



Monitoreo y Notificaciones

por Eduardo Del Valle

¿Qué significa monitorear?

- Controlar el desarrollo de una acción o un suceso a través de uno o varios monitores."en medicina se monitorea a los enfermos graves para controlar todas sus variables fisiológicas"
- Instalar monitores en un lugar para someterlo a vigilancia."los cajeros automáticos están monitoreados"
- El monitoreo, a rasgos generales, consiste en la observación del curso de uno o más parámetros para detectar eventuales anomalías. Los enfermeros pueden monitorear los signos vitales de un paciente a través de un dispositivo que refleja de manera gráfica los latidos de su corazón; en caso de advertir algún problema, son los encargados de avisar a los médicos.



El valor esta en el servicio

Herramientas de Monitoreo

- Pueden ser básicas o avanzadas
- Manuales o automáticas
- Con notificación o sin ella
- Gratis o pagadas
- Una combinación de todas las anteriores

Herramientas Básicas

- Ping

```
[PulpoPro:~ edelvall$ ping google.com -t 3  
PING google.com (172.217.8.110): 56 data bytes  
64 bytes from 172.217.8.110: icmp_seq=0 ttl=51 time=129.587 ms  
64 bytes from 172.217.8.110: icmp_seq=1 ttl=51 time=130.042 ms  
64 bytes from 172.217.8.110: icmp_seq=2 ttl=51 time=129.942 ms  
  
--- google.com ping statistics ---  
3 packets transmitted, 3 packets received, 0.0% packet loss  
round-trip min/avg/max/stddev = 129.587/129.857/130.042/0.195 ms  
PulpoPro:~ edelvall$
```


Herramientas Básicas

- Ping
- Telnet

```
[PulpoPro:~ edelvall$ telnet google.com 80
Trying 172.217.8.110...
Connected to google.com.
Escape character is '^]'.
.
HTTP/1.0 400 Bad Request
Content-Type: text/html; charset=UTF-8
Referrer-Policy: no-referrer
Content-Length: 1555
Date: Sat, 26 Jan 2019 01:53:59 GMT

<!DOCTYPE html>
<html lang=en>
  <meta charset=utf-8>
  <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width">
  <title>Error 400 (Bad Request)!!1</title>
  <style>
    *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat;-webkit-background-size:100% 100%}}#logo{display:inline-block;height:54px;width:150px}
  </style>
  <a href=//www.google.com/><span id=logo aria-label=Google></span></a>
  <p><b>400.</b> <ins>That's an error.</ins>
  <p>Your client has issued a malformed or illegal request. <ins>That's all we know.</ins>
Connection closed by foreign host.
```


