Administración de sistemas POSIX

Administración de sistemas POSIX

Gestión de usuarios

Gestión de sistemas de ficheros

Arranque y parada de servicios

Monitorización básica

Instalación y actualización de software

Gestión de usuarios

Procesos y usuarios

Tipos de procesos de usuario:

- Vinculados a un terminal (sesiones de terminal)
- Demonios (servicios)

Tipos de usuarios

- Sesiones de terminal: **usuario normal**
- Demonios
  - Privilegiados: **superusuario**
  - No privilegiados: **pseudousuario**

Principales propiedades de una cuenta de usuario en POSIX

Identificación (UID, nombre, datos personales)

Información de autenticación

Grupos a los que pertenece

Directorio base

Entorno de trabajo

Límites de uso y de recursos

Privilegios

Base de datos (BSD)

/etc/master.passwd (legible sólo por root)

```
nombre:contra:UID:GID:clase:cambio:expiración:GECOS:
directorio:intérprete
```

/etc/passwd (legible por cualquier usuario)

```
nombre:*:UID:GID:GECOS:directorio:intérprete
```

/etc/pwd.db, /etc/spwd.db

/etc/group

```
nombre:*:GID:usu1,usu2,usu3…
```

/etc/login.conf

Otros

Ejemplo de /etc/master.passwd

```
root:ayu377syDH7:0:0::0:0:Administrador:/root:/bin/csh
daemon:*:1:1::0:0::/root:/sbin/nologin
operator:*:2:5::0:0::/:/sbin/nologin
nobody:*:65534:65534::0:0::/noexiste:/sbin/nologin
pgsql:*:70:70::0:0:PostgreSQL:/usr/local/pgsql:
jmr:jfuJD8d8jH:1000:1000::0:0:Javier:/home/jmr:/bin/csh
cmt:tyu7i3:1001:1001::281713:0:Carlos:/home/cmt:/bin/sh
```

Ejemplo de /etc/group

```
wheel:*:0:root,jmr

daemon:*:1:

operator:*:5:root,jmr,cmt

bin:*:7:

bind:*:53:

pgsql:*:70:
```

Ejemplo de clases de usuarios

```
default:cputime=infinity:memoryuse=128M:maxproc=100:\
  priority=0:lang=es_ES.ISO_8859-1:\
  minpasswordlen=10:passwordtime=26w:
alumno:cputime=2h:memoryuse=64M:\
  times.allow=MoTuWeThFr0830-2130:tc=default:
profesor:tc=default:
biblioteca:hosts.allow=10.67.1.*:tc=default:
root:memoryuse=infinity:maxproc=500:\
  passwordtime=16w:tc=default:
```

Ejemplo de /etc/profile

```
PATH=/sbin:/usr/sbin:/bin:/usr/bin:/usr/X11R6/bin:/usr/local/bin
LANG=es_ES.UTF-8 ; export LANG
PS1='\h:\w\$ '
BLOCKSIZE=K ; export BLOCKSIZE
PAGER=/usr/bin/less ; export PAGER
EDITOR=/usr/local/bin/nano ; export EDITOR
PATH=$PATH:/usr/local/java/bin:/usr/local/jee/bin
CLASSPATH=/usr/local/java/jre/lib:/usr/local/jee/lib/j2ee.jar
export CLASSPATH
JAVA_HOME=/usr/local/java ; export JAVA_HOME
umask 077
PATH=$PATH:~/bin:.
alias l='ls -lg '
```

Política de generación de identificadores

Reglas de generación

Tratamiento de colisiones

Ámbito de validez

Coherencia

Reutilización

Procedimientos (FreeBSD)

Alta

- Manual: vipw, mkdir, cp, chown…
- Interactivo: adduser
- Automático/Masivo: **pw** y *scripts*

Modificación

- vipw, **pw**
- **passwd**
- chpass/chsh/chfn

Eliminación

- Manual: vipw, rm…
- **pw**
- **rmuser**

Ejemplos de uso de pw

Crear un usuario nuevo: pw useradd pepe -m -h0

Crear un grupo nuevo: pw groupadd amigos

Crear un usuario nuevo y meterlo en un grupo: pw useradd cristina -m -h0 -G amigos

Modificar atributos de un usuario: pw usermod pepe -L clase -s /usr/local/bin/bash

Añadir usuarios a un grupo: pw groupmod amigos -m alberto,luis

Quitar a usuarios de un grupo: pw groupmod amigos -d carlos,ana

Establecer valores por defecto: pw useradd -D -s /usr/local/bin/bash -M 0700

Mostrar usuarios o grupos: pw usershow pepe / pw groupshow amigos

Política por defecto para cuentas de usuario (FreeBSD)

Nombres de usuario: a la elección del administrador

UID: siguiente UID libre o a elección del administrador

Grupo: grupo único coincidente con el nombre de usuario y con siguiente GID libre o a elección del administrador

