino esta revisión en el archivo de comandos

```
##############################################################################
#    Adicionales a los que trae el nagios por defecto
# Obtenidos de http://nagios.manubulon.com/
##############################################################################

# Verifica el espacio en disco:
# ARG1 es la comunidad para snmp
# ARG2 es la letra de la unidad Windows (solo la letra sin ":")
# ARG3 es el tipo de consulta. Los valores pueden ser:
#      pl (de Percentage Left, es el porcentaje libre)
#      pu (de Percentage Used, es el porcentaje ocupado)
#      bl (de megaByte Left, es el espacio libre)
#      bu (de megaByte Used, es el espacio ocupado)
# ARG4 es el valor umbral para Warning, acorde a lo especificado en ARG3
# ARG5 es el valor umbral para Critical, acorde a lo especificado en ARG3

define command{
command_name    check_snmp_winstorage
command_line    $USER1$/check_snmp_storage.pl -H $HOSTADDRESS$ -C $ARG1$ -2 -m
^$ARG2$: -T $ARG3$ -w $ARG4$ -c $ARG5$
}
```

4.-Pruebo la definición

```
# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

Si sale error, volver atrás o corregir el error.

5.- Recargo la configuración de Nagios

```
# /etc/init.d/nagios restart
```

6.- Reviso el servicio definido en Nagios

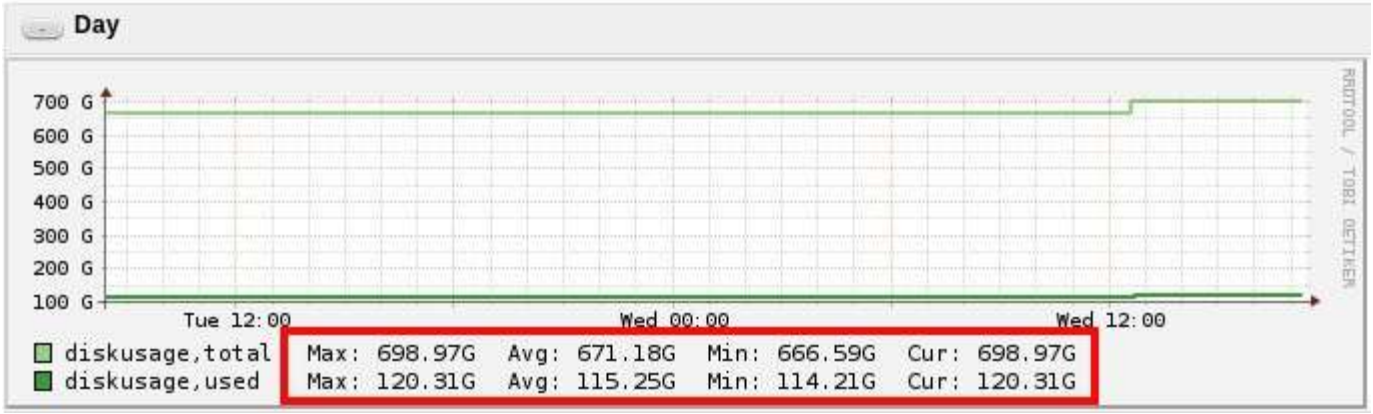
Service State Information

Current Status:	**OK**
Status Information:	DISK OK - free space: /dev/sda2 7862 MB (10%):
Performance Data:	/dev/sda2=69339MB;77180;77190;0;77200
Current Attempt:	1/3
State Type:	HARD
Last Check Type:	ACTIVE
Last Check Time:	12-07-2006 15:26:35
Status Data Age:	0d 0h 1m 45s
Next Scheduled Active Check:	12-07-2006 15:29:35
Latency:	0.073 seconds
Check Duration:	0.054 seconds
Last State Change:	21-05-2006 15:44:02
Current State Duration:	51d 23h 44m 18s
Last Service Notification:	N/A
Current Notification Number:	0
Is This Service Flapping?	N/A
Percent State Change:	N/A
In Scheduled Downtime?	**NO**
Last Update:	12-07-2006 15:28:18

¿Y si graficamos los valores?