Herramientas Básicas

- Ping
- Telnet
- Traceroute

```
[PulpoPro:~ edelvall$ traceroute google.com
traceroute to google.com (172.217.8.110), 64 hops max, 52 byte packets
 1  192.168.68.1 (192.168.68.1)  1.766 ms  0.828 ms  0.751 ms
 2  190.187.28.169 (190.187.28.169)  1.439 ms  1.608 ms  1.317 ms
 3  10.22.34.177 (10.22.34.177)  3.717 ms  1.964 ms  2.022 ms
 4  10.3.1.25 (10.3.1.25)  2.267 ms
    10.3.1.162 (10.3.1.162)  2.596 ms
    10.3.1.161 (10.3.1.161)  3.936 ms
 5  10.1.2.2 (10.1.2.2)  2.409 ms
    10.3.1.17 (10.3.1.17)  3.022 ms
    10.1.2.2 (10.1.2.2)  2.216 ms
 6  10.1.2.6 (10.1.2.6)  3.847 ms
    10.1.2.2 (10.1.2.2)  2.367 ms
    10.1.2.6 (10.1.2.6)  2.532 ms
 7  ae0-2005.lima4.lim.seabone.net (195.22.222.54)  2.602 ms
    10.76.7.29 (10.76.7.29)  3.317 ms
    186.160.196.1 (186.160.196.1)  4.526 ms
 8  10.76.7.29 (10.76.7.29)  9.144 ms
    ae0-2005.lima4.lim.seabone.net (195.22.222.54)  2.917 ms  2.696 ms
 9  ae0-2005.lima4.lim.seabone.net (195.22.222.54)  2.631 ms
    et1-0-2.santiago1.san.seabone.net (195.22.221.185)  32.071 ms
    et1-0-5.santiago1.san.seabone.net (195.22.221.189)  32.694 ms
10  72.14.216.20 (72.14.216.20)  32.567 ms  33.624 ms  35.435 ms
11  72.14.216.20 (72.14.216.20)  32.683 ms  32.485 ms
    74.125.242.3 (74.125.242.3)  33.666 ms
12  216.239.56.71 (216.239.56.71)  33.787 ms
    74.125.242.19 (74.125.242.19)  33.951 ms
    209.85.244.162 (209.85.244.162)  37.336 ms
13  216.239.62.52 (216.239.62.52)  163.179 ms  163.512 ms  162.838 ms
14  64.233.174.133 (64.233.174.133)  136.402 ms  132.208 ms
    216.239.62.52 (216.239.62.52)  163.421 ms
15  108.170.231.78 (108.170.231.78)  136.463 ms  182.450 ms
    64.233.174.133 (64.233.174.133)  175.199 ms
16  108.170.249.1 (108.170.249.1)  172.533 ms  137.664 ms
    108.170.249.17 (108.170.249.17)  131.369 ms
17  108.170.226.255 (108.170.226.255)  135.735 ms
    108.170.227.1 (108.170.227.1)  135.047 ms
    108.170.249.1 (108.170.249.1)  131.341 ms
18  108.170.227.1 (108.170.227.1)  134.220 ms
    mia07s48-in-f14.1e100.net (172.217.8.110)  130.091 ms  129.450 ms
```


Herramientas Avanzadas

- Uso de scripts

----- Verificación de estado de Tuneles y PCs 2017-11-20_19:22:56 -----				
Distribuidor		Tunel		PC
MK-01	-		ALIVE	ALIVE
MK-02	-		ALIVE	ALIVE
MK-03	-		ALIVE	ALIVE
MK-04	-		ALIVE	ALIVE
MK-05	-		ALIVE	ALIVE
MK-06	-		ALIVE	ALIVE
MK-07	-		ALIVE	ALIVE
MK-08	-		ALIVE	ALIVE
MK-10	-		ALIVE	ALIVE
MK-11	-		ALIVE	ALIVE
MK-12	-		ALIVE	ALIVE
MK-13	-		ALIVE	ALIVE
MK-14	-		ALIVE	ALIVE
MK-15	-		ALIVE	ALIVE
MK-16	-		ALIVE	ALIVE
MK-17	-		DOWN ✕	DOWN ✕
MK-19	-		ALIVE	DOWN ✕
MK-20	-		ALIVE	ALIVE
MK-21	-		ALIVE	ALIVE
MK-22	-		ALIVE	ALIVE
MK-23	-		ALIVE	ALIVE
MK-24	-		ALIVE	ALIVE
MK-25	-		ALIVE	ALIVE

Herramientas Avanzadas

- Uso de scripts

	ALIVE	ALIVE
	ALIVE	ALIVE
	ALIVE	ALIVE
	ALIVE	ALIVE
	DOWN	DOWN
cas	ALIVE	DOWN
	ALIVE	ALIVE
nen	ALIVE	ALIVE
a	ALIVE	ALIVE
si	ALIVE	ALIVE