Ejercicios de gestión de usuarios y grupos (1)

```
# pw useradd pepe -m -h0
password for user pepe:
# pw usershow pepe
pepe:...:1002:1002::0:0:User &:/home/pepe:/bin/sh
# pw groupshow pepe
pepe:*:1002:
# finger pepe
Login: pepe                             Name: User Pepe
Directory: /home/pepe                   Shell: /bin/sh
No Mail.
No Plan.
```

Ejercicios de gestión de usuarios y grupos (2)

```
# ssh pepe@localhost
Password for pepe@maquina-26-01.ars.lab.te.upm.es
...
$ id
uid=1002(pepe) gid=1002(pepe) groups=1002(pepe)
$ pwd
/home/pepe
$ ls -ld $HOME
drwxr-xr-x  2 pepe   pepe    9 Nov  5 20:22 /home/pepe
$ touch prueba1.txt
$ ls -l
total 1
-rwxr-xr-x  1 pepe   pepe    9 Nov  5 20:23 prueba1.txt
$ exit
```

Ejercicios de gestión de usuarios y grupos (3a)

```
# pw useradd -D -M 700
# pw useradd luis -m -h0 -c 'Luis Carvajal' -s /bin/csh
password for user luis:
# pw useradd ana -m -h0 -c 'Ana García'
password for user ana:
# finger luis
Login: luis                             Name: Luis Carvajal
Directory: /home/luis                   Shell: /bin/csh
No Mail.
No Plan.

# ls -l /home
total 17
drwx------  2 ana      ana      9 Nov  5 20:24 ana
drwx------  2 luis     luis     9 Nov  5 20:24 luis
drwxr-xr-x  2 pepe     pepe     9 Nov  5 20:22 pepe
```

Ejercicios de gestión de usuarios y grupos (3b)

```
# pw useradd beatriz -m -h0 -u 20001
password for user beatriz:
# ssh beatriz@localhost
Password for beatriz@maquina-26-01.ars.lab.te.upm.es:
...
$ id
uid=20001(beatriz) gid=20001(beatriz) groups=20001(beatriz)
$ exit
# pw useradd -D -s /usr/local/bin/bash
# pw useradd carlos -m -h0
password for user carlos:
```

Ejercicios de gestión de usuarios y grupos (3c)

```
# pw usershow -a
...
pepe:...:1002:1002::0:0:User &:/home/pepe:/bin/sh
luis:...:1003:1003::0:0:Luis Carvajal:/home/luis:/bin/csh
ana:...:1004:1004::0:0:Ana García:/home/ana:/bin/sh
beatriz:...:20001:20001::0:0:User &:/home/beatriz:/bin/sh
carlos:...:20002:20002::0:0:User &:/home/carlos:/usr/local/bin/bash
# pw groupshow -a
...
pepe:*:1002:
luis:*:1003:
ana:*:1004:
beatriz:*:20001:
carlos:*:20002:
```

Ejercicios de gestión de usuarios y grupos (4-5)

```
# pw lock ana
# ssh ana@localhost
Password for ana@maquina-26-01.ars.lab.te.upm.es:
Password for ana@maquina-26-01.ars.lab.te.upm.es:
Password for ana@maquina-26-01.ars.lab.te.upm.es:
ana@localhost: Permission denied (publickey,keyboard-
interactive).
# pw unlock ana
# passwd beatriz
Changing local password for beatriz
New Password:
Retype New Password:
```

Ejercicios de gestión de usuarios y grupos (6)

```
# pw usermod ana -c 'Ana Jiménez'
# finger ana
Login: ana                              Name: Ana Jiménez
Directory: /home/ana                    Shell: /bin/sh
Last login Thu Nov  5 20:25 (CET) on pts/3 from 127.0.0.1
No Mail.
No Plan.
```

Ejercicios de gestión de usuarios y grupos (7)

```
# pw usermod ana -u 5000
# ssh ana@localhost
Password for ana@maquina-26-01.ars.lab.te.upm.es:
...
Could not chdir to home directory /home/ana: Permission
denied
$ id
uid=5000(ana) gid=1004(ana) groups=1004(ana)
$ ls -ld $HOME
drwx------  2 1004  ana  9 Nov  5 20:25 /home/ana
$ exit
```

Ejercicios de gestión de usuarios y grupos (8)

```
# pw userdel carlos
# rmuser -y beatriz
Removing user (beatriz): mailspool home passwd.
# ls -l /home
total 34
drwx------  2 1004   ana     9 Nov  5 20:25 ana
drwx------  2 20002  20002   9 Nov  5 20:26 carlos
drwx------  2 luis   luis    9 Nov  5 20:24 luis
drwxr-xr-x  2 pepe   pepe    9 Nov  5 20:22 pepe
```

Ejercicios de gestión de usuarios y grupos (9)

```
# pw groupadd amigos
# pw useradd emilio -m -h0 -G amigos
password for user emilio:
# ssh emilio@localhost
Password for emilio@maquina-26-01.ars.lab.te.upm.es:
...
$ id
uid=5001(emilio) gid=5001(emilio)
groups=5001(emilio),1005(amigos)
$ exit
```

