

Ingeniería de Servidores (2014-2015)
GRADO EN INGENIERÍA INFORMÁTICA
UNIVERSIDAD DE GRANADA

Memoria Practica 3

Ignacio Romero Cabrerizo

29 de noviembre de 2014

Índice

1. Cuestión 1. 5.a) ¿Qué archivo le permite ver qué programas se han instalado con el gestor de paquetes? 5.b) ¿Qué significan las terminaciones .1.gz o .2.gz de los archivos en ese directorio?	5
2. Cuestión 2. ¿Qué archivo ha de modificar para programar una tarea? Escriba la línea necesaria para ejecutar una vez al día una copia del directorio ~/codigo a ~/seguridad/\$fecha donde \$fecha es la fecha actual	5
3. Cuestión 3. Pruebe a ejecutar el comando, conectar un dispositivo USB y vuelva a ejecutar el comando. Copie y pegue la salida del comando. (considere usar dmesg tail). Comente qué observa en la información mostrada	6
4. Cuestión 4. Ejecute el monitor de «System Performance» y muestre el resultado. Incluya capturas de pantalla comentando la información que aparece	7
5. Cuestión 5. Cree un recopilador de datos definido por el usuario (modo avanzado) que incluya tanto el contador de rendimiento como los datos de seguimiento: Todos los referentes al procesador, al proceso y al servicio web. Intervalo de muestra 15 segundos. Almacene el resultado en el directorio Escritorio logs	10
6. Cuestión 6. Instale alguno de los monitores comentados arriba en su máquina y pruebe a ejecutarlos (tenga en cuenta que si lo hace en la máquina virtual, los resultados pueden no ser realistas). Alternativamente, busque otros monitores para hardware comerciales o de código abierto para Windows y Linux	12
7. Cuestión 7. Visite la web del proyecto y acceda a la demo que proporcionan (http://demo.munin-monitoring.org/) donde se muestra cómo monitorizan un servidor. Monitorice varios parámetros y haga capturas de pantalla de lo que está mostrando comentando qué observa	13
8. Cuestión 8. Escriba un breve resumen sobre alguno de los artículos donde se muestra el uso de strace o busque otro y coméntelo	14
9. Cuestión 9. Acceda a la consola mysql (o a través de phpMyAdmin) y muestre el resultado de mostrar el "profile" de una consulta	15
10. Cuestión opcional 2: instale Nagios en su sistema (el que prefiera) documentando el proceso y muestre el resultado de la monitorización de su sistema comentando qué aparece	17
11. Cuestión Opcional 3. Haga lo mismo con Munin	20

12.Cuestión Opcional 6. Instale el monitor (AWSTATS) y muestre y comente algunas capturas de pantalla 20

Índice de figuras

2.1. Archivo crontab del sistema	5
3.1. Muestra del uso del puerto USB	6
4.1. Resultados System Performance	7
4.2. Información CPU	8
4.3. Información Procesador	9
4.4. Información Memoria	9
5.1. Recopilador Definido por usuario	10
5.2. Configuración Recopilador de Datos	10
5.3. Paso 3. Selección de contadores e instancias	11
5.4. Configuración Recopilador de Datos	11
6.1. Resultados Open Hardware Monitor	12
7.1. Resultados Munin Demo	13
7.2. Resultados Munin Demo Firewall	14
8.1. Strace a un proceso por su PID	14
8.2. Strace a un proceso y subprocesos	15
9.1. SQL Profiling	15
9.2. Sentencia SQL	16
9.3. mySQL QUERY 1	16
9.4. mySQL PROFILE	17
10.1. Monitorización con Nagios	19
11.1. Monitorización con Ganglia	20
12.1. Archivo awstats.conf	21
12.2. Configuración de awstats	21
12.3. Archivo Default de apache	21
12.4. Funcionamiento Awstats	22

1. **Cuestión 1. 5.a) ¿Qué archivo le permite ver qué programas se han instalado con el gestor de paquetes?**
5.b) ¿Qué significan las terminaciones . 1.gz o .2.gz de los archivos en ese directorio?

Podemos ver el registro de programas instalados mediante el gestor de paquetes (dpkg) desde:

```
cat /var/log/dpkg.log
```

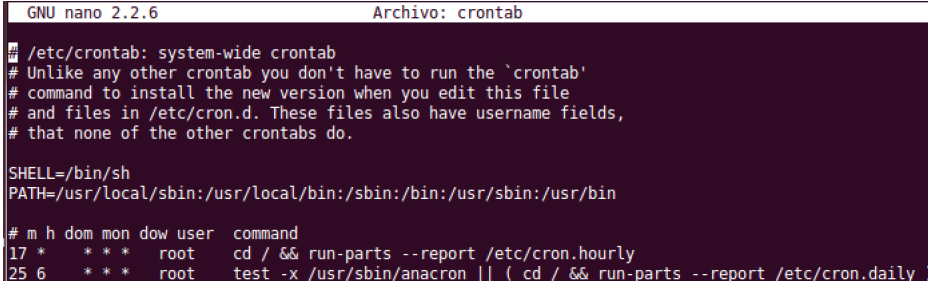
También podemos hacerlo en gnome-system-log de forma visual como se indica en la pregunta.

1.gz, 2.gz es la forma que tiene el cron de Linux de comprimir y almacenar los archivos del log del sistema pues con el paso del tiempo acaban siendo muy extensos.