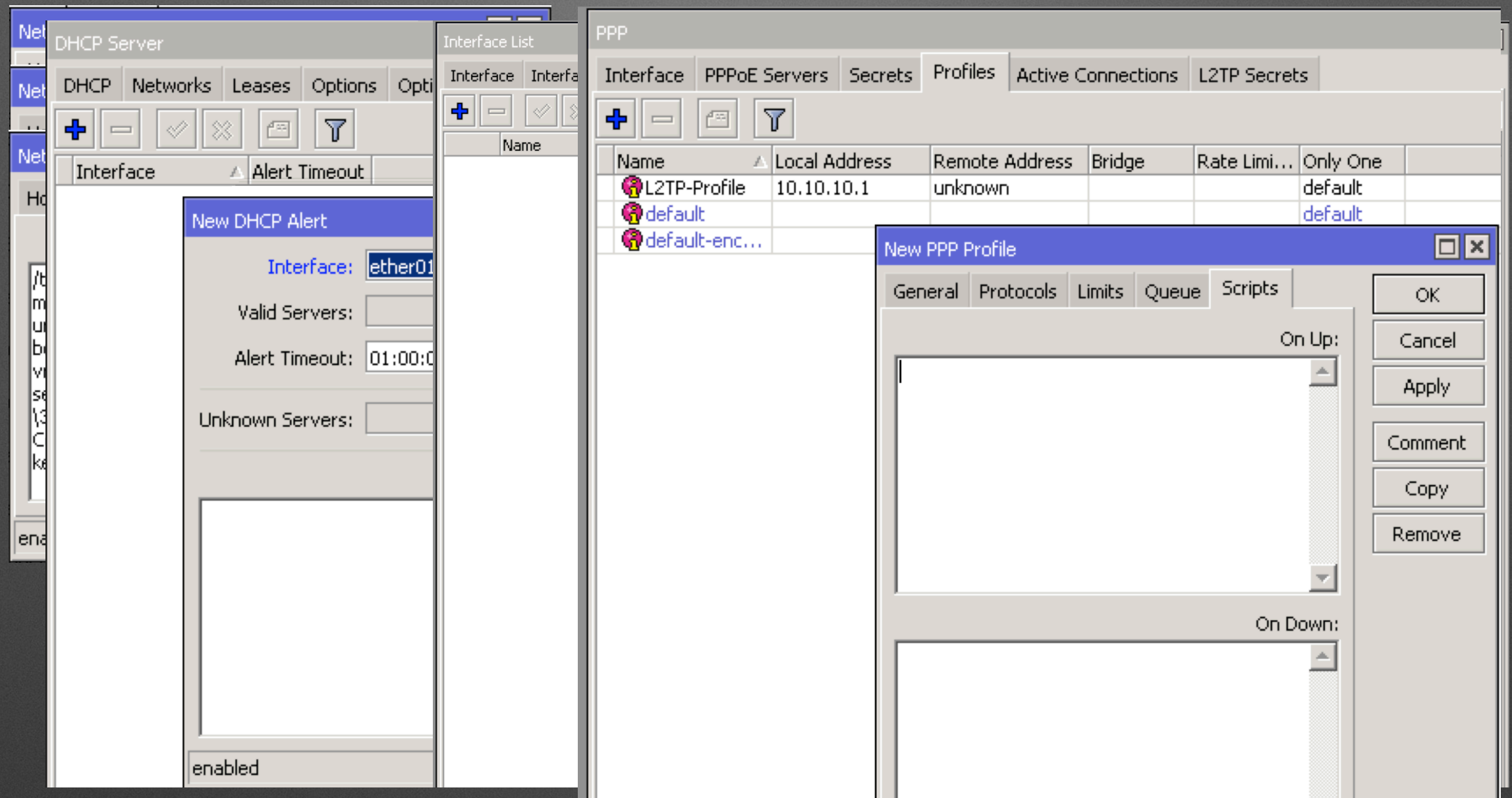
----- Verificación de estado de Tuneles y PCs 2017-11-20_19:22:56 -----			
Distribuidor		Tunel	PC
MK-01 -		ALIVE	ALIVE
MK-02 -		ALIVE	ALIVE
MK-03 -		ALIVE	ALIVE
MK-04 -		ALIVE	ALIVE
MK-05 -		ALIVE	ALIVE
MK-06 -		ALIVE	ALIVE
MK-07 -		ALIVE	ALIVE
MK-08 -		ALIVE	ALIVE
MK-10 -		ALIVE	ALIVE
MK-11 -		ALIVE	ALIVE
MK-12 -		ALIVE	ALIVE
MK-13 -		ALIVE	ALIVE
MK-14 -		ALIVE	ALIVE
MK-15 -		ALIVE	ALIVE
MK-16 -		ALIVE	ALIVE
MK-17 -		DOWN	DOWN
MK-19 -		ALIVE	DOWN
MK-20 -		ALIVE	ALIVE
MK-21 -		ALIVE	ALIVE
MK-22 -		ALIVE	ALIVE
MK-23 -		ALIVE	ALIVE
MK-24 -		ALIVE	ALIVE
MK-25 -		ALIVE	ALIVE