Ejercicios de gestión de usuarios y grupos (10-12)

```
# pw usermod pepe -G amigos
# pw groupshow amigos
amigos:*:1005:emilio,pepe
# pw groupmod amigos -m luis
# pw groupshow amigos
amigos:*:1005:emilio,pepe,luis
# pw groupmod amigos -d pepe
# pw groupshow amigos
amigos:*:1005:emilio,luis
```

Protecciones

Permisos del directorio base

Grupos para información compartida

umask

Visibilidad de procesos

Privilegios

Modelo de privilegios de POSIX

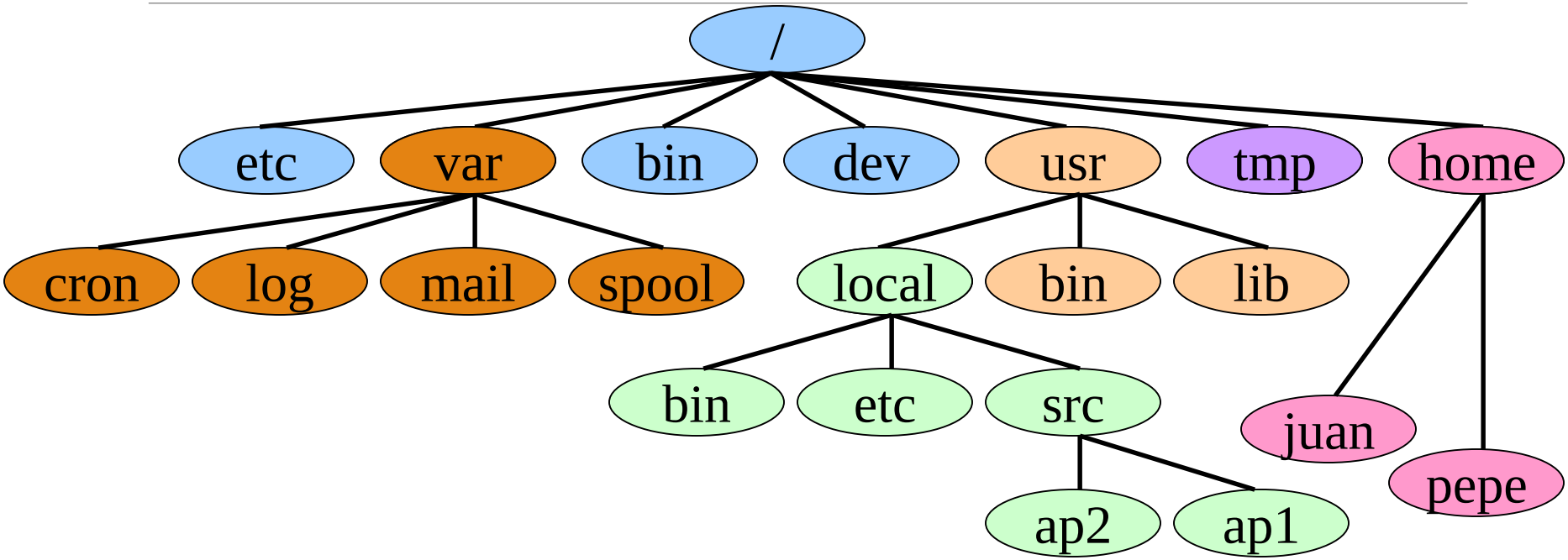
- Usuarios privilegiados (UID=0)
- Usuarios no privilegiados (UID≠0)

Formas de otorgar privilegios

- Pertenencia a determinados grupos
- Programas setuid/setgid
- Privilegios (en algunas versiones de Unix)
- sudo

Gestión de disco

Árbol de sistemas de ficheros



(Ver Filesystem Hierarchy Standard, http://www.pathname.com/fhs)

Adición de discos (FreeBSD)

1. Instalación física
2. Particionado (gpart/fdisk, bsdlabel)
3. Creación de sistemas de ficheros (newfs)
4. Montaje (mount, /etc/fstab)

Montaje manual de sistemas de ficheros

Sólo puede ser realizado por el superusuario

```
mount -t tipo -o opciones disp punto
mount -u -o opciones punto
```

```
umount punto
```