2. **Cuestión 2. ¿Qué archivo ha de modificar para programar una tarea? Escriba la línea necesaria para ejecutar una vez al día una copia del directorio ~/codigo a ~/seguridad/\$fecha donde \$fecha es la fecha actual**

El fichero de configuración principal a modificar del cron es:

```
/etc/crontab
```



```
GNU nano 2.2.6 Archivo: crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
```

Figura 2.1: Archivo crontab del sistema

Lo editamos y añadimos la siguiente línea para que cada día a la 1am realice la tarea deseada:

```
01 1 *** root cp ~r ~/codigo ~/seguridad/$(date +%F)
```

Reiniciamos el demonio de crond: `service crond restart`

3. Cuestión 3. Pruebe a ejecutar el comando, conectar un dispositivo USB y vuelva a ejecutar el comando. Copie y pegue la salida del comando. (considere usar `dmesg | tail`). Comente qué observa en la información mostrada

```
nachorc@nachorc-Parallels-Virtual-Platform: ~
nachorc@nachorc-Parallels-Virtual-Platform:~$ dmesg | tail
[ 7.938796] usb 1-2: New USB device strings: Mfr=1, Product=2, SerialNumber=3
[ 7.938798] usb 1-2: Product: Virtual Printer (Print to PDF (Mac Desktop))
[ 7.938800] usb 1-2: Manufacturer: Parallels
[ 7.938802] usb 1-2: SerialNumber: TAG11d87aca0
[ 7.978493] usb1p 1-2:1.0: usb1p0: USB Unidirectional printer dev 3 if 0 alt 0 proto 1 vid 0x203A pid 0xFFFF
[ 7.978519] usbcore: registered new interface driver usb1p
[ 10.304377] init: plymouth-stop pre-start process (2271) terminated with status 1
[ 10.569482] audit_printk_skb: 162 callbacks suppressed
[ 10.569485] type=1400 audit(1416408012.745:65): apparmor="DENIED" operation="capable" profile="/usr/sbin/cupsd" pid=637 comm="cupsd" capability=36 capname="block_suspend"
[ 14.636474] type=1400 audit(1416408016.813:66): apparmor="DENIED" operation="capable" profile="/usr/sbin/cupsd" pid=637 comm="cupsd" capability=36 capname="block_suspend"
nachorc@nachorc-Parallels-Virtual-Platform:~$ dmesg | tail
[ 26.460871] type=1400 audit(1416408028.627:67): apparmor="DENIED" operation="open" profile="/usr/lib/telepathy/mission-control-5" name="/usr/share/gvfs/remote-volume-monitors/" pid=2876 comm="mission-control" requested_mask="r" denied_mask="r" fsuid=1000 ouid=0
[ 62.827583] usb 1-3: new high-speed USB device number 4 using ehci-pci
[ 62.962875] usb 1-3: New USB device found, idVendor=2717, idProduct=0360
[ 62.962881] usb 1-3: New USB device strings: Mfr=1, Product=2, SerialNumber=3
[ 62.962884] usb 1-3: Product: MI 3W
[ 62.962886] usb 1-3: Manufacturer: Xiaomi
[ 62.962888] usb 1-3: SerialNumber: 93f8e0
[ 63.010959] usb-storage 1-3:1.1: USB Mass Storage device detected
[ 63.011178] scsi8 : usb-storage 1-3:1.1
[ 63.011351] usbcore: registered new interface driver usb-storage
```

Figura 3.1: Muestra del uso del puerto USB

Se observa en la salida del comando los detalles del puerto USB así como su configuración.

Al conectar una unidad al puerto y ejecutar de nuevo el comando, indica que ha encontrado un dispositivo con características como el `idProduct`, el nombre del dispositivo (MI 3W), el fabricante (Xiaomi) o `nº` de serie.

Una forma de obtener información más detallada del puerto USB:

```
dmesg | grep -i usb
```

4. Cuestión 4. Ejecute el monitor de «System Performance» y muestre el resultado. Incluya capturas de pantalla comentando la información que aparece

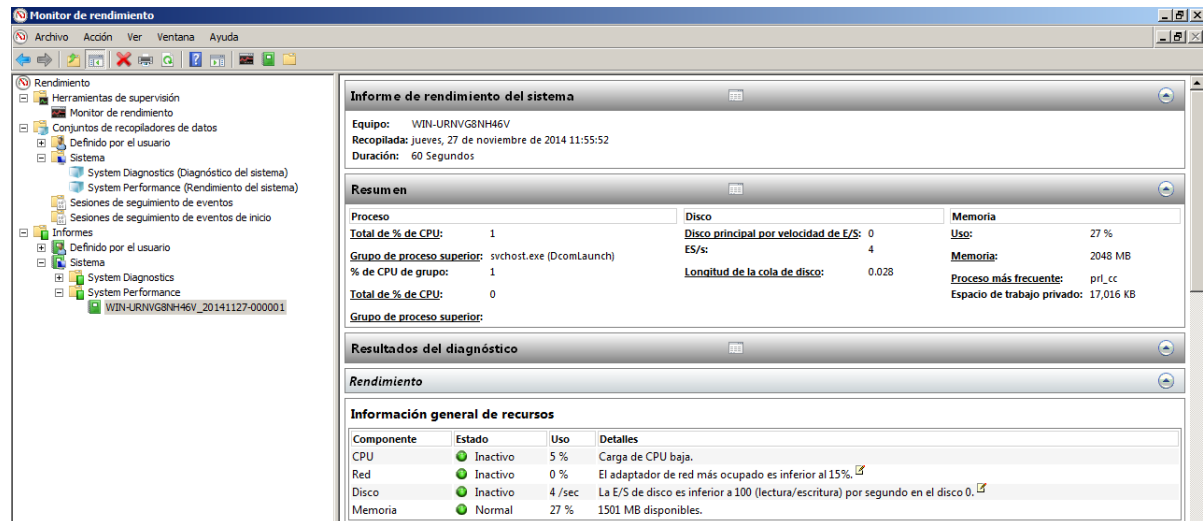


Figura 4.1: Resultados System Performance

Tras ejecutar el System Performance de Windows Server, obtenemos un diagnóstico detallado del sistema y de cada componente del equipo y su funcionamiento.