Herramientas Avanzadas

- Uso de scripts
- Unix bash o similar
- Windows batch
- Python
- Mikrotik scripts

```
#!/bin/bash
# Program name: pingall.sh
IFS=","
RED=$(tput setaf 1)
GREEN=$(tput setaf 2)
BLUE=$(tput setaf 4)
REVERSE=$(tput smso)
NORMAL=$(tput sgr0)

cd /Users/edellvall/Google\ Drive/Gloria
echo
echo "-----"
echo " Verificación de estado de Tuneles y PCs "
printf " "
date +%F_%T
echo "-----"
echo
echo "Distribuidor          Tunel    PC"
cat /Users/edellvall/Google\ Drive/Gloria/ips.txt | while read distribuidor tune
l pc
do
    printf "$distribuidor "
    # Ping the tunel
    ping -c 2 "$tunel" > /dev/null
    if [ $? -eq 0 ]; then
        printf "${BLUE}ALIVE    ${NORMAL}"
    else
        #printf "${REVERSE}${RED}DOWN    ${NORMAL}"
        printf "${REVERSE}${RED}DEAD\xE2\x98\xA0${NORMAL}    "
    fi
    # Ping the pc
    ping -c 2 "$pc" > /dev/null
    if [ $? -eq 0 ]; then
        printf "${BLUE}ALIVE    ${NORMAL}\n"
    else
        printf "${REVERSE}${RED}DEAD\xE2\x98\xA0${NORMAL}\n"
    fi
done
echo
/Users/edellvall/Google\ Drive/Gloria/pinger.sh (END)
```

¿Dónde ponerlos?