Montaje durante el arranque

/etc/fstab

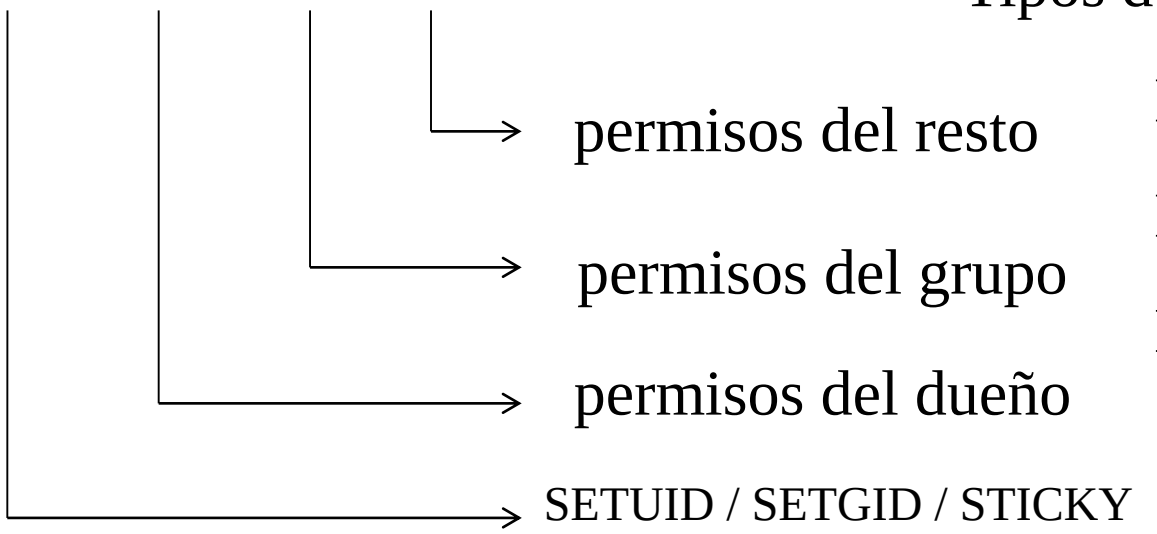
DISPOSITIVO	PUNTO	TIPO	OPCIONES	CSEG	FSCK
/dev/ada0p2	/	ufs	rw	1	1
/dev/ada0p3	/usr	ufs	rw	2	2
/dev/ada0p4	/var	ufs	rw	2	2
/dev/mirror/home	/home	ufs	rw,userquota	2	2
ioda:/db/a	/db/a	nfs	rw,nosuid	0	0
/dev/ada1p2	none	swap	sw	0	0
proc	/proc	procfs	rw	0	0
/dev/cd0	/cdrom	cd9660	ro,noauto	0	0

Permisos del sistema de ficheros

```
-rw-r--r-- 1 pepe amigos 1029 Jan 13 datos.txt
-r-sr-xr-x 1 root wheel  9650 Aug 27 /usr/bin/passwd
```

bits de permisos | dueño | grupo

UGTrwxr-xr-x



Tipos de permisos:

Lectura: r

Escritura: w

Ejecución/Paso: x

Establecimiento de permisos

Al crear:

- Dueño: el del proceso que lo creó
- Grupo: el del directorio donde se creó
- Permisos: los que defina el proceso que lo creó, restringidos por su umask

A posteriori:

- Dueño: chown (solo el superusuario)
- Grupo: chgrp (el dueño, a un grupo al que también pertenezca)
- Permisos: chmod (el dueño, a discreción)

Ejercicios sobre permisos (1)

```
$ umask
0022
$ touch f1
$ mkdir d1
$ openssl genrsa -out c1 512
...
$ ls -l
total 6
-rw-------  1 pepe  pepe  497 Nov 13 19:42 c1
drwxr-xr-x  2 pepe  pepe    2 Nov 13 19:42 d1
-rw-r--r--  1 pepe  pepe    0 Nov 13 19:42 f1
```

Ejercicios sobre permisos (2-3)

```
$ umask 077
$ touch f2
$ mkdir d2
$ openssl genrsa -out c2 512
...
$ ls -l
...
-rw-------  1 pepe  pepe  497 Nov 13 19:43 c2
drwx------  2 pepe  pepe    2 Nov 13 19:43 d2
-rw-------  1 pepe  pepe    0 Nov 13 19:43 f2

Cambio permanente:

$ vi ~/.cshrc ~/.profile ~/.bashrc ...
```

Ejercicios sobre permisos (4-8)

```
# pw useradd / groupadd ...
# mkdir /home/pruebas
# cd /home/pruebas
# mkdir alfa beta gamma delta
# chown adan           alfa
# chmod 700            alfa
# chown bea:chicas     beta
# chmod 750            beta
# chown carla:chicos   gamma
# chmod 770            gamma
# chown david          delta
# chmod 755            delta
# ls -l
total 2
drwx------  2 adan   wheel   2 Nov 13 20:06 alfa
drwxr-x---  2 bea    chicas  2 Nov 13 20:06 beta
drwxr-xr-x  2 david  wheel   2 Nov 13 20:06 delta
drwxrwx---  2 carla  chicos  2 Nov 13 20:06 gamma
```

Ejercicios sobre permisos (4-8)

Versión mejorada

```
# ls -l
total 2
drwx------  2 adan   adan    2 Nov 13 20:06 alfa
drwxr-x---  2 bea    chicas  2 Nov 13 20:06 beta
drwxr-xr-x  2 david  david   2 Nov 13 20:06 delta
drwxrwx---  2 carla  chicos  2 Nov 13 20:06 gamma

umask 007
```