Instalar algún plugin tipo NagiosGraph

Ej http://jotaerre.net/2013/07/19/instalacion-de-nagiosgraph-1-4-4-graficos-rrdtool-para-nagios/



¿Qué es un check? Ejemplo:

- Es el programa o script que esta definido en commands.cfg que se corre para alguna revision
- Se puede correr así

```
$ check_http -H 192.168.1.50

HTTP OK HTTP/1.1 200 OK - 332 bytes in 0.004 seconds |time=0.004144s;
;;0.000000 size=332B;;;0
```

http://linux.101hacks.com/unix/check-http/

CUSTOM check

- Uno puede crear su propia revisión…

```
#!/bin/bash
used_space=`df -h / | grep -v Filesystem | awk '{print $5}' | sed 's/%//g'`

case $used_space in
 [1-84]*)
  echo "OK - $used_space% of disk space used."
  exit 0
  ;;
 [85]*)
  echo "WARNING - $used_space% of disk space used."
  exit 1 ;;
 [86-100]*) echo "CRITICAL - $used_space% of disk space used."
  exit 2
  ;; *)
  echo "UNKNOWN - $used_space% of disk space used." exit 3 ;; esac
```

https://www.digitalocean.com/community/articles/how-to-create-nagios-plugins-with-bash-on-ubuntu-12-10

¿Existirán checks adicionales libres ya creados?

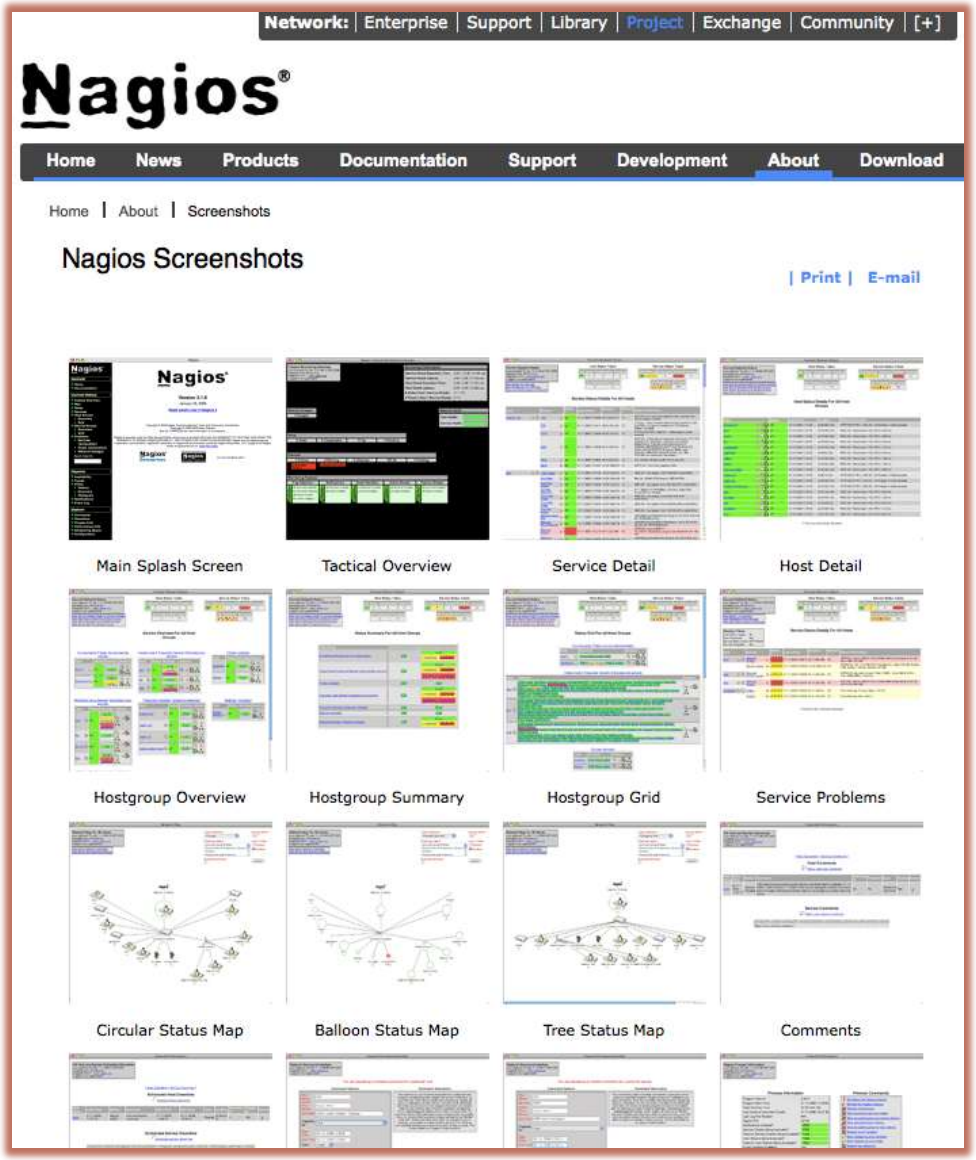
- http://exchange.nagios.org/directory/Plugins
- *http://mathias-kettner.de/check_**mk**.html*
- *http://nagios.manubulon.com/*

You can also download the all the plugins with install script : nagios-snmp-plugins.1.1.1.tgz

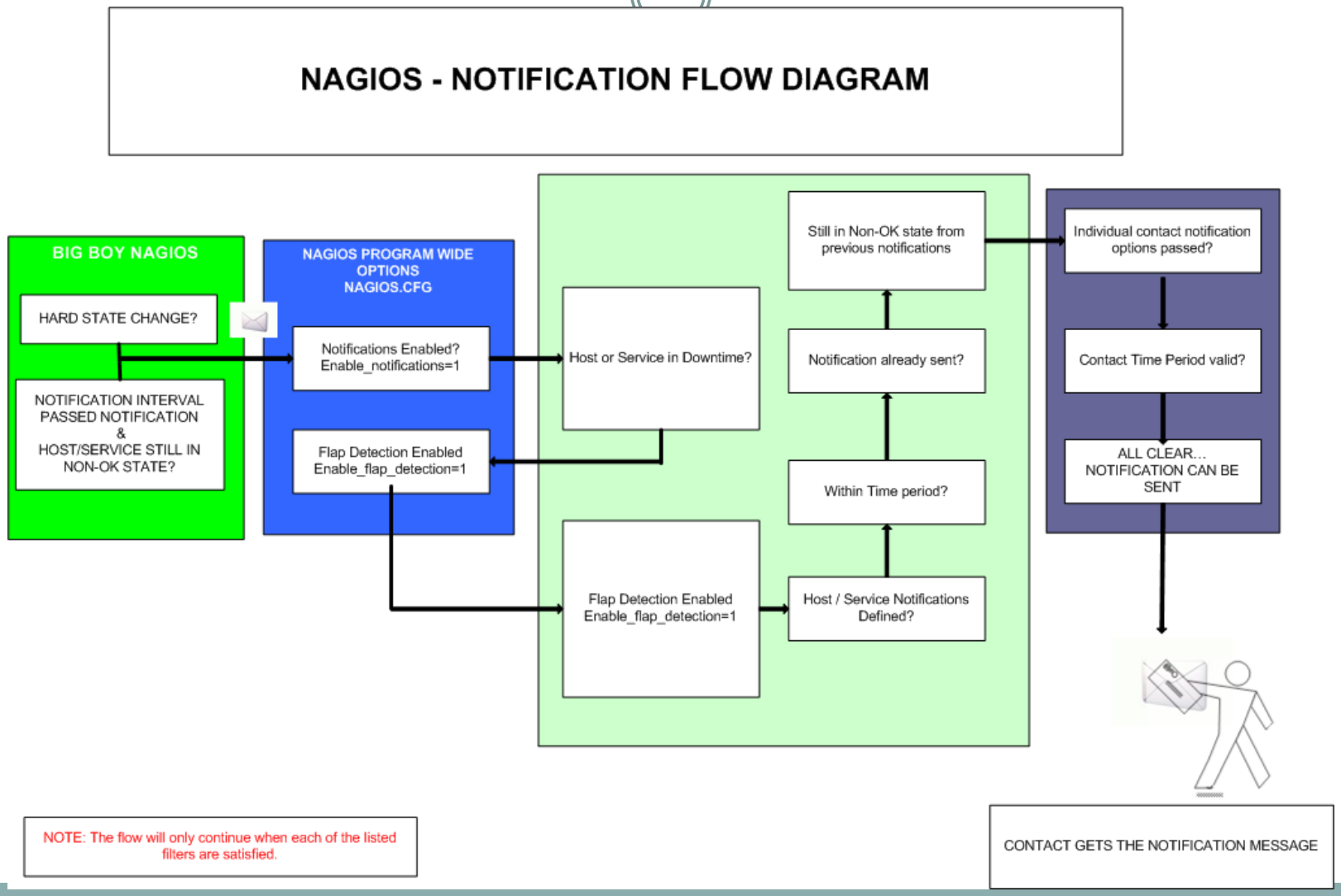
Script detail page	Description	performance output	Supported platforms / snmp agents	Download	Version
Full C package	All the rewritten scripts in C : check_snmp_int, check_snmp_process, check_snmp_storage			nagios-plugins-snmp-0.6.0.tgz	0.6.0
Full perl package	All the scripts with install script in a tgz file or in a rpm file for FC6.			nagios-snmp-plugins.1.1.1.tgz nagios-plugins-snmp-extras-1.1-1.noarch.rpm	1.1.1
