

Seguretat, rendiment i recursos

Joan Francesc Muñoz Pastor

Implantació de sistemes operatius (ASX)
Sistemes informàtics (DAM)
Sistemes informàtics (DAW)

Índex

| | |
|---|-----------|
| Introducció | 5 |
| Resultats d'aprenentatge | 7 |
| 1 Assegurament de la informació | 9 |
| 1.1 Associació de discos | 10 |
| 1.1.1 Volums distribuïts | 10 |
| 1.1.2 Volums dividits en bandes. Sistema RAID 0 | 11 |
| 1.2 Tolerància a fallades del maquinari | 12 |
| 1.3 Sistemes redundants RAID | 12 |
| 1.3.1 Sistema RAID 1 | 14 |
| 1.3.2 Sistema RAID 3 | 14 |
| 1.3.3 Sistema RAID 5 | 15 |
| 1.3.4 Sistema RAID 6 | 16 |
| 1.3.5 Sistema RAID 1+0 | 16 |
| 1.3.6 Sistema RAID 0+1 | 17 |
| 1.4 Associació d'ordinadors: clusterització | 17 |
| 1.5 Còpies de seguretat | 19 |
| 1.5.1 Tipus i nivells de còpies de seguretat | 20 |
| 1.5.2 Plans i programació de còpies de seguretat | 21 |
| 1.5.3 Programes i utilitats de la còpia de seguretat | 23 |
| 1.6 Recuperació en cas de fallada del sistema | 27 |
| 1.6.1 Punts de restauració | 27 |
| 1.6.2 Còpies de seguretat del sistema | 27 |
| 1.6.3 Opcions d'arrencada avançades | 28 |
| 1.6.4 Discos d'arrencada i de recuperació | 29 |
| 1.6.5 Recuperació del sistema en entorns virtualitzats | 30 |
| 2 Supervisió del rendiment del sistema | 31 |
| 2.1 Monitoratge del rendiment dels components d'un sistema informàtic | 32 |
| 2.1.1 Tipus de monitoratge | 32 |
| 2.1.2 Eines de monitoratge de rendiment a Windows | 33 |
| 2.1.3 Eines de monitoratge de rendiment a Linux | 36 |
| 2.1.4 Alertes de rendiment | 41 |
| 2.2 Enregistrament i monitoratge d'esdeveniments | 42 |
| 2.2.1 Eines d'enregistrament i monitoratge d'esdeveniments a Windows | 43 |
| 2.2.2 Eines d'enregistrament i monitoratge d'esdeveniments a Linux | 45 |
| 2.3 Gestió d'aplicacions i processos | 47 |
| 2.3.1 Conceptes d'aplicació, procés i servei | 47 |
| 2.3.2 Eines de gestió de tasques i processos a Windows | 48 |
| 2.3.3 Eines de gestió de tasques i processos en Linux | 49 |

| | | |
|----------|---|-----------|
| 3 | Directives de seguretat i auditories | 53 |
| 3.1 | Auditoria de sistemes informàtics | 53 |
| 3.1.1 | Àmbit de l'auditoria, aspectes auditables | 54 |
| 3.1.2 | Mecanismes d'auditoria. Informes, alarmes i accions correctives | 55 |
| 3.2 | Auditoria en sistemes operatius propietaris | 58 |
| 3.2.1 | Drets d'usuari | 58 |
| 3.2.2 | Directives de seguretat local | 58 |
| 3.2.3 | Eines d'auditoria | 59 |
| 3.2.4 | Registre de seguretat | 64 |
| 3.3 | Auditoria en sistemes operatius lliures | 64 |
| 3.3.1 | El paquet de gestió de registres syslog | 64 |
| 3.3.2 | Visualitzador d'arxius de registre | 67 |
| 3.3.3 | Auditoria d'usuaris i processos | 68 |
| 3.3.4 | Auditoria de la xarxa | 69 |
| 3.3.5 | Distribucions Linux especialitzades en auditoria i seguretat | 73 |

Introducció

Una vegada el sistema informàtic d'una empresa està en fase de producció, és a dir, està instal·lat, configurat i dona servei als usuaris, no s'acaba la feina de l'administrador de sistemes. Cal assegurar la continuïtat d'aquest servei en unes condicions òptimes, un concepte que s'anomena *disponibilitat* i que està relacionat amb la capacitat de mantenir l'operativitat del sistema malgrat les possibles fallades del maquinari o del programari.

Així doncs, l'apartat "Assegurament de la informació" d'aquesta unitat d'una banda tractarà dels sistemes de tolerància a fallades de maquinari, posant èmfasi en les solucions basades en els sistemes d'associació de discos RAID i, de l'altra, en cas de pèrdua d'informació, s'analitzaran les accions preventives més habituals mitjançant polítiques, plans i programació de còpies de seguretat. Finalment, si no s'ha pogut evitar la caiguda del sistema, es veuran els diversos mecanismes de recuperació del sistema per restituir el servei.

Hem de tenir present que no solament s'ha de garantir la continuïtat del servei sinó que a més aquest ha d'estar optimitzat i oferir en tot moment un rendiment adequat. Per poder valorar el rendiment del sistema, com a pas previ a accions per millorar-lo, es poden fer servir eines de monitoratge dels diferents components del sistema informàtic. Aquestes eines es tractaran en l'apartat "Supervisió del rendiment del sistema"; poden ser de monitoratge continu o de visualització en temps real i es complementen amb arxius on s'enregistren els esdeveniments més rellevants per poder observar-los, analitzar-los i avaluar-los.

Per acabar, l'apartat "Directives de seguretat i auditories" se centra en la seguretat del sistema i l'auditoria com a mecanisme de prevenció de pèrdues d'informació i avaries provocades per desconeixement o per atacs maliciosos d'usuaris, tant si són autoritzats com si no. En aquest sentit es farà esment del dret dels usuaris i de les polítiques i directives de seguretat local, com també de l'ús dels registres d'auditoria que permeten establir mecanismes de seguiment i alarma per endegar les accions correctives adequades.

Per treballar els continguts d'aquesta unitat, és convenient dur a terme les activitats i els exercicis d'autoavaluació del material web. D'altra banda, en el mapa conceptual de la unitat es presenta una visió general i integradora de tots els conceptes i les interrelacions d'aquests.

Resultats d'aprenentatge

En finalitzar aquesta unitat, l'alumne/a:

1. Gestiona còpies de seguretat i sistemes tolerants a errors:

- Implementa sistemes d'emmagatzematge redundant (RAID).
- Implementa i automatitza plans de còpies de seguretat.
- Documenta les operacions realitzades i els mètodes que cal seguir per a la recuperació en cas de desastres.

2. Detecta problemes de rendiment monitorant el sistema amb les eines adequades i documentant el procediment:

- Identifica els objectes monitorant en un sistema informàtic.
- Identifica els tipus d'esdeveniments.
- Utilitza eines de monitoratge en temps real.
- Monitora el rendiment mitjançant registres de comptador i de seguiment del sistema.
- Planifica i configura alertes de rendiment.
- Interpreta els registres de rendiment emmagatzemats.
- Analitza el sistema mitjançant tècniques de simulació per optimitzar el rendiment.
- Elabora documentació de suport i d'incidències.

3. Audita la utilització i l'accés a recursos identificant i respectant les necessitats de seguretat del sistema:

- Administra drets d'usuari i directives de seguretat.
- Identifica els objectes i els esdeveniments auditables.
- Elabora un pla d'auditories.
- Identifica les repercussions de les auditories en el rendiment del sistema.
- Audita esdeveniments correctes i erronis.
- Audita els intents d'accés i els accessos a recursos del sistema.
- Gestiona els registres d'auditoria.
- Documenta el procés d'auditoria i els resultats obtinguts.

1. Assegurament de la informació

Cada vegada més, la seguretat i la fiabilitat són un aspecte crucial en l'administració de sistemes informàtics que s'enfronta a un gran nombre d'amenaques i perills com ara els següents:

- **Pèrdua de dades.** Pèrdua per motius de força major (incendis, inundacions, etc.), per avaries de maquinari i de programari o per errors humans amb l'esborrament accidental o intencionat de la informació.
- **Pèrdua de disponibilitat.** Interrupció o degradació del servei per causes diverses com ara talls elèctrics, avaries o problemes en les comunicacions.
- **Intrusions.** Poden ser tant passives per la recollida de dades i espionatge com actives d'atacs maliciosos amb afectació de dades i de servei.

El concepte **disponibilitat** està relacionat amb la continuïtat operacional d'un sistema al llarg d'un període determinat i s'acostuma a expressar com un percentatge que indica el temps de funcionament i servei adequat en un temps donat.

Per exemple, una disponibilitat del 99,99% implica menys de 54 minuts de caiguda del sistema a l'any. El cost d'un sistema s'incrementa exponencialment en millorar-ne la disponibilitat, per la qual cosa sempre s'ha de cercar una solució de compromís adequada.

Aquests perills condicionen la fiabilitat del sistema. Quan parlem d'assegurar la informació ens referim a evitar-ne la pèrdua i mantenir el servei millorant la fiabilitat del sistema mitjançant els aspectes següents:

- **Prevenició de fallades.** Treballant per evitar i prevenir els errors del sistema amb mesures proactives, per exemple triant components fiables i de qualitat en el cas del maquinari i fent servir programari rigorosament dissenyat i provat. També és un bon costum preventiu l'ús periòdic d'eines de comprovació de la memòria o de la integritat del sistema d'arxius que solen posar al nostre abast els diferents sistemes operatius.
- **Emmascarament de les fallades.** Aconseguir que, quan es produeixi una fallada en un component de maquinari o programari, aquesta no esdevingui un error del sistema. Per exemple, els paquets IP porten un camp de control CRC (*cyclic redundancy check*) que permet detectar si hi ha hagut alguna fallada en la comunicació. Si aquest error es produeix, el paquet es descarta i es torna a sol·licitar sense afectar el sistema.
- **Tolerància a fallades.** Per aconseguir que el sistema continuï disponible i operatiu encara que es produeixin errades i avaries. La tolerància a

Fiabilitat

La fiabilitat (*reliability*) és una mesura de la conformitat d'un sistema amb el comportament que n'esperem al llarg del temps quan opera en l'entorn en què ha estat dissenyat.

Disposem d'eines de comprovació de la integritat del sistema d'arxius tant en Windows (ordre `chkdsk`) com en Linux (ordre `fsck`).

CRC

Els codis de redundància cíclica (CRC, *cyclic redundancy check*) són funcions polinòmiques que generen un valor fix obtingut en funció del processament d'un flux de dades determinat. Aquest valor fix es pot fer servir com a verificació, detecció i control d'errors en la transmissió d'aquestes dades.

fallades es basa en el concepte de redundància que es pot aplicar a diferents subsistemes i nivells:

- **Redundància de maquinari.** Per exemple, duplicant línies de subministrament, fonts d'alimentació, controladors o fins i tot treballant amb diferents servidors alhora (*clustering*) que poden prendre el control i mantenir el servei encara que caigui un dels nodes.
- **Redundància en les dades.** Mitjançant matrius i associacions de discos que emmagatzemen informació addicional, fins i tot duplicada, per restituir-la en cas d'avaría d'un d'ells. És el cas dels sistemes RAID.
- **Còpies de seguretat.** Consisteix a copiar íntegrament la informació fora del sistema d'explotació habitual en suports d'emmagatzematge independents.

1.1 Associació de discos

El disc dur és un dels elements més delicats del sistema informàtic. Atès que es tracta d'un sistema electromecànic que consisteix en uns plats d'alumini que giren a una gran velocitat, sembla lògic pensar que tant la seva fiabilitat com rapidesa seran inferiors a altres components de l'arquitectura de l'ordinador basats només en components electrònics i sense parts mòbils.

Per millorar les seves prestacions, els discos durs es poden associar en diferents sistemes per aprofitar més la capacitat que tenen, incrementar la velocitat d'accés o bé la seva fiabilitat i tolerància a errades. Així, els **volums distribuïts** ens permeten redistribuir i aprofitar els espais lliures, els **volums dividits en bandes** proporcionen una millora en les prestacions d'accés de lectura o escriptura, i també hi ha tota una sèrie d'associacions de discos anomenades **RAID** que proporcionen la redundància en les dades necessària per millorar la fiabilitat i la seguretat en cas d'avaries.

1.1.1 Volums distribuïts

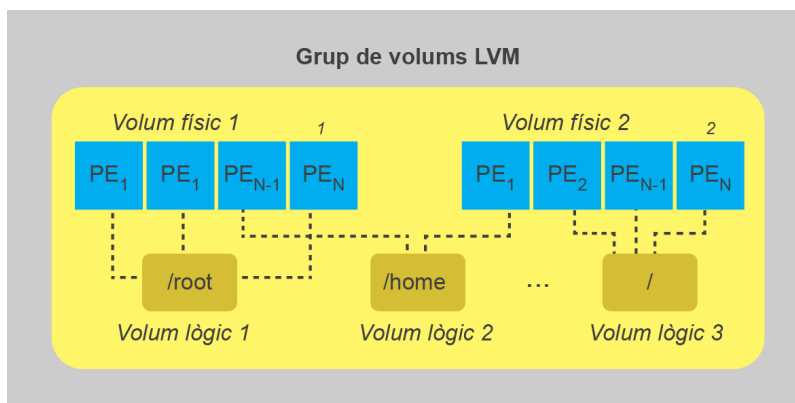
Quan volem crear un volum nou, però no tenim prou espai en un mateix disc i en canvi hi ha espai lliure en altres discos o particions, podem crear un **volum distribuït**. Ho aconseguim agafant espais lliures de diferents discos i combinant-los sota el mateix volum lògic. Identificarem aquest conjunt d'espais físics amb una única lletra, la lletra identificativa del volum lògic. Amb aquest tipus de volum aconseguim gestionar més bé l'espai de disc, ja que ens permet aprofitar petits espais lliures que d'una manera aïllada no ens eren útils. Tant Linux com Windows ens proporcionen eines per a la gestió d'aquests volums:

- **Gestor de discos de Windows.** Dintre de les eines administratives que ens

ofereixen les diferents versions de Windows, disposem de l'administrador de discos que permet la gestió de volums simples, volums distribuïts, volums seccionats (RAID 0), volums mirall (RAID 1), i també associacions RAID 5.

- **Gestor LVM de Linux.** El sistema gestor de volums lògics LVM de Linux (*logical volume manager*) utilitza volums físics (que poden ser discos sencers o particions d'un disc) que gestiona en fragments anomenats *extensions físiques* (PE, *physical extents*). Un conjunt d'aquests fragments constitueixen un volum lògic que es pot fer servir per muntar un sistema d'arxius o una partició d'intercanvi (*swap*). LVM suporta redimensionament de volums, creació d'instantànies de l'estat del volum i implementació de sistemes RAID 0 i RAID 1. En la figura 1.1 es mostra un esquema de dos volums físics que formen tres volums lògics en què es munten diferents sistemes d'arxius.

FIGURA 1.1. Esquema LVM



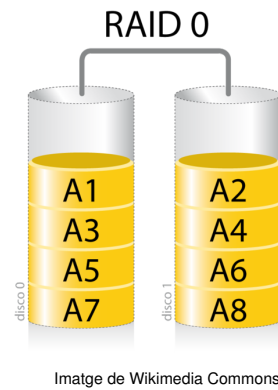
1.1.2 Volums dividits en bandes. Sistema RAID 0

El sistema RAID 0 també s'anomena **sistema de distribució en bandes**.

Els volums o conjunts dividits en bandes (*striped set* o *striped volume*) són una associació de discos que permet millorar les prestacions i la velocitat de lectura o escriptura del sistema d'emmagatzematge. Encara que també s'acostuma a anomenar *RAID 0* no són en rigor pròpiament un sistema RAID, ja que no aporta cap redundància a les dades. Per implementar aquest sistema es necessiten com a mínim dos discos i consisteix a dividir la informació en tantes parts (bandes) com discos durs instal·lats hi hagi i emmagatzemar cada part en un disc diferent d'una manera simultània. El temps de lectura i escriptura millora molt atès que s'accedeix al mateix temps a diferents discos, si bé, com que no té la informació redundant, no proporciona tolerància a errades i, per tant, s'ha de tenir previst algun altre mecanisme de seguretat per poder recuperar la informació en cas de pèrdua.

En la figura 1.2 es pot veure l'esquema conceptual d'aquest sistema.

FIGURA 1.2. Esquema d'implementació del RAID 0



1.2 Tolerància a fallades del maquinari

La **tolerància a fallades** d'un sistema informàtic és la característica que determina la capacitat del sistema a continuar funcionant correctament quan s'ha produït una fallada. Aquestes fallades es poden produir en el maquinari o en el programari.

La tolerància a errades es pot definir en tres nivells segons les necessitats i la importància de l'aplicació:

- **Tolerància completa.** El sistema continua funcionant, si més no per un temps, sense perdre funcionalitat ni prestacions.
- **Degradació acceptable.** El sistema continua funcionant amb una pèrdua parcial de funcionalitat i prestacions fins a la solució de la incidència.
- **Parada segura.** El sistema s'atura de manera ordenada per assegurar l'entorn i les dades fins a la solució de la incidència.

Si ens centrem en les fallades de maquinari, les fallades de disc són una de les més crítiques per al sistema, ja que solen comportar la pèrdua de les dades que conté, per això és un dels elements on es centren els esforços en incrementar la tolerància a errades, per exemple implementant sistemes RAID.

1.3 Sistemes redundants RAID

Un mecanisme que permet incrementar la tolerància a fallades dels discos durs és la implementació de redundància en les dades mitjançant l'associació de discos RAID.

RAID, acrònim en anglès de *redundant array of independent disks* (matriu redundat de discos independents), és un sistema d'emmagatzematge de la informació que organitza les dades en diversos discos durs, però que tenen una lògica de funcionament única (aparentment funcionen com un únic disc). L'objectiu d'aquesta associació de discos és poder augmentar el rendiment d'escriptura o lectura i el grau de disponibilitat i protecció de les dades.

La implementació del sistema RAID pot ser:

- **Implementació per maquinari.** Cal que el sistema incorpori un controlador de disc que permeti la redundància, que s'encarregui de la gestió dels discos i de la gestió de les lectures o escriptures de les dades en aquests, i si s'escau faci tots els càlculs de paritat dels sistemes RAID que ho requereixin.
- **Implementació per programari.** Consisteix en una simulació del sistema anterior per programa, es a dir, és el propi sistema operatiu qui ho gestiona, utilitzant els controladors de discos existents). El cost econòmic de la implementació sol ser més petit, però el temps del procés pot alentir força el sistema.

Es recomana la implementació dels sistemes RAID per a maquinari, ja que és més eficaç, ràpida i robusta.

El diferents nivells RAID són independents entre si i cadascun està pensat per donar solució a estratègies diferents d'assegurament de la informació.

Hi ha molts tipus i nivells de RAID estandarditzats, però els més emprats són el RAID 1, el RAID 3 i el RAID 5, perquè són relativament fàcils d'implementar i tenen una efectivitat alta i un cost no massa elevat. En la figura 1.3 es pot veure un conjunt de discos associats en RAID 5.

FIGURA 1.3. Sistema RAID 5



Imatge d'Axel Schwenke

Si combinem dos o més nivells de RAID simples, el nou nivell de RAID resultant serà un RAID múltiple, si bé els nivells de RAID simples són més freqüents, ja que aporten una eficàcia suficient en la majoria dels casos.

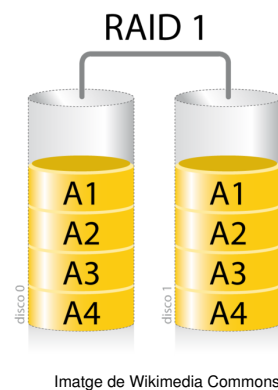
1.3.1 Sistema RAID 1

El sistema RAID 1 és un sistema simple de duplicació de la informació i no implementa paritat ni distribució en bandes.

Aquest sistema, també conegut com a *associació de discos en mirall (mirror)*, consisteix a tenir la informació duplicada en dos discos o més, de manera que ofereix un sistema molt tolerant a les fallades. Les escriptures es fan, doncs, per duplicat, i això fa que puguin ser una mica més lentes. L'inconvenient principal, però, és la quantitat d'espai de disc que es malbarata, ja que representa un aprofitament dels recursos d'emmagatzematge de tan sols el 50%. Per exemple, si es disposa de dos discos de 100 Gb fa un total de 200 Gb de recursos d'emmagatzematge, però amb un sistema RAID 1 només es podran escriure 100 Gb d'informació útil, ja que queda duplicada, i s'aprofitarà efectivament només el 50% de l'espai.

En el cas d'avaria d'un dels discos, l'altre assumeix el control amb una disponibilitat immediata i sense pèrdua d'informació. Per les característiques que té, aquest sistema es recomana en aplicacions en què la seguretat i l'alta disponibilitat siguin essencials. En la figura 1.4 es pot veure l'esquema conceptual d'aquest sistema:

FIGURA 1.4. Esquema d'implementació del RAID 1



Bit de paritat

El codi de paritat és un bit addicional que s'afegeix a les dades i que es calcula en funció de la resta de bits d'informació proporcionant d'aquesta manera un sistema senzill de detecció d'errors. El codi de paritat parell és el més emprat i el seu valor fa que el conjunt de bits de valor 1 en les dades sigui un nombre parell. La paritat parell es calcula amb facilitat amb portes lògiques de tipus XOR.

1.3.2 Sistema RAID 3

El sistema RAID 3 és un sistema simple de distribució en bandes a nivell de byte amb disc de paritat dedicada.

Aquest sistema divideix la informació en bytes i en calcula la paritat per permetre la reconstrucció de les dades en cas d'avaria. Tota la informació de paritat

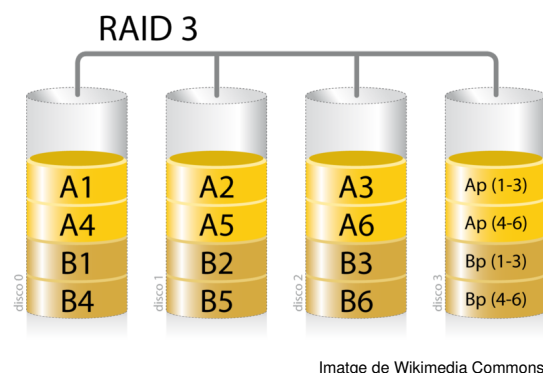
s'emmagatzema en un disc a part i, per tant, calen tres discos com a mínim per implementar un sistema RAID 3, dos discos per a les dades i un tercer per a la paritat. El càlcul de la paritat pot alentir una mica el procés d'enregistrament de dades i l'accés intensiu i continuat a aquest disc de paritat pot generar un coll d'ampolla.