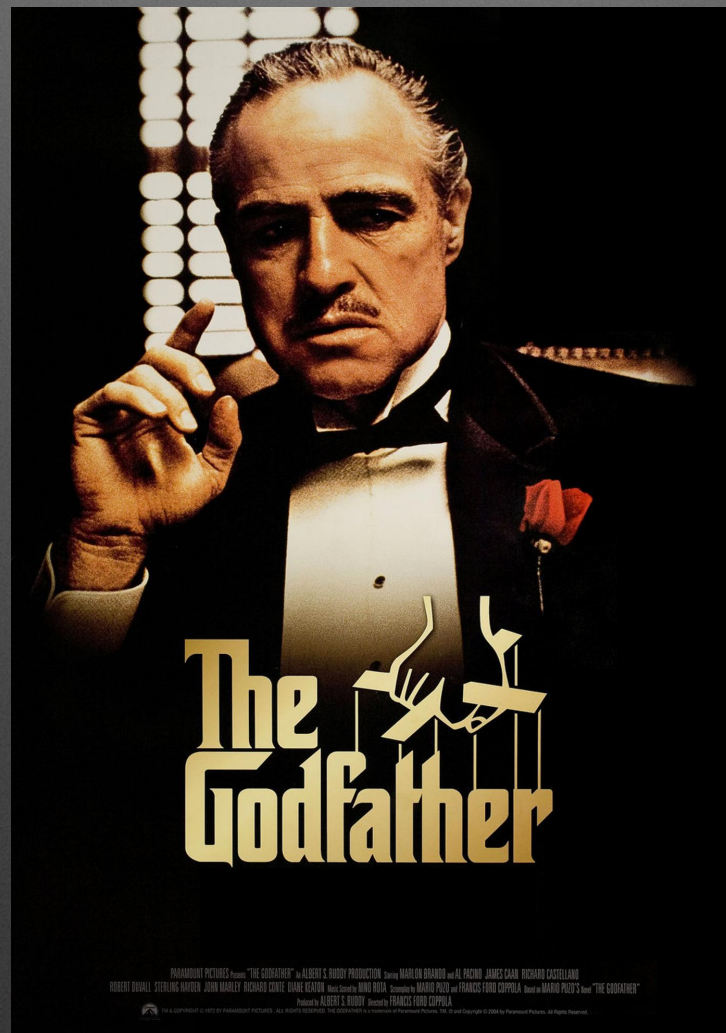
los scripts en MikroTik

Telegram

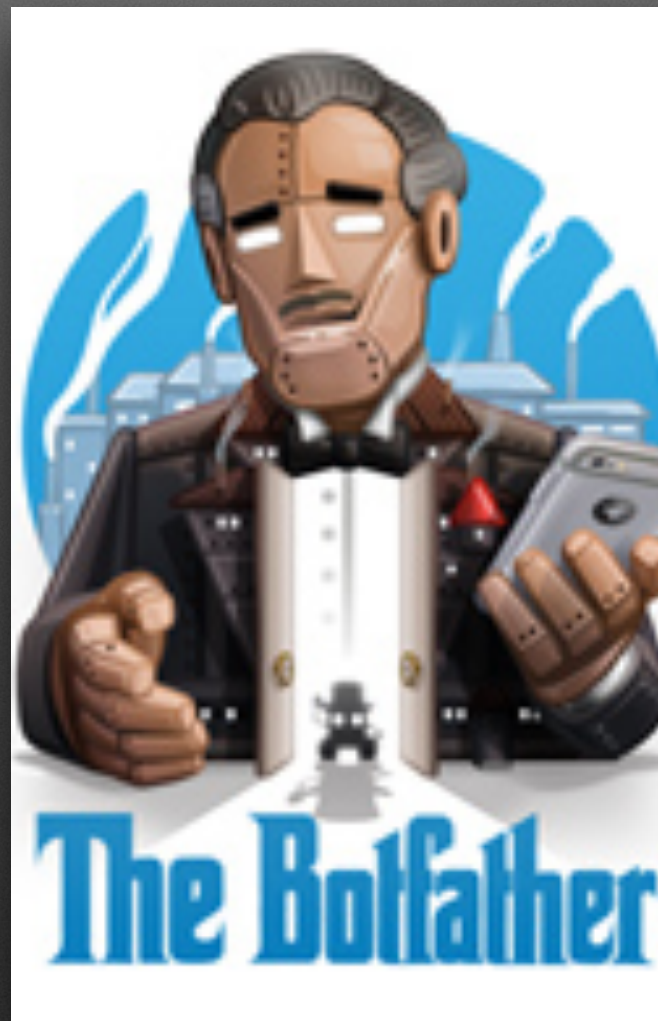


<https://telegram.org/>

El Padrino

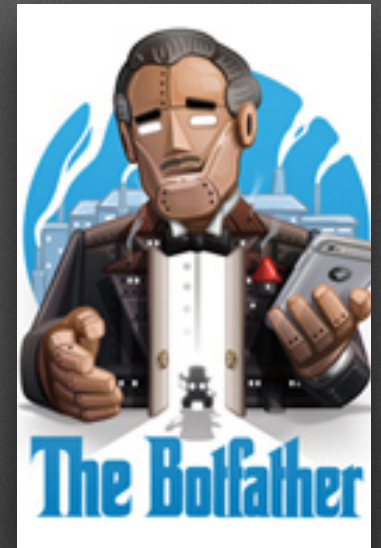


El Botfather



¿Cómo se usa?

