

# Monitorització del Sistema

René Serral-Gracià<sup>1</sup>

<sup>1</sup>Universitat Politècnica de Catalunya (UPC)

November 12, 2017

# Temari

- 1 Introducció a l'Administració de Sistemes
- 2 Instal·lació del Sistema Operatiu
- 3 Gestió d'usuaris
- 4 Gestió d'aplicacions
- 5 **Monitorització del sistema**
- 6 Manteniment del sistema de fitxers
- 7 Serveis locals
- 8 Serveis de xarxa
- 9 Protecció i seguretat
- 10 Virtualització

# Outline

- 1 Introducció
- 2 Monitorització del sistema
- 3 Gestió de processos
- 4 Monitorització d'usuaris
- 5 Monitorització d'Entrada/Sortida
- 6 Monitoritzar una Xarxa

# Outline

- 1 **Introducció**
  - Objectius
- 2 Monitorització del sistema
- 3 Gestió de processos
- 4 Monitorització d'usuaris
- 5 Monitorització d'Entrada/Sortida
- 6 Monitoritzar una Xarxa

# Objectius

## Coneixements

- Comandes de monitorització
- Significat dels diferents signals

## Habilitats

- Obtenir informació sobre el comportament del sistema
  - Activitat de CPU
  - Activitat de memòria
  - Activitat de disc
- Modificació de l'estat d'un procés
  - Canvi de prioritats
  - Aturada i continuació de processos

# Outline

## 1 Introducció

## 2 Monitorització del sistema

- CPU
- Memòria
- Disc
- Xarxa
- Usuaris
- Altres tasques de monitorització

## 3 Gestió de processos

## 4 Monitorització d'usuaris

## 5 Monitorització d'Entrada/Sortida

# Monitorització del sistema

## Per què monitorització?

- Controlar l'estat dels recursos de forma pro-activa
- Controlar l'estat dels serveis
- Seguretat

## Accions

- Automàtiques *Quan passa de un llindar -> acciona algo*
- Manuals

# Monitorització del sistema

## Què monitoritzem?

- CPU
- Memòria
- E/S
- Xarxa
- Usuaris
- Serveis
- Logs



# Monitorització del sistema

## Altres factors

- Quan es monitoritza el recurs?
- Qui ha de ser notificat quan hi ha un problema?
- Quin es el criteri per notificar un warning?
- I per un error crític?

# Activitat de CPU

## Monitoritzar

- Processadors inactius
- Processadors monopolitzats
  - Per un sol procés
  - Per un sol usuari

## Eines

`uptime, top, ps`

Estona que està  
encès l'ordinador

informació dels processos actius

# Activitat de memòria

## Monitoritzar

- Manca de memòria
- Monopolització de la memòria
  - Per un sol procés
  - Per un sol usuari
- Swap    bloquejant i baixa el rendiment

## Eines

free, vmstat, top

quanta mem  
tinc disponible

Estat de  
virtualització

Estat del sistema

# Activitat de disc

## Monitoritzar

- Sistema de fitxers
- Activitat anòmla d'entrada/sortida
- Memòria virtual
  - Excés de paginació
  - Espai lliure

monitoring system input/output device loading  
by observing the time the devices are active in  
relation to their average transfer rates.

## Eines

`vmstat`, `df`, `iostat`, `iostat`

`df` displays the  
amount of disk  
space available on  
the file system  
containing each file  
name argument.

# Activitat de Xarxa

## Monitoritzar

- Ample de banda
- Serveis locals i remots
- Connexions entrants/sortints
- Perfil del tràfic    molt tràfic -> DNS

## Eines

`ifconfig`, `netstat`, `tcpdump`, `nmap`, logs del sistema

configure the  
kernel-resident  
network interfaces,  
estadístiques de  
l'interfície

prints information  
about the Linux  
networking  
subsystem.

prints out a  
description of the  
contents of  
packets on a  
network interface

determine what hosts are available on the network,  
what services (application name and version) those  
hosts are offering, what operating systems (and OS  
versions) they are running, what type of packet  
filters/firewalls are in use

# Activitat dels usuaris

## Monitoritzar

- Sessions actives
  - Localment
  - Remotament
- Usuaris connectats
- Què fan?