check_snmp_storage	checks storages (disks, swap, memory, etc...)	Yes	All MIB-2 compliant	check_snmp_storage.pl	
check_snmp_int	checks interface states, usage on hosts, switch, routers, etc....	Yes	All MIB-2 compliant	check_snmp_int.pl	
check_snmp_process	checks if process are running, the number that are running, memory and cpu used.	No	All MIB-2 compliant	check_snmp_process.pl	
check_snmp_load	checks the load or the cpu of a machine	Yes	Linux, Windows, Cisco, AS400, HP Procurve, LinkProof, Blucoat, Nokia, Fortinet, Netscreen,HP-UX.	check_snmp_load.pl	
check_snmp_vrrp	checks the interface state of vrrp cluster	No	Nokia IP (VRRP & Clustering), LinkProof, Alteon	check_snmp_vrrp.pl	
check_snmp_cpfw	checks Checkpoint Firewall-1 status	Yes	Checkpoint Firewall-1	check_snmp_cpfw.pl	
check_snmp_mem	Checks memory and swap usage	Yes	Linux/Net-snmp, Cisco, HP Switch	check_snmp_mem.pl	
check_snmp_win	Checks windows services	No	Windows	check_snmp_win.pl	
check_snmp_css	Checks css services state	No	CSS	check_snmp_css.pl	
check_snmp_env	Checks environemental status (fan, temp, power supply).	No	Cisco, Nokia, Bluecoat, IronPort, Foundry	check_snmp_env.pl	
check_snmp_nsbox	Checks nsbox vhost & diode status.	No	NetSecureOne Netbox	check_snmp_nsbox.pl	
check_snmp_boostedge	Checks Boostedge services	No	Boostedge	check_snmp_boostedge.pl	
check_snmp_linkproof_nhr	Checks linkproof NHR	No	Radware Linkproof	check_snmp_linkproof_nhr.pl	

VISTAS DEL INTERFASE WEB:

- Táctico
- Mapa
- Detalle de Hosts
- Detalle de Servidores
- HostGroup Grid
- Status Map
- Disponibilidad
- Eventos
- ETC ETC



Notificaciones



¿Cómo se comunican los clientes?