El sistema RAID 3 fa un aprofitament de l'espai d'emmagatzematge que depèn del nombre de discos associats segons la fórmula $(n-1)/n$, en què n és el nombre de discos del RAID. Així, tenim que un sistema RAID 3 de cinc discos durs realment només n'aprofita quatre, ja que es fa servir el cinquè per emmagatzemar la paritat. L'aprofitament en aquest cas seria del 80% (cinc discos en total per quatre discos de dades efectives).

Quan un dels discos del RAID té una avaria, es perden dades, però es poden reconstruir fent servir la informació extra de paritat de què disposem.

Aquest sistema es recomana per a aplicacions monousuari que treballin amb grans registres com ara aplicacions d'imatge i vídeo. En la figura 1.5 es pot veure l'esquema conceptual d'aquest sistema.

FIGURA 1.5. Esquema d'implementació del RAID 3



1.3.3 Sistema RAID 5

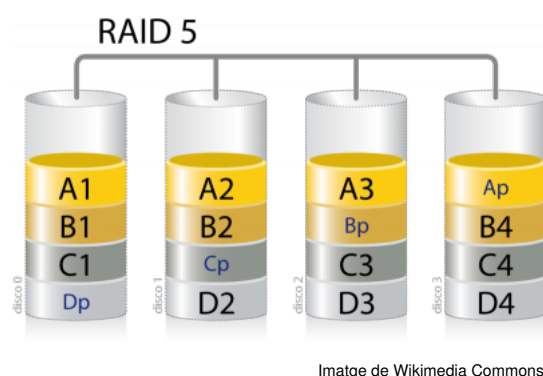
El sistema RAID 5 és un sistema simple de distribució en bandes a nivell de bloc amb paritat distribuïda.

Aquest sistema soluciona la majoria dels inconvenients del RAID 3. En primer lloc divideix la informació en blocs, no en bytes. També calcula la paritat d'aquests blocs, però, a diferència de RAID 3, no acumula aquesta informació en un sol disc sinó que la distribueix de manera homogènia i rotatòria en tots els discos, amb la qual cosa evita el coll d'ampolla d'un disc dedicat exclusivament a guardar la paritat. Tot això justifica que sigui una de les configuracions més utilitzades, ja que té un rendiment i un grau de tolerància a les fallades elevats. Es necessiten tres discos com a mínim per implementar un RAID 5 i l'aprofitament de l'espai d'emmagatzematge també depèn del nombre de discos associats i es calcula igual que en el cas de RAID 3.

Si un dels discos d'un RAID 5 falla es pot reconstruir la informació amb l'ajut de les dades de paritat. Tanmateix, en aquest cas, la velocitat de transferència de dades queda penalitzada per aquest procés de reconstrucció.

Aquest nivell RAID es recomana per a aplicacions que treballin amb arxius petits, però amb moltes transaccions d'entrada i sortida com és el cas de les bases de dades relacionals i les aplicacions de gestió. En la figura 1.6 es pot veure la informació del bloc de dades A distribuït en diversos discos, i la informació de paritat corresponent del bloc (Ap) en un altre disc. D'una manera anàloga s'observen els blocs B, C i D.

FIGURA 1.6. Esquema d'implementació del RAID 5



1.3.4 Sistema RAID 6

El sistema RAID 6 és un sistema simple de distribució en bandes a nivell de bloc amb doble paritat distribuïda.

Aquest sistema és semblant al RAID 5 però afegeix un segon bloc de paritat que també distribueix entre tots els membres de l'associació de discos.

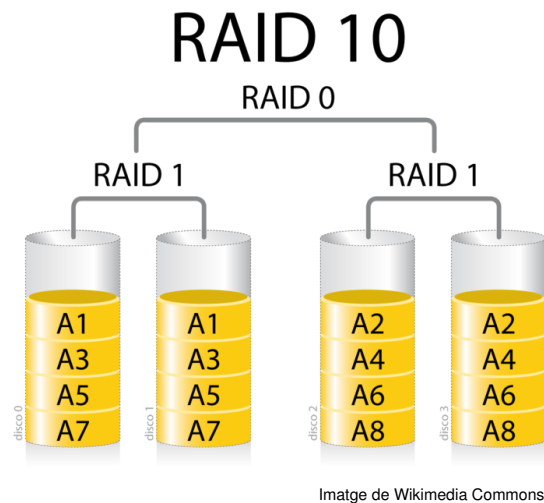
Es necessiten quatre discos com a mínim per implementar un RAID 6, i l'aprofitament de l'espai d'emmagatzematge depèn del nombre de discos associats i es calcula segons la fórmula $(n-2)/n$, en què n és el nombre de discos del RAID. Així, tenim que d'un sistema RAID 6 de cinc discos durs realment només se n'aprofiten tres, ja que se'n fan servir dos per emmagatzemar la paritat. En aquest cas, l'aprofitament seria del 60% (tres discos de dades efectives d'un total de cinc discos). És per això que el RAID 6 és una mica ineficient quan es tracta de conjunts petits de discos, però en canvi té el gran avantatge de proporcionar protecció contra fallades de dos discos alhora o contra possibles fallades i avaries en el moment crucial en què s'estan reconstruint les dades d'un disc avari.

1.3.5 Sistema RAID 1+0

El sistema RAID 1+0 és un sistema múltiple de distribució en bandes emmirallat.

Es tracta d'un exemple de RAID múltiple anomenat *RAID 1+0* o, també, *RAID 10*, en què un volum dividit en bandes per incrementar el rendiment d'accés (RAID 0) es duplica cada banda en mirall (RAID 1) per obtenir també tolerància a fallades. Encara que té una implementació més costosa, ja que calen com a mínim quatre discos durs, és un sistema recomanat per servidors de dades que requereixin al mateix temps altres prestacions d'accés i una gran fiabilitat. Fins i tot, en uns casos determinats, aquest sistema pot suportar la fallada de més d'un disc dur. En la figura 1.7 es mostra l'esquema d'implementació d'aquest RAID múltiple.

FIGURA 1.7. Esquema d'implementació del RAID 10



1.3.6 Sistema RAID 0+1

El sistema RAID 0+1 és un sistema múltiple de distribució en mirall en què cada mirall es divideix i es desa en bandes.

En el cas del RAID 0+1, les dades són primer duplicades per obtenir tolerància a errades i després cada una de les còpies és dividida en bandes i enregistrada en diferents discos durs simultàniament per millorar prestacions. No s'ha de confondre aquest sistema amb el RAID 1+0, encara que el requeriment d'espai de disc, el seu aprofitament i les prestacions d'accés són semblants.

Cal dir que el sistema RAID 1+0 proporciona una tolerància millor a errades i unes prestacions millors quant a la reconstrucció de la informació en cas de fallada d'una de les unitats.

1.4 Associació d'ordinadors: clusterització

No solament es poden associar discos durs en RAID, sinó que també es poden interconnectar ordinadors en associacions que treballen com un de sol, la qual cosa n'incrementa les prestacions quant a rendiment, seguretat i disponibilitat.

Un **clúster** és una associació d'ordinadors interconnectats mitjançant connexions d'alta velocitat i baixa latència per dur a terme el processament de manera paral·lela i distribuïda i aconseguir millores en rendiment, distribució de càrregues, escalabilitat i alta disponibilitat.

Grid computing

Una variació del sistema de clúster en què els ordinadors que hi participen poden estar distribuïts mundialment i enllaçats mitjançant Internet s'anomena **computació en malla** (de l'anglès *grid computing*). Encara que Internet no reuneix les millors condicions de latència i amplada de banda, la seva popularització ha fet sorgir projectes de computació distribuïda per aprofitar la quota de microprocessador no utilitzada dels ordinadors personals connectats a aquesta xarxa i així aconseguir fer tasques que demanen una gran quantitat de recursos i potència de càlcul a un cost molt baix i de manera col·laborativa.

Amb aquestes característiques els clústers donen suport a aplicacions que van des de la supercomputació fins a les aplicacions crítiques, passant pels servidors web, el comerç electrònic i les bases de dades d'alt rendiment. La computació basada en clústers sorgeix gràcies a la disponibilitat de microprocessadors d'alt rendiment més econòmics, la popularització de les xarxes d'alta velocitat, i també gràcies al desenvolupament d'eines de programari per a còmput distribuït, tot això davant la necessitat creixent de potència de còmput per a aplicacions en les ciències i en el àmbit comercial, i també la necessitat de disponibilitat permanent en alguns serveis.

Així doncs, les aplicacions principals dels clústers les podem classificar així:

El clúster de Google

El conegut cercador **Google** disposa de milers d'ordinadors associats en clúster sota sistema operatiu Linux, per així poder donar suport ràpid i eficient a la quantitat ingent de peticions i consultes d'informació sobre la seva base de dades de pàgines i recursos web.

- **Clústers d'alt rendiment.** Es busca crear sistemes amb una gran capacitat de processament i càlcul per executar aplicacions numèriques grans i complexes; per exemple, executar aplicacions científiques de predicció del temps, modelatge molecular, desxifratge del genoma, criptografia, etc.
- **Clústers per al balanceig de càrregues.** Els ordinadors del clúster comparteixen i es reparteixen la càrrega de treball i el trànsit dels clients. Així milloren el temps de resposta i la disponibilitat aprofitant més bé els recursos de què es disposa.
- **Clústers d'alta disponibilitat.** La redundància de servidors permet l'alta disponibilitat, ja que en treballar en paral·lel i amb redundància poden assumir les caigudes d'alguns. A més de disposar de maquinari redundant, el programari del clúster ha d'estar preparat per detectar la fallada d'un node quan es produeix i reconfigurar i distribuir la càrrega del sistema perquè el servei no es vegi afectat.

A més de les prestacions i aplicacions que s'han descrit, els clústers presenten altres avantatges importants com ara:

- **Facilitat d'administració.** Com a conseqüència de ser administrats des d'un únic punt central. A més si cal fer tasques de reparació en un node, aquest es pot desconnectar del clúster, sense que la resta de nodes deixin de funcionar.

- **Escalabilitat.** Un sistema de clusterització (*clustering*) és fàcil d'ampliar, ja que només cal afegir més nodes al sistema. D'aquesta manera es pot anar ajustant a les necessitats i requeriments canviants de la demanda de processament.

Segons les característiques del maquinari i programari associat, els clústers es poden classificar en:

- **Clústers homogenis.** Tots els equips (nodes) que formen el clúster tenen la mateixa configuració de maquinari i programari. Els programes es poden executar en qualsevol equip sense notar diferències.
- **Clústers semihomogenis.** Tots els nodes del clúster tenen una configuració de programari similar, encara que presenten maquinaris diferents. Els programes es poden executar en qualsevol node encara que amb rendiments diferents.
- **Clústers heterogenis.** Els nodes del clúster tenen configuracions de maquinari i programari diferents. No tots els serveis que ofereix un clúster es poden executar en tots els nodes.

Un clúster d'alta disponibilitat té dues estratègies possibles per respondre davant la caiguda d'un dels nodes:

1. **Actiu-passiu.** En el clúster hi ha nodes actius que executen les aplicacions, i altres de passius que no fan res però estan de suport. Si un node actiu cau, un dels passius s'activa i el substitueix. Davant una fallada es manté el servei i el rendiment del sistema. Comporta un cost més elevat per la necessitat de maquinari extra habitualment inactiu.
2. **Actiu-actiu.** Tots els nodes del clúster estan actius i executant aplicacions. Si un cau, el treball que feia es reparteix entre la resta de nodes. Davant una fallada d'un node, el clúster manté el servei, però el rendiment del clúster es redueix. Només és possible en clústers homogenis o semihomogenis.

1.5 Còpies de seguretat

Com a administradors, podem optimitzar les condicions de treball del sistema informàtic i minimitzar les fallades dels discos. Tot i així, la realitat és que els discos i els ordinadors fallen. Quan un disc s'avaria, perdem la informació que conté emmagatzemada. L'única solució per poder recuperar aquesta informació és tenir-la duplicada en un altre lloc, és a dir, tenir còpies d'aquesta informació en un suport diferent.

La **còpia de seguretat** (*backup*) és la còpia i emmagatzematge de les dades en un suport físic diferent, de manera que, en cas de fallada del suport de les dades originals, permet recuperar la informació del sistema informàtic.

A banda de les dades, es pot tenir la necessitat de salvaguardar programari o arxius clau del sistema operatiu. La còpia d'aquest programari i, fins i tot, del mateix sistema operatiu també està inclosa dins del concepte de còpia de seguretat.

Sistema gestor de bases de dades (SGBD)

Un SGBD és un programari específic dedicat a gestionar bases de dades (és a dir, conjunts de dades relacionats entre ells) per tal de facilitar, entre d'altres, l'emmagatzematge i l'accés a la informació.

En la majoria de sistemes informàtics, la major part de les dades estan organitzades per un sistema gestor de bases de dades (SGBD). En aquest cas, com que la majoria de SGBD actuals ofereixen les seves pròpies opcions per realitzar còpies de seguretat, és útil integrar-les dintre de la política de còpies de seguretat del sistema. Per a la resta de dades del sistema, caldrà utilitzar eines externes (programari especialitzat per realitzar còpies de seguretat) o bé aprofitar algunes eines que ja incorporen els mateixos sistemes operatius.

1.5.1 Tipus i nivells de còpies de seguretat

Les còpies de seguretat es poden classificar per nivells:

- **Nivell 0: Còpia total.** Periòdicament, es realitza una còpia completa de totes les dades que s'han de guardar. Aquest sistema és simple, però requereix emmagatzemar una gran quantitat de dades i el procés de còpia necessita un temps considerable. La restauració és senzilla però lenta.
- **Nivell 1: Còpia diferencial.** És una còpia parcial de les dades que han canviat respecte a la darrera còpia de nivell 0. Per tant, per restaurar, s'ha de recuperar la còpia total i l'última còpia diferencial, que conté tots els canvis i novetats respecte a la còpia total.
- **Nivell 2: Còpia incremental.** És una còpia parcial de les dades que han canviat respecte a la darrera còpia de qualsevol nivell. Les còpies parcials són més ràpides, i el volum total de dades per emmagatzemar és inferior que en el sistema de còpia total. La restauració, però, és lenta perquè cal recuperar la darrera còpia de nivells inferiors i aplicar-hi totes les incrementals següents fins a la darrera.

Un exemple de política de còpies de seguretat podria ser una empresa que fa còpies de nivell 0 (totals) el primer dilluns de cada mes, còpies de nivell 1 (diferencials) els altres dilluns i còpies incrementals la resta dels dies. Si, per exemple, es produeix una avaria el dijous de la segona setmana, per recuperar les dades caldria la còpia total del primer dilluns, la còpia diferencial del segon dilluns i les còpies incrementals del dimarts i dimecres de la segona setmana. Teniu representada aquesta política de còpies en la figura 1.8.

FIGURA 1.8. Pla de còpies de seguretat

| Dia | Còpia de seguretat | Primera setmana | | | | | Segona setmana | | | | |
|-----|----------------------------|-----------------|----|----|----|----|----------------|----|----|----|----|
| | | DI | Dt | Dc | Dj | Dv | Ds | Dg | DI | Dt | Dc |
| 1 | Còpia total Nivell 0 | ◆ | | | | | | | | | |
| 2 | Còpia incremental Nivell 2 | | ■ | | | | | | | | |
| 3 | Còpia incremental Nivell 2 | | | ■ | | | | | | | |
| 4 | Còpia incremental Nivell 2 | | | | ■ | | | | | | |
| 5 | Còpia incremental Nivell 2 | | | | | ■ | | | | | |
| 6 | Còpia diferencial Nivell 1 | | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ | ■ |
| 7 | Còpia incremental Nivell 2 | | | | | | | | | ■ | |
| 8 | Còpia incremental Nivell 2 | | | | | | | | | | ■ |

Per decidir quin nivell o combinació de nivells són els més adequats per a l'organització, cal tenir en compte, entre d'altres, els elements següents:

- El volum de dades que s'han de copiar
- El mitjà d'emmagatzematge utilitzat
- El temps del procés de còpia de seguretat.
- El temps de restauració en cas de pèrdua de dades.

1.5.2 Plans i programació de còpies de seguretat

Les decisions en el disseny d'un pla o política de còpies de seguretat es basen en un compromís entre el cost que implica efectuar-les (temps, cost de dispositius i suports de dades, dedicació de l'administrador, interrupció del servei, etc.) i el cost que comportaria la pèrdua d'aquestes dades en cas d'avaria. Per tant, per començar el disseny d'un pla de còpies de seguretat hem d'analitzar algunes característiques pròpies de les dades i respondre a les preguntes següents:

- **De quines dades fem còpies de seguretat?** Realment, els administradors de sistemes no acostumen a decidir en aquest punt, sinó que són els responsables de l'empresa els que coneixen les dades més importants i crítiques. Hi ha dades la pèrdua de les quals no representaria cap problema per a l'empresa; en canvi, n'hi ha d'altres que són d'una importància cabdal per al seu funcionament, de manera que no ens podem permetre el luxe de perdre-les. Per tant, per començar cal decidir de quines dades es faran còpies. Aquestes dades inclouen dades d'usuari, arxius de configuració, bases de dades, llibreries, programari i qualsevol tipus d'informació amb la qual treballi l'empresa.
- **Amb quina freqüència farem les còpies de seguretat?** Una decisió important pel que fa a les còpies de seguretat és la periodicitat: com més

volàtil sigui la informació de l'organització, més curt haurà de ser el període entre còpies. És a dir, una organització que canviï les seves dades molt sovint (diàriament, per exemple), segurament, haurà de fer còpies cada dia; en canvi, una organització que tingui pocs canvis en les dades pot fer còpies de seguretat amb una periodicitat setmanal o mensual. Per tant, hem de determinar la freqüència de les còpies d'aquestes dades.

Dades volàtils

El terme *volàtil* és sinònim de *fàcilment canviable, poc constant*. Quan parlem de dades volàtils ens referim a dades que periòdicament es modifiquen o s'esborren, i se'n creen de noves.

Un cop ja sabem què hem de copiar i amb quina freqüència, podem prendre decisions sobre el nostre pla:

- **Quan programem la còpia?** Mentre es duu a terme la còpia de les dades no hi pot haver accessos a aquestes per garantir que es copien totes sense cap problema de bloquejos. Per tant, el sistema ha d'estar inactiu per als usuaris de les dades. Un usuari no ha de ser necessàriament una persona; un programa pot ser un usuari de les dades. Això vol dir que mentre es realitza la còpia cap usuari de les dades no pot treballar. **Hem de buscar una franja de temps sense usuaris que permeti fer les còpies.** D'altra banda, si la disponibilitat del sistema ha de ser total i no podem deixar-lo inactiu per fer la còpia de seguretat, s'ha de recórrer a sistemes de còpia "en calent" que permeten fer-la amb el sistema en plena activitat.
- **Quin dispositiu farem servir?** A l'hora de decidir el suport, hem de tenir en compte paràmetres com la capacitat, la velocitat i el cost. Tradicionalment, el suport utilitzat en les grans empreses és la cinta magnètica que ofereix una alta capacitat, però hi ha altres alternatives, com els suports òptics extraïbles (CD, DVD, BluRay), els discos durs externs, la memòria flaix USB, una ubicació remota en la pròpia xarxa de la intranet o, fins i tot, fer servir un servei d'emmagatzematge en el núvol a Internet.

Còpies de seguretat en el núvol

Seguint la tendència actual de la descentralització de serveis en el núvol (*cloud computing*) han aparegut serveis d'emmagatzematge, sincronització i còpia de seguretat d'arxius en línia per Internet. Aquests serveis deleguen la responsabilitat de protegir les dades en el proveïdor que acostuma a disposar de grans instal·lacions, sistemes de seguretat i la darrera tecnologia en compressió i codificació. A més, aquests serveis tenen l'avantatge de ser fàcilment escalables i es pot accedir a les dades des de qualsevol ordinador connectat a Internet. Com a desavantatge trobem la reticència de moltes empreses a deixar les seves dades crítiques en mans de terceres persones i la dependència d'una bona i permanent comunicació de banda ampla. Alguns exemples de coneguts serveis de còpia de seguretat en línia són dropbox, wuala i Ubuntu one, aquest darrer exclusiu d'aquesta distribució de Linux.

- **Quin programari farem servir?** Tots els sistemes operatius incorporen eines i utilitats que permeten no solament fer les còpies de seguretat sinó també planificar-les, automatitzar-les i programar-ne la freqüència. Tanmateix, en el mercat hi ha programari específic per facilitar-nos aquestes tasques tant en codi lliure com propietari.

Finalment, oferim uns quants consells pràctics que cal tenir en compte:

- Fer més d'una còpia de seguretat de les dades més crítiques.
- Documentar tot el procés de còpia i etiquetar de la manera adient els suports que contenen les dades.
- Emmagatzemar les còpies en un lloc segur.
- No reescriure mai una còpia de seguretat si no tenim una còpia alternativa. Si justament es produeix l'avaria en el moment de fer la còpia de seguretat, perdrem la possibilitat de recuperar la informació. Per això convé disposar de dos sistemes de suport com a mínim; per exemple, un joc de còpies per als dies parells i un altre per als dies senars.

1.5.3 Programes i utilitats de la còpia de seguretat

Les operacions de còpia de seguretat (*backup*) són una part fonamental de les responsabilitats de l'administrador del sistema i, per això, els diferents sistemes operatius ofereixen aplicacions i eines que faciliten i automatitzen aquestes tasques.