## Eines

w, last, fuser, lsof

List open files, veure si alguna app obre + fitxers

usuaris

connectats al sistema

i aplicacions

displays the PIDs of processes using the specified files or file systems. Per

# Altres tasques de monitorització

## Activitat de serveis i servidors

- Càrrega del servidor Web
- Cues de correu electrònic
  - D'entrada
  - De sortida
- Cues de les impressores

## Fitxers de registre (logs)

- Errors del sistema
- Activitat anòmla (seguretat)

# Outline

- 1 Introducció
- 2 Monitorització del sistema
- 3 **Gestió de processos**
  - Canvi de prioritats
  - Els Signal
- 4 Monitorització d'usuaris
- 5 Monitorització d'Entrada/Sortida
- 6 Monitoritzar una Xarxa



# Tasques de gestió de processos

## Identificació del procés

- De qui és el procés?
- Quina tasca realitza?
  - És important?
  - És un atac? ... o un error?

ps aux

## Actuació sobre el procés

rang de -20 a 19, per defecte es 0.

Nomes pot assignar root nice amb mes prioritat (valors negatius)

- Canvi de prioritats `nice -10 ./test-new`  
`sudo nice --10 ./test-new -> nice negatiu, molta prioritat`
- Aturar i reactivar un procés `kill -STOP [ PID ]`  
`kill -CONT [ PID ]`
- Matar un procés `kill -KILL numprocés`

prioritat de 0 a 19 -> processos no interactius

prioritat de -20 a 0 -> processos interactius

# Canvi de prioritats

- En el moment d'executar el procés
  - `nice +10 comanda ...`
- Un cop ja està en execució
  - `renice +10 <pid>`
- Només root pot incrementar la prioritat

**Valors negatius indiquen prioritats més altes**

# Algun consell

## Shell a alta prioritat

- Procés més prioritari que el swap
  - Permet monitoritzar/solucionar més eficientment la situació
- Els processos fills hereten la prioritat del pare

## Prioritats relatives

- La prioritat és un terme relatiu
- Poc útil si tots els processos són molt prioritaris

# Enviament de signals a processos

```
kill <signal> <pid>
```

- -KILL: acabar l'execució del procés immediatament
- -TERM: demanar al procés que acabi (kill, per defecte)  
flush de caches, guardabases de dades
- -INT: interrompre el procés (kill, per defecte)  
ctrl + c, permet pendre accions abans que es mori. Es pot modificar en comptes de kill, aturar o otro
- -STOP: atura un procés
  - No pot entrar a la cua de ready
- -CONT: re-activa un procés aturat

```
killall <signal> <nom comanda>
```

- Envia el signal a **TOTS** els processos amb aquest nom

Signal -> interrupció que s'envia a un procés

# Outline

- 1 Introducció
- 2 Monitorització del sistema
- 3 Gestió de processos
- 4 Monitorització d'usuaris**
- 5 Monitorització d'Entrada/Sortida
- 6 Monitoritzar una Xarxa

# Monitorització d'usuaris

## Activitat d'usuaris

- `w [usuari]`
  - Llista d'usuaris connectats i la comanda que estan executant
  - Si se li dóna un username, llista les connexions que té
- `last [usuari]`
  - Llista de les darreres connexions establertes... finalitzades o no
- `finger [usuari]`
  - Llista totes les sessions o les de l'usuari donat

# Outline

- 1 Introducció
- 2 Monitorització del sistema
- 3 Gestió de processos
- 4 Monitorització d'usuaris
- 5 Monitorització d'Entrada/Sortida**
  - Exemples
- 6 Monitoritzar una Xarxa

# Monitorització de fitxers

## Activitat de fitxers

- `fuser <nom de fitxer>`
  - Identifica els processos que estan usant un fitxer
- `lsof [nom de fitxer | nom de directory]`
  - Llistat de fitxers oberts



# Activitat del disc

## Espai ocupat

- `du [nom de fitxer | nom de directori]`
  - Indica l'espai ocupat per un directori (incloent subdirectoris)

## Espai lliure

- `df [nom de fitxer | nom de directory]`
  - Espai disponible a cadascuna de les particions