Ejercicios sobre permisos (9)

```
$ id
uid=3003(david) gid=3005(david) groups=3005(david),3002(chicos)
$ ls -ld gamma gamma/f1.txt
drwxrwx---  2 carla  chicos  512 Nov 16 13:26 gamma
-rwx------  1 carla  chicos    0 Nov 16 13:26 gamma/f1.txt
$ rm gamma/f1.txt
override rwx------ carla/chicos for gamma/f1.txt? y
$ ls -ld gamma gamma/f1.txt
ls: gamma/f1.txt: No such file or directory
drwxrwx---  2 carla  chicos  512 Nov 16 13:33 gamma
```

Ejercicios sobre permisos (10)

```
$ id
uid=3004(bea) gid=3006(bea) groups=3006(bea),3003(chicas)
$ cat gamma/f2.txt
cat: gamma/f2.txt: Permission denied
# chmod o+x gamma
$ ls -ld gamma
drwxrwx--x  2 carla  chicos  512 Nov 16 13:39 gamma
$ cat gamma/f2.txt
HOLA MUNDO
$ ls -l gamma
ls: gamma: Permission denied
# chmod o+r gamma
$ ls -l gamma
-r--r--r--  1 root   chicos   11 Nov 16 13:40 gamma/f2.txt
```

Tipos de copias de seguridad

Por los ficheros que se incluyen
- Totales
- Parciales
  - Incrementales
  - Diferenciales

Sistemas alternativos
- Instantáneas
- Clonación

Medios: cinta, CD/DVD, disco duro, extraíble…

Por el destino
- Locales
- Remotas

Herramientas para copias de seguridad

Herramientas

- dump/restore
- tar, cpio, compresores (gzip, bzip2, xz…)
- rsync
- Bacula, Amanda…

Backup basics (manual de FreeBSD)

tar: ejemplos de uso

Hacer una copia

tar czf copia.tgz /home

tar cf - /home | bzip2 > copia.tbz

tar czf - /home | openssl enc -e -aes256 -pass pass:holamundo > copia.tgz

Restaurar una copia

cd directorio_de_destino

tar xzpf copia.tgz

bzcat copia.tbz | tar xpf -

cat copia.tgz | openssl enc -d -aes256 -pass pass:holamundo | tar xzpf -

Nota: uso de -pass ilustrativo. No se recomienda poner la clave en la línea de mandatos

dump/restore: ejemplos de uso

Hacer una copia

dump 0af copia.dump /home

dump 0af /dev/nsa0 /home

dump 0af - /home | bzip2 | openssl enc -e -aes256 -pass pass:holamundo > /dev/nsa0