Sistema operatiu Windows

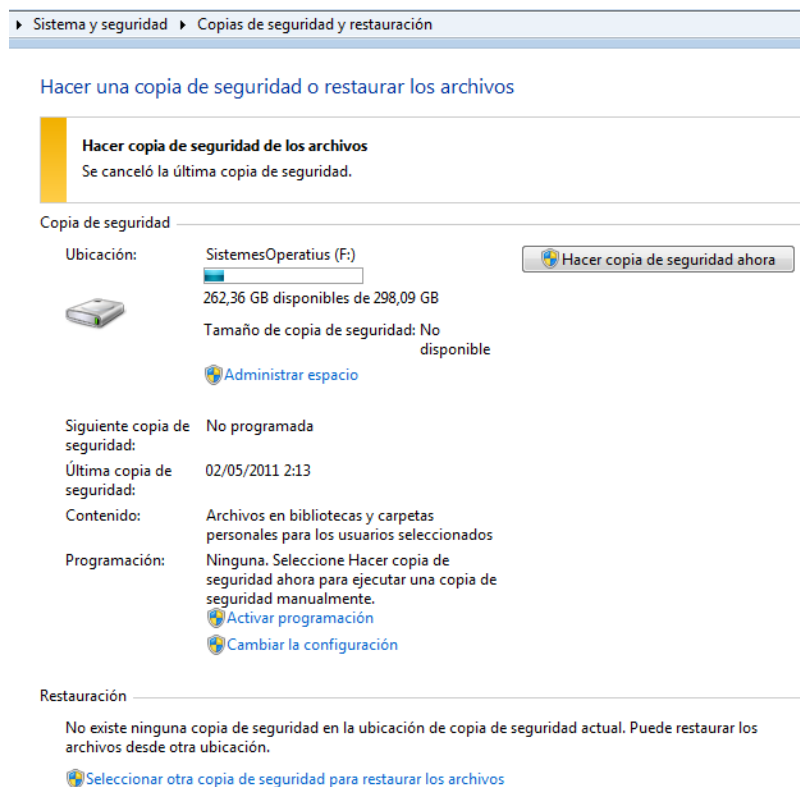
El sistema operatiu Windows permet fer còpies de seguretat amb una utilitat d'administració específica: la utilitat de còpies de seguretat de Windows es troba a **Tauler de control > Sistema i seguretat > Còpies de seguretat i restauració** (figura 1.9).

El procediment per fer còpies de seguretat amb aquesta utilitat és senzill i està sempre guiat:

- El primer que s'ha de fer és ajustar la configuració de la còpia de seguretat amb l'opció **Canviar la configuració**.
- Llavors podrem triar la **unitat de destinació** on es vol guardar la còpia de seguretat, que pot ser, per exemple, un disc extern, un CD o DVD enregistrable o bé una unitat remota mitjançant l'accés de xarxa.
- A continuació es pot deixar que el mateix sistema operatiu triï automàticament els arxius dels quals es farà còpia de seguretat. Per defecte, selecciona els arxius guardats en biblioteques, en l'escriptori i en les carpetes predeterminades de Windows que inclou AppData, contactes, escriptori, baixades, preferits, vincles, jocs guardats i cerques.
- En cas que la unitat de destinació estigui formatada amb el sistema d'arxius NTFS i tingui prou espai lliure, s'inclourà també una **imatge del sistema** amb tots els controladors i les opcions de configuració del registre.

- Alternativament, també es pot fer una selecció manual dels arxius que es vol incloure en la còpia de seguretat.
- Finalment es pot configurar la **programació automàtica** de la còpia indicant el dia de la setmana, l'hora i la freqüència (diària, setmanal o mensual).

FIGURA 1.9. Còpies de seguretat i restauració



Aquesta mateixa aplicació disposa de l'**opció de restauració** per recuperar el contingut d'una còpia de seguretat anterior.

Sistema operatiu Linux

El sistema operatiu Linux disposa de diferents ordres i comandes en l'entorn de consola de text per a la realització d'operacions d'empaquetatge d'arxius, compressió i còpies de seguretat. Les ordres i utilitats més emprades són les següents:

- Ordre **tar**: és l'ordre més senzilla que incorporen totes les distribucions de Linux i que permet empaquetar i comprimir estructures completes de directoris. Se'n mostren les opcions principals en la taula 1.1.

TAULA 1.1. Opcions habituals de l'ordre "tar"

| Opció curta | Opció GNU | Descripció |
|-------------|-----------|--------------------------------------|
| -c | -create | Crea un arxiu tar |
| -r | -append | Afegeix arxius a un empaquetatge tar |
| | | |

TAULA 1.1 (continuació)

| Opció curta | Opció GNU | Descripció |
|-------------|-----------|--|
| -u | -update | Actualitza els arxius d'un empaquetatge tar |
| -d | -diff | Compara un empaquetatge tar amb els arxius del disc |
| -t | -list | Mostra els continguts d'un arxiu empaquetat tar |
| -x | -extract | Extreu els arxius d'un empaquetatge tar |
| -z | -gzip | Comprimeix o descomprimeix l'arxiu empaquetat |
| -N | -newer | Empaqueta arxius creats a partir d'una data concreta |
| -v | -verbose | Mostra informació dels arxius al llarg del procés de creació o extracció |

Vegem algunes opcions d'aquesta ordre a tall d'exemple:

1. Copia el contingut del directori de configuració /etc.

```
1 $ tar -cvf Copia_etc.tar /etc
```

2. Copia tots els directoris dels usuaris i els comprimeix. Quan es fa servir l'opció de compressió, s'acostuma a indicar en l'extensió de l'arxiu resultant, que esdevé .tar.gz, o bé, .tgz.

```
1 $ tar -cvzf Copia_home.tgz /home
```

3. Restaura i descomprimeix la còpia de seguretat anterior. Els arxius restaurats se situen en el directori de treball.

```
1 $ tar -xvzf Copia_home.tgz
```

4. Copia tots els arxius del directori personal del superusuari ("root directory") creats després de la data indicada.

```
1 $ tar cvf file.tar --newer "2010-03-07 18:32:00" /root
```

- Ordre **rsync**. Aquesta ordre permet la còpia remota d'arxius i directoris d'un ordinador a un servidor remot. Ofereix diverses facilitats per efectuar còpies de seguretat remotes, com ara copiar només els arxius que han estat modificats, conservar la informació original de propietaris i permisos o efectuar la compressió de dades.

Exemple: Copia els directoris dels usuaris a un directori de còpia de seguretat (/var/backup) en el servidor remot (equip anomenat "alumnes"). Heu de comprimir les dades i conservar la informació de propietaris i permisos

```
1 $ rsync -az /home alumnes:/var/backup
```

- **Ordre `dump/restore`.** Aquestes utilitats es poden instal·lar fàcilment al sistema (`sudo apt-get install dump`) i permeten realitzar còpies de seguretat de diversos tipus i nivells, de tot un sistema d'arxius especificat. Es mostren les opcions més importants en la taula 1.2.

TAULA 1.2. Opcions més importants de l'ordre "dump"

| Opció | Descripció |
|------------|---|
| -0 fins -9 | Especifica el nivell de la còpia de seguretat. El nivell 0 és la còpia total. Qualsevol altre nivell fa còpies incrementals respecte la darrera còpia de seguretat de nivell inferior |
| -f disp | Aquesta opció permet definir l'arxiu o dispositiu on es farà la còpia del sistema d'arxius. També es pot especificar un arxiu o dispositiu remot posant el nom del servidor de destinació |
| -S | Indica una estimació de l'espai necessari per a la còpia de seguretat |

Alguns exemples d'ús de l'ordre `dump`:

1. Còpia total en cinta (`/dev/tape`) de la partició de disc `hd5`

```
1 $ dump -0 -f /dev/tape /dev/hda5
```

2. Restauració de la còpia total anterior. Per restaurar arxius individuals es pot fer servir l'opció `-i` (*interactive*) que permet a l'usuari triar els arxius que vol recuperar.

```
1 $ restore -if /dev/tape
```

3. Còpia diferencial respecte a la darrera còpia total feta en una cinta SCSI (`/dev/st0`) d'un servidor remot anomenat "alumnes".

```
1 $ dump -1 -f alumnes:/dev/st0 /dev/hda5
```

- **Amanda.** És l'acrònim anglès de *advanced maryland automatic network disk archiver*. En el cas de necessitar aplicacions de còpia de seguretat més complexes, en xarxa i centralitzades des d'una sola interfície, també es disposa de solucions en codi lliure, com, per exemple, `amanda`. Aquesta aplicació utilitza una arquitectura client-servidor per donar servei de còpia de seguretat als servidors i estacions de treball d'una xarxa, i fa servir utilitats natives en el client (comandes `dump` i `GNU tar`). Amanda funciona amb una gran quantitat de sistemes UNIX, distribucions de Linux i, fins i tot, hi ha un client natiu per a Windows per fer també còpies d'ordinadors amb aquest sistema operatiu.

1.6 Recuperació en cas de fallada del sistema

Com ja hem dit, per molt que treballem en la prevenció i la tolerància de fallades del sistema, sempre es pot produir una avaria, un atac o un conjunt de circumstàncies que afectin la disponibilitat del sistema. Aleshores, l'objectiu consisteix a minimitzar els temps de recuperació del sistema i que torni a estar operatiu al més aviat possible.

En general, el procediment de recuperació dependrà molt del sistema operatiu que fem servir i que ens pot subministrar diferents eines i aplicacions per solucionar i restaurar l'operativitat de l'equip. En són exemples els punts de restauració, les eines de recuperació o les imatges del disc del sistema.

1.6.1 Punts de restauració

En alguns casos, el sistema deixa de funcionar perquè la instal·lació és defectuosa o s'ha incorporat un controlador que no hi és compatible o està mal configurat i bloqueja o fa inestable el sistema. Aquests casos es poden intentar solucionar recuperant un punt de restauració previ.

Un **punt de restauració** és la representació de l'estat dels arxius del sistema de l'equip en un moment donat.

És una mena de fotografia de l'estat de les bases de dades del sistema; així, en cas de problemes es pot recuperar la configuració d'un estat anterior. Els punts de restauració es poden realitzar periòdicament d'una manera automatitzada i també quan es detecta que es volen fer canvis en l'equip, per exemple, la instal·lació d'un programa. Aquesta idea de crear punts de restauració la fan servir, per exemple, els sistemes operatius Windows i els programes de virtualització com ara VirtualBox.

El sistema operatiu Windows 7 permet fer i recuperar punts de restauració amb una consola específica que es troba a **Tauler de control->Sistema i seguretat->Sistema->Protecció del sistema**.

1.6.2 Còpies de seguretat del sistema

Una **còpia de seguretat del sistema** és una imatge exacta de la unitat o partició que inclou el sistema operatiu, la seva configuració i els programes i arxius instal·lats.

La restauració d'una imatge del sistema no permet recuperar arxius individuals, així que es recomana efectuar còpies de seguretat normals dels arxius personals si es vol tenir la possibilitat de restaurar només un arxiu o uns arxius concrets.

El sistema operatiu Windows 7 permet fer imatges de tot el sistema amb una consola específica que es troba a **Tauler de control->Sistema i seguretat->Còpies de seguretat i restauració** i en aquesta finestra s'ha de triar l'opció Crear una imatge del sistema.

A més de les eines de clonatge que subministren els mateixos sistemes operatius, hi ha programari tant propietari (Ghost, Acronis) com de codi lliure (Clonezilla) que faciliten les tasques de creació i restauració d'imatges d'unitats senceres i particions de discos durs.

1.6.3 Opcions d'arrencada avançades

Les diferents versions dels sistemes operatius Windows acostumen a incorporar eines i funcions que permeten reparar un sistema que no es pot iniciar. **Les opcions d'arrencada avançades** consisteixen en un menú de text que ens ofereix una sèrie d'eines i opcions que permeten iniciar el sistema amb un nombre mínim de controladors de dispositiu i de serveis. Així doncs, quan el sistema no funciona correctament a causa de la instal·lació d'un nou programa o controlador es pot utilitzar alguna d'aquestes opcions d'arrencada per eliminar manualment el programari que crea el conflicte.

La consola d'opcions d'arrencada avançada consta de les opcions següents:

- **Mode segur.** Permet iniciar el sistema amb els controladors bàsics de teclat, ratolí, monitor, unitats de disc, vídeo en baixa resolució, serveis predeterminats del sistema i sense connectivitat de xarxa.
- **Mode segur amb funcions de xarxa.** És com el mode segur, però amb les funcions de connectivitat en xarxa habilitades.
- **Mode segur amb símbol de sistema.** Permet arrencar el sistema amb els controladors bàsics indicats anteriorment, però inicia la sessió en mode text amb el símbol de sistema (prompt) en comptes de carregar el mode gràfic de l'escriptori de Windows.
- **Habilitar el registre d'arrencada.** Aquesta opció permet, al llarg del procés d'arrencada, enregistrar en un arxiu d'informació la indicació de tots els controladors i serveis que es van carregar. D'aquesta manera, es pot consultar posteriorment per obtenir informació que ajudi a determinar la causa del problema. També es pot activar aquesta opció mitjançant la consola de configuració del sistema (tecla_windows+R i emprar la utilitat msconfig.exe).
- **Habilitar vídeo de baixa resolució.** Permet iniciar el sistema amb el control bàsic de vídeo a una resolució de 640 x 480 píxels quan se sospita que el problema pot ser motivat per una configuració errònia de la targeta de vídeo.
- **Darrera configuració vàlida coneguda.** Permet iniciar el sistema amb la informació que Windows tenia en les bases de dades del registre (*registry*) abans dels últims canvis realitzats, per si aquests canvis són els responsables que el sistema no arrenqui correctament.

Per accedir a les opcions d'arrencada avançades a Windows cal prémer la tecla de funció F8 a l'inici del procés d'arrencada del sistema.

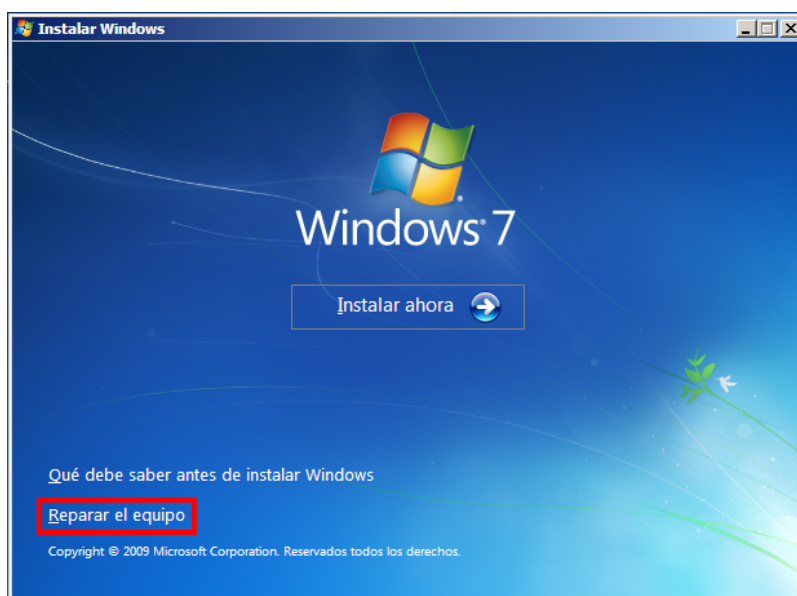
L'arxiu que enregistra el que succeeix en el procés d'arrencada s'anomena ntbtlog.txt i es troba en el directori \Windows.

- **Mode de restauració de serveis de directori.** Duu a terme una revisió del disc i restaura el directori SYSVOL i el directori actiu. S'utilitza només en equips que siguin controladors de domini i requereix l'autenticació com a administrador del domini.
- **Mode de depuració.** Mitjançant aquesta opció, el sistema envia informació de depuració a un altre equip connectat mitjançant cable de sèrie al port COM2.
- **Deshabilitar el reinici automàtic en cas d'error del sistema.** Opció útil per evitar que Windows quedi atrapat en un bucle en el qual torni a iniciar la màquina automàticament en produir-se un error en el sistema.
- **Deshabilitar l'ús obligatori de controladors signats.** Permet la càrrega de controladors de dispositiu que no estiguin reconeguts per Microsoft.

1.6.4 Discos d'arrencada i de recuperació

En cas que el nostre equip ni tan sols pugui arrencar amb les opcions avançades caldrà fer servir el disc CD o DVD d'instal·lació per accedir a l'**entorn de recuperació del sistema**. Una vegada iniciat el procés d'instal·lació, ens ofereix la possibilitat de reparar l'equip, tal com es mostra en la figura 1.10.

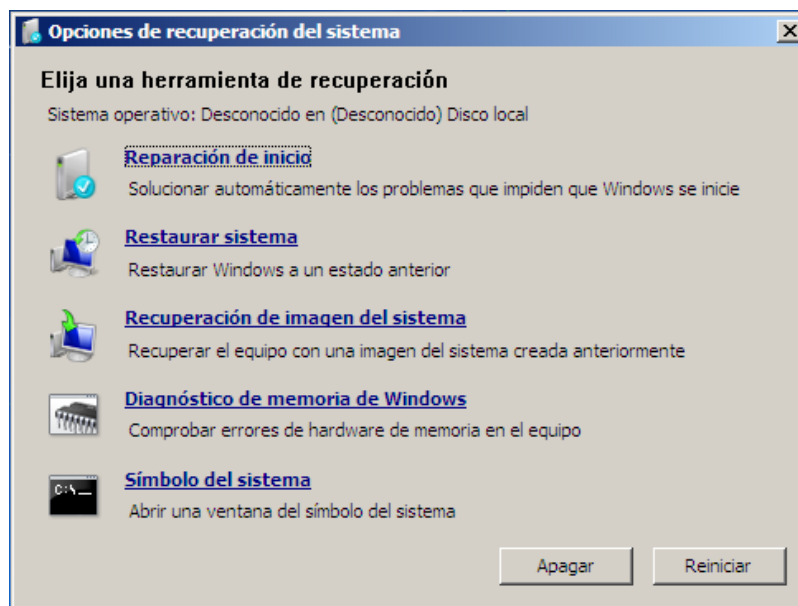
FIGURA 1.10. Accés a l'entorn de recuperació de Windows 7



Aquest entorn ens proporciona una sèrie d'opcions i diagnòstics que ens permet recuperar un punt de restauració anterior o, fins i tot, restaurar una imatge sencera del sistema, realitzar un diagnòstic de la memòria o accedir a una consola d'ordres de text que podem veure en la figura 1.11.

Per crear un disc d'arrencada i reparació de Windows 7 es pot fer des de **Tauler de control->Sistema i seguretat->Còpies de seguretat i restauració->Crear un disc de reparació del sistema**.

FIGURA 1.11. Opcions de recuperació del sistema



Quan no es disposa del disc original d'instal·lació, hi ha la possibilitat de crear prèviament un **disc d'arrencada i reparació** que permet accedir a aquestes eines i diagnòstics.

1.6.5 Recuperació del sistema en entorns virtualitzats

Encapsulament

Les màquines virtuals encapsulen sistemes sencers, és a dir, el mateix sistema operatiu, la configuració del maquinari i els programes d'aplicació en arxius independents portables i fàcils de manejar i copiar.

No es pot oblidar que la tendència actual és fer servir sistemes virtualitzats que proporcionen una característica fonamental, l'**encapsulament**, que facilita i millora els processos de clonació, còpia i recuperació del sistema. Davant una avaria de l'ordinador, és molt senzill instal·lar una màquina virtual en qualsevol altre equip i arrencar de nou la còpia del sistema encapsulat. Es redueixen així els temps de parada i recuperació davant qualsevol incident i, fins i tot, permet la migració en calent de màquines virtuals d'un servidor físic a un altre sense pèrdua de servei.

2. Supervisió del rendiment del sistema

Repasant el concepte de *sistema informàtic* recordem que està format per tres parts ben diferenciades:

- **Maquinari:** conjunt de components i elements físics.
- **Programari:** conjunt de programes informàtics, tant de sistema com d'aplicació.
- **Usuaris:** conjunt de persones que utilitzen o gestionen el sistema.

Analitzar i millorar el rendiment de tot el sistema comporta fer-ho amb cada una de les parts que el formen. Ens centrarem ara en l'estudi dels rendiments del maquinari i del programari, ja que es tracta de les parts del sistema que són responsabilitat de l'administrador.

Per **rendiment del sistema** entenem la capacitat del sistema de dur a terme les tasques sol·licitades d'una manera eficient en un espai de temps determinat. Un bon rendiment del sistema suposa que realitza les tasques de forma eficient i minimitzant el temps requerit.

La supervisió del rendiment del sistema es centra en tres àmbits administratius:

- L'anàlisi i el monitoratge del comportament i el rendiment dels diversos components del maquinari i del programari del sistema informàtic.
- L'enregistrament i el monitoratge dels esdeveniments de rellevància comunicats pel sistema operatiu o les aplicacions.
- La gestió dels processos i serveis en execució pel sistema i l'ús que fan dels recursos del sistema.

Per a aquesta gestió i anàlisi, els diversos sistemes operatius ens ofereixen eines i sistemes de supervisió que ens ajudaran a detectar i resoldre problemes concrets; per exemple, una càrrega de treball excessiva dels components principals, com ara la memòria i el processador, el control de la disponibilitat del sistema mitjançant l'historial d'esdeveniments o el bloqueig d'un procés o servei concret que ocasioni problemes.

2.1 Monitoratge del rendiment dels components d'un sistema informàtic

El **monitoratge del rendiment** fa referència a la vigilància i la supervisió de determinats paràmetres per assegurar que el funcionament del sistema assoleix el resultat òptim previst i que es detecten les possibles desviacions.

Hi ha un gran nombre d'objectes i components susceptibles d'enregistrar el seu comportament per així gestionar i monitorar el seu rendiment. Com a elements més habituals d'aquest monitoratge podem destacar els següents:

- El funcionament del processador o processadors del sistema.
- La memòria interna, la memòria cau, la memòria d'intercanvi.
- Els discos o qualsevol sistema d'emmagatzematge extern.
- Els sistemes de comunicació de xarxa.
- El funcionament de les pròpies aplicacions i serveis, com el comportament de l'accés a bases de dades o el servei de pàgines web.

Cada un d'aquests components es pot controlar mitjançant uns paràmetres determinats. Per exemple, en el cas del disc dur es poden controlar paràmetres com ara la velocitat mitjana de transferència, el nombre de lectures i d'escriptures o el tant per cent d'ocupació del dispositiu. Aquests paràmetres en general s'anomenen **comptadors** i poden ser seleccionats per establir diferents criteris d'anàlisi del rendiment.

2.1.1 Tipus de monitoratge

La funció de vigilància i supervisió del rendiment del sistema es pot fer en dos àmbits temporals que marquen els diferents **tipus de monitoratge**:

- **Monitoratge en temps real.** Les eines de monitoratge en temps real ens presenten la informació canviant del que està succeint mentre visualitzem el comportament dels diversos components; és a dir, el comportament que tenen en temps real.
- **Monitoratge continuat.** Aquest monitoratge permet fer controls periòdics de l'estat del sistema i emmagatzemar aquesta informació en mostres i intervals predeterminats per donar un visió estadística de l'evolució de l'estat del sistema durant un període determinat de temps en estudi.