## Activitat d'entrada/sortida

- `vmstat`
- `iostat`
- `iotop`

# Exemple top

Si ejecuto top -H en vez de tasks veré threads

10:01:50 up 4 days, 8:40, 5 users, load average: 1.77, 1.51, 1.56  
 Tasks: 281 total, 1 running, 279 sleeping, 0 stopped, 1 zombie  
 Cpu0 : 13.2 us, 3.3 sy, 0.0 ni, 82.9 id, 0.3 wa, 0.0 hi, 0.3 si, 0.0 st  
 Cpu1 : 10.2 us, 1.5 sy, 0.0 ni, 87.3 id, 0.3 wa, 0.0 hi, 0.6 si, 0.0 st  
 Cpu2 : 12.7 us, 1.5 sy, 0.0 ni, 84.6 id, 0.6 wa, 0.0 hi, 0.6 si, 0.0 st  
 %Cpu3 : 16.3 us, 1.7 sy, 0.0 ni, 81.6 id, 0.0 wa, 0.0 hi, 0.3 si, 0.0 st  
 Mem : 16314076 total, 5436464 free, 3590272 used, 7287340 buff/cache  
 Swap: 16360444 total, 16318936 free, 41508 used. 10859404 avail Mem

el total és 100

	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
17901	rserrall	1	0	1429512	265436	126648	S	16.5	1.6	4:51.75	slack
17115	rserrall	5	0	2640856	349772	137352	S	9.6	2.1	5:00.66	gnome-shell
17340	rserrall	1	0	1667320	157220	91880	S	4.6	1.0	0:33.14	slack
444	root	-51	0	0	0	0	S	2.0	0.0	17:17.13	irq/17-i2c_desi
17133	rserrall	1	0	562520	236400	201880	S	1.7	1.4	0:51.53	Xwayland
17343	rserrall	1	0	471912	48636	30472	S	1.7	0.3	0:00.92	python2
8210	rserrall	1	0	3021200	577976	253764	S	1.3	3.5	4:42.75	firefox
286	root	-51	0	0	0	0	S	1.0	0.0	8:01.12	irq/17-idma64.1
20211	rserrall	6	0	46988	3904	3044	R	1.0	0.0	0:00.33	top
19472	root	1	0	0	0	0	S	0.7	0.0	0:11.71	kworker/u8:2
6	root	1	0	0	0	0	S	0.3	0.0	13:19.49	ksoftirqd/0
7	root	1	0	0	0	0	S	0.3	0.0	2:02.42	rcu_preempt
17	root	1	0	0	0	0	S	0.3	0.0	13:23.78	ksoftirqd/1
23	root	1	0	0	0	0	S	0.3	0.0	14:30.76	ksoftirqd/2
29	root	1	0	0	0	0	S	0.3	0.0	16:11.32	ksoftirqd/3
445	root	-51	0	0	0	0	S	0.3	0.0	3:06.32	irq/51-DLL075B:
621	message+	1	0	48732	6700	3072	S	0.3	0.0	4:09.41	dbus-daemon

# Sortida vmstat

```
# vmstat -n 30
```

procs		-----memory-----				---swap--		-----io----		-system--		-----cpu-----			
r	b	swpd	free	buff	cache	si	so	bi	bo	in	cs	us	sy	id	wa
0	10	249496	54376	6172	113464	3	2	35	52	36	57	9	1	83	6
1	10	249496	8132	6188	3584	13	0	38	12	353	611	5	0	88	7
1	10	124949	4960	6204	3720	0	54	26	6	349	611	5	5	86	4
1	9	109496	2832	6220	3840	10	10	26	6	352	623	1	10	85	4
1	8	49496	1708	3236	2848	13	117	13	6	349	595	1	25	65	10
1	9	9496	596	1252	1976	150	200	26	14	349	607	3	20	72	4



# Activitat

Tenim un servidor de bases de dades amb 1 CPU (amb hyperthreading)

- Quin problema creieu que hi ha al servidor? *es fa servir per mes coses que per un servidor de base de dades*
- Quines accions faríeu? *consultar-ho, marta-lo o fer systop*

```
top - 09:38:09 up 1 day, 18:29, 6 users, load average: 4.08, 4.93, 4.39
Tasks: 425 total, 12 running, 413 sleeping, 0 stopped, 0 zombie
%Cpu(s): 91.0 us, 6.8 sy, 0.9 ni, 1.3 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem : 16355660 total, 125088 free, 6559812 used, 9670760 buff/cache
KiB Swap: 33691644 total, 33689476 free, 2168 used. 8286212 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
4102	pcomp	20	0	2920500	1.029g	98884	S	46.1	6.6	103:32.24	firefox-esr
12802	pcomp	20	0	102332	68188	14164	R	30.6	0.4	0:00.93	chrome-bg-proc
12818	pcomp	20	0	80856	51980	17732	R	22.4	0.3	0:00.68	chrome-bg-proc
12835	pcomp	20	0	88840	49892	10524	R	17.1	0.3	0:00.52	chrome-bg-proc
3947	pcomp	20	0	2207552	505540	69276	S	14.5	3.1	49:25.10	gnome-shell
12861	pcomp	20	0	75972	37808	10480	R	12.2	0.2	0:00.37	chrome-bg-proc
12834	pcomp	20	0	65460	25816	8488	R	11.2	0.2	0:00.34	chrome-bg-proc
12873	pcomp	20	0	69680	32032	10508	R	9.2	0.2	0:00.28	chrome-bg-proc
12858	pcomp	20	0	59056	18824	8452	R	7.6	0.1	0:00.23	chrome-bg-proc
12833	pcomp	20	0	14312	11436	1356	R	6.9	0.1	0:00.21	mysqld

# Activitat

## Tenim un servidor

- Quin problema creieu que hi ha al servidor?
- Quines accions faríeu?