Restaurar una copia

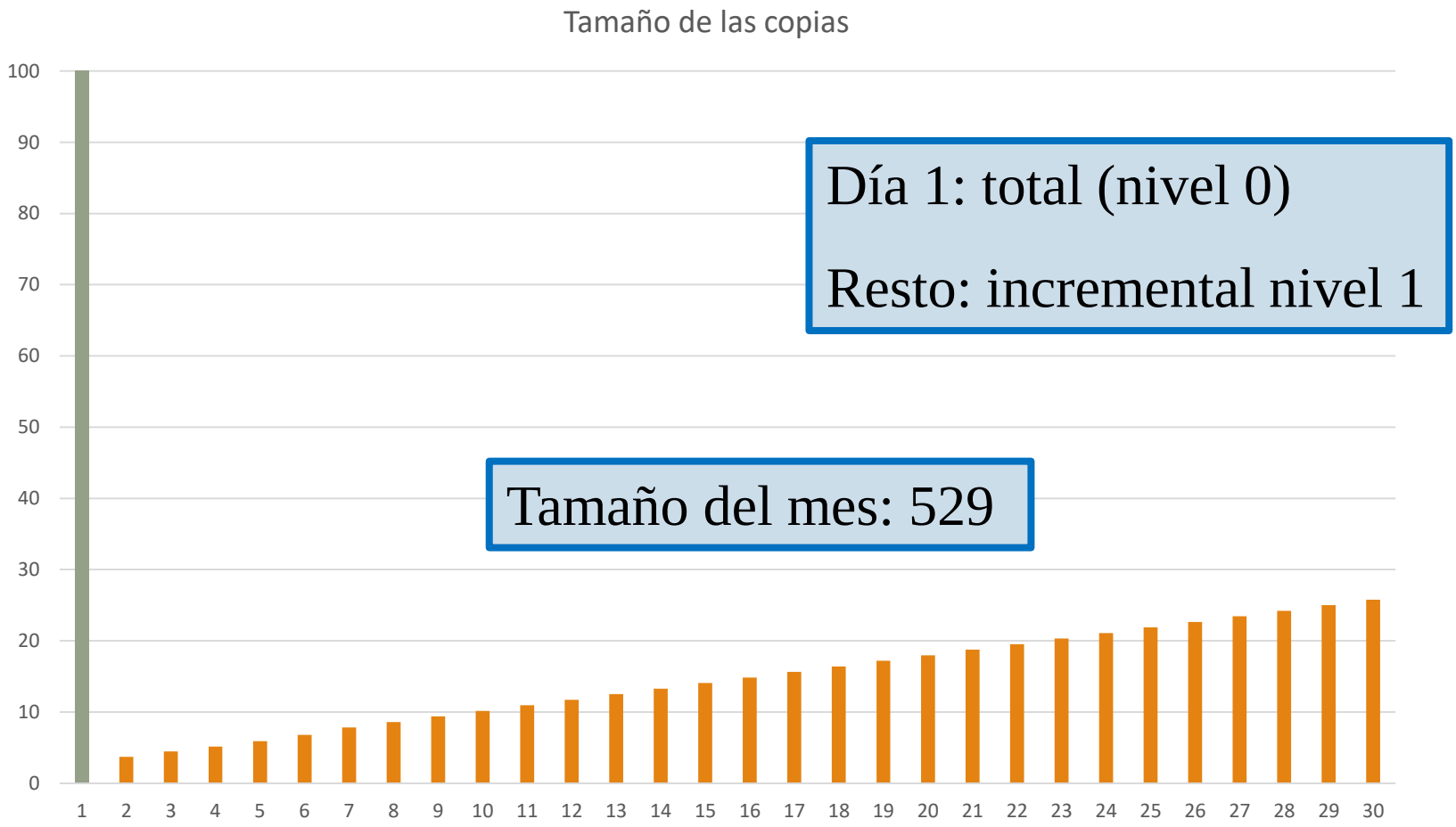
cd directorio_de_destino

restore -ivf /dev/nsa0

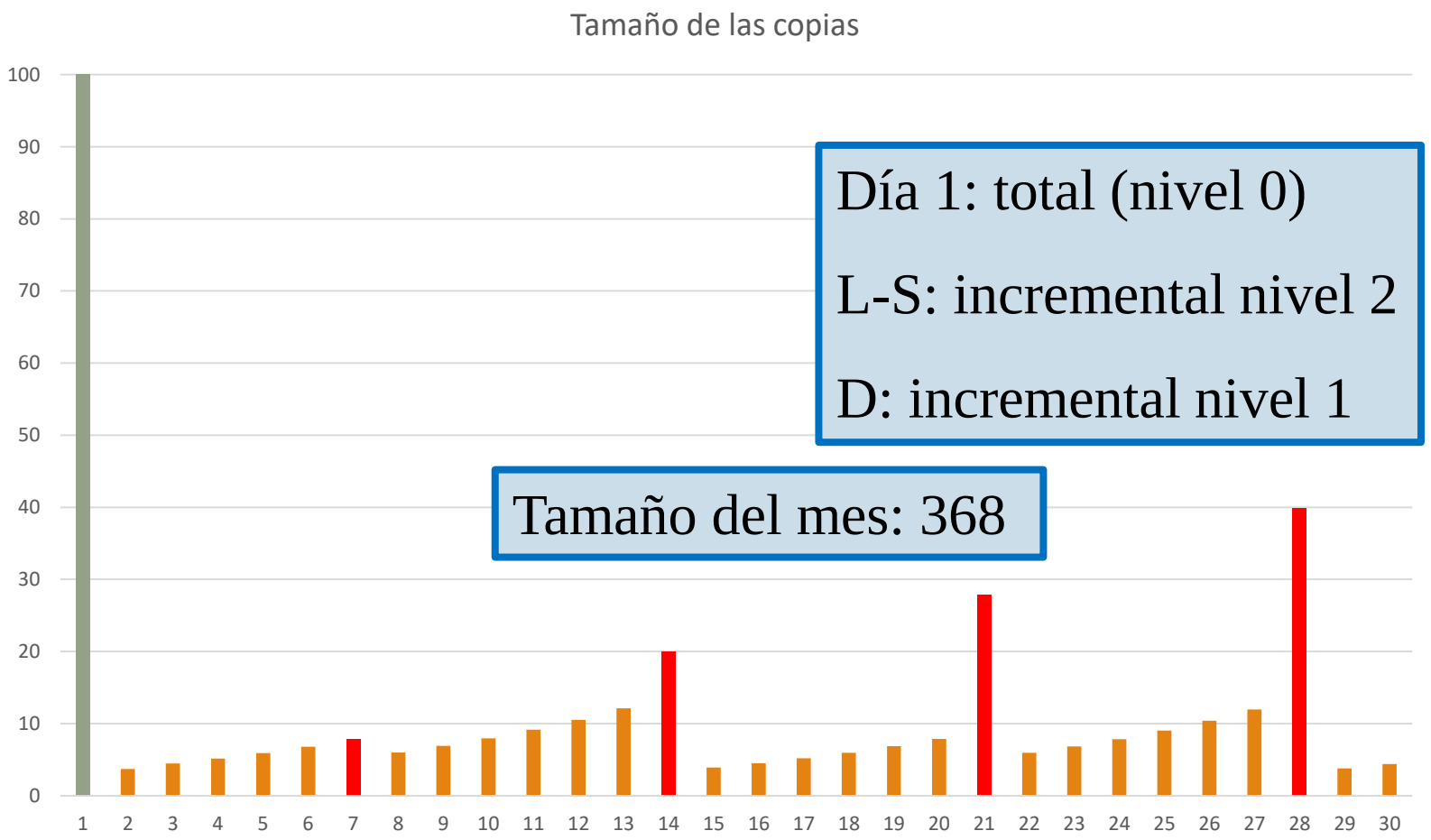
openssl enc -e -aes256 -pass pass:holamundo < /dev/nsa0 | bunzip2 | restore -ivf -