S'ha de tenir en compte que el fet de monitorar el sistema comporta una sobrecàrrega, ja que les ordres o aplicacions necessiten recursos del propi sistema per funcionar. Per exemple, si fem servir un monitoratge de tipus continuat, la sobrecàrrega serà més gran com més petit sigui l'interval de mostreig, es a dir quan més gran sigui la freqüència de presa de mostres. Aquesta sobrecàrrega s'ha de tenir en compte a l'hora d'analitzar les dades de rendiment obtingudes.

2.1.2 Eines de monitoratge de rendiment a Windows

Les diferents versions de Windows ens ofereixen algunes eines i utilitats de monitoratge del rendiment com ara el monitor de recursos, el monitor de rendiment i l'índex d'avaluació de l'experiència de Windows.

Monitor de recursos

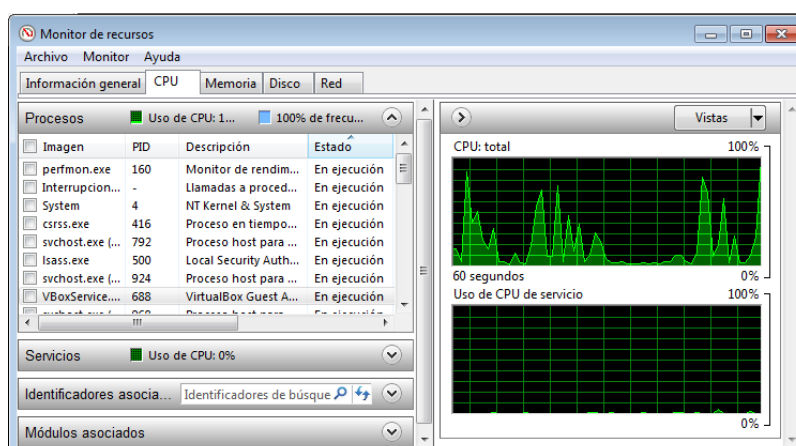
El monitor de recursos de Windows és una eina que permet la supervisió en temps real de diferents components del sistema i també informació sobre com els processos i serveis utilitzen aquests recursos. Aquesta aplicació permet a més analitzar els processos que no responen, identificar els arxius que fan servir les aplicacions i controlar processos i serveis.

El monitor de recursos inclou cinc seccions: **informació general**, **CPU**, **memòria**, **disc** i **xarxa**, com es veu en la figura 2.1. La secció d'informació general mostra les dades bàsiques de l'ús dels recursos del sistema i cada una de les altres mostren informació específica incloent-hi, a la part dreta, gràfics on es mostra informació **en temps real** de la utilització del recurs.

A més de poder ordenar els processos per diferents criteris, els resultats es poden filtrar i obtenir la informació dels recursos emprats només per un procés determinat o per un conjunt de processos.

Per accedir al monitor de recursos, cal fer servir la finestra d'execució (Tecla Windows+R) i cridar l'executable `resmon.exe`; o bé, en el menú principal triar Tauler de Control Sistema i seguretat Eines administratives Monitor de rendiment.

FIGURA 2.1. Monitor de recursos



Monitor de rendiment

Per accedir al monitor de rendiment cal fer servir la finestra d'execució (Tecla Windows+R) i cridar l'executable perfmon.exe; o bé, en el menú principal triar Tauler de control Sistema i seguretat Eines administratives Monitor de rendiment.

Windows 7 inclou dues plantilles estàndard de recollida anomenades *diagnòstic del sistema* (*system diagnostics*) i *rendiment del sistema* (*system performance*).

El monitor de rendiment de Windows és una eina complexa i molt completa que proporciona diverses utilitats per analitzar el rendiment del sistema. Des d'una sola consola es pot supervisar en temps real el rendiment de les aplicacions i dels recursos del maquinari, personalitzar les dades que es vol guardar en els registres, definir llindars per a alarmes i accions automàtiques, generar informes i veure dades de rendiments històrics.

Per dur a terme aquesta tasca fa servir tres grans fonts d'informació: els comptadors de rendiment, les dades de seguiment d'esdeveniments i la informació de configuració.

- **Comptadors de rendiment.** Són mesures de l'estat o de l'activitat del sistema. Poden ser generats pel sistema operatiu o formar part d'aplicacions individuals. El monitor de rendiment de Windows sol·licita el valor dels comptadors de rendiment en intervals de temps especificats.
- **Dades de seguiment d'esdeveniments.** Es recullen de proveïdors de seguiment que són components del sistema operatiu o d'aplicacions individuals que informen d'accions o esdeveniments concrets en el sistema.
- **Informació de configuració.** Es recull dels valors de les claus del registre de Windows (*registry*). El monitor de rendiment de Windows pot enregistrar el valor d'una clau del registre a una hora o en un interval especificat.

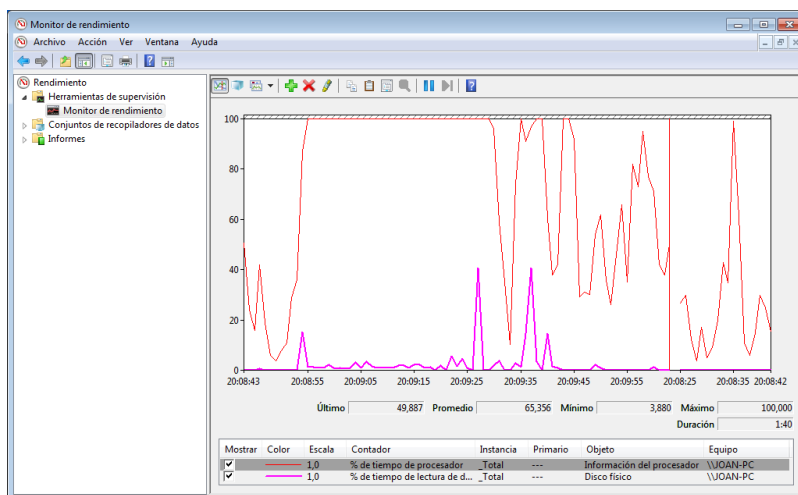
Tota aquesta informació es pot configurar i combinar en conjunts de recopiladors de dades específics per analitzar un problema o una situació concrets. Es pot fer servir el monitor de rendiment per examinar l'efecte que tenen en el rendiment els programes que s'executen i es pot obtenir la informació tant en temps real com mitjançant la recollida de dades històriques per fer-ne l'anàlisi posterior.

Com es veu en la captura de pantalla de la figura 2.2, aquesta consola disposa de tres grans grups d'eines:

- El **monitor de rendiment** pròpiament dit és una utilitat de representació gràfica que serveix per visualitzar dades sobre els comptadors de rendiment tant en temps real com des d'arxius de registre. L'aspecte de la representació gràfica és configurable i es poden anar afegint diversos comptadors triats d'una llarga llista de components disponibles.
- Els **conjunts de recopiladors de dades** (*data collector set*) agrupen les diferents configuracions per a la recollida de dades en elements reutilitzables per fer servir en diferents escenaris de supervisió del rendiment. Es poden dissenyar i configurar manualment, però també s'inclouen plantilles predeterminades que ajuden els administradors de sistemes a començar a recollir d'una manera immediata dades de rendiment específiques d'una problemàtica concreta o d'un escenari de supervisió determinat.
- Els **informes** es generen automàticament i serveixen per ajudar a interpretar la informació sobre el rendiment, recollida pels diferents conjunts de

recopiladors de dades activats. Hi ha dos informes estàndard anomenats *informes de sistema* que corresponen als dos conjunts de recopiladors de dades predeterminats.

FIGURA 2.2. Monitor de rendiment




Índex d'avaluació de l'experiència de Windows

L'avaluació de l'experiència en Windows (figura 2.3) mesura la capacitat del sistema i expressa aquesta mesura en forma d'un número de puntuació total, com es pot veure en la figura 2.3. Cada component de maquinari rep també una puntuació individual que pot proporcionar informació del rendiment dels components més importants per donar una referència de l'estat d'avenç tecnològic en què es troben i ajudar a decidir quins d'aquests components tenen prioritat a l'hora d'actualitzar el sistema.

FIGURA 2.3. Índex d'experiència de Windows

Evaluar y mejorar el rendimiento del equipo

La Evaluación de la experiencia en Windows evalúa componentes clave del sistema según una escala que va desde 1,0 a 7,9.

| Componente | Qué se evalúa | Puntuación | Puntuación total |
|------------------------------|--|------------|---|
| Procesador: | Cálculos por segundo | 4,2 |  Determinado por la puntuación más baja |
| Memoria (RAM): | Operaciones de memoria por segundo | 4,5 | |
| Gráficos: | Rendimiento del escritorio de Windows Aero | 1,0 | |
| Gráficos de juego: | Rendimiento de gráficos en 3D para negocios y juegos | 1,0 | |
| Disco duro principal: | Velocidad de transferencia de datos en el disco | 6,1 | |



¿Qué significan estos números?



Ver e imprimir información detallada del sistema y su rendimiento



Sugerencias para mejorar el rendimiento de su equipo.



Obtener más información sobre puntuaciones y software en línea

La puntuación es la actual
Última actualización: 25/04/2011 4:27:01



Volver a ejecutar la evaluación

Per accedir a l'índex d'avaluació de l'experiència de Windows cal triar en el menú principal Tauler de control Sistema i seguretat Centre d'activitats Veure informació del rendiment*.

2.1.3 Eines de monitoratge de rendiment a Linux

Els sistemes operatius Linux incorporen diverses eines per al monitoratge del rendiment del sistema. Hi ha una gran diversitat d'opcions, des d'ordres que introduïm en la consola de text fins a d'altres que treballen en mode gràfic.

Eines i ordres integrades a Linux

La manera més ràpida de conèixer l'estat del sistema és executant ordres des de la consola. A continuació mostrem una llista de les ordres més utilitzades que ens donen informació del sistema:

- **uptime.** Dóna l'hora del sistema, el temps que fa que està encès, la quantitat d'usuaris connectats i la càrrega mitjana del sistema durant l'últim minut, els últims cinc minuts i els últims quinze minuts.

```
1 $ uptime
2 1151:25 up 58 min, 3 users, load average: 1.38, 1.35, 0.96
```

- **time.** Permet executar una ordre o aplicació i enregistrar els recursos que ha emprat. Per defecte, només presenta el temps real (estimat amb el rellotge del sistema) i el temps de CPU emprat tant en mode usuari com en mode sistema. Tanmateix, aquesta mateixa ordre executada amb privilegis de superadministrador i fent servir diferents modificadors pot subministrar més paràmetres d'informació.

```
1 $ time gedit
2 real 0 min 13289 s
3 user 0 min 1380 s
4 sys 0 min 2016 s
```

- **vmstat.** Dóna informació de l'estat de la memòria física, de la memòria virtual, de l'intercanvi entre memòria interna i disc (*swapping*), de les transferències de disc, de les interrupcions i de l'ús del processador. Admet l'ús de modificadors i permet el monitoratge continuat.

```
1 $ vmstat
2procs-----memory-----swap-----io-----system-----cpu-----
3 r b swpd free buff cache si so bi bo in cs us sy id wa
4 1 0 0 340392 67368 420560 0 0 111 47 115 295 6 20 73 1
```

La informació que mostra aquesta ordre és resumeix en la taula [2.1](#).

TAULA 2.1. Camps d'informació de l'ordre "vmstat"

| Secció | Descripció |
|--------|--|
| Procs | Processos en espera de ser executats (r) i en estat d'espera (b) |
| Memory | Memòria virtual (swpd), memòria lliure (free), memòria intermèdia (buff) i memòria cau (cache) |
| Swap | Accessos a memòria swap. Swap in i Swap out |
| IO | Blocs enviats i rebuts des de dispositius d'entrada o sortida |
| System | Nombre d'interrupcions per segon (in) i nombre de canvis de context (cs) |
| CPU | Percentatges de distribució de temps entre el mode usuari (us), el mode sistema (sy) i el temps ociós (id) |

- **free.** Utilització de la memòria del sistema. Concretament, la memòria total, la memòria en ús, la memòria lliure, la memòria compartida en ús, el nombre de *buffers* utilitzats i les mides de la memòria cau. Permet monitoratge continuat.

```

1 $ free
2           total        used        free      shared    buffers     cached
3 Mem:      1026484      686092      340392          0       67368      420584
4 -/+ buffers/cache:      198140      828344
5 Swap:      1952760          0      1952760

```

- **df.** Utilització de disc. Per a cada unitat muntada, mostra l'espai utilitzat i l'espai lliure. Admet modificadors.

```

1 $ df
2 S. arxius      Blocs    1 K      En ús    Lliures  %Ús Muntat a
3 /dev/sda1      4804736  2406072  2154596  53% /
4 none           509016   264     508752   1% /dev
5 none           513240   488     512752   1% /dev/shm
6 none           513240   96      513144   1% /var/run
7 none           513240   0       513240   0% /var/lock
8 none           513240   0       513240   0% /lib/init/rw
9 none           4804736  2406072  2154596  53% /var/lib/ureadahead/
10 debugfs
   /dev/sda3      3592128  103352  3306300  4% /home

```

- **du.** Utilització de disc. Per a cada directori mostra l'espai utilitzat. Admet modificadors.

```

1 $ du -h Documents/
2 3,5 M Documents/Ubuntu_Free_Culture_Showcase
3 112 K Documents/Logos
4 7,9 M Documents/

```

- **hdparm.** Mostra el valor dels paràmetres més importants d'un disc i permet modificar-ne alguns. Admet modificadors.

```
1 $ sudo hdparm /dev/sda1
2 /dev/sda1:
3   multcount    = 128 (on)
4   IO_support   = 1 (32-bit)
5   readonly     = 0 (off)
6   readahead    = 256 (on)
7   geometry     = 1305/255/63, sectors = 9762816, start = 2048
```

- **netstat.** Informació de l'estat de la xarxa del sistema. Dóna protocols, quantitats de bytes d'entrada i sortida, origen i destinació de la comunicació.

Informació del nucli

Sistema d'arxius virtual

Definim el directori `/proc` com a virtual perquè no hi és realment en el disc sinó que el nucli del sistema operatiu el crea dins la memòria RAM.

El directori del primer nivell de jerarquia **/proc** conté un sistema d'arxius virtual. Les consultes que hi podem fer ens poden servir per obtenir informació del funcionament en el mateix sistema.

Alguns arxius i directoris interessants que hi trobem són:

- **/proc/cpuinfo.** Informació sobre el processador. Per exemple, el tipus, fabricació, model i rendiment.
- **/proc/devices.** Llista de controladors de dispositiu configurats en el nucli que està funcionant actualment.
- **/proc/diskstats.** Conté informació estadística de les operacions d'entrada/-sortida per cada dispositiu de disc.
- **/proc/dma.** Mostra quins canals de DMA (accés directe a memòria) s'estan utilitzant.
- **/proc/filesystems.** Llista dels sistemes d'arxius configurats dins el nucli.
- **/proc/interrupts.** Mostra quines línies d'interruptió s'estan utilitzant, i per cadascuna, un comptador de quantes n'hi ha hagut.
- **/proc/ioports.** Mostra quins ports d'entrada/sortida s'estan utilitzant.
- **/proc/loadavg.** La mitjana de la càrrega del sistema expressada en tres indicadors que representen la mitjana de processos en marxa en el darrer minut, cinc minuts i quinze minuts.
- **/proc/meminfo.** Informació sobre la utilització de la memòria, tant la física com la d'intercanvi.
- **/proc/net.** Directori amb arxius d'informació d'estat sobre protocols de xarxa. Els fa servir l'ordre **netstat**.
- **/proc/partitions.** Conté el noms de les particions del sistema i la seva mida en blocs.
- **/proc/stat.** Diverses estadístiques sobre el nucli del sistema, com el temps que el CPU ha fet servir fent diferents tipus de treballs, el nombre d'interrupcions ateses o el temps transcorregut des de l'arrancada del sistema.

- **/proc/version.** La versió de nucli del sistema operatiu.

Tot i que els fitxers que es poden consultar a **/proc** acostumen a ser arxius de text de lectura fàcil amb l'ordre **cat** o qualsevol processador de textos, de vegades el format en dificulta la interpretació. És per això que hi ha altres ordres del mateix sistema que agafen aquesta informació i la presenten a l'usuari d'una manera més elaborada perquè l'entengui millor. Per exemple, l'ordre **free** llegeix el fitxer **/proc/meminfo**, i l'ordre **uptime** accedeix i presenta la informació de l'arxiu **/proc/loadavg**.

Paquet d'eines de monitoratge "sysstat"

El paquet sysstat és un conjunt d'eines de monitoratge de rendiment per a sistemes Linux. Proporciona dades instantànies de rendiment i es poden emmagatzemar en arxius històrics. En entorns de servidor, aquestes dades proporcionen informació valuosa per detectar carències i colls d'ampolla del sistema.

L'ordre d'instal·lació és la següent:

```
1 sudo apt-get install sysstat
```

Algunes de les eines que inclou aquest paquet són les següents:

- **mpstat.** Recull informació del rendiment de cadascun dels processadors del sistema. Permet el monitoratge continuat i admet modificadors.
- **iostat.** És una eina més completa que l'anterior, ja que a més de presentar estadístiques de la CPU, dona informació dels dispositius d'entrada i sortida, les particions i els sistemes d'arxius.
- **pidstat.** Informació estadística dels processos de Linux.
- **sar** (*system activity report*). Recull, enregistra i presenta informació sobre l'estat dels components principals del sistema (CPU, memòria, discos, interrupcions, interfícies de xarxa, consoles, nuclis, etc.) i de la seva càrrega en temps real i d'una manera continuada. Emmagatzema les dades en els arxius **/var/log/saxx**, on **xx** és el dia del mes del monitoratge. Aquests arxius permeten l'anàlisi *a posteriori* de la informació. SAR admet modificadors molt interessants com ara els següents:
 - **-P** : Dóna informació per a cada processador.
 - **-r** : Dóna informació del rendiment de la memòria.
 - **-B** : Dóna informació relativa a la paginació de la memòria.
 - **-W** : Dóna informació relativa al *swapping*.
 - **-d** : Dóna informació del rendiment de disc.
 - **-n** : Dóna informació relativa a la xarxa.

Totes les ordres accepten com a paràmetre el nombre de mostres que volem capturar i l'interval entre mostres expressat en segons. Vegem-ne uns quants exemples.

1. Volem obtenir tres valors d'ús de CPU separats un segon:

| | | | | | | | | |
|---|--|-----|-------|-------|---------|---------|--------|-------|
| 1 | \$ sar 1 3 | | | | | | | |
| 2 | Linux 2.6.32-28-generic (jmunoz-desktop) 26/04/11 _i686_ (1 CPU) | | | | | | | |
| 3 | | | | | | | | |
| 4 | 12:54:20 | CPU | %user | %nice | %system | %iowait | %steal | %idle |
| 5 | 12:54:24 | all | 0,75 | 0,00 | 16,00 | 0,00 | 0,00 | 83,25 |
| 6 | 12:54:28 | all | 0,50 | 0,00 | 9,02 | 0,25 | 0,00 | 90,23 |
| 7 | 12:54:32 | all | 0,25 | 0,00 | 11,97 | 0,00 | 0,00 | 87,78 |
| 8 | Average: | all | 0,50 | 0,00 | 12,33 | 0,08 | 0,00 | 87, |

2. Volem veure l'ús dels diferents processadors del sistema:

| | | | | | | | | | |
|---|--|-------|------|-------|-------|---------|------|-------|----------|
| 1 | \$ mpstat -P ALL | | | | | | | | |
| 2 | Linux 2.6.32-28-generic (jmunoz33-desktop) 26/04/11 _i686_ (1 CPU) | | | | | | | | |
| 3 | | | | | | | | | |
| 4 | 12:56:13 | CPU | %usr | %nice | %sys | %iowait | %irq | %soft | %steal % |
| | guest | %idle | | | | | | | |
| 5 | 12:56:13 | all | 2,51 | 1,19 | 14,45 | 0,42 | 0,27 | 0,10 | 0,00 |
| | 0,00 | 81,05 | | | | | | | |
| 6 | 12:56:13 | 0 | 2,51 | 1,19 | 14,45 | 0,42 | 0,27 | 0,10 | 0,00 |
| | 0,00 | 81,05 | | | | | | | |

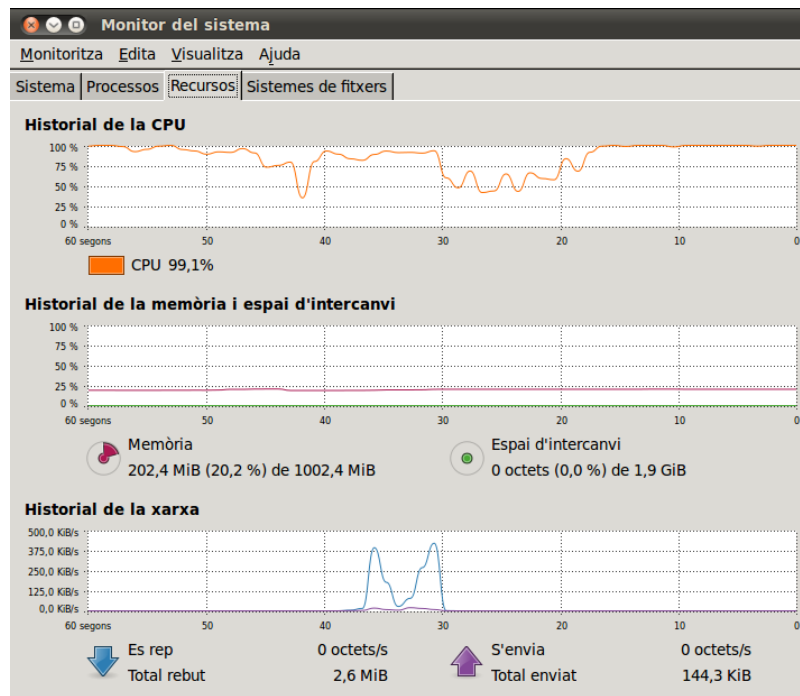
3. Volem veure el percentatge d'ús dels processos més actius:

| | | | | | | | | |
|----|--|------|------|---------|--------|------|-----|-----------------|
| 1 | \$ pidstat 1 2 | | | | | | | |
| 2 | Linux 2.6.32-28-generic (jmunoz33-desktop) 26/04/11 _i686_ (1 CPU) | | | | | | | |
| 3 | | | | | | | | |
| 4 | 13:00:09 | PID | %usr | %system | %guest | %CPU | CPU | Command |
| 5 | 13:00:10 | 984 | 0,00 | 1,72 | 0,00 | 1,72 | 0 | Xorg |
| 6 | 13:00:10 | 1101 | 0,00 | 0,86 | 0,00 | 0,86 | 0 | hald-addon-stor |
| 7 | 13:00:10 | 1357 | 0,00 | 0,86 | 0,00 | 0,86 | 0 | wnck-applet |
| 8 | 13:00:10 | 1868 | 0,00 | 3,45 | 0,00 | 3,45 | 0 | firefox-bin |
| 9 | 13:00:10 | 2508 | 2,59 | 5,17 | 0,00 | 7,76 | 0 | pidstat |
| 10 | | | | | | | | |
| 11 | 13:00:10 | PID | %usr | %system | %guest | %CPU | CPU | Command |
| 12 | 13:00:11 | 984 | 1,01 | 5,05 | 0,00 | 6,06 | 0 | Xorg |
| 13 | 13:00:11 | 1868 | 0,00 | 3,03 | 0,00 | 3,03 | 0 | firefox-bin |
| 14 | 13:00:11 | 2323 | 0,00 | 1,01 | 0,00 | 1,01 | 0 | gnome-terminal |
| 15 | 13:00:11 | 2508 | 0,00 | 9,09 | 0,00 | 9,09 | 0 | pidstat |
| 16 | | | | | | | | |
| 17 | Average: | PID | %usr | %system | %guest | %CPU | CPU | Command |
| 18 | Average: | 984 | 0,47 | 3,26 | 0,00 | 3,72 | — | Xorg |
| 19 | Average: | 1101 | 0,00 | 0,47 | 0,00 | 0,47 | — | hald-addon-stor |
| 20 | Average: | 1357 | 0,00 | 0,47 | 0,00 | 0,47 | — | wnck-applet |
| 21 | Average: | 1868 | 0,00 | 3,26 | 0,00 | 3,26 | — | firefox-bin |
| 22 | Average: | 2323 | 0,00 | 0,47 | 0,00 | 0,47 | — | gnome-terminal |
| 23 | Average: | 2508 | 1,40 | 6,98 | 0,00 | 8,37 | — | pidstat |

Eines gràfiques de monitoratge de rendiment

La majoria de distribucions de Linux porten incorporada una eina gràfica senzilla, el **monitor del sistema**, que, entre d'altres funcions, per mitjà d'una pestanya, permet visualitzar l'historial de rendiment de la CPU, de la memòria, de l'espai d'intercanvi i l'activitat de la xarxa, tal com es pot veure en la figura 2.4.