```
top - 16:31:15 up 3:04, 20 users, load average: 29.76, 17.88, 10.19
Tasks: 1016 total, 2 running, 1013 sleeping, 1 stopped, 0 zombie
Cpu(s): 2.5%us, 1.2%sy, 0.0%ni, 86.8%id, 9.4%wa, 0.0%hi, 0.1%si, 0.0%st
Mem: 65969572k total, 33193236k used, 32776336k free, 8656k buffers
Swap: 16777208k total, 7635416k used, 9141792k free, 31292k cached
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
3164	tst8	20	0	23.1g	21g	584	R	100.0	34.1	7:44.76	emacs
4576	tst8	20	0	104m	1080	476	S	53.3	0.0	2:17.90	genarray.sh
1010	root	20	0	0	0	0	D	2.0	0.0	2:07.06	kmirrord
3342	g_users	20	0	15868	1528	476	R	1.0	0.0	1:43.80	top
168	root	20	0	0	0	0	S	0.3	0.0	0:02.09	events/21
2568	tst6	20	0	101m	376	240	S	0.3	0.0	1:27.30	sshd

# Outline

- 1 Introducció
- 2 Monitorització del sistema
- 3 Gestió de processos
- 4 Monitorització d'usuaris
- 5 Monitorització d'Entrada/Sortida
- 6 Monitoritzar una Xarxa**

# Monitoritzar una Xarxa

## Sistemes integrats

- Centralitzen la informació de diferents servidors
  - Recursos
  - Serveis
  - Uptime
  - Connectivitat
  - Logs
- Faciliten la detecció de problemes
- NagiOS, Splunk

# Exemple Nagios XI

**Nagios<sup>®</sup>**  
**XI™**

Logged in as: nagiosadmin

System OK: 

Logout

[Home](#) [Views](#) [Dashboards](#) [Reports](#) [Configure](#) [Help](#) [Admin](#)

## Dashboard Tools

 Add New Dashboard  
 Deploy Dashboards


## My Dashboards

 Home Page  
 Empty Dashboard



## Add Dashlets

 Available Dashlets  
[Manage Dashlets](#)


### Hostgroup 'newtest' Status Grid

Host	Services
 192.168.1.91	Ping

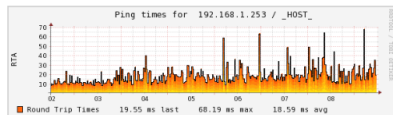
Last Updated: 2011-04-09 11:35:23

Network Health
Host Health 
Service Health 

Last Updated: 2011-04-09 11:35:26

 88.6%   
 192.168.1.4  
 Drive E: Disk Usage

### 192.168.1.253 Host Performance Graph



### Hostgroup 'linux-servers' Status Grid

Hosts	Services
 egalstad.hsd1.mn.comcast.net	
 localhost	

Last Updated: 2011-04-09 11:35:25

Services				
66 Critical	3 Warning	14 Unknown	59 Ok	1 Pending
25 Unhandled Problems	1 Unhandled Problems	8 Unhandled Problems	2 Disabled	1 Disabled
31 On Problem Hosts		8 On Problem Hosts		
1 Acknowledged		1 Disabled		

Last Updated: 2011-04-09 11:35:26

Image source: <http://www.nagios.com/>

Nagios XI 2011R1.1 Copyright © 2008-2011 Nagios Enterprises, LLC.

 Check for Updates

 About [Legal](#)



# Treball personal

- Eines de còpia de seguretat
  - dump
  - tar
  - gzip, bzip2, zip, rar, partimage, Norton Ghost