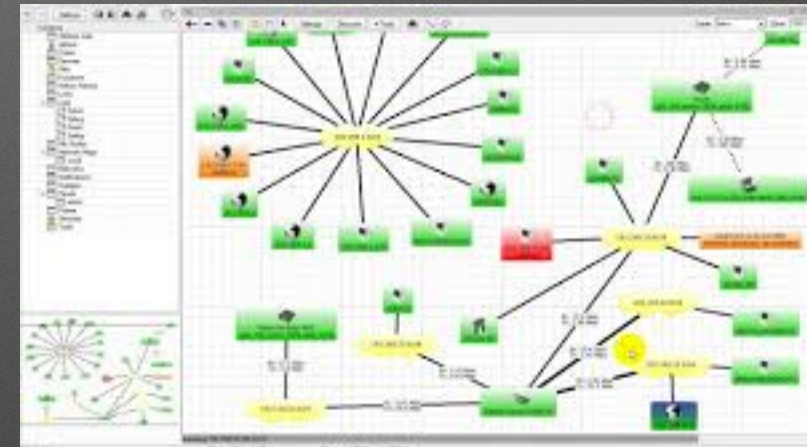
- Creat el BOT
 - /newbot
- Nombre común
- Nombre interno
- Token: 742282904:AAH_w9mYJXWNMqRV_ue1ToJIVFhg8PRsuL4
- Script generico:
 - /tool fetch mode=https http-method=get url="https://api.telegram.org/bot[token]/sendMessage\3Fchat_id=[chat_id]&text=[texto]" keep-result=no



Demo

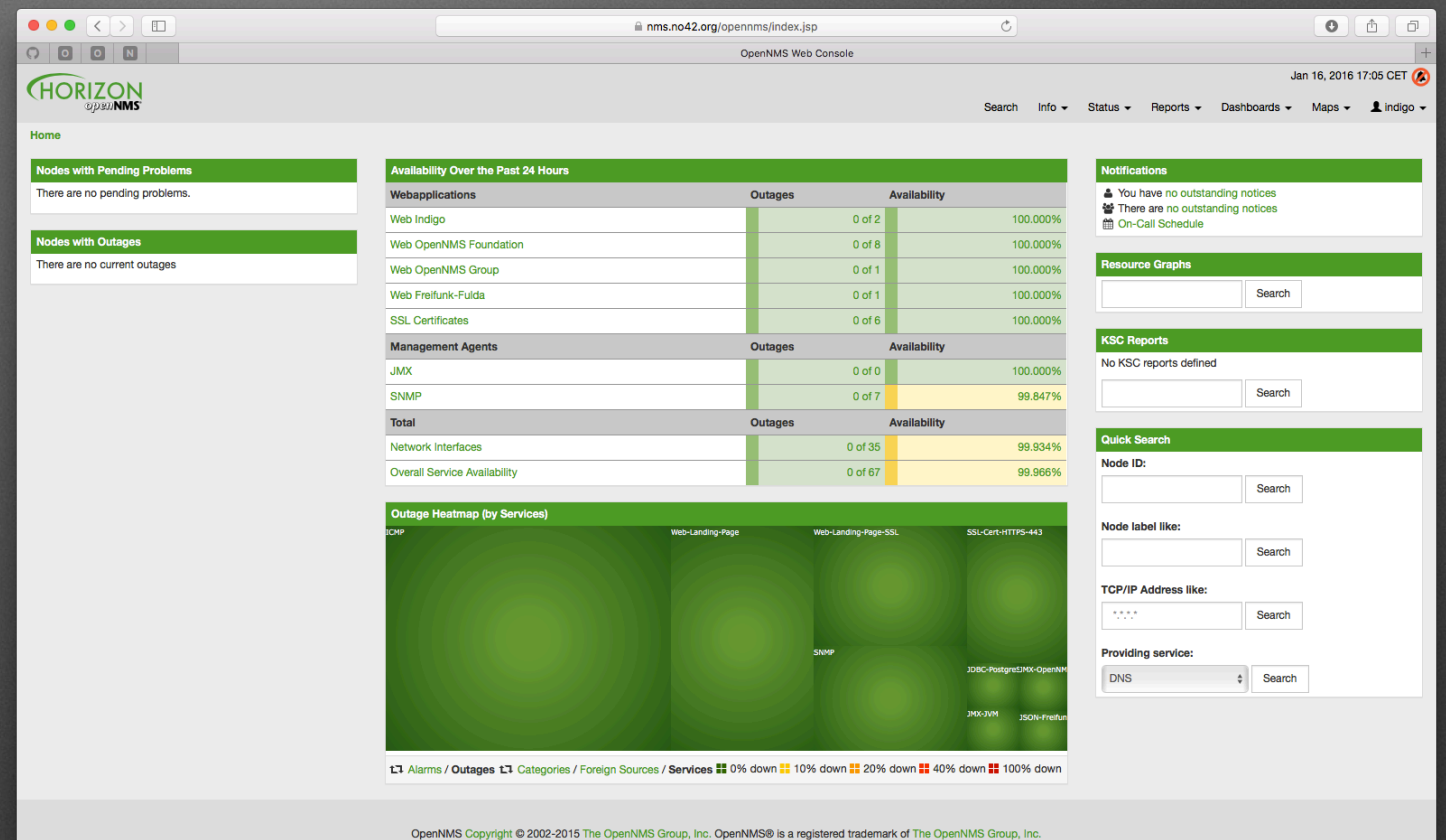
¿Qué viene después?