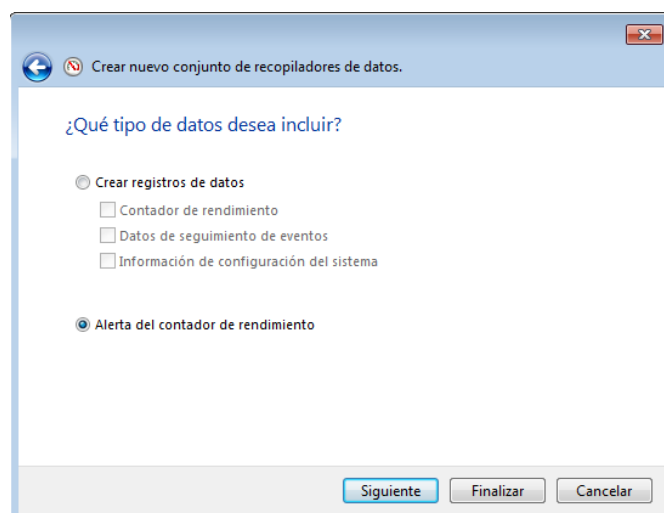
FIGURA 2.4. Monitor de sistema, secció de recursos



2.1.4 Alertes de rendiment

A vegades no n'hi ha prou amb la visualització en temps real del que succeeix en els objectes monitorats del sistema o en l'anàlisi posterior de dades emmagatzemades. En algunes situacions potser cal un avís o una reacció immediata en el moment just en què es produeix una situació concreta i, per tant, es necessita algun sistema que controli contínuament l'evolució del rendiment i ens alerti o efectui automàticament alguna acció en cas que els paràmetres no s'ajustin al que hem establert.

FIGURA 2.5. Creació d'alarmes



Les **alertes de rendiment** permeten definir límits per als diferents comptadors de rendiment i activen alertes si aquests valors són superiors o inferiors als límits establerts.

A Windows, aquesta possibilitat és implementada en l'aplicació ja comentada: el monitor de rendiment, que permet configurar alertes mitjançant la creació per part de l'usuari d'un tipus específic de recopilador de dades, tal com es pot veure en la figura 2.5.

La creació d'una alerta consisteix a:

1. Triar un o diversos comptadors de rendiment entre tots els que hi ha disponibles.
2. Indicar el llindar per defecte o per excés que farà saltar l'alerta.
3. Establir les accions que es duran a terme si se sobrepassa aquest llindar. Les opcions disponibles són les següents:
 - Enregistrar una incidència en el registre d'esdeveniments.
 - Iniciar en el moment de l'alerta un conjunt de recopiladors de dades específic per poder analitzar el problema amb detall a partir del moment de l'alarma.
 - Executar una tasca o un programa administratiu determinats.

Per accedir al monitor de rendiment, cal fer servir la finestra d'execució (TeclaWindows+R) i cridar l'executable perfmon.exe; o bé, en el menú principal triar Tauler de control Sistema i seguretat Eines administratives Monitor de rendiment. Aleshores cal seleccionar la secció "Conjunts de recopiladors de dades", subsecció "Definits per l'usuari". En aquest punt es pot crear un nou recopilador de dades amb menú Acció Nou Conjunt recopilador de dades i triant la Creació manual (avançada) ens trobarem les possibilitats següents: creació de registres de dades i alerta del comptador de rendiment.

2.2 Enregistrament i monitoratge d'esdeveniments

Un **esdeveniment** és una acció determinada de l'usuari o un procés significatiu originat pel sistema operatiu o les aplicacions.

Un esdeveniment queda enregistrat perquè l'administrador ha definit que és prou important per tenir-se en compte. Per tant, cal fer una tasca prèvia, que consisteix a definir quins tipus d'esdeveniments es vol que quedin enregistrats.

Si fem una classificació bàsica de la tipologia dels incidents, obtindrem la llista següent:

- **Esdeveniments del sistema.** Són generats pel mateix sistema operatiu; per exemple, un tancament no previst del sistema.
- **Esdeveniments d'aplicació.** Són generats per les aplicacions o els programes d'aplicació que s'estan executant. Els programadors que han dissenyat l'aplicació decideixen quins esdeveniments volen controlar. N'és un exemple la impossibilitat d'obrir un arxiu que l'aplicació necessita.

- **Esdeveniments de seguretat.** Són relatius a la seguretat; per exemple, els accessos dels usuaris o l'esborrament d'un recurs del sistema. L'enregistrament d'aquests esdeveniments de seguretat és responsabilitat de l'administrador i entra en el camp de l'**auditoria informàtica**.

2.2.1 Eines d'enregistrament i monitoratge d'esdeveniments a Windows

El sistema operatiu Windows guarda la informació sobre les incidències i esdeveniments en uns arxius de registre determinats que després poden ser visualitzats i interpretats amb eines com ara el **visor d'esdeveniments** o el **monitor de fiabilitat**.

Arxius de registre

Un **arxiu de registre** (*log file*) és un fitxer, generalment de text, en què el sistema operatiu o les aplicacions enregistren informació i dades rellevants de les incidències i esdeveniments que es van produint, per a la gestió i l'anàlisi posteriors.

En el cas del sistema operatiu Windows, aquests esdeveniments es guarden en diferents arxius de registre. Els més importants són els següents:

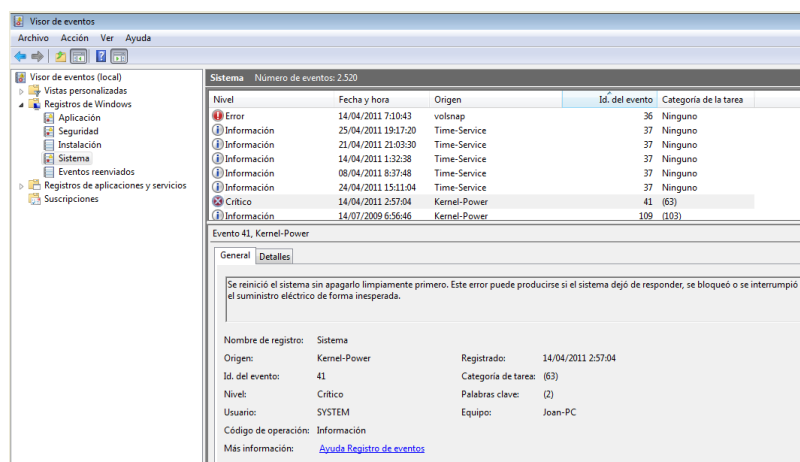
- **Registre d'aplicació.** Conté esdeveniments enregistrats per programes i aplicacions. Els desenvolupadors d'aplicacions determinen les incidències que volen enregistrar; per exemple, en un gestor de bases de dades, l'intent erroni d'escriptura en un arxiu de només lectura.
- **Registre de sistema.** Conté els registres de seguiment del sistema operatiu i guarda tota una sèrie d'accions predeterminats; per exemple, el canvi de l'hora del sistema.
- **Registre d'instal·lació.** Registra esdeveniments relacionats amb la instal·lació de programes i actualitzacions.
- **Registre de seguretat.** Enregistra els esdeveniments relatius a seguretat com els inicis de sessió vàlids i no vàlids o els accessos a uns recursos determinats, com ara crear, obrir, modificar o esborrar arxius. Aquest registre es troba inactiu per defecte i l'administrador el pot activar mitjançant les funcions d'auditoria de les directives de grup del directori actiu o les directives locals de seguretat.

Visor d'esdeveniments

El visor d'esdeveniments és una eina per visualitzar, filtrar, analitzar i gestionar els diferents esdeveniments enregistrats pel sistema en els arxius de registre.

Els components d'informació que es guarden d'un esdeveniment són la capçalera i la descripció. En la capçalera hi ha el tipus d'esdeveniment que, segons la seva importància, pot ser informativa, d'advertiment, d'error o crítica. Els esdeveniments de seguretat, en canvi, es classifiquen com d'accés correcte auditat o accés erroni auditat. A més del tipus d'esdeveniment, la capçalera inclou informació rellevant com la data i l'hora en què s'ha produït, un número identificatiu de l'esdeveniment, l'origen del programa o aplicació que l'ha generat i l'usuari i equip on s'ha generat, tal com es veu en la figura 2.6.

FIGURA 2.6. Visor d'esdeveniments



El visor permet guardar la informació dels esdeveniments en arxius de format propi (extensió .evtx), en format text (.txt), en arxius de full de càlcul delimitat (.csv) o bé en format xml (extensió .xml).

Monitor de fiabilitat

El monitor de fiabilitat és una eina que quantifica errors, fallades i canvis en el sistema i la seva configuració i proporciona un **índex d'estabilitat** que varia entre 1 (el menys estable) i 10 (el més estable), tal com es veu en la figura 2.7. Qualsevol canvi en l'equip o qualsevol problema que es produeixi afectarà l'índex d'estabilitat que es representa en una gràfica temporal amb la notació diària dels esdeveniments quantificats.

Els tipus d'esdeveniments que presenta estan identificats clarament amb icones i són els següents:

- **Errors crítics.** Poden ser errors d'aplicació, de sistema operatiu o d'altres. Per exemple, quan el sistema es tanca inesperadament de manera incorrecta.
- **Advertiments.** Errors menys greus, però que cal documentar, com la instal·lació fallida d'una actualització.

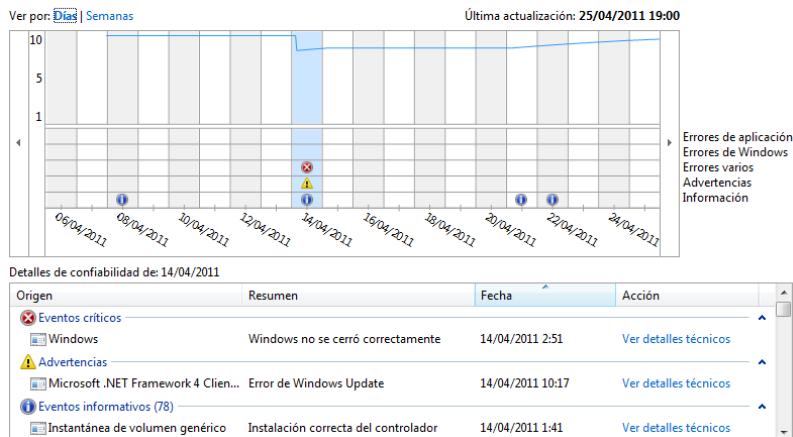
Per accedir al visor d'esdeveniments cal fer servir la finestra d'execució (TeclaWindows+R) i cridar la consola eventvwr.msc; o bé, en el menú principal triar Tauler de control Sistema i seguretat Eines administratives Visor d'esdeveniments.

- **Esdeveniments informatius.** En principi no comporten la pèrdua de fiabilitat, però cal tenir-los en compte per a possibles diagnòstics. Per exemple, la instal·lació correcta d'un controlador determinat.

FIGURA 2.7. Monitor de fiabilitat

Revise el historial de confiabilidad y problemas del equipo

El índice de estabilidad evalúa la estabilidad general del sistema en una escala del 1 al 10. Si selecciona un período de tiempo específico, puede revisar los problemas específicos de hardware y software que han afectado al sistema. [Cómo usar el Monitor de confiabilidad.](#)



Per accedir al monitor de fiabilitat cal fer servir la finestra d'execució (Tecla Windows+R) i cridar l'executable perfmonrel; o bé, en el menú principal triar Tauler de control Sistema i seguretat Centre d'activitats i, aleshores, obrir la secció de Manteniment Veure historial de fiabilitat*.

Es pot fer servir el monitor de fiabilitat per diagnosticar problemes intermitents. Per exemple, es podria establir la correlació entre la instal·lació d'un programa o controlador determinat i l'augment posterior de la inestabilitat del sistema.

2.2.2 Eines d'enregistrament i monitoratge d'esdeveniments a Linux

La majoria dels arxius de registre a Linux es guarden, seguint l'estructura jeràrquica estàndard de Linux (FHS), en el directori /var/log. Hi ha dos tipus d'arxius de registre, els de text pla, que poden ser llegits per qualsevol editor de text, i els binaris, que depenen d'aplicacions i ordres externes per veure la informació que contenen.

Arxius de registre en format de text pla

Els principals arxius de registre en format de text pla són els següents:

- **/var/log/syslog.** És l'arxiu de registre més important, ja que per defecte és on s'enregistren tots els tipus d'esdeveniments que no disposen d'un arxiu específic. Un exemple del contingut d'aquest fitxer és el següent:

```
1 $ cat /var/log/syslog
2 Apr 26 11:06:24 jmunoz33-desktop anacron[737]: Job 'cron.daily' terminated
3 Apr 26 11:06:24 jmunoz33-desktop anacron[737]: Normal exit (1 job run)
4 Apr 26 11:17:01 jmunoz33-desktop CRON[1695]: (root)
5 Apr 26 11:25:07 jmunoz33-desktop acpid: client 984[0:0] has disconnected
6 Apr 26 11:25:07 jmunoz33-desktop acpid: client connected from 984[0:0]
```

Estàndard de jerarquia de sistemes d'arxius (FHS)

FHS són les inicials de *filesystem hierarchy standard* i defineix els directoris principals i els continguts d'aquests en sistemes Linux o en altres sistemes de la família Linux. Fou dissenyat originàriament el 1994 per estandarditzar els sistemes d'arxius entre distribucions GNU/Linux. Està basat en l'organització tradicional dels sistemes UNIX.

```

7 Apr 26 11:25:07 jmunoz33-desktop acpid: 1 client rule loaded
8 Apr 26 11:25:45 jmunoz33-desktop init: tty1 main process ended, respawning
9 Apr 26 11:26:47 jmunoz33-desktop init: tty2 main process ended, respawning
10 Apr 26 11:26:49 jmunoz33-desktop acpid: client 984[0:0] has disconnected
11 Apr 26 11:26:49 jmunoz33-desktop acpid: client connected from 984[0:0]
12 Apr 26 11:26:49 jmunoz33-desktop acpid: 1 client rule loaded

```

- **/var/log/messages.** Conté missatges informatius del sistema operatiu.
- **/var/log/auth.log.** Conté el registre de totes les autenticacions en el sistema, tant les correctes com les fallides.
- **/var/log/debug** S'hi emmagatzema la informació de depuració (*debug*) dels programes que executem en el sistema.
- **/var/log/kern.log.** Conté els missatges provinents del nucli del sistema operatiu (*kernel*).
- **/var/log/daemon.log.** Conté les anotacions dels diferents dimonis que s'estan executant en el sistema.
- **/var/log/mail.log.** Conté informació de tots els missatges que entren i surten del servidor de correus SMTP.
- **/var/log/boot.log.** Conté els missatges d'arrencada del sistema.
- **\$HOME/.bash_history.** Conté l'historial de totes les ordres executades per un determinat usuari en la *shell bash*.

Arxius de registre en format binari

Els principals arxius de registre en format binari són els següents:

- **/var/log/wtmp.** Enregistra tota la informació de connexions i desconnexions del sistema. Com que és un arxiu binari, per veure el contingut cal un programa extern. En aquest cas, l'ordre **last**.

```

1 $ last
2 jmunoz pts/0 :0.0 Tue Apr 26 10:59 still logged in
3 jmunoz tty7 :0 Tue Apr 26 10:58 still logged in
4 reboot system boot 2.6.32-28-generi Tue Apr 26 10:53 - 11:17 (00:23)
5 jmunoz pts/0 :0.0 Sun Apr 24 07:44 - 08:19 (00:34)
6 jmunoz pts/0 :0.0 Sun Apr 24 06:28 - 06:33 (00:04)
7 jmunoz tty7 :0 Sun Apr 24 06:20 - crash (2+04:32)

```

- **/var/run/utmp.** Conté la informació dels usuaris connectats en un moment determinat. Es pot obtenir mitjançant les ordres **w** o bé **who**:

```

1 $ w
2 11:19:24 up 26 min, 2 users, load average: 0,61, 0,36, 0,33
3 USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
4 jmunoz tty7 :0 10:58 26:33 25.41s 1.13s gnome-session
5 jmunoz pts/0 :0.0 10:59 0.00s 0.79s 0.03s w
6 jmunoz@jmunoz33-desktop:/var/run$

```

- **/var/log/lastlog**. Conté la data i l'hora de la darrera connexió de tots els usuaris que hi ha en el sistema. L'ordre per veure aquesta informació és **lastlog**.

```

1 $ lastlog
2 Usuari      Port      Des de      Últim
3 root        tty1      dg mar 27 23:37:21 +0200 2011
4 daemon
5 bin         **No ha entrat mai**
6 jmunoz      tty1      dl mar 28 00:17:25 +0200 2011
7 vboxadd    **No ha entrat mai**
8 prova      tty1      dg mar 27 23:51:11 +0200 2011
9 alumnel    **No ha entrat mai**

```

- **/var/log/faillog**. Informa dels intents d'entrada erronis que s'han fet en el sistema. El visor per veure el contingut és l'ordre **faillog**.

2.3 Gestió d'aplicacions i processos

Per poder analitzar i millorar el rendiment del sistema no solament cal tenir present el comportament dels components del maquinari o enregistrar i estudiar els esdeveniments que es van produint. És necessari també tenir control sobre el programari que s'està executant en un moment determinat, aplicacions, serveis i els processos que generen, per poder veure els recursos que estan consumint, l'estat en què es troben i, eventualment, poder-los aturar, canviar-ne la prioritat o eliminar definitivament de la memòria.

2.3.1 Conceptes d'aplicació, procés i servei

Una **aplicació** informàtica generalment es considera un programa dissenyat per interaccionar amb l'usuari; per tant, s'executa en primer pla (*foreground*) amb una interfície d'usuari determinada, per ajudar-lo en la realització d'una tasca concreta. Són exemples típics d'aplicacions els programes d'ofimàtica, els navegadors, els reproductors multimèdia, etc.

Un **servei**, en canvi, és un programa normalment associat al sistema operatiu, encara que també es pot utilitzar de manera manual, i que treballa en segon pla (*background*) sense interfície d'usuari, donant suport a altres programes. Els serveis proporcionen prestacions com servei de pàgines web, el registre d'esdeveniments, serveis d'impressió, criptografia, etc.

El concepte de **procés** té més a veure amb el funcionament intern del sistema operatiu i consisteix en una sèrie d'instruccions allotjades a la memòria i que, mitjançant cues i un mecanisme de planificació, accedeixen a la CPU per executar-se. Així doncs, qualsevol aplicació o servei, quan s'endeguen, generen un o més processos en el sistema.

Servei

El terme *servei* s'acostuma a fer servir en entorns Windows i correspon al concepte i la funcionalitat del dimoni (*daemon*) en la terminologia de Linux.

Totes aquestes aplicacions i serveis, i els processos que generen, es poden monitorar i gestionar amb les eines adequades.

2.3.2 Eines de gestió de tasques i processos a Windows

En el sistema operatiu Windows disposem de dues eines principals per a la gestió d'aplicacions, serveis i processos: la consola de serveis i la consola d'administració de tasques.