Nota: uso de -pass ilustrativo. No se recomienda poner la clave en la línea de mandatos

Ejemplo de copias incrementales



Ejemplo de copias incrementales



Arranque y parada de servicios

Manejo de servicios (FreeBSD)

Configuración: /etc/rc.conf

- nombreservicio_enable="YES/NO"
- nombreservicio_flags="-x -y -z"

sysrc nombreservicio_enable=YES

Arranque y parada

- Scripts en /etc/rc.d y /usr/local/etc/rc.d

service SERVICIO start/stop/restart/status/…

Programación de tareas

crontab

minutos horas día_mes mes día_semana mandato

```
*/5 * * * *  wget -q -O /dev/null http://moodle/cron.php
30 23 * * 6  find /var/tmp -mtime +7 -delete
```

at, atq, atrm, atrun

Monitorización del sistema

Objetivos de la monitorización

Detectar y solucionar problemas a tiempo

Averiguar las causas de problemas

Afinar el comportamiento del sistema

Predecir tendencias de uso futuras

Facturar por el uso del sistema

Vigilar la seguridad del sistema

Justificar la toma de decisiones

Tipos de monitorización

Datos históricos

Datos en tiempo real

Auditoría de seguridad

Pruebas periódicas

Inspección física

Datos históricos

Selección de los parámetros de interés

Periodo de muestreo / Bajo demanda

Almacenamiento de la información

- Condensación, compresión, archivación y expiración de la información

Herramientas de análisis

Datos en tiempo real

Selección de los parámetros de interés

Definición de umbrales de atención

Mecanismos de alerta

- Cómo alertar y a quién

Respuesta activa

Consumo de recursos instantáneos

Auditoría de seguridad

Orientada hacia la seguridad del sistema

Filtros para la detección de actividades sospechosas

Respuesta activa

Consumo de recursos

Pruebas periódicas

Permiten hacer comprobaciones del sistema más completas y a alto nivel

Han de coordinarse con la actividad normal del sistema

Inspección física

Impresoras

Cableado

Estado de los equipos

Ambiente del centro de cálculo

Consolas

Monitorización y ajuste del sistema

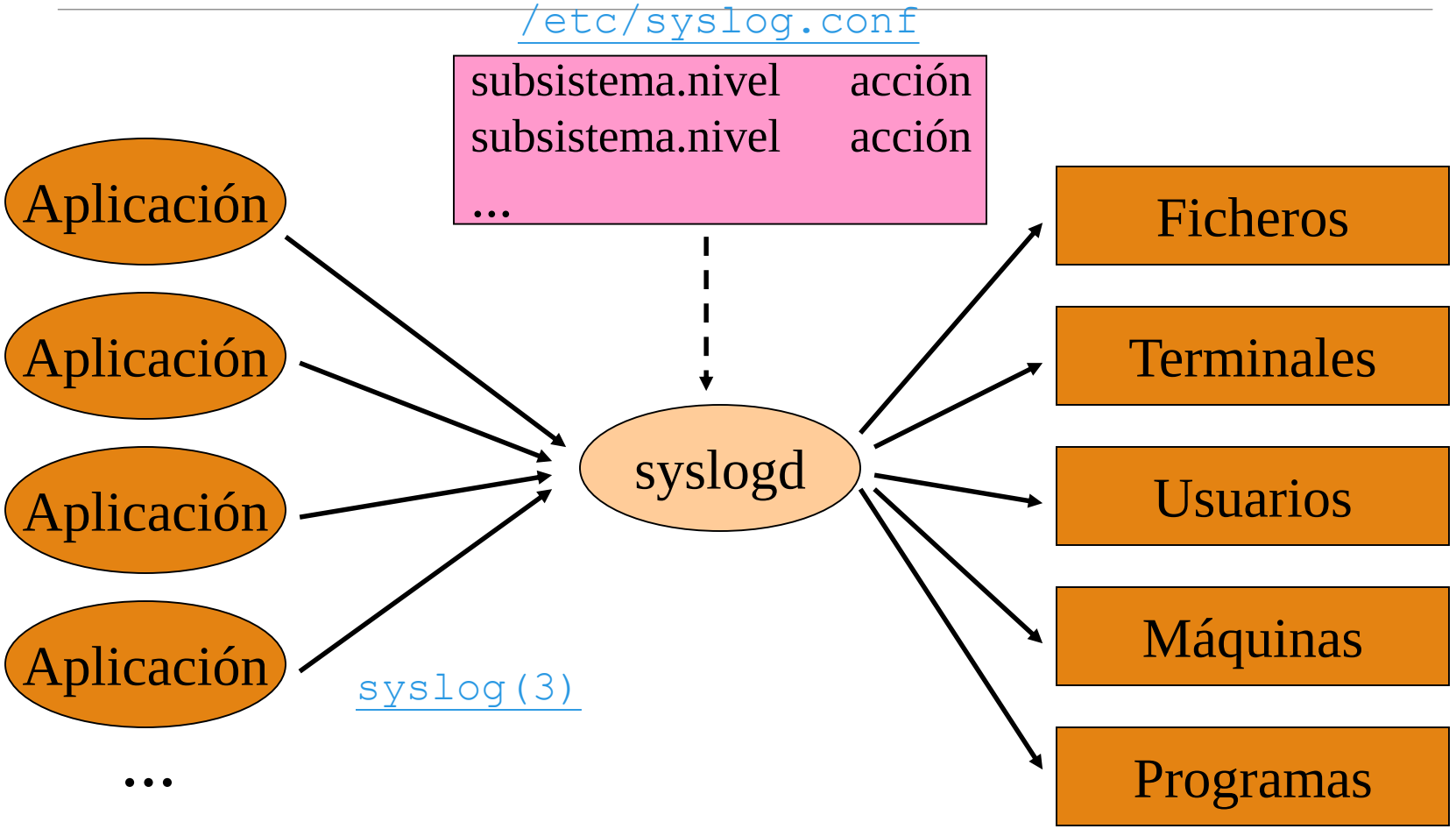
Datos históricos
- syslogd
- vmstat, iostat, fstat, pstat, netstat, nfsstat, ipcs...