Como se observa en la imagen anterior, System Performance muestra un **resumen** global indicando los usos de CPU, Memoria y Disco. Además de este resumen se detallan individualmente cada uno de la siguiente forma:

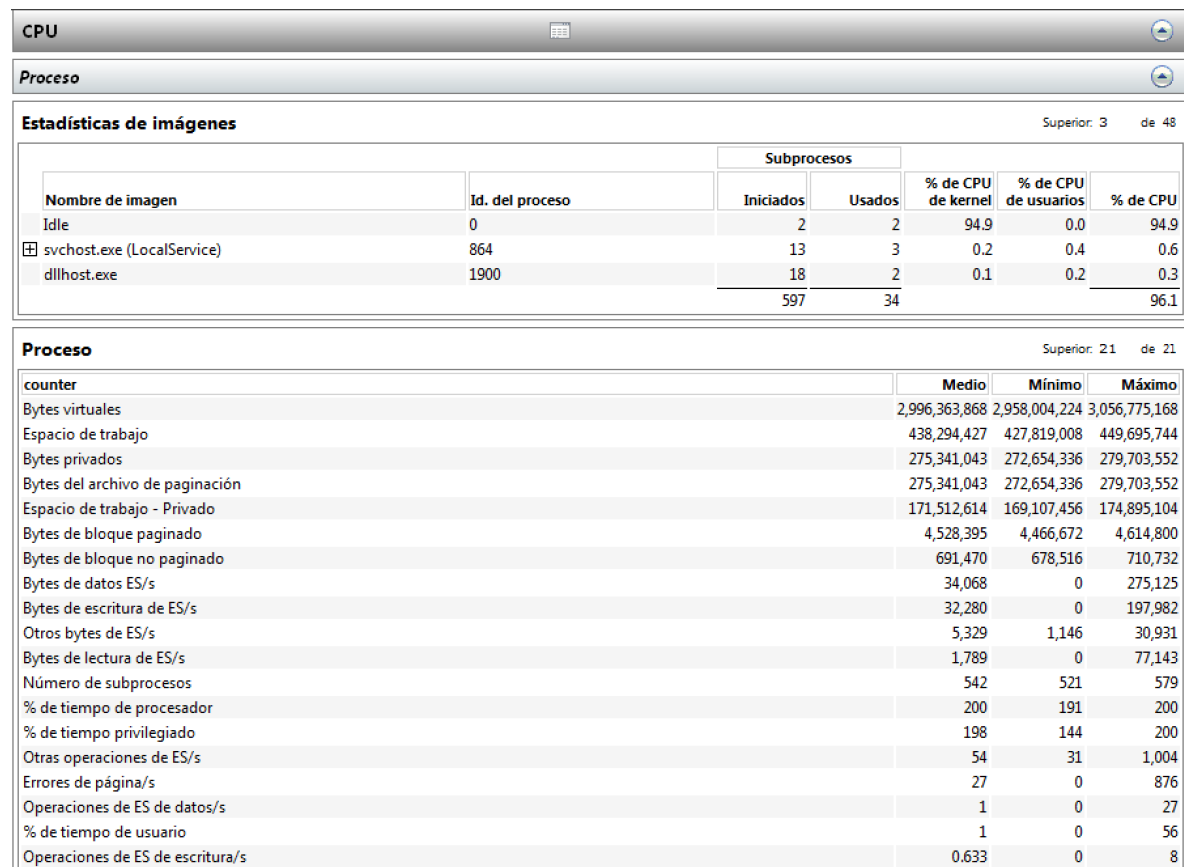


Figura 4.2: Información CPU

En la información detallada de la CPU se obtienen los usos medios, mínimos y máximos de los contadores del sistema, así como los subprocesos que están corriendo actualmente. Tenemos información también de la Red (TCP, IP ó UDP), el Disco Duro o la Memoria, donde se muestran los Procesos, su Id y el espacio de trabajo que usan al igual que la memoria que utilizan.

Procesador				Superior: 9 de 9
counter	Medio	Mínimo	Máximo	
Interrupciones/s	152	134	515	
% de tiempo inactivo	99	52	100	
DPC en cola/s	13	4	96	
% de tiempo de procesador	1	0	48	
% de tiempo de usuario	0.65	0	28	
% de tiempo privilegiado	0.507	0	20	
Velocidad de DPC	0.148	0	5	
% de tiempo de DPC	0.026	0	0.781	
% de tiempo de interrupción	0.013	0	0.781	

Tiempo de usuario del procesador por CPU				Superior: 3 de 3
Instancia	Medio	Mínimo	Máximo	
1	1.039	0	45	
0	1	0	52	
_Total	1	0	48	

Interrupciones del procesador por CPU				Superior: 3 de 3
Instancia	Medio	Mínimo	Máximo	
_Total	152	134	515	
0	81	70	277	
1	71	64	239	

Figura 4.3: Información Procesador

Red	
TCP	
Interfaz	
IP	
UDP	
Disco	
Archivos activos	
División de disco	
Disco físico	
Memoria	
Proceso	

Memoria						Superior: 10 de 48
Proceso	Id. del proceso	Confirmar (KB)	Espacio de trabajo (KB)	Compartible (KB)	Privado (KB)	
pri_cc	2896	136,748	27,444	10,428	17,016	
Oobe	2088	599,648	40,544	26,812	13,732	
svchost##3	816	151,628	29,596	16,612	12,984	
mmc	2696	167,652	28,436	16,988	11,448	
explorer	2772	183,648	29,736	19,028	10,708	
svchost##2	756	47,184	11,892	4,960	6,932	
svchost##6	952	95,308	15,280	9,008	6,272	
rundll32	1852	67,444	11,744	5,912	5,832	
csrss##1	404	51,228	9,296	3,904	5,392	
svchost##4	864	44,684	10,992	5,876	5,116	

Figura 4.4: Información Memoria

5. Cuestión 5. Cree un recopilador de datos definido por el usuario (modo avanzado) que incluya tanto el contador de rendimiento como los datos de seguimiento: Todos los referentes al procesador, al proceso y al servicio web. Intervalo de muestra 15 segundos. Almacene el resultado en el directorio Escritorio logs