La **consola de serveis**. Permet realitzar diferents accions sobre serveis en equips locals i remots, com ara:

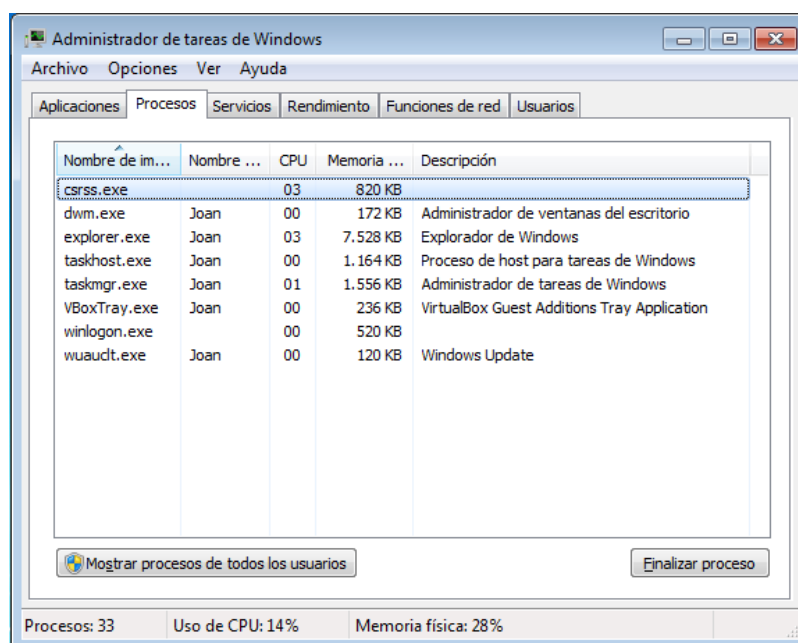
- Iniciar, aturar, reprendre o deshabilitar serveis.
- Configurar accions de recuperació si es produeix un error en un servei (per exemple, reiniciar el servei automàticament o reiniciar l'equip).
- Habilitar o deshabilitar serveis per a un perfil de maquinari específic.
- Exportar i guardar informació dels serveis en un arxiu .txt o .csv.
- Veure l'estat i la descripció de cada servei.
- Veure les dependències dels serveis.

Per accedir a la consola de serveis cal fer servir la finestra d'execució (TeclaWindows+R) i cridar la consola services.msc; o bé, en el menú principal triar Tauler de control Sistema i seguretat Eines administratives Serveis.

La **consola d'administració de tasques** mostra i gestiona les aplicacions, els processos i els serveis que s'estan executant en l'equip en un moment determinat (vegeu la figura 2.8). També es pot fer servir per supervisar el rendiment de l'equip, comprovar l'estat i el funcionament de la xarxa i veure i enviar missatges als usuaris connectats a l'equip. També és molt útil per tancar un programa o procés que ha quedat penjat i no respon.

Per accedir a la consola d'administració de tasques cal fer servir la combinació de tecles CTRL+MAJÚSCULA+ESC, o bé mitjançant la finestra d'execució (TeclaWindows+R), i cridar l'aplicació taskmgr.exe perquè aparegui la finestra següent.

FIGURA 2.8. Consola d'administració de tasques



2.3.3 Eines de gestió de tasques i processos en Linux

Per administrar i gestionar processos en Linux es poden fer servir directament ordres de consola, si bé també és pot treballar des de l'entorn gràfic amb la utilitat de monitoratge del sistema.

Ordres de consola

El sistema operatiu Linux disposa de diferents ordres en l'entorn de consola de text per a la gestió i el monitoratge de processos.

- **ps.** En la majoria de sistemes operatius de la família Unix, l'ordre **ps** (*process status*) permet visualitzar els processos en execució. Si no hi posem cap argument, només es mostraran els processos iniciats per l'usuari actual i que fan referència al terminal que utilitza.

```
1 ps
2 PID TTY          TIME CMD
3 2065 pts/0    00:00:00 bash
4 2082 pts/0    00:00:00 ps
```

La primera columna mostra l'identificador del procés (*process identifier*, PID), la terminal associada al procés (columna TTY), el temps acumulat d'ús de CPU (columna TIME) i finalment l'ordre que ha generat el procés (CMD). Si hi afegim algunes opcions (aux) podem obtenir més informació:

```
1 ps aux
2 USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
3 root         1   0.0  0.1  2804  1624 ?        Ss   05:43   0:01 /sbin/init
4 root         2   0.0  0.0      0     0 ?        S    05:43   0:00 [kthreadd]
5 root         3   0.0  0.0      0     0 ?        S    05:43   0:00 [migration/0]
```

- **pstree.** Aquesta ordre mostra una llista de processos en forma d'arbre seguint la jerarquia de processos Unix que permet identificar fàcilment quin és el procés pare d'un altre.

```
1 pstree -A
2 init--+-NetworkManager--+-dhclient
3     |                       '---{NetworkManager}
4     |--3*[VBoxClient]---{VBoxClient}}
5     |--VBoxService---6*[{VBoxService}]
6     |--acpid
7     |--atd
8     |--avahi-daemon---avahi-daemon
9     |--bonobo-activati---{bonobo-activat}
10    |--clock-applet---{clock-applet}
11    |--console-kit-dae---63*[{console-kit-da}]
12    |--cron
13    |--cupsd
14    |--4*[dbus-daemon]
15    |--4*[dbus-launch]
16    '---2*[gconfd-2]
```

- **top.** Correspon a la presentació interactiva dels processos, en temps real (actualització cada tres segons) i ordenats pel percentatge d'ús de CPU. La primera línia d'informació és la mateixa que dona l'ordre **uptime**. A continuació mostra informació dels processos en execució: PID (identificador), USER (propietari), PRI (prioritat), NI (prioritat d'usuari nice), VIRT (memòria virtual), RES (memòria resident), SHARE (memòria compartida), STAT (R running, S sleeping, Z zombie, T stopped), LC (últim processador utilitzat), %CPU (percentatge de processador utilitzat), %MEM (percentatge de memòria física utilitzada), TIME (temps d'utilització del processador) i COMMAND (nom de l'ordre).

```

1 top
2 top - 07:58:28 up 2:14, 2 users, load average: 0.03, 0.26, 0.38
3 Tasks: 151 total, 1 running, 150 sleeping, 0 stopped, 0 zombie
4 Cpu(s): 0.3%us, 4.6%sy, 0.0%ni, 94.7%id, 0.0%wa, 0.3%hi, 0.0%si, 0.0%st
5 Mem: 1026484k total, 636624k used, 389860k free, 67172k buffers
6 Swap: 1952760k total, 0k used, 1952760k free, 375648k cached
7
8 PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
9 976 root 20 0 48900 22m 7852 S 9.6 2.3 12:33.54 Xorg
10 2062 jmunoz33 20 0 117m 13m 10m S 7.0 1.3 0:08.14 gnome-terminal
11 2093 jmunoz33 20 0 2548 1200 904 R 1.0 0.1 0:00.11 top
12 1 root 20 0 2804 1624 1172 S 0.0 0.2 0:01.68 init
13 2 root 20 0 0 0 0 S 0.0 0.0 0:00.04 kthreadd
14 3 root RT 0 0 0 0 S 0.0 0.0 0:00.00 migration/0
15 4 root 20 0 0 0 0 S 0.0 0.0 0:00.10 ksoftirqd/0
16 5 root RT 0 0 0 0 S 0.0 0.0 0:00.00 watchdog/0
17 6 root 20 0 0 0 0 S 0.0 0.0 0:01.03 events/0

```

Qualsevol usuari pot reduir la prioritat dels seus processos, però només el superusuari pot augmentar la prioritat d'un procés.

- **kill, killall.** Aquestes dues ordres es fan servir per enviar senyals a processos. L'ordre **kill** necessita com a argument el PID ('identificador de procés'), mentre que **killall** té com a argument el nom del procés. Per defecte, totes dues envien el senyal 15 (TERM: acabament del programa).
- **nice, renice.** El primer permet arrancar un procés assignant-li una prioritat determinada, mentre que **renice** permet canviar la prioritat d'un procés ja endegat. L'ordre **nice** té com a argument el nom de l'ordre que genera el procés sobre el qual volem actuar. La prioritat definida per defecte és 10 i el rang de prioritat pot anar de -20 (prioritat màxima) fins a 19 (prioritat mínima).

Eines gràfiques

La mateixa eina gràfica del **monitor del sistema**, a més de visualitzar en temps real els recursos, per mitjà d'una pestanya permet controlar els processos que s'estan executant i el consum de recursos del sistema que fan (vegeu la figura 2.9).

Per a cada procés actiu en el sistema mostra la informació següent:

- El nom del procés.
- L'estat en què es troba el procés (adormit, parat, en execució).

- L'identificador corresponent (PID).
- El tant per cent d'ocupació de processador que està utilitzant.
- La prioritat d'execució.
- La quantitat de memòria que fa servir.

Seleccionant un d'aquests processos podem efectuar diferents accions:

- Posar en espera i relançar el procés.
- Aturar-lo d'una manera ordenada o immediata.
- Canviar-ne la prioritat d'execució.
- Visualitzar el mapa de memòria corresponent.
- Visualitzar els arxius oberts amb els quals treballa.

El mapa de memòria d'un procés és un esquema de l'ús de memòria que fa el procés: segments utilitzats, adreces, mides, etc.

El monitor del sistema es pot configurar canviant l'interval de recollida de dades, els paràmetres monitorats i el tipus de gràfic de presentació.

FIGURA 2.9. Monitor de sistema, secció de processos

Monitor del sistema

Monitoritza

Edita

Visualitza

Ajuda

Sistema

Processos

Recursos

Sistemes de fitxers

Mitjanes de càrrega dels últims 1, 5 i 15 minuts: 1,48, 0,78, 0,37

| Nom del procés | Estat | % CPU | Prioritat | Identificador | Memòria |
|--------------------------|--------------|-------|-----------|---------------|-----------|
| bluetooth-applet | Adormit | 0 | 0 | 1399 | 1,6 MiB |
| bonobo-activation-server | Adormit | 0 | 0 | 1447 | 804,0 KiB |
| clock-applet | Adormit | 0 | 0 | 1503 | 2,6 MiB |
| dbus-daemon | Adormit | 0 | 0 | 1359 | 696,0 KiB |
| dbus-launch | Adormit | 0 | 0 | 1358 | 268,0 KiB |
| evolution-alarm-notify | Adormit | 0 | 0 | 1538 | 2,3 MiB |
| gconfd-2 | Adormit | 0 | 0 | 1362 | 2,0 MiB |
| gconf-helper | Adormit | 0 | 0 | 1417 | 588,0 KiB |
| gdu-notification-daemon | Adormit | 0 | 0 | 1464 | 1,5 MiB |
| gnome-keyring-daemon | Adormit | 0 | 0 | 1270 | 440,0 KiB |
| gnome-panel | Adormit | 0 | 0 | 1392 | 3,9 MiB |
| gnome-power-manager | Adormit | 0 | 0 | 1384 | 1,6 MiB |
| gnome-screensaver | Adormit | 0 | 0 | 1469 | 1,3 MiB |
| gnome-session | Adormit | 0 | 0 | 1288 | 1,4 MiB |
| gnome-system-monitor | Executant-se | 49 | 0 | 1564 | 4,1 MiB |

3. Directives de seguretat i auditories

El terme *auditar* significa recollir i analitzar dades per obtenir informació rellevant i emetre informes que deixin constància d'una situació determinada. En l'entorn informàtic, l'auditoria és un procés que permet recollir i avaluar evidències per determinar la productivitat, la integritat de les dades i l'ús eficient dels recursos, però en especial fa referència als aspectes de vigilància i supervisió de seguretat d'un sistema informàtic.

3.1 Auditoria de sistemes informàtics

El procediment d'auditoria de sistemes informàtics constitueix una eina de seguretat preventiva, ja que informa als administradors dels esdeveniments que poden ser perillosos i suggereix millores, alhora que permet enregistrar un rastre de responsabilitats en el cas de delictes i intromissions no autoritzades, amb la qual cosa constitueix també un suport en l'anàlisi forense.

Podem considerar com a **objectius de l'auditoria** de sistemes informàtics, entre d'altres, els següents:

- Evitar frau, espionatge i delictes informàtics.
- Controlar els accessos a les bases de dades.
- Acomplir la llei de drets d'autor, evitar la pirateria de programari i el seu ús no autoritzat.
- Protegir els secrets industrials o comercials i també informació financera, tecnològica o logística.
- Avaluar els riscos en matèria de seguretat.
- Comprovar l'ús eficient dels recursos evitant usos aliens a l'organització.
- Evitar en la mesura que sigui possible la pèrdua de la continuïtat del servei.

El procés d'auditoria consta d'una sèrie de parts que es poden resumir en les següents etapes:

- **Avaluació de l'entorn auditable.** Establiment dels components de maquinari i dels programes i serveis que constitueixen l'entorn del sistema que s'ha de controlar.
- **Definició d'abast i objectius de l'auditoria.** Concreció de l'àmbit de l'auditoria i dels objectius que es pretenen assolir.

Anàlisi forense

Pretén recollir, preservar, analitzar i presentar dades que han estat processades digitalment i emmagatzemades en un suport informàtic amb l'objectiu de facilitar la reconstrucció d'esdeveniments delictius i anticipar accions no autoritzades que afectin els sistemes informàtics.

- **Elaboració d'un pla i un programa de treball.** Definició dels aspectes que cal auditar segons els objectius fixats.
- **Definició d'activitats i execució de l'auditoria.** Recollida de dades i anàlisi d'aquestes, a més de l'establiment d'accions, alarmes i accions correctives.
- **Redacció d'un informe final.** Informe de la situació, conclusions i suggeriments de millora.
- **Seguiment de la situació avaluada.** Comprovació de l'evolució i millora del sistema avaluat amb la incorporació de les mesures correctores obtingudes.

3.1.1 Àmbit de l'auditoria, aspectes auditables

El primer pas per a l'establiment d'una política i un pla d'auditoria és la determinació dels aspectes que ens interessa controlar, cosa que es traduirà en les tipologies i les categories d'esdeveniments que es volen auditar.

Per exemple, en el sistema operatiu Windows es pot activar l'auditoria de les categories bàsiques següents:

- **Accés a objectes.** Audita l'ús d'alguns recursos del sistema, com ara els arxius, els directoris, els recursos compartits, les impressores o els objectes del directori actiu.
- **Accés al servei de directori.** Audita els esdeveniments que es generen cada vegada que un usuari o un equip accedeix al servei de directori.
- **Canvi de directiva.** Audita els canvis en els permisos d'usuari, auditoria i relacions de confiança.
- **Seguiment de processos.** Audita els processos del sistema i els recursos que s'utilitzen.
- **Ús de privilegis.** Audita la utilització de permisos i privilegis d'usuari.
- **Esdeveniments d'inici de sessió.** Audita els esdeveniments lligats a l'inici i el tancament de connexions remotes als sistemes de xarxa.
- **Esdeveniments d'inici de sessió de compte.** Audita els esdeveniments relacionats amb l'inici i el tancament de sessions.
- **Esdeveniments de sistema.** Audita el procés d'arrencada, el tancament i el reinici del sistema, a més de les accions que afecten la seguretat del sistema o el registre de seguretat.
- **Administració de comptes.** Audita els esdeveniments que es generen quan es creen, es modifiquen o s'eliminen comptes d'usuari, d'equip o de grup.

Per defecte, en el sistema operatiu Windows vénen deshabilitats tots els aspectes auditables.

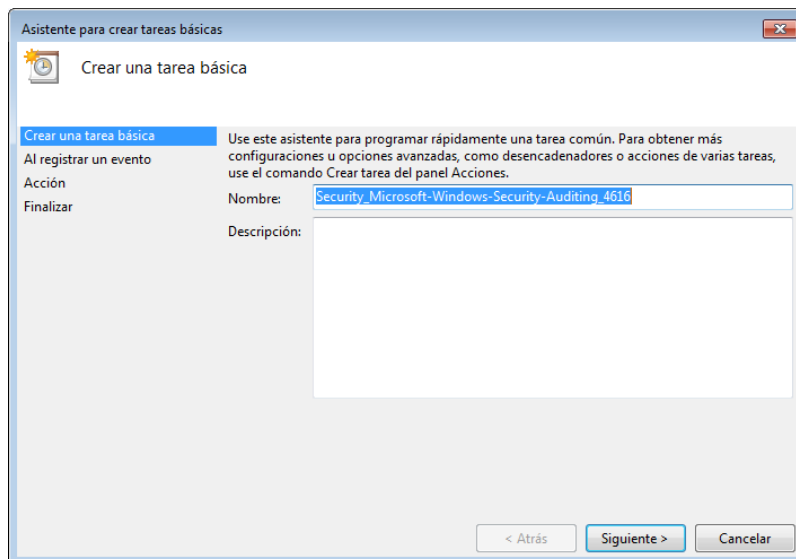
Dintre de cada aspecte auditable es pot configurar, per a una anàlisi posterior, l'enregistrament d'accions que finalitzin de manera correcta, de manera errònia o tots dos casos. És molt important elaborar un pla d'auditoria correcte per triar només els aspectes auditables que siguin realment necessaris, ja que cal tenir en compte que qualsevol acció d'enregistrament d'esdeveniments comporta la dedicació de recursos i, per tant, una repercussió negativa en el rendiment del sistema.

3.1.2 Mecanismes d'auditoria. Informes, alarmes i accions correctives

Les eines d'auditoria proporcionen diferents mecanismes d'actuació. D'una banda, l'enregistrament dels diversos esdeveniments programats aporta dades que es poden filtrar i analitzar per extreure conclusions i establir proves forenses; de l'altra, és possible programar alarmes que es disparin en unes condicions determinades i realitzin tasques i accions programades en temps real segons els esdeveniments produïts.

En el sistema operatiu Windows, el mateix **visor d'esdeveniments** ens proporciona un assistent per crear alarmes i tasques programades.

FIGURA 3.1. Assistent per crear tasques bàsiques



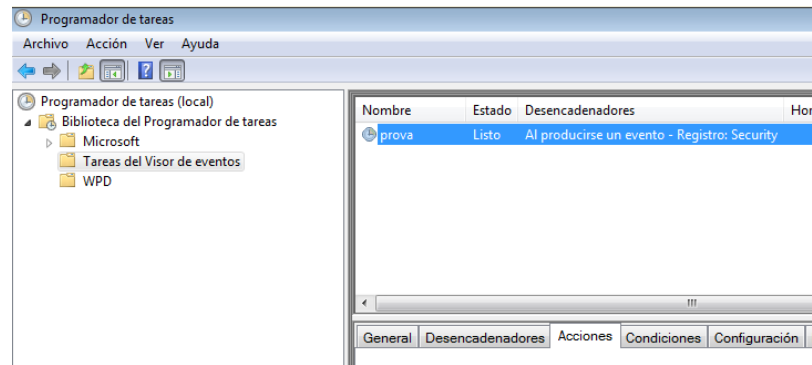
Per accedir a l'assistent de tasques del visor d'esdeveniments cal fer servir la finestra d'execució (TeclaWindows+R) i cridar la consola eventvwr.msc; o bé, en el menú principal triar Tauler de control Sistema i seguretat Eines administratives Visor d'esdeveniments. Aleshores cal triar un dels registres de Windows, marcar l'esdeveniment que activarà l'alarma i amb el menú contextual (botó dret del ratolí) seleccionar Adjuntar tasca a aquest esdeveniment. Sortirà l'assistent que es mostra en la figura 3.1.

Aquest assistent ens facilita la creació de tasques i alarmes associades a un esdeveniment concret. Al llarg de les pantalles de l'assistent ens demanarà que concretament les accions associades a la tasca d'entre aquestes tres:

- Iniciar un programa executable o un guió (*script*).
- Enviar un correu electrònic.
- Mostrar un missatge d'avertiment a la pantalla.

Una vegada finalitzat l'assistent, quedarà configurada una nova tasca bàsica. Per modificar aquesta tasca creada per l'assistent i fer una configuració més completa, o bé, per crear una tasca manualment des de zero, es pot fer servir directament el **programador de tasques** que disposa d'uns disparadors d'alarma específics per a esdeveniments del registre de seguretat i auditoria (vegeu la figura 3.2).

FIGURA 3.2. Programador de tasques



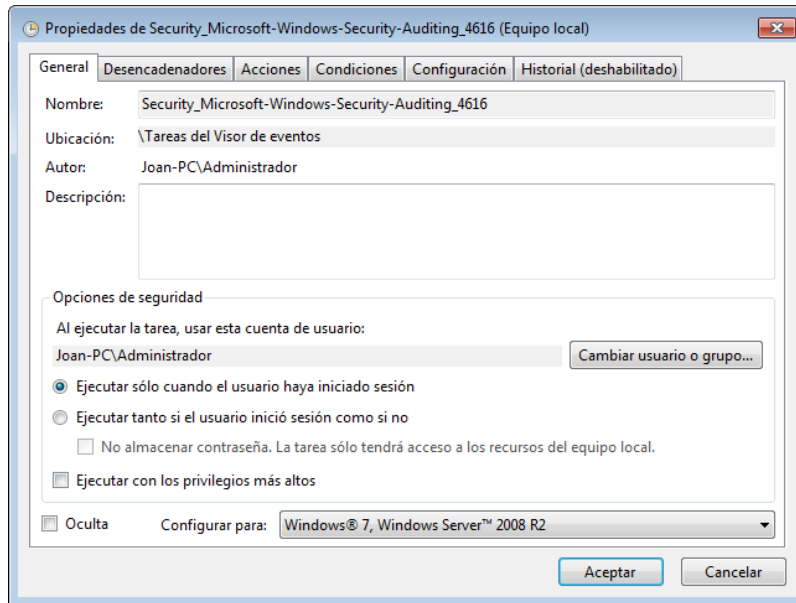
Una vegada endegat el programador de tasques es pot accedir a la secció corresponent a “**tasques del visor d'esdeveniments**” que ens permetrà la gestió de les alarmes configurant l'esdeveniment o el conjunt d'esdeveniments que la fan disparar i establint les possibles accions associades a l'alarma.

La configuració de les tasques i alarmes és molt més precisa que la configurada amb l'assistent i, tal com es veu en la figura 3.3, permet definir:

- **Característiques generals:** es tracta de dades com el nom, l'autor i la descripció de la tasca i el compte d'usuari i privilegis amb què s'ha d'executar.
- **Desencadenants:** permet definir un o diversos esdeveniments o desencadenants que disparin la tasca programada.
- **Accions:** concreta les accions associades a la tasca, missatge d'avís, correus electrònics o executar un programa o guió. També permet definir més d'una acció.
- **Condicions:** es tracta d'una sèrie de condicionants que, juntament amb els desencadenants, determinen si s'executa o no la tasca. Algunes d'aquestes condicions són que l'equip hagi estat inactiu un temps determinat, que l'equip estigui connectat a la xarxa d'alimentació de corrent altern sense fer ús de bateria o que tingui una determinada connexió de xarxa disponible.
- **Configuració:** inclou configuracions addicionals que afecten el comportament de la tasca programada, com ara definir els intents d'inici d'una tasca si aquesta no s'executa per alguna raó, limitar el temps d'execució d'una tasca programada o determinar si s'endega o no una nova instància de la tasca si ja n'hi ha una en marxa.
- **Historial:** en cas d'estar habilitat, enregistra l'historial de tasques programades que s'han executat.