Datos en tiempo real
- vmstat, iostat, fstat, pstat, netstat, nfsstat, ipcs...
- ktrace/kdump

Paquetes de software
- Nagios, Zabbix, Snort…

Ajuste
- sysctl
- recompilación del núcleo

syslogd


/etc/syslog.conf
subsistema.nivel acción
subsistema.nivel acción
...
Aplicación
Aplicación
Aplicación
Aplicación
...
syslogd
syslog(3)
Ficheros
Terminales
Usuarios
Máquinas
Programas

Ejemplo de /etc/syslog.conf

```
*.err;auth.notice;mail.crit    /dev/console
*.notice;kern.debug;mail.crit  /var/log/messages
mail.info                      /var/log/maillog
lpr.info                       /var/log/lpd-errs
cron.*                         /var/log/cron
*.err                          root
daemon.=debug                  /opt/pru/daem-pruebas
*.emerg                        *
*.emerg                        @madre.oceano.es
security.*                     /var/log/security
local0.*                       |exec /usr/bin/xms
!ppp
*.*                            /var/log/ppp.log
```

Rotación de ficheros (newsyslog)

/etc/newsyslog.conf

```
/var/log/cron                600  3     1000 *        J
/var/log/debug.log           640  5     *    24       J
/var/log/daily.log           640  7     *    @T00     JN
/var/log/maillog             640  7     *    $W6D0    J
/var/log/monthly.log         640  12    *    $M1D0    JN
/var/log/sendmail.st         640  10    *    168      B
```

Herramientas de monitorización

vmstat

iostat

fstat

pstat

netstat

nfsstat

systat

ipcs

uptime

sar

top

xperfmon++

xsystat

xload

gkrellm

Nagios

Zabbix

Snort

Ejemplo de datos estadísticos

vmstat -w 5

```
procs      memory      page                    disks     faults      cpu
r b w      avm    fre  flt  re  pi  po  fr  sr ad0 ac0   in   sy  cs us sy id
0 4 0   218480   8676    3   0   0   0   0   0   0   0  245  931 288  0  8 92
3 4 0   218480   8668    4   0   6  13   0   0   0   0  239  855 258 22  4 75
4 4 0   219064  11352   75   0   2   0  74 149  31   0  267  929 344 84 10  6
```

fstat

```
USER     CMD          PID   FD MOUNT      INUM MODE         SZ|DV R/W
javier   less        3540 text /usr     299801 -r-xr-xr-x   77824  r
javier   tcsh        1534   wd /home   3102976 drwxr-xr-x    5120  r
isabel   soffice.bin 1409    8 /home   1853302 -rw-r--r--  280616  r
jgarcia  kvt          441    5 /          6519 crw-rw-rw-   ptyp2 rw
```

iostat -w 5

```
tty             ad0              cpu
tin tout  KB/t tps  MB/s  us ni sy in id
  1   42  6.85  50  0.33   4  0 16  2 78
  0    0  3.07 182  0.54   4  0 17  2 77
  1    9  2.19 101  0.22   2  0  9  3 86
  0    0  3.74 124  0.45   4  0 10  2 85
  1    5  3.88  70  0.26   2  0  5  2 91
```