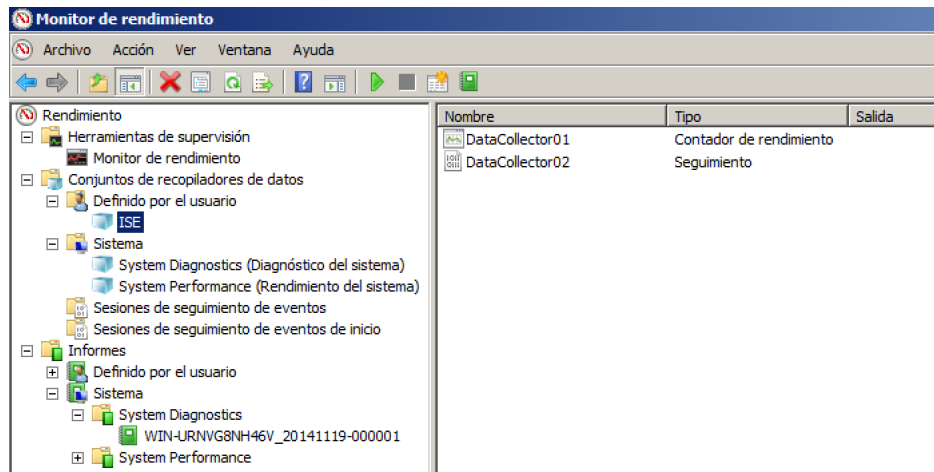
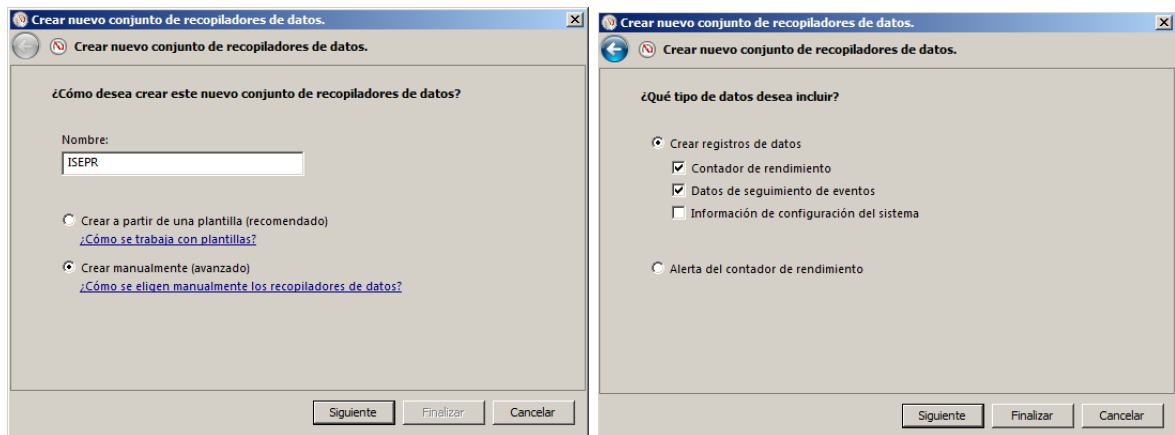


Figura 5.1: Recopilador Definido por usuario



(a) Paso 1. Crear manualmente (avanzado)

(b) Paso 2. Crear registro de datos

Figura 5.2: Configuración Recopilador de Datos

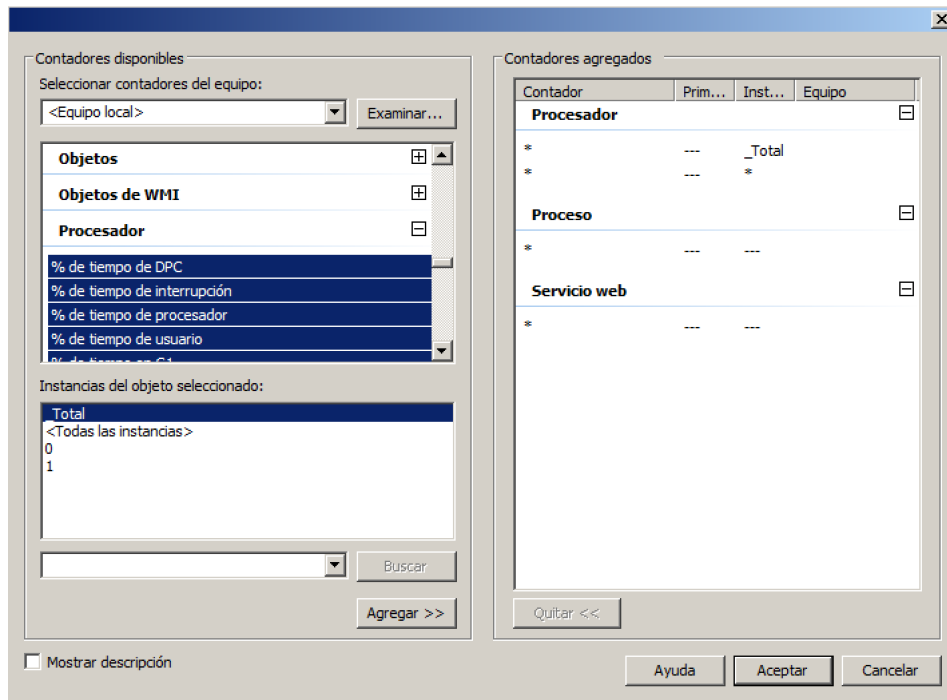
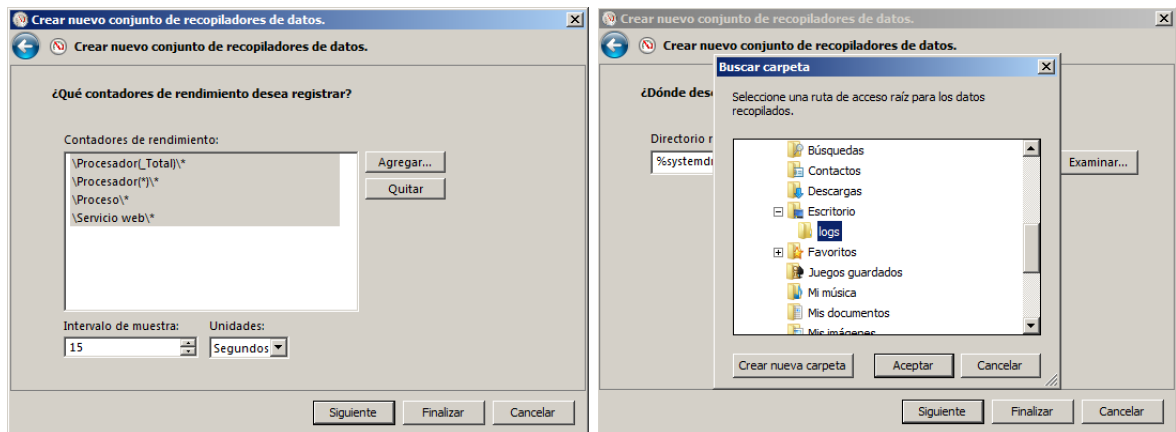