Es pot endegar el programador de tasques mitjançant Tauler de control Sistema i seguretat Programar tasques, o bé fent servir la finestra d'execució (Tecla_Windows+R) i executar la consola Tasksschd.msc.

FIGURA 3.3. Propietats del programador de tasques



Les alarmes ens poden ajudar a detectar una invasió de seguretat i permeten adoptar ràpidament mesures per avaluar els danys presents, limitar els danys causats i conservar les proves per a una anàlisi forense posterior. Algunes de les possibles accions que s'aconsella realitzar en cas d'una invasió de seguretat són les següents:

- Desconnectar la xarxa.
- Realitzar una imatge del disc immediatament després de l'atac.
- Analitzar la vulnerabilitat que ha aprofitat l'atacant i cercar la manera d'evitar que es repeteixi.
- Cercar proves en els arxius de registre i auditoria.
- Modificar les contrasenyes en els sistemes afectats.
- Documentar tot el desenvolupament de la incidència i elaborar un pla de resposta per evitar que torni a succeir.

D'altra banda, els **informes d'auditoria** són essencials per comunicar les conclusions sobre la informació històrica i les tendències i per facilitar l'anàlisi estadística del comportament del sistema informàtic. Són molt útils quan els administradors dels sistemes han de presentar informació periòdica de la situació funcional i de seguretat del sistema als gerents i auditors perquè puguin prendre les millors decisions empresarials.

3.2 Auditoria en sistemes operatius propietaris

El sistema operatiu Windows ens proveeix d'eines i recursos per a la gestió de la seguretat i la realització de tasques d'auditoria. Alguns d'aquests mecanismes són l'assignació de **drets d'usuaris**, les **directives de seguretat i auditoria** i els **arxius de registre** d'esdeveniments. A més, com a eines de gestió, es disposa de la **consola d'edició de directives**, del **visor d'esdeveniments** i de la **consola de programació de tasques**.

3.2.1 Drets d'usuari

En el sistema operatiu Windows, el que poden fer els usuaris dintre del sistema és determinat pels permisos i drets que tinguin concedits. Els permisos indiquen l'accés que un usuari o grup té a objectes específics com ara arxius, directoris i impressores. Els **drets d'usuari**, en canvi, s'apliquen al sistema sencer, com, per exemple, la capacitat de fer còpies de seguretat o d'iniciar una sessió en el servidor.

El drets d'usuari es poden classificar en dues categories:

- **Drets d'inici de sessió.** Impliquen la capacitat de connectar-se a un equip de maneres específiques; per exemple, tenir accés a un equip des de la xarxa, poder iniciar una sessió local o mitjançant el servei de terminal.
- **Privilegis.** Permeten als usuaris i grups efectuar accions específiques sobre el sistema com ara canviar l'hora, instal·lar controladors, apagar el sistema o configurar auditories de seguretat.

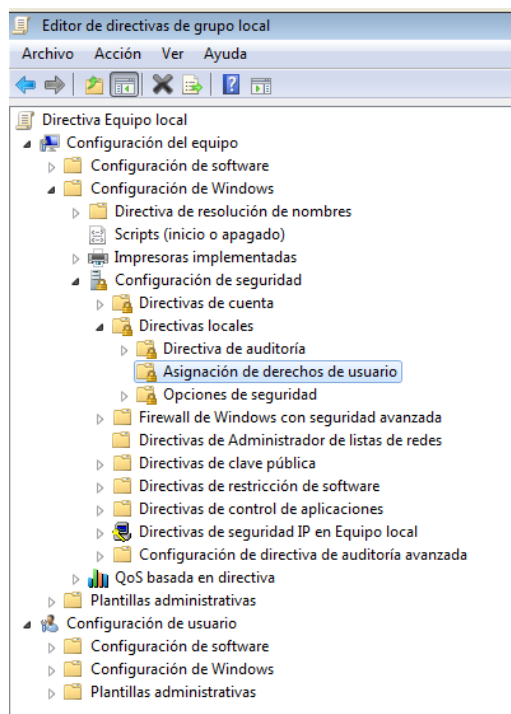
Els drets d'usuari es poden assignar d'una manera individual però habitualment, per simplificar-ne l'administració, són característics dels grups i un usuari s'assigna a un grup determinat en funció dels drets que necessita.

3.2.2 Directives de seguretat local

L'assignació o eliminació de drets d'usuari i l'activació de l'auditoria es pot fer a nivell de domini mitjançant directives de grup del directori actiu o bé a nivell local en equips individuals, per mitjà de les **directives de seguretat local** que es configuren amb una consola administrativa específica que es pot veure en la figura [3.4](#).

Una directiva definida a nivell de domini en un entorn de directori actiu té sempre més prioritat i substituirà la configuració de la directiva local.

FIGURA 3.4. Directives de seguretat local



La consola d'edició de directives de grup local a Windows es pot obrir amb la finestra d'execució (TeclaWindows+R) i utilitzant la consola gpedit.msc. Una vegada oberta, cal triar a la secció de l'esquerra el menú de Configuració de l'equip i obrir el submenú Configuració de Windows Configuració de seguretat Directives locals*. Aleshores apareixerà una finestra com la figura 3.4

En aquesta secció de configuració de directives de seguretat local tenim al nostre abast l'edició de tres tipus de directives:

- **Directives d'auditoria.** Permet habilitar l'enregistrament per a l'auditoria de diferents esdeveniments, com ara l'inici de sessions, l'accés a objectes o l'ús de privilegis.
- **Assignació de drets d'usuari.** Es poden establir els drets i privilegis que tenen assignats els diferents usuaris i grups. Alguns dels drets d'usuari que es poden configurar són la possibilitat d'iniciar una sessió local, el dret de poder analitzar el rendiment del sistema, administrar el registre de seguretat i auditoria o, simplement, determinar la possibilitat de canviar l'hora del sistema i la zona horària.
- **Opcions de seguretat.** Per configurar determinades opcions de seguretat generals no associades a un usuari o grup concret. Per exemple, permetre apagar el sistema sense iniciar una sessió, canviar el nom del compte d'invitat i del compte d'administrador o restringir l'accés a disquets i unitats òptiques de CD-ROM.

3.2.3 Eines d'auditoria

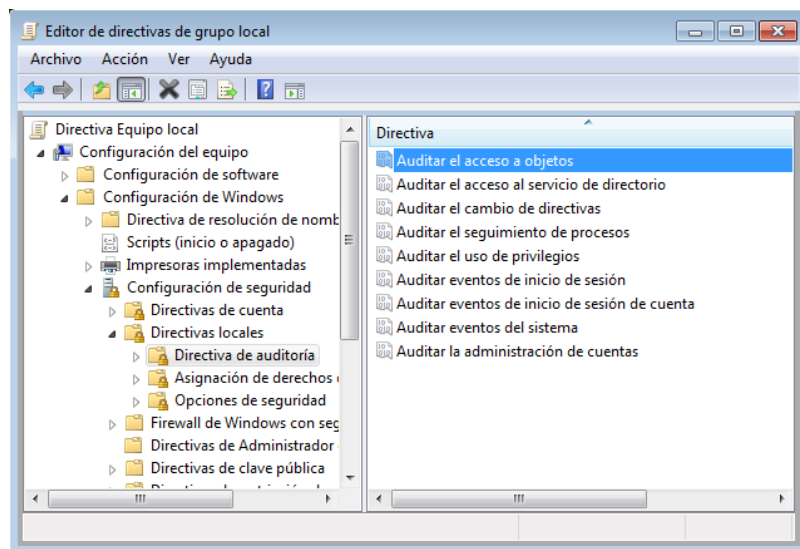
Dintre de les diferents eines d'auditoria que posen al nostre abast les darreres versions de Windows, trobem les consoles gràfiques que permeten, d'una banda, la configuració de les **categories bàsiques d'auditoria** i, de l'altra, un ajust més acurat basat en subcategories gestionades per les **opcions avançades d'auditoria**.

També a nivell de consola es disposa d'una ordre de línia d'ordres anomenada **auditpol.exe**, que permet un control complet de totes les opcions d'auditoria.

Eines d'auditoria bàsica

La configuració de les categories bàsiques d'auditoria es duu a terme mitjançant la consola d'edició de directives de grup local.

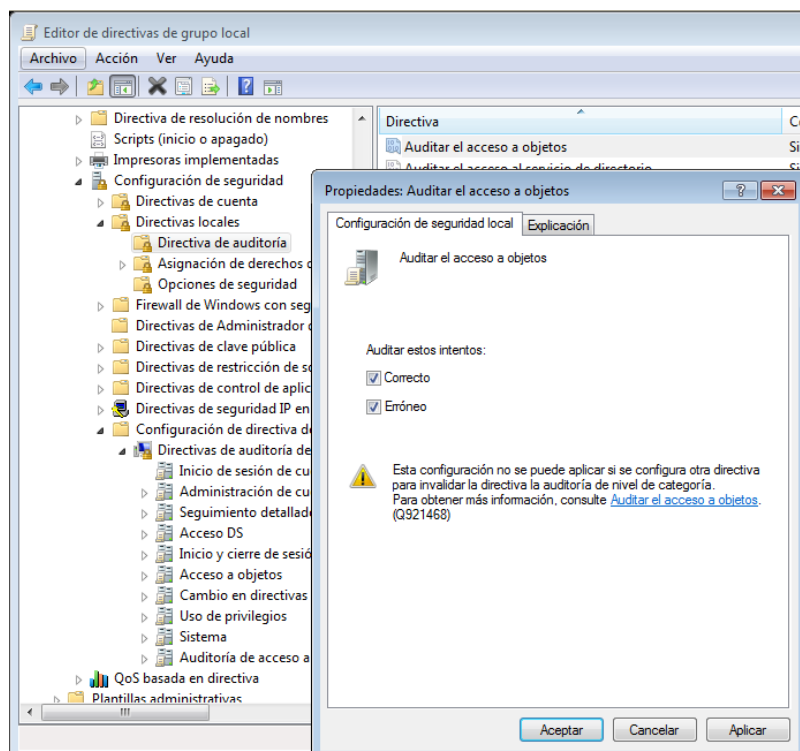
FIGURA 3.5. Directives d'auditoria bàsiques



La consola d'edició de directives d'auditoria bàsica a Windows es pot obrir amb la finestra d'execució (Tecla Windows+R) i endegant la consola d'edició de directives de grup local gpedit.msc. Una vegada oberta, cal triar a la secció de l'esquerra el menú de "Configuració de l'equip" i obrir el submenú Configuració de Windows Configuració de seguretat Directives locals Directiva d'auditoria. Aleshores apareixerà una finestra com la de la figura 3.5.

Aquestes nou categories bàsiques es poden activar tant per enregistrar esdeveniments correctes com erronis, marcant la casella corresponent, tal com es mostra en la figura 3.6.

FIGURA 3.6. Activació de la categoria que s'ha d'auditar



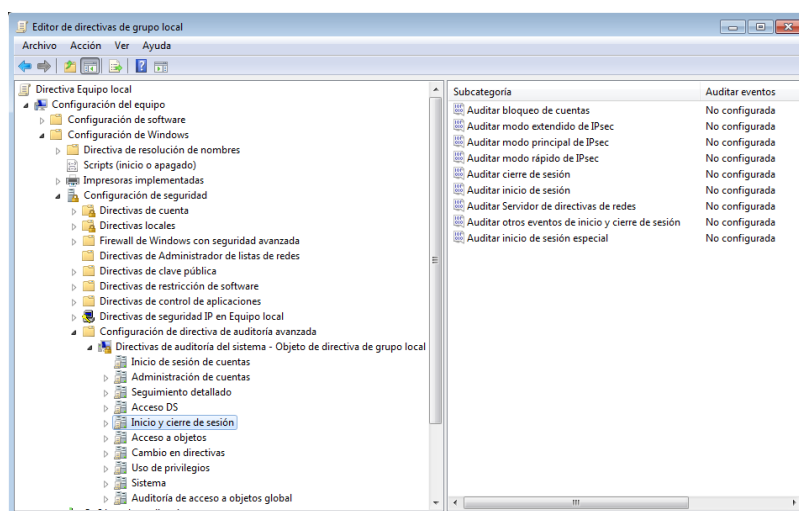
Eines d'auditoria avançades

Amb l'activació de les directives de seguretat local corresponents a auditoria es pot establir una configuració bàsica, però, si volem establir polítiques més complexes i acurades d'auditoria, les darreres versions de Windows posen al nostre abast opcions de configuració més avançades i completes.

En la configuració bàsica d'auditoria disposem de només nou configuracions bàsiques d'actuació; en canvi, la configuració d'auditoria avançada, tot i que afecta conceptes similars, pot discernir fins a 53 subcategories diferents i, per tant, permet als administradors ser més selectius en el nombre i el tipus d'esdeveniments per auditar. Per exemple, allà on l'auditoria bàsica proporciona una sola configuració per a l'inici de sessió de compte, la directiva d'auditoria avançada permet quatre configuracions diferents de manera independent. Habilitar la configuració d'inici de sessió de compte bàsica seria equivalent a establir les quatre configuracions d'inici de sessió de compte avançades.

Aleshores apareixeran les categories bàsiques d'auditoria i, en seleccionar-ne una qualsevol, les subcategories que té associades, tal com mostra la figura 3.7.

FIGURA 3.7. Directives d'auditoria avançada



Les nou categories bàsiques (eines d'auditoria bàsica) i les 53 subcategories (eines d'auditoria avançades) es presenten a la taula 3.1:

TAULA 3.1. Categories bàsiques i subcategories avançades d'auditoria

| Categoria bàsica | Subcategories |
|---------------------------------|---|
| 1. Categoria d'accés d'objectes | 1.1 Sistema d'arxius 1.2 Registre 1.3 Objecte de nucli 1.4 SAM 1.5 Serveis de certificació 1.6 Aplicació generada 1.7 Manipulació d'identificadors 1.8 Recurs compartit de fitxers 1.9 Col·locació de paquets de plataforma de filtratge 1.10 Connexió de plataforma de filtratge 1.11 Altres esdeveniments d'accés a objectes 1.12 Recurs compartit de fitxers detallat |

La configuració avançada només es pot fer servir en equips amb sistema operatiu Windows 7, Windows Vista, Windows Server 2008 R2 o Windows Server 2008.

La consola d'edició de directives d'auditoria avançada a Windows es pot obrir amb la finestra d'execució (Tecla Windows+R) i utilitzant la consola d'edició de directives de grup local gpedit.msc. Una vegada oberta, cal triar a la secció de l'esquerra el menú de "Configuració de l'equip" i obrir el submenú Configuració de Windows Configuració de seguretat Configuració de directives de seguretat avançada Directives d'auditoria del sistema.

La configuració d'auditoria bàsica i l'avançada no s'haurien de fer servir al mateix temps, ja que poden tenir interaccions no volgudes.

Per activar l'auditoria avançada cal definir prèviament la directiva següent a la consola d'edició de directives de grup local gpedit.msc. Una vegada oberta, cal triar a la secció de l'esquerra el menú de "Configuració de l'equip" i obrir el submenú Configuració de Windows Configuració de seguretat Directives locals Opcions de seguretat Auditoria: forçar que la configuració de subcategoria de directiva d'auditoria (Windows Vista o posterior) invalidi la configuració de categoria de directiva d'auditoria.

TAULA 3.1 (continuació)

| Categoria bàsica | Subcategories |
|---|--|
| 2. Categoria d'accés al servei de directori | 2.1 Accés del servei de directori 2.2 Canvis de servei de directori 2.3 Replicació de servei de directori 2.4 Replicació de servei de directori detallada |
| 3. Categoria de canvi de directives | 3.1 Canvi en la directiva d'auditoria 3.2 Canvi de la directiva d'autenticació 3.3 Canvi de la directiva d'autorització 3.4 Canvi de la directiva del nivell de regles de MPSSVC 3.5 Canvi de la directiva de plataforma de filtratge 3.6 Altres esdeveniments de canvi de directives |
| 4. Categoria de seguiment de processos | 4.1 Creació del procés 4.2 Finalització del procés 4.3 Activitat DPAPI 4.4 Esdeveniments de RPC |
| 5. Categoria d'ús de privilegis | 5.1 Ús de privilegi confidencial 5.2 Ús de privilegi no confidencial 5.3 Altres esdeveniments d'ús de privilegi |
| 6. Categoria d'inici o tancament de sessió | 6.1 Inici de sessió 6.2 Tancament de sessió 6.3 Bloqueig de compte 6.4 Mode principal d'IPsec 6.5 Mode ràpid d'IPsec 6.6 Mode estès d'IPsec 6.7 Inici de sessió especial 6.8 Altres esdeveniments d'inici i tancament de sessió 6.9 Servidor de directives de xarxes |
| 7. Categoria d'inici de sessió del compte | 7.1 Validació de credencials 7.2 Operacions de vals de servei Kerberos 7.3 Altres esdeveniments d'inici de sessió de comptes 7.4 Servei d'autenticació Kerberos |
| 8. Categoria d'administració de comptes | 8.1 Administració de comptes d'usuari 8.2 Administració de comptes d'equip 8.3 Administració de grups de seguretat 8.4 Administració de grups de distribució 8.5 Administració de grups d'aplicacions 8.6 Altres esdeveniments d'administració de comptes |
| 9. Categoria sistema | 9.1 Canvi d'estat de seguretat 9.2 Extensió del sistema de seguretat 9.3 Integritat del sistema 9.4 Controlador IPsec 9.5 Altres esdeveniments de sistema |

Eines de la línia d'ordres

En l'entorn textual de la línia d'ordres es disposa d'una ordre específica per visualitzar i configurar la política d'auditoria en les diverses categories i subcategories. Es tracta de l'ordre **auditpol.exe**, que té la sintaxi següent:

1 `auditpol [<subcomandament><opcions>]`

TAULA 3.2. Subordres disponibles per a l'ordre auditpol

| Subordre | Descripció |
|----------|---|
| /get | Visualitza la configuració de la política d'auditoria |
| /set | Edita i canvia la política d'auditoria |

Per utilitzar l'ordre de consola auditpol (taula 3.2), heu d'executar-la com a usuari administrador. Per exemple, engegant una consola amb els permisos adequats: Inici\Tots els programes\Accessoris\Símbol de sistema i ara amb el menú contextual (botó dret del ratolí) triar "Executar com a administrador".

TAULA 3.2 (continuació)

| Subordre | Descripció |
|---------------|---|
| /list | Llista els elements configurables |
| /backup | Guarda la configuració d'auditoria a un arxiu de còpia de seguretat |
| /restore | Recupera la configuració d'auditoria guardada en un arxiu |
| /clear | Esborra la configuració d'auditoria de tots els usuaris |
| /remove | Permet eliminar la configuració d'auditoria d'un usuari concret |
| /resourceSACL | Configura la llista de control d'accés de sistema |
| /? | Presenta la informació d'ajuda a la línia d'ordres |

Vegem alguns exemples d'utilització:

1. Obtenir informació addicional sobre les opcions de la subordre:

```
1 C:\auditpol /list /?
```

2. Llistar les categories d'auditoria:

```
1 C:\auditpol /list /category
```

3. Llistar totes les categories i subcategories d'auditoria:

```
1 C:\auditpol /list /subcategory:*
```

4. Esborrar tota la política d'auditoria configurada:

```
1 C:\auditpol /clear
```

5. Activar l'auditoria d'esdeveniments correctes i erronis de la categoria "Inici / tancament de sessió":

```
1 C:\auditpol /set /category:"Inicio / cierre de sesión" /success:enable /failure:enable
```

6. Visualitzar la configuració actual d'auditoria de totes les categories i subcategories:

```
1 C:\auditpol /get /category:*
```

7. Activar l'auditoria només d'esdeveniments erronis de la subcategoria d'accés al Registry:

```
1 C:\auditpol /set /subcategory:"Registro" /failure:enable
```

8. Guardar en l'arxiu auditpol.txt tots els valors de les directives d'auditoria configurades:

```
1 C:\auditpol /backup /file:auditpol.txt
```

3.2.4 Registre de seguretat

Una vegada activades les categories per auditar tota la informació rellevant dels esdeveniments seleccionats, s'enregistra en un arxiu anomenat *registre de seguretat*.

El registre de seguretat és l'arxiu on es detalla la informació dels diversos esdeveniments especificats en les directives d'auditoria habilitades.

Cal no confondre...

...el registre de seguretat amb el registre de configuració de Windows (*registry*), que és la base de dades on es guarden les configuracions i opcions sobre tot el programari, maquinari, usuaris i preferències del sistema operatiu.

El visor d'esdeveniments en Windows es pot obrir des de **Tauler de control | Sistema i seguretat | Eines administratives-Visor d'esdeveniments**.

Cada entrada del registre conté informació important sobre l'esdeveniment auditat incloent-hi si l'intent va tenir èxit o va ser erroni, la data i l'hora en què es va produir, la seva categoria i identificació, i l'usuari i l'equip auditats.

Aquest registre de seguretat pot ser analitzat i gestionat per diverses eines d'auditoria. Les diferents versions de Windows permeten observar i administrar aquest arxiu, juntament amb els arxius de registre d'aplicacions i de sistema, mitjançant el **visor d'esdeveniments i seguretat**.

Amb aquesta eina podem ordenar els registres per qualsevol camp, o bé, per a més eficiència, es poden crear filtres perquè només apareguin els esdeveniments en què s'està interessat. També, des d'aquesta consola, hem de tenir cura del manteniment del registre de seguretat fixant la mida màxima d'aquest arxiu i indicant les accions que s'han d'efectuar quan se sobrepassa aquesta capacitat.

3.3 Auditoria en sistemes operatius lliures

Com és habitual en el món del codi lliure, per fer qualsevol tasca tant d'administració com d'aplicacions d'usuari, trobem una gran quantitat d'opcions, utilitats i programes que es poden instal·lar al sistema. En auditoria de seguretat també disposem de moltes opcions, algunes de les quals estan incloses en la majoria de distribucions, com ara la gestió dels arxius de registre mitjançant el dimoni *syslogd*.