- Notificaciones
- Aplicaciones
- Dude



¿Qué viene después?

- Notificaciones
- Aplicaciones
 - Dude
 - OpenNMS



¿Qué viene después?

- Notificaciones
- Aplicaciones
 - Dude
 - OpenNMS
 - Oráculo de MKE Solutions

Q Events Viewer

Search Next Rows: 10 Type: ALL Category: ALL Category Device: ALL Devices READ Filter Search

Prev Next

Date	Type	Status	Device	Category	Variable	Value Before	Actual Value	Details
Tuesday at 5:15am	WARNING	UNREAD	Router Casa PAPA Maxi / 192.168.20.1 MKE Solutions	backup	export	NA	→ NA	Remote Backup too small size=
Tuesday at 3:48am	WARNING	UNREAD	Core Sauce / 1.1.2.234 MKE Solutions	ping	down	N/A	→ N/A	Device is DOWN since 5 minutes ago
Tuesday at 3:00am	WARNING	UNREAD	Server Alameda / 1.1.2.206 MKE Solutions	reboot	uptime	13:09:01	→ 00:00:59	Reboot Device
Tuesday at 2:10am	INFO	UNREAD	Router BGP / 1.1.2.244 MKE Solutions	bgp	uptime	3d23:48:29	→ 00:02:09	Change value for peer BGP
Tuesday at 2:00am	INFO	UNREAD	Octavia Core / 1.1.3.16 Testing Debug	interface	link-downs	1	→ 2	Change for Interface ether10 Value (link-downs)
Tuesday at 1:37am	WARNING	UNREAD	Core Sauce / 1.1.2.234 MKE Solutions	ping	down	N/A	→ N/A	Device is DOWN since 5 minutes ago
Monday at 11:20pm	WARNING	UNREAD	Core Sauce / 1.1.2.234 MKE Solutions	ping	down	N/A	→ N/A	Device is DOWN since 5 minutes ago
Monday at 9:35pm	WARNING	UNREAD	Level 3 - / 1.1.2.220 MKE Solutions	reboot	uptime	1w5d10:38:07	→ 00:09:26	Reboot Device
Monday at 9:17pm	WARNING	UNREAD	Level 3 - / 1.1.2.220 MKE Solutions	ping	down	N/A	→ N/A	Device is DOWN since 5 minutes ago
Monday at 1:50pm	WARNING	UNREAD	Server Alameda / 1.1.2.206 MKE Solutions	reboot	uptime	00:15:03	→ 00:04:01	Reboot Device

¿Qué viene después?

- Notificaciones
- Aplicaciones
- Dude
- OpenNMS
- Oráculo de MKE Solutions
- Dashboards



Siguientes pasos

- Experimenten
- SI en Sandbox NO en Producción
- Sigam curiosos
- Pregunten
- Comparense
- Aspiren a más



Gracias!