Figura 5.3: Paso 3. Selección de contadores e instancias



(a) Paso 4. Intervalo y Unidades

(b) Paso 5. Elegir ruta creación (nueva carpeta logs en Escritorio)

Figura 5.4: Configuración Recopilador de Datos

6. Cuestión 6. Instale alguno de los monitores comentados arriba en su máquina y pruebe a ejecutarlos (tenga en cuenta que si lo hace en la máquina virtual, los resultados pueden no ser realistas). Alternativamente, busque otros monitores para hardware comerciales o de código abierto para Windows y Linux

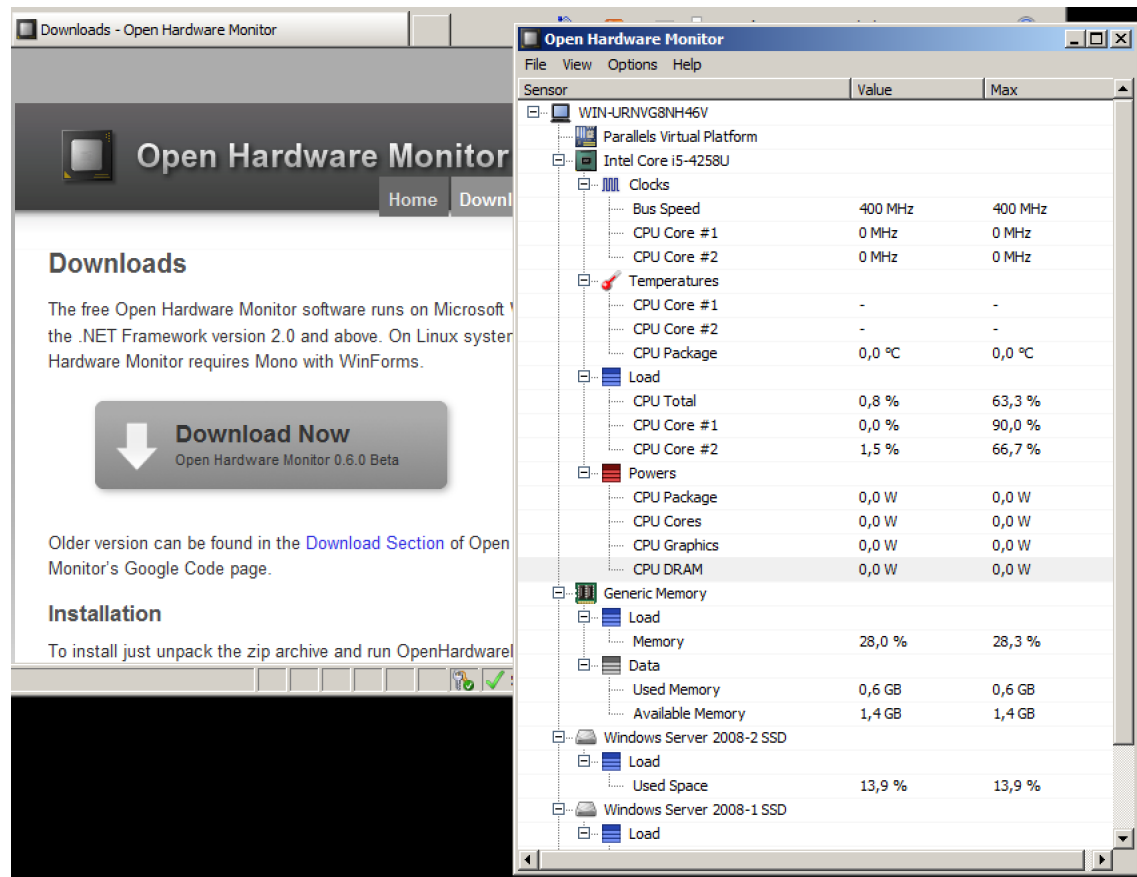


Figura 6.1: Resultados Open Hardware Monitor

OTROS:

AbpMon: <http://www.iarsn.com/abpmon.html>

HWMonitor: <http://www.cpuid.com/softwares/hwmonitor.html>

7. Cuestión 7. Visite la web del proyecto y acceda a la demo que proporcionan (<http://demo.munin-monitoring.org/>) donde se muestra cómo monitorizan un servidor. Monitorice varios parámetros y haga capturas de pantalla de lo que está mostrando comentando qué observa

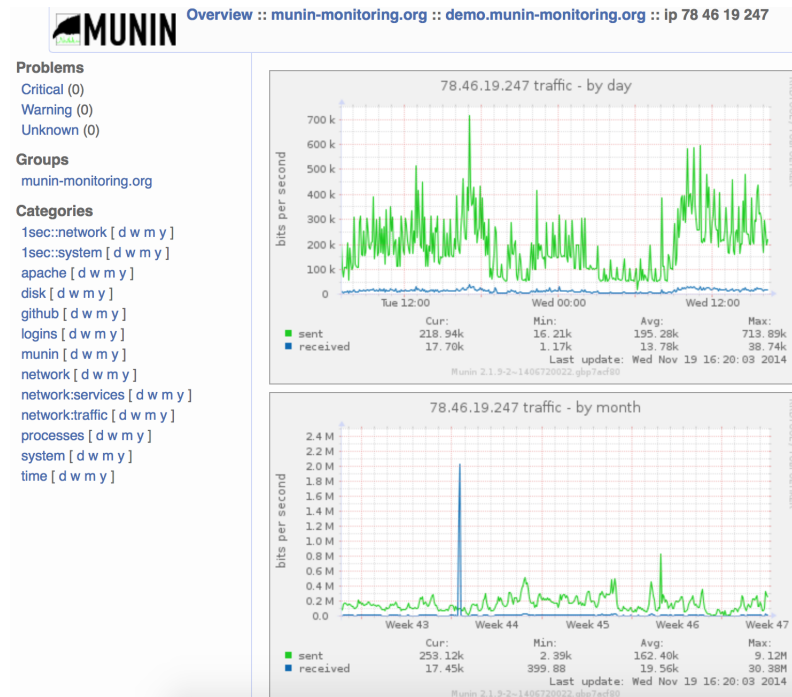


Figura 7.1: Resultados Munin Demo

En el gráfico se puede estudiar en este caso, el tráfico de la red para la IP 78.46.19.247 al día y respecto al mes. Muestra los paquetes enviados y recibidos a lo largo de ese tiempo.