http://www.kilala.nl/Sysadmin/index.php?id=708

A quick comparison

	SSH	NRPE	SNMP	SNMP traps	NSCA
Connection initiation	Srv -> Clnt	Srv -> Clnt	Srv -> Clnt	Clnt -> Srv	Clnt -> Srv
Security	Encryption TCP wrappers Key pairs	Encryption Access List TCP wrappers	Access List (v2) Password (v3)	Access List (v2) Password (v3) TCP wrappers	Encryption Access List TCP wrappers
Configuration	On server	On client	On client	On client and On server	On client
Difficulty	Easy	Moderate	Hard	Hard	Moderate

Conclusiones / Recomendaciones

- No es lo mismo tener Nagios funcionando con localhost monitoreado, que tener monitoreado la totalidad de servicios críticos de la totalidad de los hosts críticos mostrando valores correctos y notificando a los destinatarios en secuencia y horario correctos
- Una vez que se tienen buenos datos se obtiene automática la información necesaria para la planificación de crecimiento, la detección temprana de fallas, el respaldo auditable de revisiones realizadas , etc.
- Si usted esta acostumbrado al «wizard» «yes, yes,yes» y le es muy complicado tocar los archivos de configuración y estudiar a fondo protocolos y sistema operativo, existe la versión paga con soporte NAGIOS que por unos > 10K$US puede monitorear hasta 50 hosts

Algunos links de interés.

http://www.linuxfunda.com/2013/04/02/steps-to-configure-nagiosgraph-with-nagios-core/
http://sachinharma.blogspot.com/2013/08/nagiosgraph-graphs-in-nagios-on_7.html
http://omdistro.org/
http://mathias-kettner.com/check_mk.html
http://exchange.nagios.org/directory/Most_Favoured
http://www.techrepublic.com/blog/linux-and-open-source/nagios-xi-wizards-make-setup-a-snap-for-network-monitoring/2637/#.
https://www.icinga.org/

Gracias!!!