3.3.1 El paquet de gestió de registres *syslog*

En el sistema operatiu Linux, tota la informació i els arxius d'esdeveniments que genera el sistema queda enregistrada en nombrosos arxius de text que es poden localitzar al subdirectori */var/log*. Tots aquests arxius, la configuració d'aquests, el contingut, les alarmes, etc. es genera i es pot administrar i configurar mitjançant el paquet d'aplicació *syslog* que inclou el **dimoni *syslogd***.

El paquet *syslog* disposa d'un altre dimoni anomenat *klogd* que s'encarrega exclusivament dels missatges del nucli del sistema (*kernel*).

Syslog és el paquet estàndard *de facto* per controlar, readreçar i administrar missatges d'esdeveniments en una xarxa TCP/IP i s'acostuma a fer servir per a tasques administratives i d'auditoria.

En les darreres versions d'algunes distribucions de Linux es fa servir el dimoni rsyslogd, que ofereix algunes prestacions més, però mantenint la compatibilitat amb syslogd.

L'arxiu principal de configuració és /etc/syslog.conf (si utilitzeu el syslog tradicional); o bé, /etc/rsyslog.conf (si utilitzeu rsyslog). Aquest arxiu conté les regles o directives de configuració d'auditoria constituïdes per un selector i una acció. Al seu torn, el selector està format per un generador i una prioritat determinada separats per un punt, seguint aquesta sintaxi:

| | | |
|---|---------------------|-------|
| 1 | Generador.Prioritat | Acció |
|---|---------------------|-------|

Aquests conceptes es descriuen a continuació.

- **Generador.** Es tracta d'una paraula clau que identifica el tipus de programa o tasca que ha generat el missatge d'esdeveniment. Les possibles categories de generadors es presenten en la taula 3.3.

TAULA 3.3. Categories de generadors d'esdeveniments

| Generador | Descripció |
|-----------|---|
| authpriv | És utilitzat per les aplicacions que gestionen les autoritzacions del sistema (per exemple, per fer entrar dins el sistema o canviar de perfil amb sudo). |
| cron | És utilitzat per eines de programació automàtica de tasques com cron o anacron. |
| daemon | Normalment, inclou els generadors que no entren en cap altra categoria. |
| kern | Es tracta de missatges del nucli del sistema. |
| lpr | Es tracta de missatges relacionats amb la gestió de la impressió al sistema. |
| mail | Es tracta de servidors de correu i eines de processament de correu. |
| news | És un servidor de notícies. |
| syslog | Es tracta de missatges generats de manera interna per syslog. |
| user | El poden utilitzar les aplicacions d'usuari del sistema. |
| uucp | Subsistema UUCP (unix-unix copy), és un sistema de còpia d'arxius i missatgeria. |

- **Prioritat.** Indica la importància del missatge. Els possibles valors ordenats de menys a més importància s'indiquen en la taula 3.4.

TAULA 3.4. Nivells de prioritat

| Prioritat | Descripció |
|-----------|---|
| debug | Només s'utilitza quan s'està provant una aplicació, ja que mostra una gran quantitat d'informació i pot afectar el rendiment del sistema. |
| | |

TAULA 3.4 (continuació)

| Prioritat | Descripció |
|----------------|--|
| info | Es tracta de missatges d'informació. |
| notice | Es tracta d'esdeveniments significatius que no són necessàriament errors, però que s'han de tenir en compte. |
| warning | Advertiments que, tot i que no són errors, poden tenir algun tipus de repercussió. |
| error | Es tracta de missatges d'error. |
| crit | Són missatges d'error crítics, com fallades de maquinari. |
| alert | Són missatges crítics d'error que s'haurien de solucionar immediatament. |
| emerg | Es tracta de missatges molts greus que normalment impliquen que el sistema quedarà inoperatiu. |

- **Acció.** Correspon a l'acció que s'ha de prendre quan es compleix un selector. Normalment, indica la ruta de l'arxiu d'enregistrament on s'ha de guardar l'esdeveniment, però també es pot enviar als usuaris, a una impressora o es pot enviar el missatge a un altre ordinador que faria de servidor d'arxius d'enregistrament.

A més, hi ha algunes **regles sintàctiques** per construir les directives:

- Es poden especificar múltiples generadors separant-los per comes (,).
- Es pot fer servir el símbol d'asterisc (*) per referir-se a la totalitat dels generadors o de les prioritats.
- Quan s'indica una prioritat es tracta de la prioritat mínima per disparar la directiva i, per tant, comprèn les prioritats superiors. És a dir, si un selector indica que s'enregistrin esdeveniments de prioritat “alert” també registrarà els de prioritat superior “emerg”.
- Si volem que la prioritat no inclogui les superiors, ho hem d'indicar amb el símbol d'igual (=).
- Es pot especificar més d'un selector en una directiva separant-los amb el símbol de punt i coma (;).

Vegem-ne uns quants exemples.

1. Enviar tots els missatges del nucli i els missatges de prioritat crítica o superior de qualsevol generador a l'arxiu /var/log/syslog:

```
1 kern.*;*.crit    /var/log/syslog
```

2. Enviar els missatges generats pel correu i pel servei uucp de prioritat notice o superior a l'arxiu /var/log/mail:

| | | |
|---|-------------------------------|----------------------------|
| 1 | <code>mail,uucp.notice</code> | <code>/var/log/mail</code> |
|---|-------------------------------|----------------------------|

3. Enviar tots els missatges de prioritat error (no els de prioritat superior ni inferior) al servidor de nom `server.midomini.org`:

| | | |
|---|-----------------------|-----------------------------------|
| 1 | <code>*.=error</code> | <code>@server.midomini.org</code> |
|---|-----------------------|-----------------------------------|

A mesura que el sistema es manté en funcionament i les diferents incidències generen missatges, els arxius de registre creixen en mida. Si els deixéssim augmentar indefinidament, arribaria un moment en què la seva manipulació seria feixuga.

En Linux, per solucionar aquest inconvenient, és habitual trobar la utilitat **logrotate**, que es pot executar diàriament des d'un guió a **/etc/cron.daily**. El seu funcionament es controla amb el fitxer de configuració **/etc/logrotate.conf**.

Aquesta aplicació permet que, quan els arxius de registre arriben a una mida determinada (o quan passa un determinat temps), se'ls canviï el nom –per exemple, *messages*, per *messages.0*. Aquesta operació d'anar canviant el nom s'anomena *rotació* i és convenient efectuar-la periòdicament, i conservar així diverses versions anteriors dels fitxers d'enregistrament. Fins i tot es pot configurar perquè la utilitat comprimeixi les versions antigues dels arxius estalviant espai.

Cal esmentar que, de vegades, ens podem trobar amb determinats missatges del mateix sistema operatiu, com errors de maquinari o informacions importants, que apareixen en la consola de text. Aquests missatges no estan relacionats amb *syslog*, sinó que, normalment, estan generats per subsistemes del propi nucli i controladors de dispositius, que envien errors i avisos directament a pantalla. Si treballem en un entorn gràfic, no ho apreciarem, ja que no es mostraran. Hi ha administradors que, interessats en aquests missatges, redirigeixen la sortida de consola a una finestra de terminal gràfic per mantenir-se informats.

3.3.2 Visualitzador d'arxius de registre

Per poder veure d'una manera còmoda i ordenada el contingut dels arxius de registre del directori `/var/log` es disposa d'una eina gràfica que inclouen la majoria de distribucions Linux anomenada **visualitzador de registres del sistema** (*system log viewer*), que es pot veure en la figura 3.8.

Aquesta petita aplicació (vegeu la figura 3.8) permet visualitzar els arxius d'esdeveniments i registres d'auditoria, filtrar dades amb expressions regulars i veure en temps real els canvis que es produeixen en tots els arxius de registres oberts.

Per poder accedir a tots els arxius de registre calen privilegis d'administrador.

FIGURA 3.8. Visualitzador de registres



El visualitzador de registres del sistema es troba en el menú de Sistema Administració o bé es pot engegar des de la consola amb l'ordre `gnome-system-log*`.

Per fer aquesta tasca, el Linux ens proporciona la utilitat `acct`, que en cas de no estar preinstal·lada en la distribució la podem instal·lar fàcilment. En el cas de l'Ubuntu: `$ sudo apt-get install acct`.

3.3.3 Auditoria d'usuaris i processos

Per preveure i identificar els danys i intrusions tant d'usuaris autoritzats com d'atacants externs es poden activar sistemes d'auditoria que enregistren l'activitat de processos i usuaris. Aquests sistemes permeten veure i verificar totes les ordres executades per un usuari, incloent l'ocupació de CPU i memòria. Amb el sistema d'auditoria de processos, l'administrador del sistema sempre podrà saber quina ordre s'ha executat, qui l'ha executat, en quin moment i amb quins recursos.

Aquest paquet conté diferents ordres incloent:

- **ac**: mostra estadístiques sobre el temps de connexió dels usuaris.
- **lastcomm**: mostra informació sobre quines ordres i instruccions s'han executat.
- **accton**: activa i desactiva l'activitat d'auditoria de processos.
- **sa**: fa un resum de les ordres executades prèviament.

Vegem-ne uns quants exemples:

1. Activa l'auditoria de processos. Per defecte, tota la informació s'enregistra en l'arxiu `/var/log/account/pacct`.

```
1 $ sudo accton on
2 Turning on process accounting, file set to the default '/var/log/account/pacct'
```

2. Presenta el temps de connexió del sistema en hores. L'opció `-d` el classifica per dies.

```
1 $ ac -d
2 Aug 25 total      10.76
3 Aug 27 total      0.05
4 Aug 28 total      2.29
5 Today total      5.53
```

3. Presenta el temps de connexió de cada usuari.

```
1 $ ac -p
2 root 10.11
3 jmunoz33 29.48
4
5 total 39.59
```

4. Indica les ordres executades per un usuari particular amb indicació de data, hora i terminal. L'ordre lastcomm pot ser seleccionada per usuaris, terminals o bé pel mateix nom de l'ordre.

```
1 $ lastcomm jmunoz
2 lastcomm jmunoz stderr 0.05 secs Tue Aug 30 08:21
3 ac jmunoz stderr 0.01 secs Tue Aug 30 08:18
4 accton jmunoz stderr 0.02 secs Tue Aug 30 08:11
5 man jmunoz stderr 0.34 secs Tue Aug 30 08:10
6 pager jmunoz stderr 0.01 secs Tue Aug 30 08:10
```

5. Presenta un resum de la informació sobre les ordres executades indicant quantes vegades s'han cridat i els recursos que han fet servir. El recursos que s'han emprat es representen amb quatre valors:

- **re:** temps real en minuts de rellotge
- **cp:** temps sumat d'usuari i de sistema en minuts de CPU
- **avio:** mitjana d'operacions d'entrada/sortida per execució
- **k:** temps mitjà d'ús del nucli

La informació obtinguda amb l'ordre **sa** ens dona informació que ens pot posar en alerta en relació amb problemes d'usuaris/processos que estiguin fent servir recursos excessius.

```
1 $ sa
2 881 425.07re 2.83cp 0avio 1083k
3 8 2.39re 0.15cp 0avio 1451k apt-get
4 14 1.14re 0.12cp 0avio 2799k dpkg
5 2 5.52re 0.02cp 0avio 1465k bash
6 32 0.43re 0.01cp 0avio 1268k bash*
7 2 1.14re 0.01cp 0avio 931k man
8 16 0.02re 0.00cp 0avio 856k ls
9 5 0.01re 0.00cp 0avio 951k tar
10 11 0.03re 0.00cp 0avio 547k find
```

6. Visualitza el nombre de processos i minuts de CPU usats per cada usuari.

```
1 $sa -m
2 912 757.96re 3.07cp 0avio 1094k
3 root 654 299.68re 2.10cp 0avio 814k
4 jmunoz33 197 375.59re 0.94cp 0avio 1872k
5 man 56 0.11re 0.03cp 0avio 1057k
6 www-data 5 82.58re 0.01cp 0avio 7580k
```

3.3.4 Auditoria de la xarxa

Una part molt important de les tasques d'auditoria i seguretat correspon al sistema de comunicació i xarxa que són una de les fonts principals de problemes de

rendiment, intrusions i forats de seguretat. La captura, recollida i anàlisi d'aquesta informació que corre per la xarxa és crucial per optimitzar l'amplada de banda i per protegir les dades que hi circulen. El Linux disposa d'un bon grapat d'eines que ens aporten informació sobre la connexió, protocols i paquets d'informació a la xarxa. Algunes d'aquestes eines són **netstat**, **netwatch**, **tcpdump**, **ethereal**, **ntop** i **nessus**.

- **netstat**. És una eina que ens permet supervisar les connexions actives del nostre *host*, taules d'encaminament i estadístiques de les interfícies. Es fa servir per trobar problemes en la xarxa, mesurar el trànsit i estimar el rendiment. Entre la informació que subministra trobem:
 - Llista de les connexions de xarxa actives amb la nostra màquina: adreça IP, port client i port servidor de la connexió.
 - Processos i executables implicats en la creació de la connexió.
 - Llista de les interfícies de xarxa en el sistema.
 - Comparació de trànsit de la xarxa, errors i estadístiques de col·lisions, taules d'encaminament.
 - Elaboració d'estadístiques sobre els protocols de la xarxa, paquets i errors enviats i rebuts.

Aquesta ordre resulta molt útil per saber quines connexions són obertes, quins ports estan escoltant i quins són els processos, serveis i aplicacions que tenen establertes connexions remotes. Alguns dels seus paràmetres es presenten a la taula 3.5:

TAULA 3.5. :table:Table8:: Paràmetres de l'ordre netstat

| Paràmetre | Descripció |
|---------------------------|--|
| -r, - --route | Mostra la taula d'encaminament |
| -i, - --interfaces | Mostra la taula d'interfícies |
| -g, - --groups | Mostra els membres del grup multidifusió |
| -s, - --statistics | Mostra estadístiques de xarxa |
| -v, - --verbose | Mostra més informació a la sortida |
| -e, - --extend | Mostra més informació |
| -p, - --programs | Mostra contínuament les estadístiques de la xarxa (fins a interrompre el programa) |
| -l, - --listening | Mostra els <i>server sockets</i> que estan a l'espera, "escoltant" |

Vegem-ne uns quants exemples:

1. Visualitzar connexions TCP actives.

```

1 $ netstat -t
2 Active Internet connections (w/o servers)
3 Proto Recv-Q Send-Q Local Address           Foreign Address         State
4 tcp        0      1 jmunoz-desktop.:33269  fxfeeds.mozilla.org:www SYN_SENT

```

2. Mostrar estadístiques originades per connexions TCP.

```

1 $ netstat -s -t
2 IcmpMsg:
3   OutType69: 112
4 Tcp:
5   492 active connections openings
6   5 passive connection openings
7   5 failed connection attempts
8   7 connection resets received
9   0 connections established
10  16652 segments received
11  11287 segments send out
12   6 segments retransmitted
13   0 bad segments received.
14  27 resets sent
15 UdpLite:
16 TcpExt:
17   272 TCP sockets finished time wait in fast timer
18   110 delayed acks sent
19   13277 packet headers predicted
20   463 acknowledgments not containing data payload received
21   863 predicted acknowledgments
22   2 congestion windows recovered without slow start after partial ack
23   4 other TCP timeouts
24   1 connections reset due to unexpected data
25   2 connections reset due to early user close
26   1 connections aborted due to timeout
27 IpExt:
28   InMcastPkts: 75
29   OutMcastPkts: 77
30   InOctets: 12211604
31   OutOctets: 1158344
32   InMcastOctets: 7144
33   OutMcastOctets: 7224

```

3. Mostrar la taula d'encaminament.

```

1 $ netstat -r
2 Kernel IP routing table
3 Destination      Gateway          Genmask         Flags   MSS Window  irtt Iface
4 10.0.2.0          *               255.255.255.0   U        0 0        0 eth0
5 link-local        *               255.255.0.0     U        0 0        0 eth0
6 default          10.0.2.2        0.0.0.0         UG       0 0        0 eth0

```

4. Mostrar les interfícies de xarxa actives.

```

1 $ netstat -i
2 Kernel Interface table
3 Iface  MTU Met  RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
4 eth0    1500 0    17709      0      0 0      12529      0      0 0
5   BMRU
6 lo     16436 0      52      0      0 0        52      0      0 0
7   LRU

```

- **netwatch.** Aquesta utilitat analitza la xarxa al més alt nivell i mostra de manera dinàmica i en temps real l'activitat en la Xarxa. A més permet avaluar fàcilment la càrrega de cada servei sobre l'amplada de banda disponible. Per disposar d'aquesta utilitat s'ha d'instal·lar en l'Ubuntu el paquet netdiag mitjançant **\$ sudo apt-get install netdiag**.

- **tcpdump.** És una eina en línia d'ordres que té com a utilitat principal analitzar el trànsit que hi ha per la Xarxa. Permet a l'usuari capturar i

Els programes que capturen i analitzen els paquets que viatgen per la Xarxa s'anomenen en anglès **sniffers**.

mostrar els paquets transmesos i rebuts en la Xarxa a la qual l'ordinador està connectat. Vegem-ne un exemple:

```
1 sudo tcpdump -ieth0 -A -s1500 >netData.txt 2>netErr.txt
```

En aquest exemple hem de considerar el paràmetres indicats a la taula 3.6:

TAULA 3.6. Paràmetres ordre tcpdump

| Paràmetre | Descripció |
|------------------------|--|
| -ieth0 | Per capturar els paquets de la interfície eth0 |
| -A | Per imprimir cada paquet rebut en codificació ASCII |
| -s1500 | Mida màxima del paquet en bytes |
| >netData.txt | Per readreçar la sortida estàndard i enviar els paquets interceptats a l'arxiu de text netData.txt |
| 2>netErr.txt | Per readreçar la sortida d'errors i enviar els missatges d'error a l'arxiu de text netErr.txt |

Després de fer servir la Xarxa, per exemple fent una consulta al navegador, podem accedir a l'arxiu netData.txt i identificar i llegir els paquets generats. Aquests paquets inclouen una marca de temps (*timestamp*) i informació com la IP, el port del client, el protocol de transmissió, etc. Per exemple:

```
1 17:23:58.451117 ARP, Request who-has 10.0.2.2 tell jmunoz-desktop.local, length
2 28
3 ..... 'E|.
4 .....
5 17:23:58.452082 ARP, Reply 10.0.2.2 is-at 52:54:00:12:35:02 (oui Unknown),
6 length 46
7 .....RT..5.
8 ..... 'E|.
9 17:23:58.452185 IP jmunoz-desktop.local.40517 > www.brntech.com.tw.domain:
10 38096+ AAAA?
11 start.ubuntu.com. (34)
12 E..>..@.u.
13 .....E.5.*.....start.ubuntu.com.....
```

- **wireshark**. Abans més conegut com a **ethereal**, és un analitzador de protocols utilitzat per fer anàlisis i solucionar problemes en xarxes de comunicacions, per desenvolupar programari i protocols, i com una eina didàctica per a l'educació. La funcionalitat de què proveeix és similar a la de tcpdump, ja que permet veure tot el trànsit que hi ha en una xarxa, però afegeix una interfície gràfica i moltes opcions d'organització i filtratge de la informació obtinguda.
- **ntop** (de *network top*). Una altra eina que permet monitorar en temps real una xarxa. Inclou un microservidor web i genera taules i gràfiques en pàgines web. Així doncs, l'usuari pot veure les estadístiques de monitoratge directament amb el navegador.

Per instal·lar aquesta aplicació en l'Ubuntu:

```
1 $ sudo apt-get install ntop
```

Endeguem l'aplicació amb:

```
1 $ sudo ntop
```

i a partir d'aquest moment podem consultar les dades recopilades de la xarxa amb el mateix navegador en l'adreça <http://localhost:3000>.

- **nessus** (<http://www.nessus.org>). És una eina per analitzar vulnerabilitats en equips i fer auditories de seguretat a més d'oferir suggeriments per corregir els problemes de seguretat que es troben. **nessus** disposa d'una arquitectura de client-servidor que consisteix en **nessusd**, el dimoni **nessus**, que fa de servidor i fa l'escaneig al sistema de destinació, i **nessus**, el client (basat en consola o gràfic) que mostra l'avanç i l'informe dels escanejos. Disposa d'una llarga llista de proves de vulnerabilitat programades en un llenguatge específic NASL (*nessus attack scripting language*, llenguatge script d'atac **nessus** per les seves sigles en anglès). Aquest llenguatge script està optimitzat per interaccionar amb xarxes i ens permet crear els nostres propis scripts d'atac i provar-los. Els resultats de l'escaneig es poden exportar en diversos formats, com text net, XML, HTML, i LaTeX.

3.3.5 Distribucions Linux especialitzades en auditoria i seguretat

Atesa la gran quantitat d'eines de codi lliure d'aplicació en l'àmbit de la seguretat i l'auditoria, han aparegut algunes distribucions de Linux específicament dissenyades per a aquesta finalitat. Com per exemple BackTrack o Wifislax:

- **BackTrack** (<http://www.backtrack-linux.org/>) és una d'aquestes distribucions, potser la més popular, actualment basada en Debian/Ubuntu i que facilita les tasques d'auditoria informàtica, prova de seguretat i anàlisi forense, ja que incorpora una gran quantitat d'eines i utilitats per posar a prova les vulnerabilitats i els forats de seguretat del sistema, com ara les següents:

- Analitzadors de protocols
- Rastrejadors de ports
- Arxius d'*exploits*
- Analitzadors de paquets de xarxa (*sniffers*)
- Eines d'anàlisi forense
- Utilitats de detecció, auditoria i anàlisi de xarxes sense fil
- Anàlisi d'aplicacions web
- Eines d'enginyeria social

Exploit

Exploit, (de l'anglès *to exploit*, que significa 'explotar' o 'aprofitar'), consisteix en un programa o seqüència d'ordres que aprofita forats de seguretat i vulnerabilitats per causar comportaments no volguts en els programes informàtics o en el maquinari. En molts casos, l'Exploit té com a objectiu accedir al sistema informàtic, prendre'n el control o disposar de privilegis en aquest sistema, que ataca en benefici propi o com a plataforma i origen d'atacs a tercers.

- **Wifislax** (<http://www.wifislax.com/>) és una distribució de Linux basada en *slax* de la família de distribucions *slackware* i orientada per l'auditoria de seguretat de xarxes sense fil. Una de les principals avantatges és que incorpora els controladors per la majoria de targetes de xarxes sense fil així com gran quantitat d'utilitats i eines específiques per aquest tipus de xarxa cada vegada més emprada i molt procliu a intrusions problemes de seguretat.