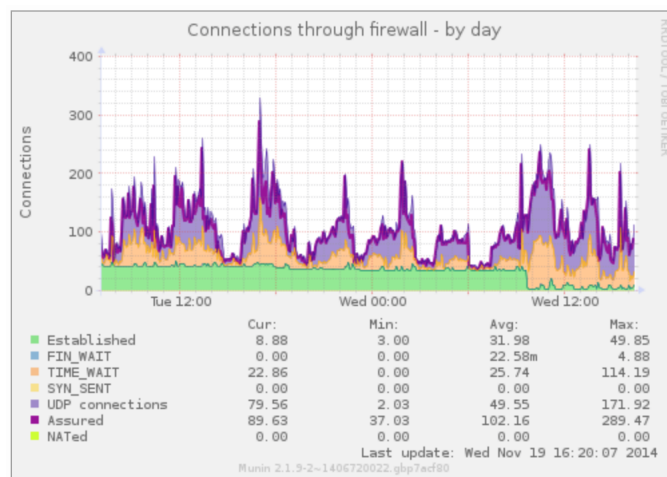


Figura 7.2: Resultados Munin Demo Firewall

En el gráfico anterior se muestra el tráfico (mínimo, máximo y medio) generado por el Firewall durante el día por las diferentes conexiones, desde el UDP a la NAT.

8. Cuestión 8. Escriba un breve resumen sobre alguno de los artículos donde se muestra el uso de strace o busque otro y coméntelo

Strace es una de las mejores utilidades incluidas en la mayoría de distros Linux en monitorización de la ejecución de un programa (llamadas y señales) y detección de fallos. Es una buena forma por ejemplo, de detectar problemas con httpd (si no podemos encontrarlos en el log).

En resumen, strace es capaz de visualizar todas las interacciones de un comando o programa con el sistema viendo todo lo que está haciendo desde que se inicia hasta que finaliza, incluso es capaz de hacerle pruebas de rendimiento y estabilidad.

Podemos obtener las trazas de un proceso en ejecución pasando el PID mediante la opción -p:

```
nachorc@nachorc-Parallels-Virtual-Platform:~$ ps
  PID TTY          TIME CMD
 2827 pts/1    00:00:00 bash
 4757 pts/1    00:00:00 ps
nachorc@nachorc-Parallels-Virtual-Platform:~$ sudo strace -p 2827
Process 2827 attached - interrupt to quit
wait4(-1, ^C <unfinished ...>
Process 2827 detached
```

Figura 8.1: Strace a un proceso por su PID

✓ Mostrando registros 0 - 29 (30 total, La consulta tardó 0.0004 seg)

```
SELECT *
FROM `CHARACTER_SETS`
LIMIT 0 , 30
```

Mostrar : 30 fila(s) iniciando en la fila # 0 en modo horizontal

+ Opciones

CHARACTER_SET_NAME	DEFAULT_COLLATE_NAME	DESCRIPTION	MAXLEN
big5	big5_chinese_ci	Big5 Traditional Chinese	2
dec8	dec8_swedish_ci	DEC West European	1
cp850	cp850_general_ci	DOS West European	1
hp8	hp8_english_ci	HP West European	1
koi8r	koi8r_general_ci	KOI8-R Relcom Russian	1
latin1	latin1_swedish_ci	cp1252 West European	1
latin2	latin2_general_ci	ISO 8859-2 Central European	1
swe7	swe7_swedish_ci	7bit Swedish	1
ascii	ascii_general_ci	US ASCII	1
ujis	ujis_japanese_ci	EUC-JP Japanese	3
sjis	sjis_japanese_ci	Shift-JIS Japanese	2
hebrew	hebrew_general_ci	ISO 8859-8 Hebrew	1
tis620	tis620_thai_ci	TIS620 Thai	1

Figura 9.2: Sentencia SQL

```
SHOW PROFILE FOR QUERY1
```

✓ Su consulta se ejecutó con éxito

```
SHOW PROFILES
```

+ Opciones

Query_ID	Duration	Query
1	0.00015625	SELECT * FROM `CHARACTER_SETS` LIMIT 0 , 30

Figura 9.3: mySQL QUERY 1

✓ Su consulta se ejecutó con éxito	
SHOW PROFILE FOR QUERY1	
✓ Su consulta se ejecutó con éxito	
SHOW PROFILE	
+ Opciones	
Status	Duration
starting	0.000011
Waiting for query cache lock	0.000003
checking query cache for query	0.000020
checking permissions	0.000003
Opening tables	0.000020
System lock	0.000004
init	0.000008
optimizing	0.000003
statistics	0.000005
preparing	0.000004
executing	0.000024
Sending data	0.000016
end	0.000002
query end	0.000002

Figura 9.4: mySQL PROFILE

SHOW PROFILE indica el uso de recursos para las sentencias ejecutadas en la sesión actual. Muestra una lista de las declaraciones más recientes enviadas al servidor. Si añadimos como en la imagen anterior, la cláusula n (1) mediante QUERY se muestra información para esa declaración en vez de para la más reciente.

10. Cuestión opcional 2: instale Nagios en su sistema (el que prefiera) documentando el proceso y muestre el resultado de la monitorización de su sistema comentando qué aparece

Para instalar y configurar Nagios seguimos los siguientes pasos:

sudo -s

```
apt-get install wget build-essential apache2 php5 openssl perl make php5-gd  
libgd2-xpm libgd2-xpm-dev
```

```
./configure --with-command-group=nagcmd  
make all  
make install  
make install-init  
make install-config  
make install-commandmode  
make install-webconf
```

Creamos en el sistema un usuario y grupo específico para Nagios:

```
useradd nagios  
groupadd nagcmd  
usermod -a -G nagcmd nagios  
htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

Instalamos los plugins descargados de su web necesarios para que Nagios funcione correctamente:

```
./configure --with-nagios-user=nagios --with-nagios-group=nagios  
make  
make install
```

Reiniciamos el servicio apache e iniciamos nagios:

```
/etc/init.d/apache2 restart  
service nagios start
```

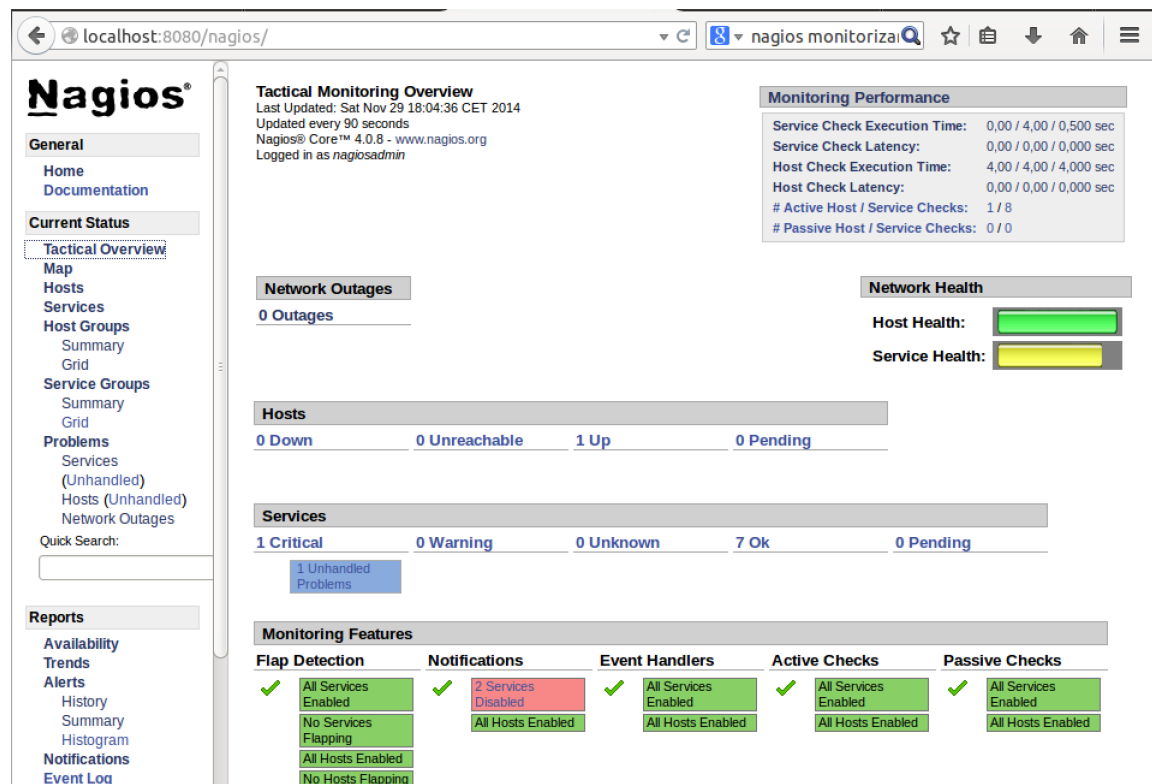


Figura 10.1: Monitorización con Nagios

Tras realizar el login en Nagios obtenemos toda la información del sistema, de los servicios, los Hosts y las redes actuales.

En la parte derecha se indica la Vida de Hosts y Servicios así como los tiempos de ejecución de cada uno.

11. Cuestión Opcional 3. Haga lo mismo con Munin

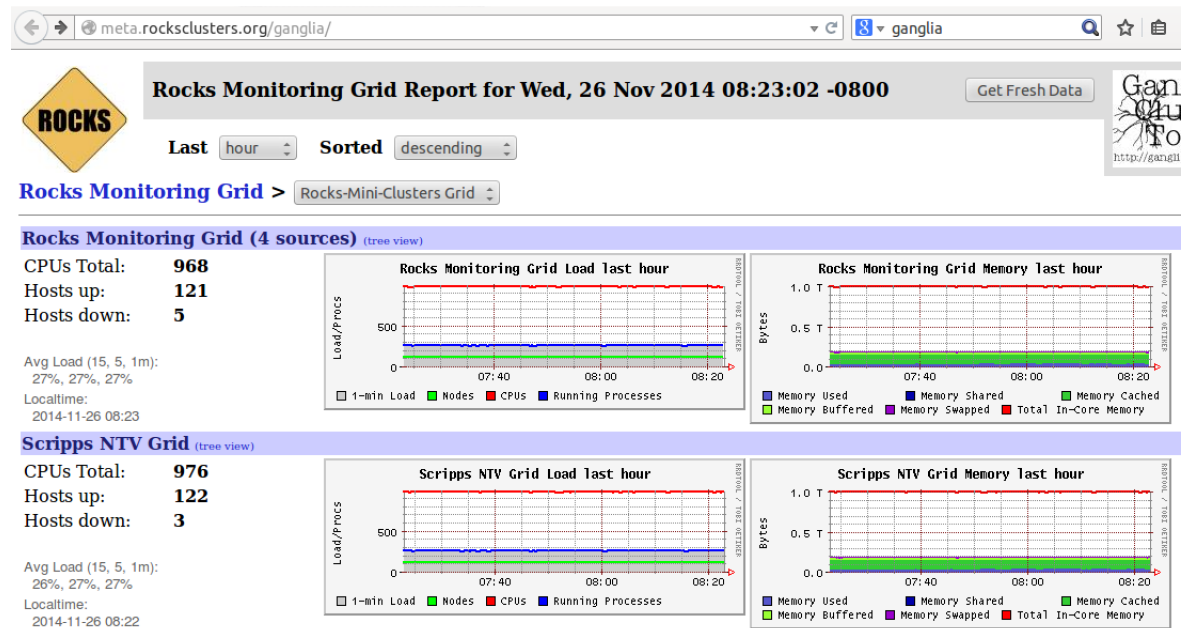


Figura 11.1: Monitorización con Ganglia

En los gráficos podemos observar una demo de los tiempos de ejecución de los procesos y Bytes consumidos por los Nodos, CPU y Memoria usada y compartida en la última hora sobre Rocks Grid Clusters.

12. Cuestión Opcional 6. Instale el monitor (AWSTATS) y muestre y comente algunas capturas de pantalla

```
sudo apt-get install awstats
```

```
sudo apt-get install awstats
```

Realizamos una copia seguridad del archivo de configuración:

```
sudo cp /etc/awstats/awstats.conf /etc/awstats/awstats.bk.com.conf
```

Configuramos el parámetro **SiteDomain** en el archivo de configuración anterior:

```
SiteDomain="localhost"
```

```
sudo /usr/lib/cgi-bin/awstats.pl -config=domain.com -update
```

```

GNU nano 2.2.6                               Archivo: awstats.conf
# server name, used to reach the web site.
# If you share the same log file for several virtual web servers, this
# parameter is used to tell AWStats to filter record that contains records for
# this virtual host name only (So check that this virtual hostname can be
# found in your log file and use a personalized log format that include the
# %virtualname tag).
# But for multi hosting a better solution is to have one log file for each
# virtual web server. In this case, this parameter is only used to generate
# full URL's links when ShowLinksOnUrl option is set to 1.
# If analyzing mail log, enter here the domain name of mail server.
# Example: "myintranetserver"
# Example: "www.domain.com"
# Example: "ftp.domain.com"
# Example: "domain.com"
#
SiteDomain="localhost"

```

Figura 12.1: Archivo awstats.conf

```

nachorc@nachorc-Parallels-Virtual-Platform:~$ sudo /usr/lib/cgi-bin/awstats.pl -config=domain.com -update
Create/Update database for config "/etc/awstats/awstats.conf" by AWStats version 7.0 (build 1.971)
From data in log file "/var/log/apache2/access.log"...
Phase 1 : First bypass old records, searching new record...
Searching new records from beginning of log file...
Dropped lines in file: 0
Parsed lines in file: 0
Found 0 dropped records,
Found 0 comments,
Found 0 blank records,
Found 0 corrupted records,
Found 0 old records,
Found 0 new qualified records.

```

Figura 12.2: Configuración de awstats

Editamos el archivo `/etc/apache2/sites-available/default` (o `000-default`) y añadimos lo siguiente:

```

GNU nano 2.2.6                               Archivo: default

CustomLog ${APACHE_LOG_DIR}/access.log combined

Alias /doc/ "/usr/share/doc/"
<Directory "/usr/share/doc/">
    Options Indexes MultiViews FollowSymLinks
    AllowOverride None
    Order deny,allow
    Deny from all
    Allow from 127.0.0.0/255.0.0.0 ::1/128
</Directory>

Alias /awstatsclasses "/usr/share/awstats/lib/"
Alias /awstats-icon "/usr/share/awstats/icon/"
Alias /awstatscss "/usr/share/doc/awstats/examples/css"
ScriptAlias /awstats/ /usr/lib/cgi-bin/
Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch

</VirtualHost>

```

Figura 12.3: Archivo Default de apache

```
service apache2 restart
```

Entramos a Awstats (en la dirección y puerto configurados en apache), en nuestro caso:
<http://localhost:8080/awstats/awstats.pl>

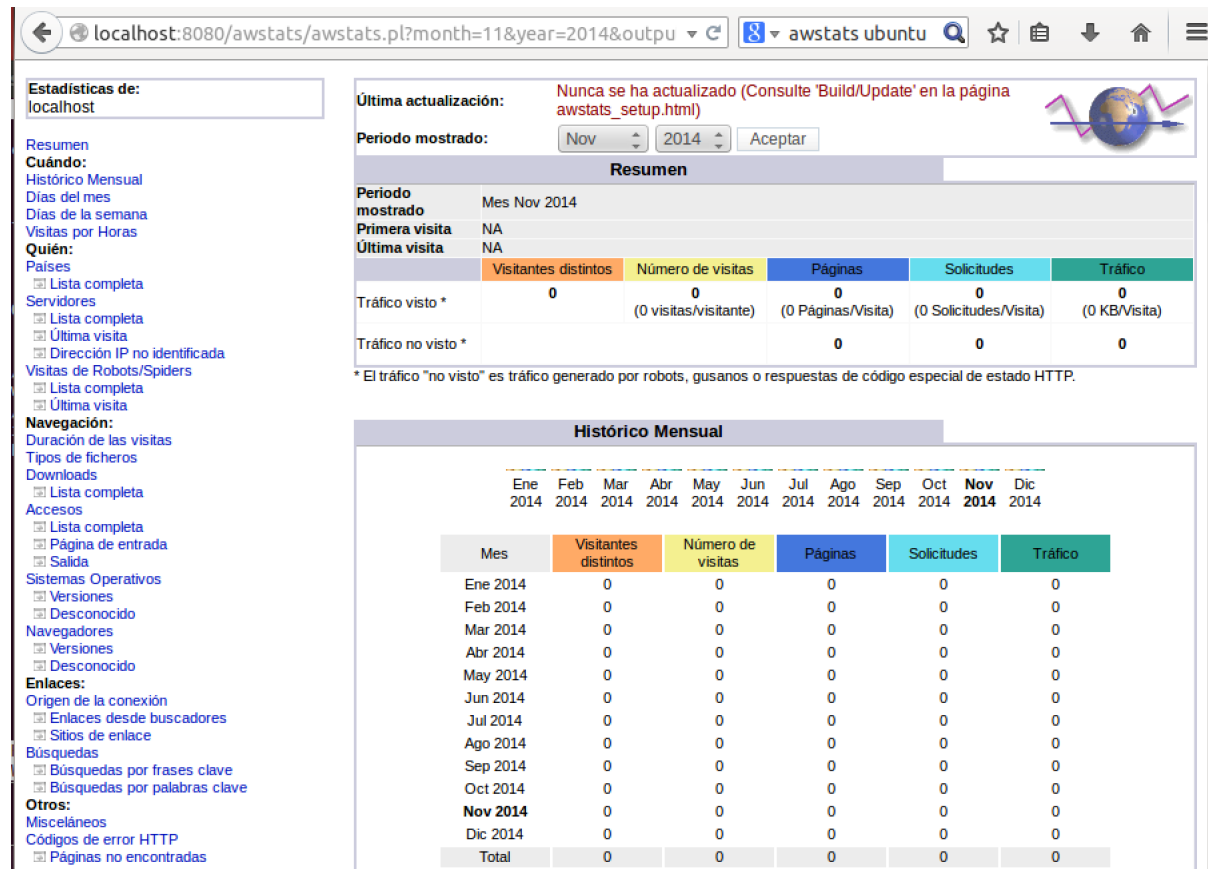


Figura 12.4: Funcionamiento Awstats